actusécu

By xmco

AVRIL 2026

DOSSIER

La confiance, enjeu essentiel des forums cybercriminels

ARTICLE

L'OSINT au service des missions Red Team

63

AVRIL 2026

Responsable de publication : Clémence Illouz, XMCO - Direction artistique / Réalisation : Romain Mahieu, agence plusdebleu - Contributeurs : Les consultants du cabinet XMCO. Crédits photo : ©XMCO, ©AdobeStock. Contact Rédaction : actusecu@xmco.fr

L'édito

Marc BEHAR, PDG et Fondateur d'XMCO

Vis ma vie … !

Un concept devenu un classique pour beaucoup d'entre vous. Nous vous proposons dans ce nouveau numéro de l'actu-sécu, dans notre premier article, de vous mettre à la place des attaquants, qui rencontrent des soucis pour se faire confiance entre eux ! C'est l'arroseur arrosé !
Imaginez-vous qu'ils trouvent le moyen de s'arnaquer entre eux…

Dans le second article, c'est à la place de nos consultants Redteam que vous pourrez vous projeter, notamment lors des phases initiales de nos missions : celles où nous cherchons à recueillir le maximum d'informations sur les clients qui nous mandatent. Pour des raisons évidentes, nous avons masqué certains termes et certains noms d'outil : d'une part, nous ne souhaitons pas encourager d'activité d'OSINT « sauvage » alors que l'activité est particulièrement encadrée.

D'autre part, la diffusion des outils pourrait laisser penser qu'une mission de Redteam ne consiste qu'en une combinaison optimale d'outils. Dans la vraie vie, ce sont bien l'expérience, la maîtrise technique et la finesse de nos consultants qui permettent de réussir nos missions de Redteam. Qu'ils utilisent des outils, certains très puissants, est un fait, voire parfois, une condition nécessaire. Mais c'est tellement loin d'être suffisant…

Bonne lecture ! ■

Le saviez-vous ?

6867

C'est le nombre de bulletins Yuno, notre service de veille en cybersécurité, produits cette année.

5597

Bulletins sur des **Vulnérabilités corrigées**

248

Bulletins sur des **vulnérabilités sans correctif disponible**

105

Bulletins sur des **codes d'exploitation publics**

917

Bulletins sur les **cybermenaces et l'écosystème cyber**

24%

C'est le pourcentage d'augmentation de CVE publiées entre 2024 (40 243) et 2025 (49 920)

160%

C'est le pourcentage d'augmentation du nombre du bulletins critiques envoyés à nos clients Yuno entre 2024 (78) et 2025 (203)

32%

C'est le pourcentage d'augmentation des CVE publiées et activement exploitées entre 2024 (186) et 2025 (245) d'après le catalogue KEV (Known Exploited Vulnerabilities)

Sommaire

Numéro 63

63

Vous avez manqué le précédent numéro de notre Actusécu ? Demandez votre exemplaire papier* à contact@xmco.fr

*Dans la limite des stocks disponibles.

yuno décrypte

Que s'est-il passé dans le monde de la cyber ces dernières semaines ?

Yuno, notre service de veille cyber, vous informe au quotidien des dernières menaces et vulnérabilités identifiées par le CERT-XMCO. L'occasion ici de revenir sur l'exploitation de **deux vulnérabilités 0-day** affectant **Ivanti Endpoint Manager Mobile** (EPMM) ainsi que sur **la compromission du mécanisme de mise à jour de Notepad++**.
Les deux vulnérabilités affectant Ivanti EPMM, référencées **CVE-2026-1281 et CVE-2026-1340 (CVSSv3.1 : 9.8)**, provenaient d'un contrôle insuffisant de la génération de code et permettaient à un attaquant distant et non authentifié d'exécuter du code arbitraire.

- Dès le 29 janvier 2026, **elles ont été corrigées via des correctifs temporaires** (RPM) par Ivanti, qui a indiqué qu'elles avaient déjà été exploitées en tant que 0-day par des acteurs malveillants. **La version 12.8.0.0 d'Ivanti EPMM qui corrigera durablement ces vulnérabilités**, n'a toutefois pas encore été publiée par l'éditeur, qui indique qu'**elle sera disponible au cours du premier trimestre 2026**.

Depuis lors, **les autorités néerlandaises** ont indiqué le 6 février 2026 que deux institutions publiques avaient été victimes de l'exploitation de ces deux vulnérabilités, qui a permis à des attaquants d'accéder à des données professionnelles des collaborateurs.

Afin d'endiguer ces risques, **Yuno recommande donc d'installer les correctifs temporaires fournis par Ivanti** ainsi que de prendre connaissance des guides partagés par l'éditeur afin d'assister les efforts de détection de leur exploitation.

- **La compromission du mécanisme de mise à jour de Notepad++** a pour sa part été annoncée par l'éditeur Don Ho le 2 février 2026. Ce dernier a alors indiqué que des attaquants avaient compromis un serveur d'hébergement partagé, leur permettant de **contourner le mécanisme de vérification des mises à jour et ainsi de conduire des utilisateurs à installer des mises à jour malveillantes du logiciel**.

L'attaque aurait débuté en juin 2025 et aurait été opérée par le groupe d'attaquant nommé Lotus Blossom, parrainé par l'État chinois. Ceux-ci ont déployé divers malware tels qu'une porte dérobée (backdoor) baptisée Chrysalis à des fins probables de collecte d'informations sensibles. Selon les chercheurs de Palo Alto, plusieurs organisations notamment localisées en Europe auraient été affectées.

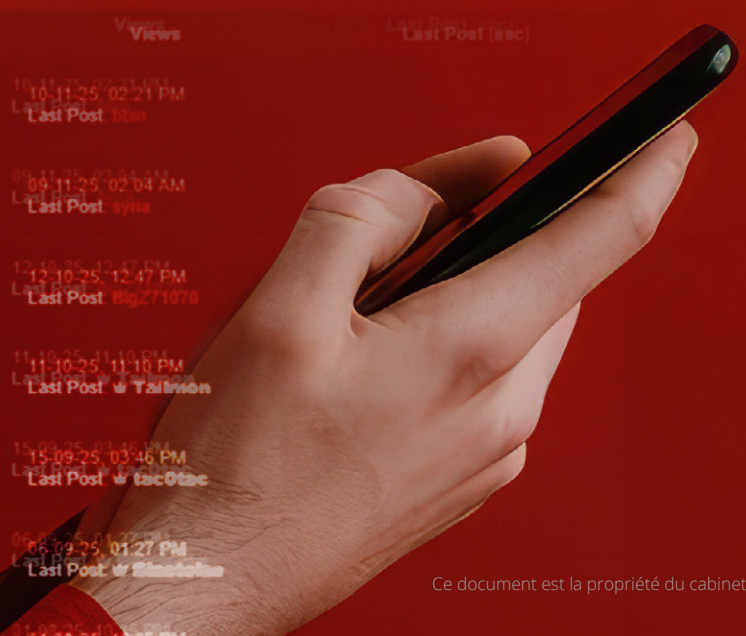
En réaction, **Don Ho a annoncé avoir migré vers un nouveau fournisseur de service d'hébergement et a progressivement implémenté des mécanismes de durcissement** du système de vérification des mises à jour au sein des versions 8.8.9 et 8.9.1 puis de la version 8.9.2 qui a été publiée le 16 février 2026.

Bien que cette campagne aurait ciblé un nombre de victimes limité, **Yuno recommande d'effectuer la mise à jour de Notepad++ vers la version 8.9.2 ainsi que d'intégrer aux dispositifs de détection les indicateurs de compromission (IoCs) fournis par l'ancien fournisseur de service d'hébergement de Don Ho, par Rapid7 et par Palo Alto**.

Pour en savoir plus sur l'anticipation des menaces cyber par Yuno :
www.xmco.fr/yuno-veille-vulnerabilites-cybersecurite/

La confiance, enjeu essentiel des forums cybercriminels

Par Ambroise DA SILVA, Julie ARNOUX et Nicolas BOUSSANGE, experts XMCO.



La confiance, enjeu essentiel des forums cybercriminels

Introduction

Dans l'écosystème cybercriminel tout comme dans n'importe quel système financier, la confiance est la clé. Lorsqu'un **attaquant A** souhaite acheter un produit ou un service auprès d'un **attaquant B**, aucun des deux ne connait l'identité de l'autre. Chacun utilise un pseudo et prend plus ou moins de précautions pour protéger son identité. Résultat : comment peut-on faire confiance à un inconnu sur une marketplace cybercriminelle ?

De nombreux autres facteurs complexifient l'équation de la confiance : les cas d'exitscam, les saisies d'infrastructures par les autorités, l'impossibilité de porter plainte auprès des autorités nationales en cas d'arnaques ou de fuite de données internes dues à un membre «rebel» (ex : Conti, BlackBasta) rendent difficile toute relation de confiance sur les plateformes du Deep/Darkweb.

Faisons une rapide incise : dans le cadre de cet article nous parlerons de "Deep et Dark Web" de façon indistincte. Ce raccourci s'explique par le fait que de nombreux forums et marketplaces étudiés ont, à la fois, une version clearweb et darkweb (TOR). L'objet de cet article est d'étudier l'écosystème cybercriminel en nous basant sur un échantillon de forums représentatifs comme XSS, Exploit, RAMP et DarkForums.

De façon générale, l'écosystème du Deep / Darkweb est en perpétuelle évolution avec des nouveaux sites régulièrement créés et supprimés. À titre d'exemple, le rapport d'un de nos confrères de 2019 identifiait 8 400 sites en .onion comme étant en ligne sur un total 55 000 domaines .onion, soit seulement 15%.

Ce changement permanent des domaines onion, souvent dû à une panne, une arnaque ou bien une opération de démantèlement par la police, peut déstabiliser les utilisateurs.

Face à cela, la communauté cybercriminelle a su s'organiser et générer de la confiance de différentes façons :

- Une restriction des inscriptions sur le forum ;
- La modération des contenus partagés par les administrateurs du forum ;
- La mise en place d'un système de réputation des membres, avec des grades et des points de réputation ;
- L'intervention d'un tiers dans la transaction, souvent appelé « Escrow » ;
- La mise en place d'un tribunal pour le règlement des différends entre 2 membres.

Dans le cadre de cet article, nous reviendrons tout d'abord en détail sur les enjeux et les mécanismes permettant de créer de la confiance sur le Deep/Darkweb.
Puis, nous nous intéresserons au système de tribunal et notamment celui de DarkForums, héritier de Breachforums, Breached et RaidForums.

L'importance de la confiance dans l'écosystème cybercriminel

Mécanismes de construction et de gestion de la confiance sur les forums cybercriminels

Avant de détailler les mécanismes de confiance, il est important de définir les différents profils des acteurs en présence.

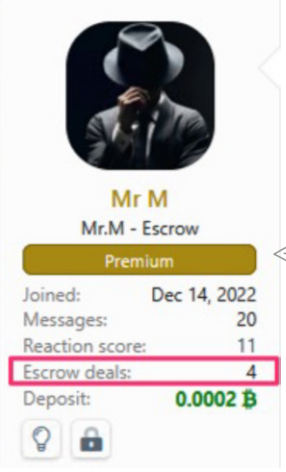
Les forums et marketplaces comme tout marché en économie sont un lieu de rencontre entre une offre et une demande. D'un côté, des attaquants cherchent à acheter un bien ou un service tels qu'une base de données, un accès à un serveur distant ou bien un outil de fraude. Tandis que de l'autre, des vendeurs proposent lesdits biens et services à un prix fixé par eux-mêmes.
Ce montant correspond généralement à une valeur en dollars sous la forme de cryptomonnaies (Bitcoin Monero, Zcash ou encore Ethereum, etc) ou bien des « crédits » sur le forum. Par exemple, sur BreachForums, Leakbase et Instant-Hack, il est possible d'acheter une base de données moyennant l'utilisation de « crédits ». Ces derniers peuvent être gagnés lorsque l'on partage du contenu comme des messages, des bases de données ou bien en achetant directement sur le forum.

Publication sur Leakbase de la base de données « OroPocket » moyennant le paiement de 7 crédits (appelés « #CR »)

Afin de définir un cadre et de le faire respecter, chaque forum possède des administrateurs et/ou des modérateurs. Cela peut être une ou plusieurs personnes. L'administrateur/Owner est responsable de l'infrastructure sous-jacente au forum, tandis que le modérateur est davantage chargé de s'assurer que les membres du forum ont un comportement adapté aux règles de la plateforme et de supprimer des contenus / bannir des membres dans le cas contraire. Certains membres peuvent être promus modérateur par l'administrateur s'ils en font la demande, si leur réputation est suffisamment élevée et/ou s'ils ont des liens privilégiés avec l'administrateur.

Aperçu des comptes des administrateurs de DarkForums, Leakbase, Exploit, XSS et RAMP

Afin de faciliter les relations entre acheteurs et vendeurs, il existe des membres spécialisés tels que les garants/escrow. Ces derniers assurent ainsi le rôle de médiateurs lors d'une transaction sur le forum : recevoir l'argent de l'acheteur et attendre la validation de ce dernier avant de verser la somme au vendeur, moyennant une commission comprise entre 3 et 10%[1]. Le système d'escrow repose sur la réputation de l'escrow, censée garantir à l'acheteur qu'il ne se fera pas arnaquer. Un escrow est généralement un membre du forum qui achète et vend lui-même depuis un certain temps, est bien intégré dans l'écosystème et jouit d'une réputation élevée.



Certains forums comme XSS permettent même d'afficher le nombre de transactions « réussies » par un escrow sur son profil.

(Ci-contre) Aperçu du profil XSS d'un escrow avec un compteur du nombre de deals réussis.

[1] *« Escrow Systems on Cybercriminal Forums: The Good, the Bad and the Ugly" : https://reliaquest.com/blog/escrow-systems-on-cybercriminal-forums/*

Ce système de réputation est un facteur indispensable dans la construction de la confiance entre les membres des forums ■

Une bonne réputation peut être obtenue de plusieurs façons, souvent complémentaires. Ces informations sont généralement visibles pour tous les autres membres :

• L'ancienneté du compte de l'utilisateur, gage de fidélité et d'implication sur le forum.

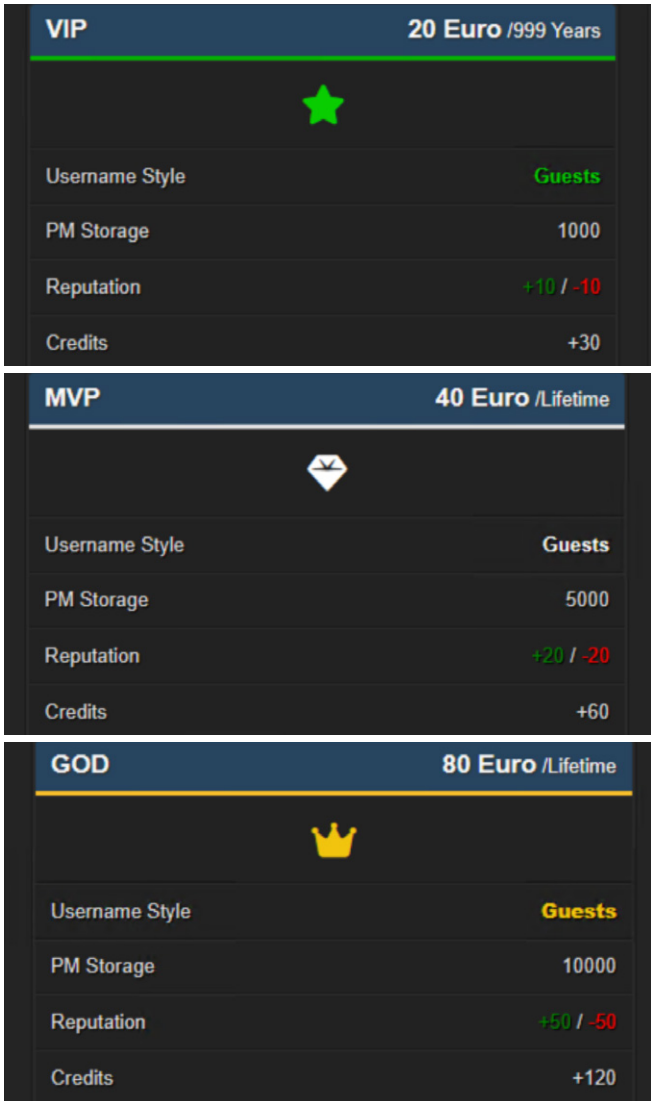
• Le nombre de publications et de commentaires faits par un utilisateur. Plus le membre est un important contributeur sur le forum et plus cela signifie qu'il est intégré à l'écosystème.

• Les « reviews » par les autres membres du forum. Sur plusieurs forums comme DarkForums, il est possible de donner des points de réputation ou d'en retirer sur un autre compte. Ainsi, un membre avec une mauvaise note de réputation aura moins de chances d'être pris au sérieux.

• Le fait de faire un deposit en cryptomonnaies sur son compte, preuve que le propriétaire du compte est un client « fiable ». C'est notamment le cas sur les forums XSS, BHF et Exploit.

Aperçu du compte XSS d'un vendeur avec un dépôt de 0,017 Bitcoin, soit environ 1 539 dollars (au moment de la rédaction de cet article).

• L'acquisition d'un « grade ». Les grades varient grandement d'un forum à l'autre. Vous trouverez ci-dessous un exemple avec les grades disponibles à l'achat sur le site DarkForums. N'importe qui peut acheter un grade donc il ne s'agit pas forcément d'un gage de confiance. Toutefois, tout comme sur XSS, cela indique que le propriétaire du compte a de l'argent et souhaite s'en servir. L'obtention d'un grade octroie un certain nombre de fonctionnalités comme l'obtention de crédits pour acheter sur la plateforme et de points de réputations.



Aperçu du système de grade sur DarkForums

Défaillances et abus : l'omniprésence des arnaques

Malgré la présence de mécanismes destinés à encadrer les transactions, les forums et marketplaces cybercriminelles sont quotidiennement confrontés à diverses formes

d'arnaques. L'anonymat, l'absence de recours légaux et la logique opportuniste au sein de ces derniers favorisent les abus et fragilisent les rapports de confiance entre l'ensemble des acteurs.

Un phénomène en particulier est de plus en plus démocratisé : l'**exit scam**. Tel que traité dans l'**Actu Sécu n°61 – Hors-Série – Dossier spécial Dark Web**, l'exit scam désigne une fraude dans laquelle les administrateurs ferment brutalement une marketplace après en avoir dérobé les fonds présents, parfois sous prétexte d'une fausse attaque DDoS.

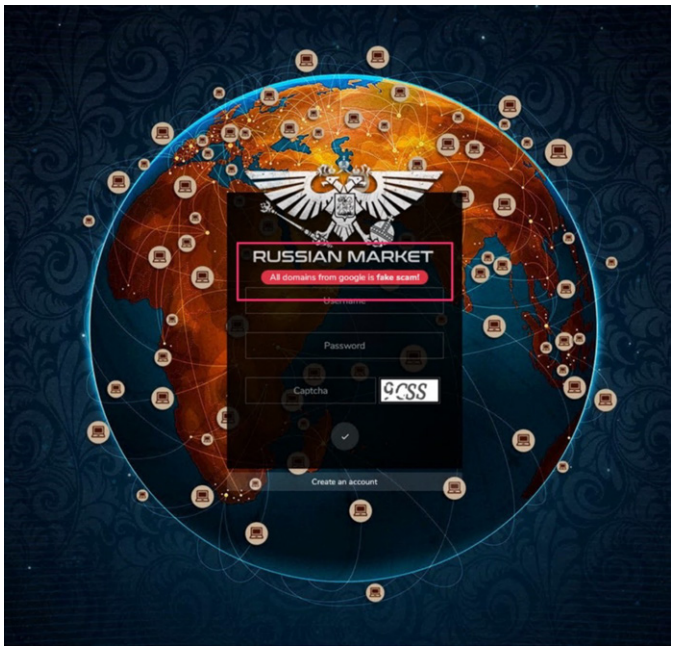
« Cette disparition peut ou non s'accompagner d'une mise hors ligne de la plateforme. Nightmare en 2019, Apollon et BitBazaar en 2020 ou encore Tor2Door fin 2023 sont des exemples notoires de Scam Exit. Ces multiples occurrences sur un intervalle de seulement quelques années ont contribué à dégrader la confiance des utilisateurs envers ce type de plateforme. »

Cependant, la fraude peut émerger de tous les côtés : de la part des administrateurs tel que vu précédemment, mais aussi des acheteurs qui ne paient pas leurs achats ou les contestent après réception, ou très régulièrement des vendeurs. Il est en effet très difficile d'estimer la fiabilité et la véracité des publications sur les forums du darkweb puisque la majorité des vendeurs qui prétendent détenir des bases de données volées ou des accès sont en réalité des fraudeurs qui abusent de la réputation qu'ils se sont construite.

Pour ce faire, ils utilisent plusieurs techniques :

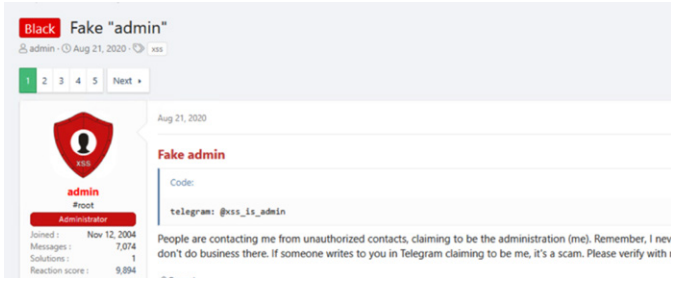
- Revendre d'anciennes bases de données publiques en les présentant comme des données récentes ;
- Revendre d'anciennes bases de données publiées par d'autres cybercriminels ;
- Mélanger des fragments de vraies fuites de données avec des données totalement fabriquées comme c'est de plus en plus le cas avec les combolists[2] ;
- Créer de fausses identités ou se faire passer pour des groupes connus (LockBit, Bjorka, IntelBroker, LeakBase / Chucky)[3] ;
- Etc.

Face à ces arnaques et notamment aux cas de sites de phishing ciblant des attaquants, de nombreux administrateurs font de la sensibilisation auprès de leurs membres en communiquant des domaines usurpant les leurs. On peut par exemple citer le cas de la marketplace RussianMarket.



Aperçu de la mire d'authentification de Russian Market où l'on voit un avertissement sur les domaines enregistrés auprès de Google.

Enfin, tout comme des cadres d'entreprises, les administrateurs des forums peuvent subir des usurpations d'identité. Cela fut notamment le cas de l'administrateur de XSS qui, en 2020, a expliqué que de faux comptes Telegram usurpaient son identité auprès de membres de XSS afin de leur extorquer de l'argent.



Aperçu d'un thread créé par l'administrateur de XSS où il liste de faux-comptes Telegram usurpant son nom

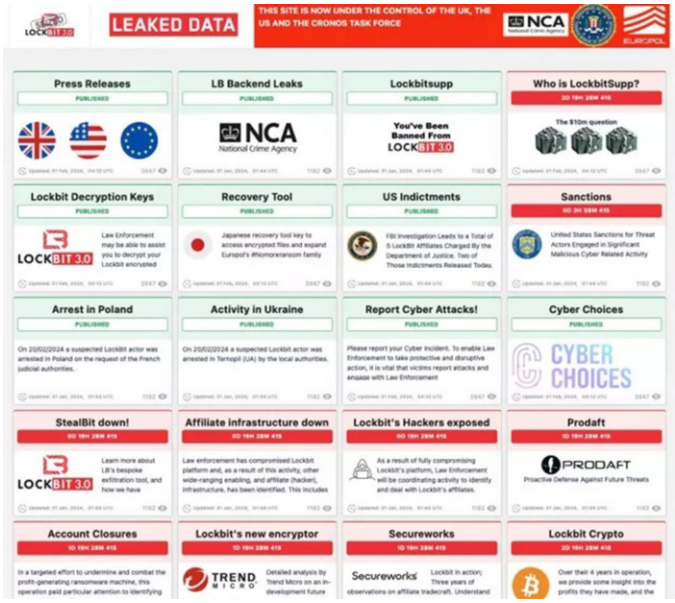
[2] *"Combolists and ULP Files on the Dark Web: A Secondary and Unreliable Source of Information about Compromises" : https://www.group-ib.com/blog/combolists-ulp-darkweb/*

[3] *"Who's Afraid of the Dark? Hype Versus Reality on the Dark Web" : https://www.group-ib.com/blog/dark-web-fraud/*

Pression croissante des autorités et transformation des forums

D'après le rapport annuel sur la cybercriminalité 2025 publié par le COMCYBER-MI[4], **348 000** atteintes numériques ont été enregistrées en 2024, soit une augmentation de **+74% en 5 ans**. Face à l'évolution et la récente **industrialisation** des activités cybercriminelles, les autorités et analystes spécialisés ont nettement renforcé leurs activités de surveillance et mènent désormais des actions coordonnées afin de démanteler les plateformes où s'échangent données volées, services illicites, outils de fraude etc. Les opérations internationales d'envergure menées ces dernières années par les États, ont mis en évidence leur capacité à infiltrer, voire prendre le contrôle des espaces d'échanges cybercriminels et saper toute confiance.

Le 19 février 2024, **l'Opération Cronos**[5], coordonnée par Europol et menée conjointement par les forces de l'ordre de 10 pays dont la France, a permis de neutraliser une partie du réseau de l'opérateur de ransomwares LockBit3.0 via notamment la saisie de 34 serveurs et l'interpellation de deux individus impliqués. Cette opération était très offensive avec une "quasi-guerre psychologique" livrées aux attaquants. En effet, les forces de l'ordre ont utilisé le site Onion et le visuel du site vitrine de LockBit pour faire du « teasing » sur l'avancement de l'opération avec l'utilisation d'un minuteur avant de publier progressivement les informations de l'opération. Parmi celles-ci, on trouve notamment la révélation de l'identité de LockbitSupp, le leader présumé du groupe de ransomware LockBit. Cette stratégie de « doxxing » a porté un sérieux coup à la réputation de LockBit et le ransomware, qui a longtemps été leader du marché du Ransomware-as-a-Service, a vu ses affiliés partir progressivement chez les concurrents. Ainsi, même si les membres de LockBit ont tenté de reconstruire leur infrastructure après l'opération Cronos, l'absence de confiance engendrée par l'opération a été fatale.



Aperçu du site de LockBit parodié par les forces de l'ordre pour communiquer sur l'opération et mettre la pression sur les membres du groupe de ransomware.

Créé en 2022 à la suite de la fermeture de RaidForums et Breached, BreachForums s'est imposé comme l'une des plus grandes marketplaces cybercriminelles spécialisée notamment dans l'achat/revente de données volées. En mai 2024, une opération menée par le FBI avec le soutien de partenaires internationaux a abouti à la saisie de ce dernier ainsi qu'à l'arrestation de Baphomet, l'un des principaux administrateurs du forum. Les autorités ont confirmé avoir infiltré la plateforme avant la saisie, ce qui leur a permis de collecter des données sur les utilisateurs, les transactions et les activités d'extorsion menées via le site. En 2025, une nouvelle série d'arrestations ont vu tomber plusieurs membres du groupe Shiny Hunters ainsi qu'un ancien modérateur de BreachForums nommé IntelBroker[6].

[4] COMCYBER-MI, « Rapport annuel sur la cybercriminalité 2025 » , juill. : https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2025-07/Rapport-annuel-sur-la-Cybercriminalit%C3%A9-2025-V2.pdf

[5] EUROPOL, « Law enforcement disrupt world's biggest ransomware operation – LockBit was the most deployed ransomware variant across the world | Europol ». : https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[6] « Serial Hacker "IntelBroker" Charged For Causing $25 Million In Damages To Victims": https://www.justice.gov/usao-sdny/pr/serial-hacker-intelbroker-charged-causing-25-million-damages-victims

Message posté sur BreachForums suite à sa saisie par les forces de l'ordre

Fin mai 2024 a lieu la plus vaste opération jamais réalisée contre les botnets : l'**Opération ENDGAME**[7].

Coordonnée par Europol et soutenue par la France, l'Opération ENDGAME est une série d'opérations dédiées au démantèlement des réseaux de botnets utilisés pour déployer des logiciels malveillants à grande échelle tels que des ransomwares. Entre le 27 mai et le 29 mai 2024, a lieu la perturbation de plusieurs botnets dont **IcedID, SmokeLoader, Pikabot et Bumblebee**. L'enquête a notamment permis de cartographier les infrastructures C2 de ces derniers et de neutraliser plus de 100 serveurs.

Enfin, entre le 11 et le 13 novembre 2025 a eu lieu la dernière phase de l'opération ENDGAME avec le démantèlement des infrastructures de l'un des infostealers les plus actifs **Rhadamanthys**, du trojan **VenomRAT** ainsi que du botnet **Elysium**. Les actions menées par les autorités ont permis la suppression ou la perturbation de plus de 1000 serveurs.

Ces opérations de plus en plus nombreuses et massives traduisent un durcissement de la réponse internationale face à l'industrialisation de la cybercriminalité et témoignent de l'instabilité et de la vulnérabilité de l'écosystème cybercriminel. Ces actions exercent une pression constante qui ne se limite pas aux infrastructures : elle s'immisce au cœur des relations entre acteurs, renforçant ainsi les incertitudes et suspicions de la part des utilisateurs et administrateurs des plateformes.

Stratégies d'adaptation des cybercriminels

Face à la recrudescence des opérations de démantèlement et d'infiltrations des autorités, les cybercriminels ont été contraints d'adapter leurs pratiques afin de rétablir les conditions de confiance et maintenir leur équilibre déjà structurellement précaire. Cela se traduit notamment par le durcissement des contrôles et des conditions d'accès, l'anticipation des risques de saisie, ainsi qu'une migration croissante vers d'autres plateformes parfois plus difficiles à surveiller.

Durcissement des contrôles d'accès et règlements intérieurs

Afin de renforcer l'anonymat et rendre leurs accès plus difficiles aux membres moins qualifiés techniquement, certains forums sont entièrement privés et sont accessibles uniquement sur le darknet TOR avec des sites en .onion. C'est notamment le cas du forum de discussion Dread connu comme étant « le Reddit du Darkweb ». D'autres tel que Leakbase sont disponibles uniquement sur le clearweb. Pour autant, la majorité des plateformes cybercriminelles les plus actives telles que DarkForums, Exploit, XSS, RussianMarket ou Ramp, sont accessibles à la fois sur TOR et sur le clearweb, ce qui les rend d'autant plus accessibles. Par ailleurs, ces dernières ont toutes mis en place un système de redondance et sont consultables via une multitude d'URLs, garantissant la survie du forum en cas de takedown de l'un des domaines.

Afin de renforcer la confiance et limiter au maximum les cas de scam, les contrôles d'accès aux marketplaces ont été considérablement renforcés ces dernières années :

[7] *« Operation Endgame » . : https://www.operation-endgame.com/*

• Certains forums tels que **CryptBB** sont des cercles fermés dont le lien .onion circule uniquement sur des canaux Telegram restreints ;

• L'accès à certains forums est conditionné par une excellente réputation sur d'autres plateformes. Par exemple, l'accès à la marketplace russophone **Ramp** n'est possible qu'en cas de bonne réputation sur **XSS** et **Exploit** ;

• L'accès à certaines marketplaces est conditionné par l'abondement d'un solde en cryptomonnaie tel que sur **RussianMarket** ;

• D'autres sont accessibles uniquement sur invitation avec un lien d'activation ou via un système de cooptation et particulièrement les forums russophones ;

• Une « **modération en aval** » avec la création d'un **tribunal** pour le règlement des différends entre membres est mise en place sur quasiment toutes les marketplaces et forums. Ce mécanisme permet à chaque membre (acheteur ou vendeur) de déposer plainte contre un autre membre lorsqu'il se sent lésé. Un administrateur/modérateur du forum va alors agir en tant que juge pour résoudre le conflit et exécuter une peine (ex : demande de fourniture de preuves matérielles, demande de remboursement, ban provisoire/permanent du forum etc.). Nous reviendrons plus en détails sur ce système dans cet article.

Par ailleurs, chaque plateforme cybercriminelle a mis en place ses propres règles de plus en plus exigeantes, notamment :

• La modération des contenus partagés. Par exemple, le forum Leakbase est connu pour prohiber le partage de données liées à la Russie. De même, les forums DarkForums et XSS n'autorisent pas de contenus liés à des activités de ransomware.

• Le ban du « leeching », afin d'écarter les utilisateurs qui ne participent pas à la communauté et ainsi écarter les potentiels enquêteurs infiltrés. Le « leeching » désigne les membres qui commentent massivement les publications d'autres membres avec des messages type « Thank you » afin de débloquer le contenu du post sans contribuer en retour ;

• La signature d'un règlement intérieur sur certaines plateformes que les membres sont tenus de suivre au risque d'être définitivement bannis.

Repli vers d'autres plateformes

Les infrastructures du darkweb et en particulier TOR, sont considérées comme particulièrement instables. La méfiance croissante envers TOR – régulièrement visé par des opérations de démantèlement, l'arrestation d'administrateurs, la fermeture de sites – a poussé les acteurs cybercriminels à déplacer leurs échanges vers des environnements perçus comme moins exposés et décentralisés.

Parmi ces alternatives, les services de messagerie, permettent de répondre à un besoin d'anonymat et d'accessibilité. Afin de décentraliser leurs activités, il est d'ailleurs courant que les cybercriminels passent par des messageries telles que **Jabber**, **Tox** et particulièrement **Telegram** en parallèle des forums afin de décentraliser leurs activités des forums.

Parmi ces services de messagerie, Telegram s'est imposé comme un véritable écosystème parallèle accessible au plus grand nombre car il ne nécessite ni prérequis technique, ni réputation et la modération y a longtemps été très faible.
Telegram est aujourd'hui largement utilisé par les cybercriminels pour tous types d'activités :

• La circulation massive de **données volées** (combolists, logs d'infostealers, bases de données compromises…) ;

• La coordination de **campagnes hacktivistes** et les revendications d'attaques, notamment celles du collectif Noname057 (16) ;

• La vente de services liés à de la **Fraude** (Fullz, Scama, configs…) notamment sur le canal francophone FraudeAcademy devient FrenchConnection ;

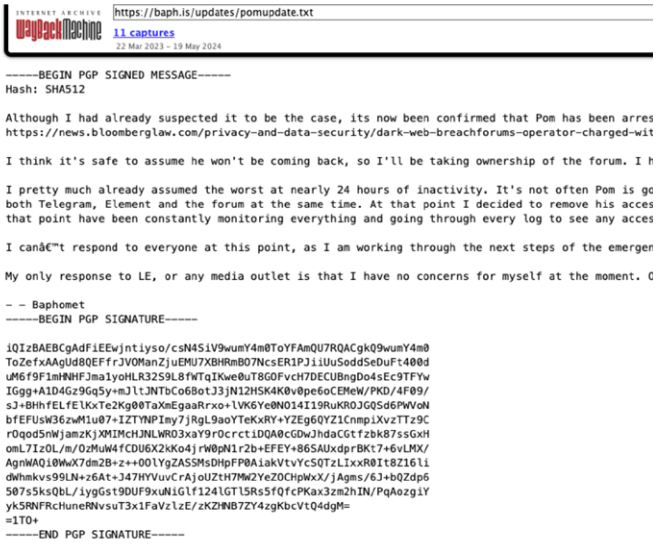
• La vente de **Malwares-as-a-Service** (MaaS) tels que les infostealers (StealC, Vidar, Rhadamanthys, Raccoon, Redline…) et de **Ransomwares-as-a-Service** (RaaS) ;

Telegram est également devenu le médium privilégié de certains groupes cybercriminels particulièrement organisés et prolifiques comme les administrateurs de BreachForums pour communiquer après de leur communauté. On pense notamment à la chaîne Telegram « The Jacuzzi » utilisée pour assurer les échanges entre membres indépendamment des différentes opérations de saisies des services par les forces de l'ordre[8] depuis la fermeture de RaidForums en 2022.

Aperçu d'un message partagé sur la chaîne Telegram annonçant l'arrestation de l'un des administrateurs de BreachForums

Un autre cas intéressant est l'utilisation par certains administrateurs d'une clé PGP pour chaque message afin de certifier qu'il s'agit bien d'eux. On peut citer le cas de l'ancien administrateur de BreachForums Baphomet qui utilisait son site baph[.]is ainsi qu'une clé PGP pour communiquer auprès des membres du forum sur l'évolution de la situation en décembre 2023. De fait, lorsque l'un des administrateurs nommé PomPompurin a été arrêté par le FBI, de nombreux soupçons sont apparus sur le risque d'une infiltration du forum par les forces de l'ordre. Certains membres parlaient même du forum comme d'un « honey pot ». La confiance était fortement ébranlée et Baphomet a tenté de maintenir cette confiance par ce biais.

Il a communiqué ainsi pendant un certain temps et notamment pour annoncer la remise en ligne du nouveau domaine du forum.



Aperçu d'une communication faite par Baphomet au sujet de l'arrestation de Pompompurin sur son site baph[.]is et utilisant une clé PGP. (source : WayBackMachine)

Système de tribunal

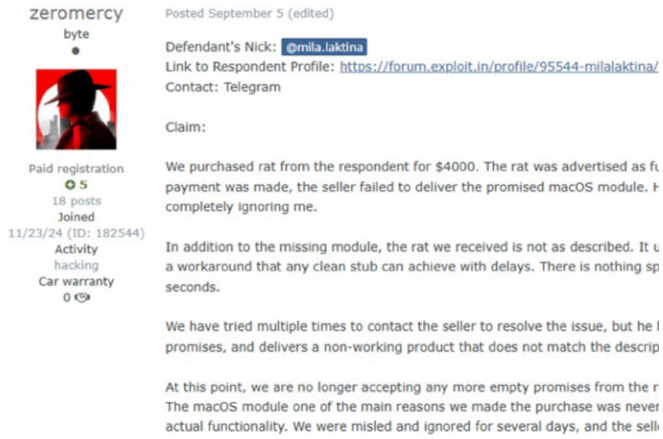
Dans le cadre de cet article, le CERT-XMCO s'est particulièrement intéressé au système de tribunaux sur les forums cybercriminels. Les juridictions des tribunaux n'ayant pas cours sur les deep et darkweb, les administrateurs des différents forums ont dû créer des sections spécifiques où chaque membre estimant avoir subi un préjudice après une transaction avec un autre membre peut « porter plainte ».

Tout comme au tribunal, le plaignant peut déposer une plainte. Pour ce faire, il doit publier un message dans la section adaptée en expliquant le contexte, en nommant expressément l'accusé, en précisant le montant du litige et en fournissant un maximum de preuves pour appuyer sa demande. Certains forums comme XSS invitent chaque partie à publier toutes les

[8] *https://socradar.io/breachforums-seized-once-again-what-is-next/*

preuves directement sur le thread de la plainte. Cela permet d'assurer une certaine transparence sur les décisions prises par l'administrateur mais aussi de laisser la possibilité aux autres membres d'apporter une expertise spécifique ou un témoignage supplémentaire.

Les thématiques des litiges sont assez diverses : **la vente d'un produit défectueux** tel qu'un malware (défectueux) censé être indétectable (communément surnommé « FUD » sur les forums), **le silence du vendeur** après avoir reçu l'argent avec souvent la suppression de son compte Telegram ou encore un **escrow** qui n'a pas honoré ses engagements.



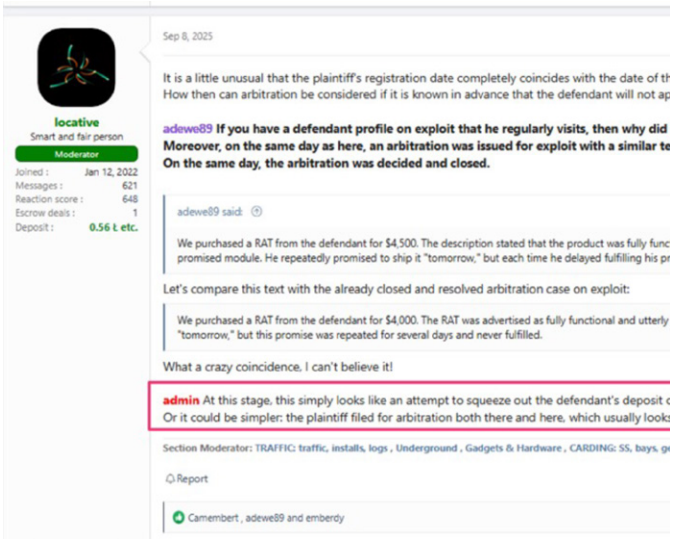
Aperçu d'une plainte publiée sur Exploit au sujet d'un malware défectueux

Lorsqu'un membre est accusé par un autre, l'administrateur laisse généralement 24h à ce dernier pour se défendre et selon les preuves fournies, va procéder à une sanction plus ou moins grande. Cela peut aller de la demande de remboursement jusqu'au ban définitif du compte de l'accusé. Certains forums comme BreachForums permettaient au membre banni de faire appel de la décision.

Bien que chaque forum ait son système de tribunal, certains forums s'alignent sur des décisions prises par d'autres concernant un membre. On peut par exemple citer les liens importants entre les forums XSS et Exploit. De nombreux membres ont des comptes sur les 2 plateformes et font référence à l'un et l'autre sur leurs publications.

Il arrive « malheureusement » que ce système de tribunal soit utilisé à mauvais escient par certains membres, portant un coup à la confiance dans le forum. On peut tout d'abord citer les cas d'acteurs qui créent de fausse plainte contre un membre. Le CERT-XMCO a vu plusieurs cas où le plaignant était accusé d'avoir généré de fausses captures d'écran de conversation sur Telegram avec des outils d'intelligence artificielle. Comment, dans ce cas, savoir qui ment et qui dit la vérité.

Un second cas de malversation est l'utilisation du tribunal à des fins de vengeance. Lorsqu'une des parties n'est pas satisfaite de la décision du tribunal d'un **forum A**, il est possible qu'il dépose plainte contre le même utilisateur sur un **forum B**. Cette vengeance peut permettre de ruiner la réputation de l'accusé voire de lui faire perdre de l'argent si son compte est crédité d'un dépôt en cryptomonnaies et que le compte se fait bannir. Cette situation a été évoquée sur le forum XSS en septembre 2025 lorsqu'un membre avait déposé plainte contre un autre sur Exploit et sur XSS.
Le CERT-XMCO a mené une analyse d'ampleur du système de tribunal du forum DarkForums depuis sa création. C'est l'objet de la partie suivante.



Aperçu de la publication (traduite du russe) sur XSS où un modérateur suspecte le plaignant de vouloir faire perdre à l'accusé l'argent de son deposit

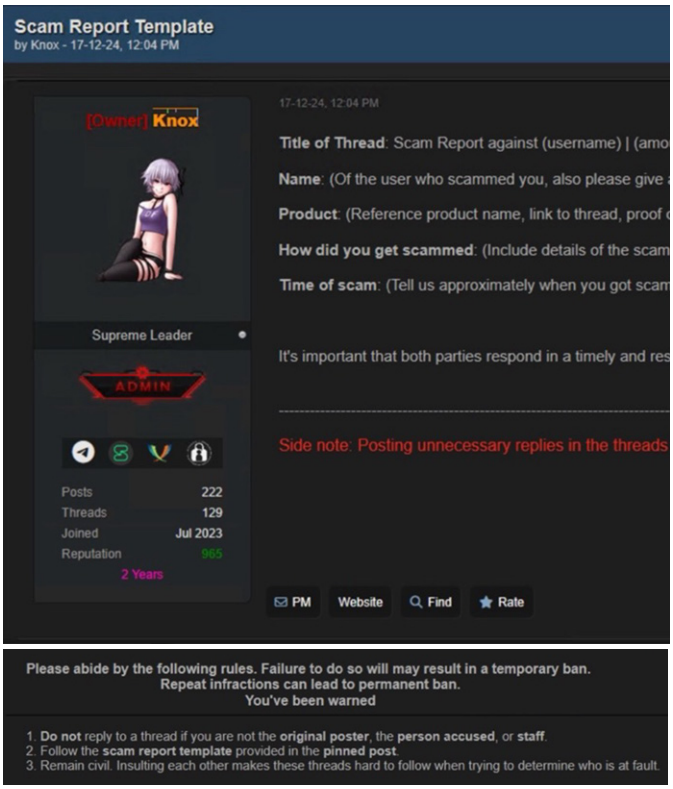
Administrateurs, litiges et confiance : analyse du systeme de scam reports sur darkforums

DarkForums, un forum cybercriminel actif en ligne depuis 2022 sous le nom DARK4RMY Forums, a vu son activité augmenter de plus de 600 % entre avril et juin 2025[9]. Cette progression s'explique par sa volonté de se positionner comme successeur de BreachForums, démantelé en août 2025 par un consortium international incluant la France et les États-Unis. DarkForums reprend l'ensemble des codes et des centres d'intérêt de BreachForums, notamment la vente et la diffusion de bases de données volées, de malwares ou encore de données confidentielles. Un autre élément hérité de BreachForums est le système de règlement des litiges, qui s'effectue via des publications accessibles publiquement.

La section dédiée au dépôt de litige entre deux utilisateurs est nommée « scam reports » sur le forum. Un utilisateur – que l'on appellera le plaignant – peut ainsi signaler un différend aux administrateurs concernant un autre membre, dans cet article désigné comme « l'accusé ». Cette partie propose une analyse qualitative, mais également quantitative de 61 scam reports publiés sur DarkForums entre le 30 décembre 2024 – date du tout premier scam report public – et le 21 novembre 2025.

État des lieux de la section scam reports sur Darkforums

Comme mentionné plus haut, les litiges entre utilisateurs – ou scam reports – sont hérités de BreachForums. Ils se trouvent dans une section dédiée, intitulée « Scam Reports », qui regroupe les règles à respecter pour déposer un litige, un modèle de plainte à remplir, ainsi que deux sous-sections : la première contient l'ensemble des tickets encore ouverts, tandis que la seconde, une section d'archives, rassemble les tickets résolus mais toujours accessibles aux utilisateurs.



Aperçu du modèle à utiliser pour soumettre un litige

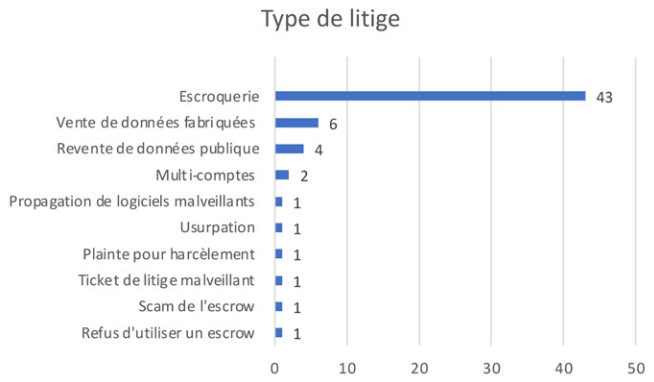
L'analyse des scam reports montre que la majorité des tickets de litige concernent des escroqueries : il s'agit d'un type de fraude dans lequel un utilisateur ne respecte pas sa part d'une transaction sur le forum – en ne livrant pas le produit promis ou en ne payant pas – afin de tromper l'autre partie.

En deuxième position apparaissent les cas de vente de données fabriquées. Dans ce scénario, un vendeur prétend détenir certains types de données (bases de données, documents confidentiels, etc.) et les commercialise, alors que ces données sont en réalité modifiées ou entièrement falsifiées. Ce type d'arnaque est particulièrement fréquent dans la vente de combolists (bases de données composées de couples identifiants/mots de passe) normalement utilisées dans des attaques par énumération : les listes proposées sont souvent générées artificiellement et donc inutilisables.

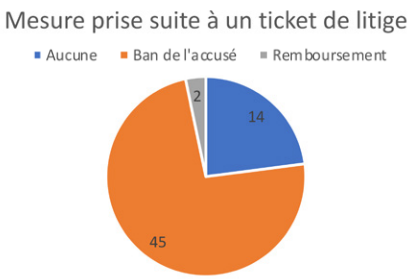
[9] *https://www.kelacyber.com/blog/darkforums-chronicles/*

Enfin, en troisième position, on observe des litiges liés à la revente de données publiques. Les accusés revendent alors des informations librement accessibles – parfois déjà partagées sur DarkForums ou sur d'autres forums cybercriminels – en se les réappropriant pour en tirer un profit indu.

On peut également noter que le montant médian des escroqueries s'élève à 210 $. La moyenne, quant à elle, atteint 374 $, mais elle est moins représentative car tirée vers le haut par quelques plaintes portant sur des montants particulièrement élevés. Les litiges recensés vont d'un minimum de 4 $ à un maximum de 2 000 $.



Sur ces 61 scam reports, 47 ont donné lieu à une décision finale. Dans 45 cas, l'accusé a été exclu du forum – ou « ban », selon la terminologie employée par les administrateurs. Dans seulement deux cas, le plaignant a obtenu un remboursement de la part de l'accusé. Enfin, 14 litiges sont restés sans dénouement. Précisons que dans la catégorie « aucune », plusieurs situations sont possibles : l'admin a peut-être décidé d'un non-lieu, il n'a peut-être pas vu le ticket, ou il l'a simplement ignoré.



Comme il n'est pas possible de faire la différence entre ces cas, ils sont tous regroupés sous « aucune mesure prise », puisque les non-lieux ne sont jamais indiqués clairement.

Pour conclure cet aperçu des scam reports, notre analyse montre que, lorsque la date de dénouement est identifiable, il s'écoule en moyenne huit jours entre l'ouverture et la clôture d'un ticket.

Analyse de l'efficience des mécanismes de résolution de litiges

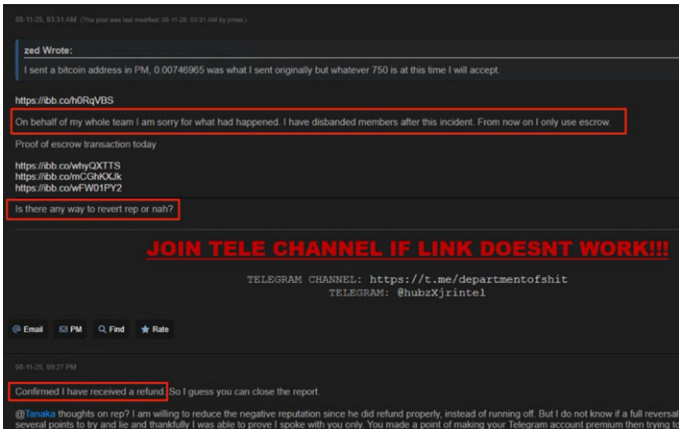
TRANSPARENCE DU SYSTÈME DE SCAM REPORTS ■

Dans un premier temps, la transparence des scam reports contribue à renforcer la confiance entre les utilisateurs, en leur permettant d'identifier plus facilement les membres fiables et ceux qui le sont moins.
En complément du système de litige, chaque utilisateur possède également une réputation sur le forum. Tout membre peut attribuer des points positifs ou négatifs à un autre. Il est à noter que seuls les utilisateurs ayant acheté un rang supérieur peuvent attribuer plus de ±1 point : plus le rang est élevé, plus le nombre des points qu'ils peuvent accorder augmente, jusqu'à ±30 pour les rangs les plus élevés.

Dans l'exemple ci-dessous, le plaignant « zed » affirme avoir été escroqué par un groupe cybercriminel nommé « jrintel » : il aurait payé une base de données qui ne lui aurait jamais été livrée. Après l'intervention d'un modérateur nommé « Tanakaa », un membre de « jrintel » a expliqué qu'un autre affilié du groupe avait escroqué « zed ». Ce membre aurait alors été exclu du groupe, et « jrintel » a remboursé « zed ».

Comme le ticket est public, plusieurs utilisateurs de DarkForums ont attribué une mauvaise réputation à « jrintel ». Le groupe a ensuite demandé aux administrateurs s'il était possible d'annuler ces points négatifs, maintenant que zed avait été dédommagé.

Il semble que les administrateurs aient effectivement supprimé une partie des évaluations négatives. Toutefois, en consultant le profil de jrintel, on constate qu'il subsiste encore plusieurs baisses de réputation, accompagnées de messages précisant qu'elles sont liées à l'escroquerie initiale envers « zed ».



Aperçu du message d'excuse de jrintel accompagné de la demande de retire les points négatifs de réputation

Ainsi, lorsqu'un utilisateur – qu'il soit acheteur ou vendeur – souhaite effectuer une transaction avec un autre membre, il peut vérifier si celui-ci a déjà fait l'objet d'un ticket de litige ou si sa réputation est trop faible avant de s'engager dans l'échange.

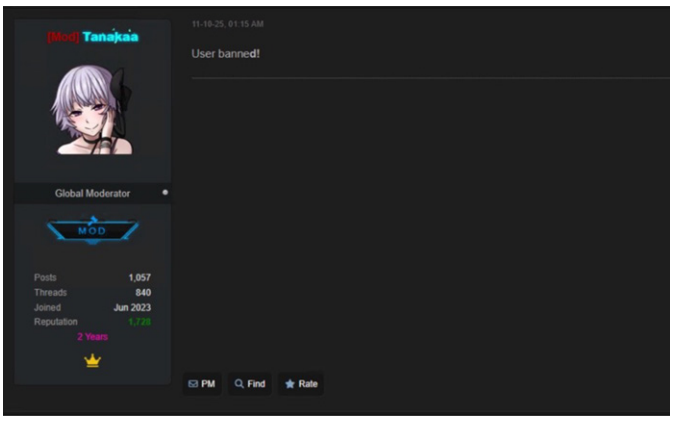
Réactivité et haut taux de prise de mesure des administrateurs

Deuxièmement, et en lien avec le point précédent, le haut niveau de réactivité des administrateurs permet de mieux faire face aux problèmes d'escroquerie. Comme mentionné précédemment, le délai moyen entre l'ouverture et la clôture d'un ticket est d'environ huit jours. Durant cet intervalle, l'administrateur en charge mène une enquête – plus ou moins approfondie selon les cas – afin de déterminer si l'accusé a effectivement commis une fraude.

D'après nos investigations, quatre utilisateurs semblent intervenir régulièrement dans la gestion des scam reports :

- « Knox », administrateur du site ;
- « Tanakaa », modérateur ;
- « cRime », qui n'est pas modérateur mais possède le rang « God », le plus élevé du forum pour les utilisateurs ;
- « AnonOne », qui était modérateur avant d'être récemment exclu pour exit scam.

Le fait que plusieurs membres disposant de rôles élevés participent au traitement des litiges contribue à maintenir un haut niveau de réactivité, ce qui permet d' « assainir » rapidement le forum et, par conséquent, de renforcer la confiance des utilisateurs dans le mécanisme de résolution de litiges.

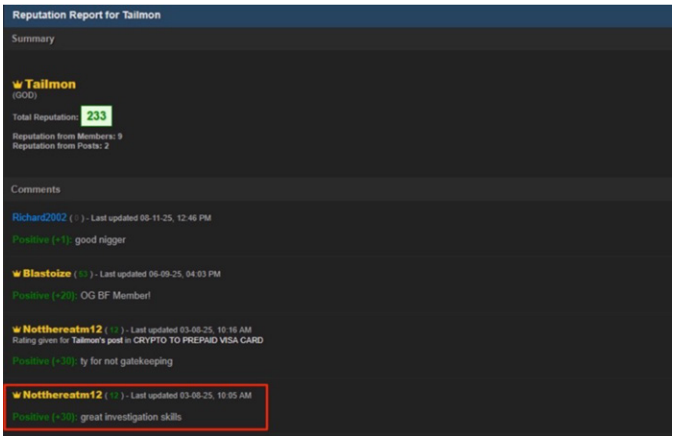


Aperçu de Tanakaa prenant la décision d'exclure un utilisateur

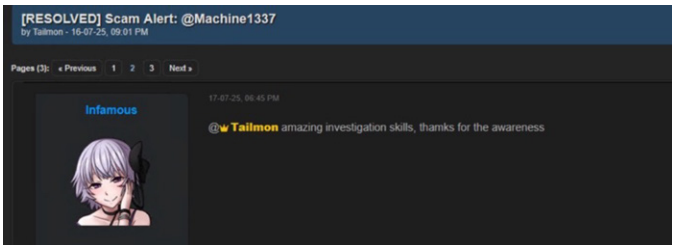
L'émergence d'utilisateurs jouant un rôle de " justiciables "

Du fait que les tickets soient publics, certains utilisateurs se sont attribué la mission d'identifier les escrocs actifs sur le forum. Ce rôle de « justiciable » leur permet non seulement de contribuer à renforcer la confiance, mais aussi d'améliorer leur propre réputation, facilitant ensuite la vente de leurs produits ou services.
Un exemple représentatif est l'utilisateur « Tailmon ». Sur ses douze publications sur DarkForums, cinq sont des scam reports visant à dénoncer des escrocs. Il intervient

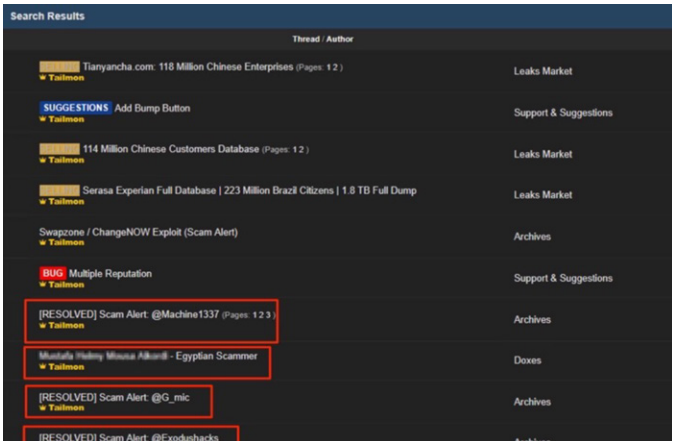
également fréquemment dans les tickets d'autres plaignants, en commentant pour les aider à mener leur enquête sur l'accusé. Il semblerait également que « Tailmon » réalise des investigations sur d'autres forums cybercriminels, comme XSS.
Plusieurs utilisateurs l'ont remercié pour ses investigations, lui attribuant des points de réputation.



Aperçu de don de réputation suite aux investigations de Tailmon



Utilisateur remerciant Tailmon pour son investigation



Aperçu de don de réputation suite aux investigations de Tailmon

Les limites du système de scam reports

Une réparation financière très limitée ■

Comme mentionné plus haut, sur les 61 scam reports analysés, seuls deux ont abouti au remboursement de la victime, 14 n'ont pas eu de dénouement et 45 ont conduit à l'exclusion de l'accusé. Ainsi, dans les trois quarts des cas, les modérateurs ne peuvent pas dédommager les plaignants. En effet, contrairement à d'autres forums cybercriminels qui exigent un dépôt pouvant servir de garantie en cas d'escroquerie, DarkForums n'en demande aucun.

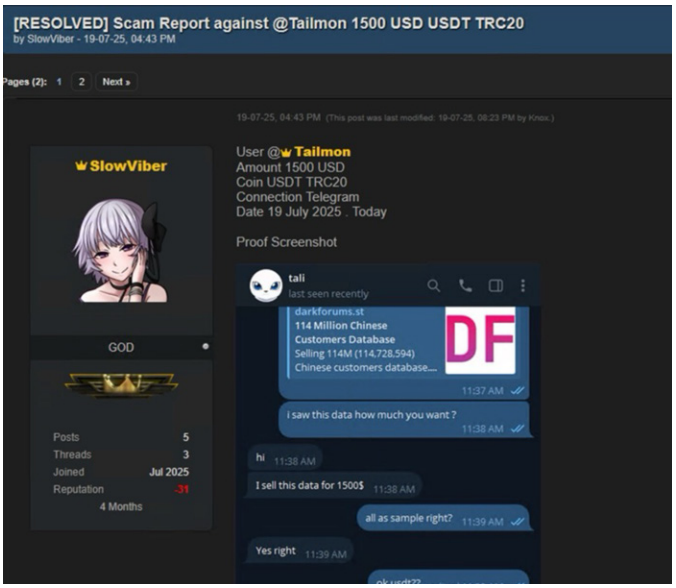
Certains utilisateurs déclarent avoir été victimes d'escroqueries allant jusqu'à 2 000 dollars, et une simple exclusion de l'escroc apparaît insuffisante au regard du préjudice subi – d'autant que nombre d'entre eux créent rapidement un nouveau compte pour continuer à cibler d'autres victimes. Bien que le multiaccounting (le fait de posséder plusieurs comptes) soit interdit sur DarkForums, il reste très difficile à détecter.

DÉTOURNEMENTS DES SCAM REPORTS ET ACCUSATIONS MALVEILLANTES ■

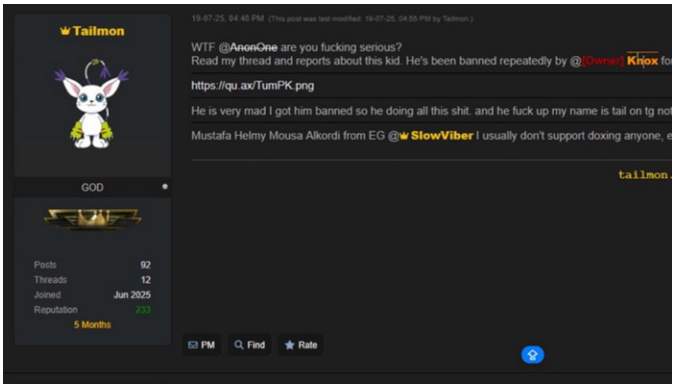
Enfin, du fait que les scam reports soient publics, ils peuvent être détournés pour nuire à d'autres utilisateurs. Un exemple révélateur concerne un ticket ouvert par un certain « SlowViber » contre « Tailmon » – l'utilisateur « justiciable » présenté précédemment – l'accusant d'une escroquerie de 1 500 dollars.

Après vérification par les modérateurs, il est apparu que « SlowViber » faisait partie des utilisateurs que « Tailmon » avait contribué à faire exclure dans le cadre de ses enquêtes. Pour se venger, « SlowViber » aurait donc fabriqué un faux scam report afin de porter atteinte à la réputation de « Tailmon ».

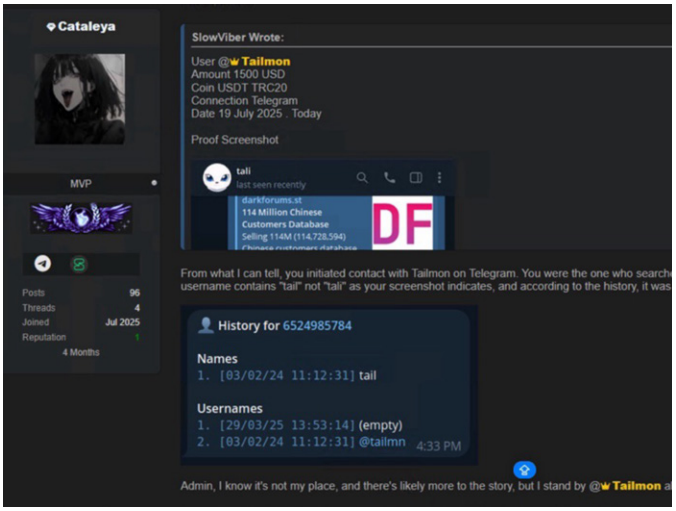
Ce cas n'est pas isolé : il est souvent difficile de prouver qu'un scam report est mensonger, ce qui ouvre la porte à diverses manipulations. L'ouverture de tickets fallacieux contre des concurrents, ou simplement en réaction à un conflit entre utilisateurs, constitue ainsi une pratique relativement courante sur les forums cybercriminels, où la réputation joue un rôle central dans la capacité à vendre, acheter ou collaborer.



Scam report fallacieux de SlowViber contre Tailmon



Réponse de Tailmon aux accusations



L'administrateur Knox conclut à l'innocence de Tailmon

Conclusion

ÉVOLUTION DES MECANISMES DE RESOLUTION DE CONFLITS

Pour conclure, l'analyse du système de scam reports sur DarkForums montre que, malgré certaines limites – comme l'absence fréquente de remboursement et la possibilité d'accusations malveillantes – ce mécanisme reste essentiel pour réguler les échanges entre utilisateurs. La transparence des tickets, la réactivité des administrateurs et l'implication de certains membres dans la détection des escrocs permettent de mieux identifier les utilisateurs fiables et, ainsi, de réduire les risques lors des transactions.

En définitive, même si le système n'est pas parfait, il contribue tout de même à renforcer la confiance entre les utilisateurs du forum au moment d'échanger des données ou des services. Les scam reports ne suppriment pas la fraude, mais ils apportent un minimum de contrôle et de visibilité qui participe à la stabilité du forum.

Même si tous les mécanismes évoqués précédemment permettent de réduire en partie les risques de se faire escroquer, d'avoir affaire aux forces de l'ordre ou à des chercheurs en cybersécurité, les attaquants sont obligés de « faire avec ». Certains utilisateurs parlaient d'une fin des forums après la saisie de RaidForums/Breached/BreachForums mais force est de constater que la fréquentation demeure.

Le paysage a cependant évolué et au lieu d'avoir un «hub» comme RaidForums, la population d'attaquants s'est déportée vers Breachstar, DarkForums et/ou Leakbase. C'est donc en résumé «business as usual» avec des attaquants qui ont toujours autant besoin les uns des autres depuis qu'ils se sont spécialisés dans une tâche en particulier.

On peut tout de même imaginer qu'avec la baisse des barrières techniques pour devenir attaquant (grâce à la démocratisation d'outils d'IA ainsi que l'amélioration des interfaces utilisateurs par les administrateurs), il y aura de plus en plus d'attaquants et donc de plus en plus de cas de litiges. Les modérateurs et administrateurs vont donc devoir trouver de nouvelles façons d'industrialiser la gestion de leur forum.

L'OSINT au service des missions Red Team

Par Etienne Le Dizes, expert XMCO.

Le contexte

Une entreprise dispose de plusieurs options afin d'évaluer son niveau de maturité en sécurité informatique. Les tests d'intrusion, les audits de code, ou encore les audits de configuration ne ciblent qu'une infime partie du système d'information d'une entreprise. Les exercices Red Team visent à couvrir l'ensemble du périmètre d'une entreprise, sans pour autant chercher l'exhaustivité. Cet article est axé sur les opérations Red Team, en particulier sur la phase de renseignement - appelée phase OSINT - débutant chaque mission.

Les méthodes présentées dans l'article prennent pour cible XMCO. Cet article ne vise en aucun cas à être exhaustif, que ce soit concernant les outils ou les étapes de la méthodologie proposés. Le projet OSINT Framework référence un grand nombre d'outils dédiés aux différents aspects intervenant dans le cadre de recherches d'informations en source ouverte.

Un écosystème riche

Le renseignement d'origine sources ouvertes, ou Open-Source Intelligence (OSINT), est une discipline informatique visant à obtenir et exploiter des informations sur une cible en ne tirant parti que d'informations disponibles publiquement.

Le gouvernement américain a fondé en 2005 l'Open Source Center afin d'institutionnaliser la collecte d'informations publiques au service du renseignement national. Depuis, plusieurs collectifs civils se sont formés : Bellingcat en 2014, qui participe à la lutte contre la criminalité à l'échelle mondiale, ou encore OSINT-FR en 2019, qui vise à rassembler des amateurs d'OSINT à un niveau national.

Le renseignement public n'est pas illégal. En revanche, la loi française encadre cette discipline afin d'éviter les débordements dus à l'exploitation de données mises en ligne. Ainsi, l'article 323-1 du Code Pénal précise que « Le fait accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende ». Les peines prononcées sont plus lourdes lorsque les actions illégales s'accompagnent de suppression ou de modification de données, ou encore lorsque les systèmes ciblés appartiennent à l'État. Il est alors vital dans une pratique OSINT de s'assurer que les données collectées proviennent de sources publiques. Il est également important de savoir que l'accès à du contenu disponible publiquement mais explicitement classifié comme « confidentiel » est condamnable par la loi.

Une fois les informations collectées, l'exploitation de ces dernières doit se faire conformément à la loi en vigueur. En effet, il est explicitement interdit par l'article 223-1-1 du Code Pénal « de révéler, de diffuser ou de transmettre [...] des informations relatives à [...] une personne [...] aux fins de l'exposer [...] à un risque direct ». La pratique de l'OSINT doit donc être effectuée de manière consciente et en toute connaissance des lois la régissant.

L'OSINT est un domaine pouvant être divisé en plusieurs catégories, qui diffèrent selon le type de données traitées. Chacune des catégories dispose de ses propres méthodes et outils dédiés à la collecte ainsi qu'à l'analyse des données.

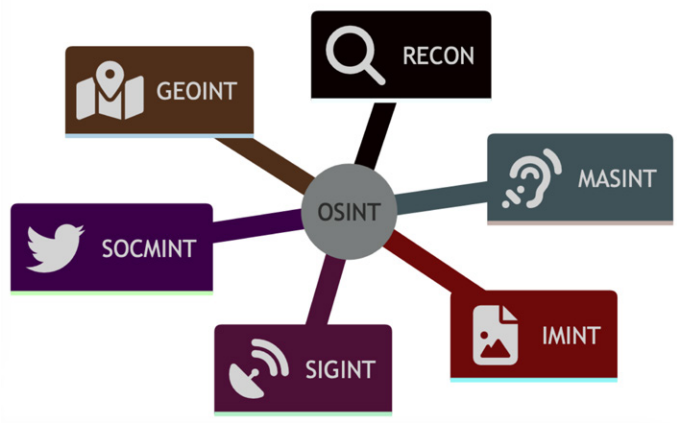
On distingue ainsi les catégories suivantes :

- **SOCMINT** (Social Media Intelligence), pour la recherche d'informations sur les réseaux sociaux ;
- **IMINT** (Imagery Intelligence), pour la re cherche d'informations depuis des images capturées par des téléphones, satellites, avions, drones, etc. ;
- **GEOINT** (Geospatial Intelligence), qui re prend les concepts de l'IMINT en y ajoutant des données complémentaires telles que les données géologiques ou météorologiques ;

- **SIGINT** (Signals Intelligence), en lien avec les signaux électromagnétiques et communications radio ;

- **MASINT** (Measurement and signature intelligence), destiné à l'analyse des mesures effectuées à partir d'un capteur ;

- **RECON**, relative à la collecte et à l'analyse de données à partir des services réseau exposés sur Internet.



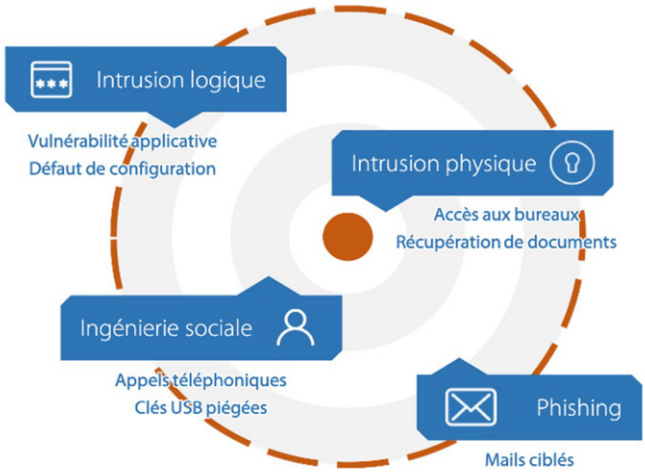
Les différentes catégories du renseignement d'origine sources ouvertes

Un OSINTeur peut être amené à utiliser indifféremment l'un ou l'autre de ces domaines, en fonction du type de données qu'il rencontre durant sa démarche. Par exemple, la RECON visera à découvrir le périmètre logique d'une cible le plus exhaustivement possible tandis que le SOCMINT permettra d'obtenir des informations sur des personnes ou sur l'activité de l'entreprise.

Les audits red Team

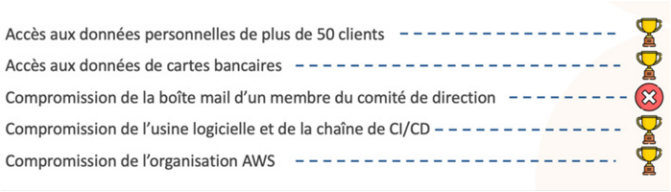
Le but d'un audit Red Team est d'évaluer le niveau de sécurité logique, physique et humain d'une entreprise et la capacité de ses équipes techniques à détecter et à déjouer des attaques en temps réel. Une opération Red Team est l'occasion pour une entreprise d'évaluer sa maturité cyber et de mettre à l'épreuve ses procédures vis-à-vis des risques majeurs qu'elle considère.

À la différence des tests d'intrusion ciblant un périmètre spécifique, un exercice Red Team vise l'intégralité de l'environnement d'une entreprise et favorise une approche en profondeur. L'objectif est de simuler une attaque réelle en jouant le rôle d'un *threat actor* qui exploiterait des failles aux niveaux humain, logique, et physique. Un tel exercice se déroule généralement sur plusieurs semaines, permettant aux auditeurs d'élaborer, de préparer puis de mettre à l'œuvre leurs scénarios d'attaque ciblant les objectifs, et ce tout en utilisant des TTPs (Tool, Tactics and Procedures) les plus discrètes possible afin de préserver l'OPSEC (sécurité opérationnelle) de l'exercice.



Différents vecteurs exploités dans le cadre d'un exercice Red Team

Au préalable, le client et les auditeurs définissent des "trophées". Il s'agit d'objectifs à atteindre durant l'exercice Red Team, qui symbolisent des risques importants identifiés et inclus dans le *threat model* du client : compromission d'un serveur spécifique car considéré comme extrêmement critique, accès à la boîte mail d'un membre du comité exécutif, récupération d'un secret accessible uniquement par un nombre très restreint d'employés, etc.



Exemples de trophées définis en amont d'une mission Red Team avec le client

Au début d'une opération Red Team, les auditeurs se mettent dans le rôle d'un attaquant ne disposant d'aucune information sur le périmètre de sa cible.

L'exercice démarre donc forcément par une phase de découverte des périmètres logiques, physiques et humains, afin d'acquérir un maximum d'informations sur la cible et son environnement. Les informations collectées durant cette phase seront utilisées durant les phases suivantes de la mission. C'est lors de cette première étape qu'il est pertinent de faire intervenir l'OSINT.

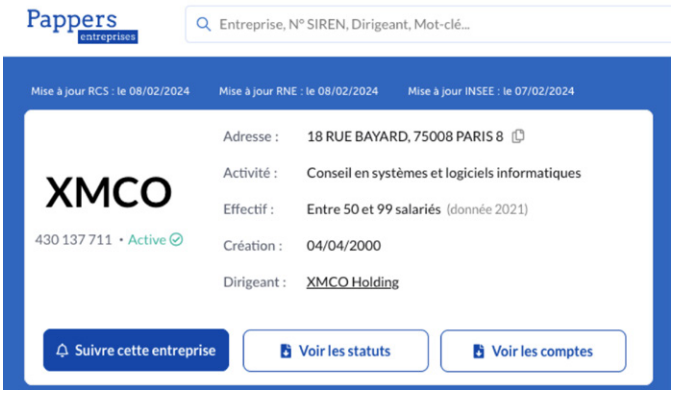
> **Les étapes d'une méthodologie OSINT appliquée lors d'une mission Red Team**

La phase OSINT précède généralement toute autre action lors d'une mission Red Team, le but étant de récolter passivement, c'est-à-dire sans entrer directement en contact avec l'environnement de l'entreprise, un maximum d'informations. Les auditeurs visent à simuler un attaquant réel et démarrent donc le plus souvent avec le minimum d'informations possible concernant la cible, soit le nom de l'entreprise uniquement. Une méthodologie OSINT permet d'évoluer de cet état initial très restreint à un état de connaissance approfondie sur la cible et ses environnements logique, humain et physique. Les méthodologies associées à ces types d'environnements sont décrites dans les sous-parties suivantes. La démarche OSINT doit être appliquée à l'entreprise, mais également à ses filiales dans le cas où ces dernières font partie du périmètre de l'exercice Red Team. Il est ainsi nécessaire de les identifier en premier lieu.

Identification des filiales

Si les filiales sont comprises dans le périmètre de l'exercice Red Team, il convient de les considérer dans les cibles et de ne pas se concentrer uniquement sur l'environnement de la maison mère. En effet, la réalisation d'actions sur le système d'information d'une filiale moins mature et donc moins supervisée est plus complexe à détecter pour les équipes de cyberdéfense.
Une bonne connaissance des filiales permettra aux auditeurs de mieux appréhender les prochaines phases de l'opération.

Entre autres, le service Pappers regroupe de précieuses informations sur l'environnement économique de l'entreprise :



Consultation des informations légales, juridiques et financières d'XMCO à l'aide du service Pappers

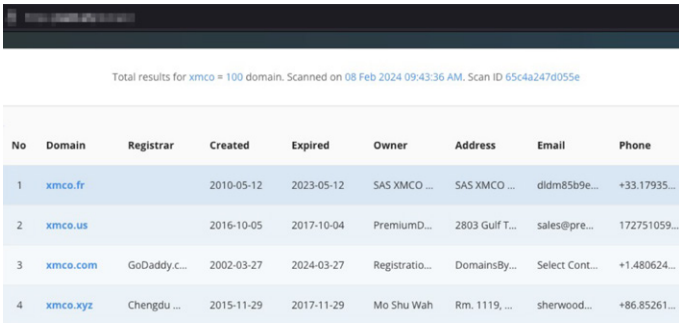
Ce dernier compile différentes sources d'informations, telles que l'Insee, l'INPI, le BODACC. En particulier, l'Institut National de la Propriété Intellectuelle (INPI) met à disposition une base de données regroupant les marques déposées en France, via l'URL suivante : https://data.inpi.fr/. Il est alors possible d'identifier les marques déposées par l'entreprise cliente. Autrement, Linkedin est une mine d'or et permet également de mapper les différentes filiales des entreprises avec présence à l'international.

Préparation de l'intrusion logique

RECONNAISSANCE PASSIVE DE L'INFRASTRUCTURE INFORMATIQUE

L'étape de reconnaissance passive de l'infrastructure IT d'une entreprise permet d'identifier ses actifs informatiques, représentant autant de vecteurs d'attaque potentiels pour les auditeurs. Ces derniers s'appliquent à énumérer entre autres les domaines, sous-domaines, adresses IP, les services réseau exposés sur Internet mais également les solutions SaaS utilisées par l'entreprise.

À partir du nom d'une entreprise, il est facile d'identifier son site vitrine via un moteur de recherche. Le module *domain* de l'outil [redacted] peut également être utile dans l'identification du site principal d'une entreprise.



Total results for xmco = 100 domain. Scanned on 08 Feb 2024 09:43:36 AM. Scan ID 65c4a247d055e

No	Domain	Registrar	Created	Expired	Owner	Address	Email	Phone
1	xmco.fr		2010-05-12	2023-05-12	SAS XMCO ...	SAS XMCO ...	dldm85b9e...	+33.17935...
2	xmco.us		2016-10-05	2017-10-04	PremiumD...	2803 Gulf T...	sales@pre...	172751059...
3	xmco.com	GoDaddy.c...	2002-03-27	2024-03-27	Registratio...	DomainsBy...	Select Cont...	+1.480624...
4	xmco.xyz	Chengdu ...	2015-11-29	2017-11-29	Mo Shu Wah	Rm. 1119, ...	sherwood...	+86.85261...

Recherche de noms de domaine à partir du mot clé « xmco » sur le service [redacted]

Le site vitrine est un bon point d'entrée dans l'infrastructure informatique. Il permet d'obtenir le nom de domaine principal. À partir du domaine identifié, il convient d'élargir la reconnaissance de la surface logique aux sous-domaines.

Avec comme donnée d'entrée le nom de domaine principal, il est possible d'interroger différentes sources d'informations. Le projet **OWASP Amass** tire ses informations de plusieurs sources et retourne des noms d'hôtes associés à un nom de domaine.

```
└─o amass enum --passive -d xmco.fr
xmco.fr (FQDN) --> mx_record --> mail.xmco.fr (FQDN)
xmco.fr (FQDN) --> a_record --> 51.255.137.129 (IPAddress)
mail.xmco.fr (FQDN) --> a_record --> 176.31.230.51 (IPAddress)
blog.xmco.fr (FQDN) --> cname_record --> www.xmco.fr (FQDN)
www.xmco.fr (FQDN) --> cname_record --> xmco.fr (FQDN)
serenety-node12.xmco.fr (FQDN) --> a_record --> 212.129.10.245 (IPAddress)
blog-pci.xmco.fr (FQDN) --> cname_record --> www.xmco.fr (FQDN)
cc.xmco.fr (FQDN) --> cname_record --> pentest-ng.xmco.fr (FQDN)
vpn.cert.xmco.fr (FQDN) --> a_record --> 51.255.137.130 (IPAddress)
pentest-raw.xmco.fr (FQDN) --> cname_record --> pentest-www.xmco.fr (FQDN)
serenety.xmco.fr (FQDN) --> cname_record --> leportail.xmco.fr (FQDN)
leportail.xmco.fr (FQDN) --> a_record --> 51.255.137.129 (IPAddress)
pentest-neo.xmco.fr (FQDN) --> a_record --> 62.210.83.22 (IPAddress)
evidence.xmco.fr (FQDN) --> a_record --> 51.255.137.129 (IPAddress)
abuse.xmco.fr (FQDN) --> cname_record --> www.xmco.fr (FQDN)
serenety-node2.xmco.fr (FQDN) --> a_record --> 212.83.184.15 (IPAddress)
serenety-node9.xmco.fr (FQDN) --> a_record --> 212.129.7.154 (IPAddress)
176.31.0.0/16 (Netblock) --> contains --> 176.31.230.51 (IPAddress)
212.129.0.0/18 (Netblock) --> contains --> 212.129.10.245 (IPAddress)
```

Énumération des noms d'hôtes associés au domaine xmco.fr à l'aide de l'outil Amass

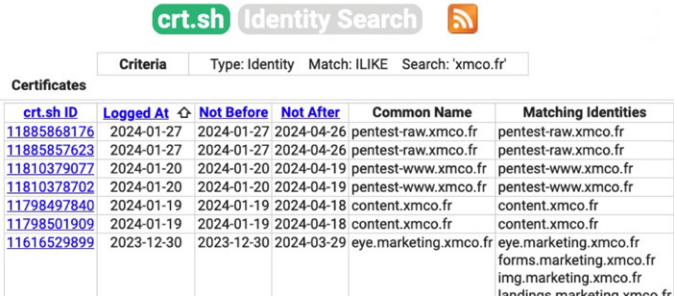
L'initiative [redacted] propose plusieurs outils utiles pour la reconnaissance passive, notamment **subfinder**. Il s'agit d'un programme en ligne de commande dédié à la découverte passive de sous-domaines et basé sur plusieurs sources telles que **LeakIX**, [redacted] ou **Wayback Archive**. Combiné à **httpx** pour probe les résultats, ils permettent d'identifier des services intéressants ainsi que les *cloud providers* utilisés par la cible.

```
└─o subfinder -d xmco.fr

                     __    _____           __
   _____  __  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.5 (latest)
[INF] Loading provider config from [redacted]
[INF] Enumerating subdomains for xmco.fr
evidence.xmco.fr
pentest-delta.xmco.fr
serenety-node1.xmco.fr
blog-pci.xmco.fr
pentest-ng.xmco.fr
landings.news.xmco.fr
forms.news.xmco.fr
img.marketing.xmco.fr
xmco.fr
eye.marketing.xmco.fr
```

Découverte de sous-domaines xmco.fr à l'aide de l'outil subfinder

Pour certaines sources d'informations, il est nécessaire de créer un compte gratuitement et de se voir autoriser un nombre de requêtes raisonnables par mois. Ceci peut suffire dans le cadre d'une prestation Red Team.

Il est également judicieux de tirer parti du Certificate Transparency. Il s'agit d'une base de données publique de certificats générés, sous la forme de fichiers de journalisation. Ce mécanisme permet aux navigateurs de vérifier la validité d'un certificat. Cette base de données peut être consultée via le service **crt.sh**.



crt.sh Identity Search

Criteria	Type: Identity Match: ILIKE Search: 'xmco.fr'

Certificates

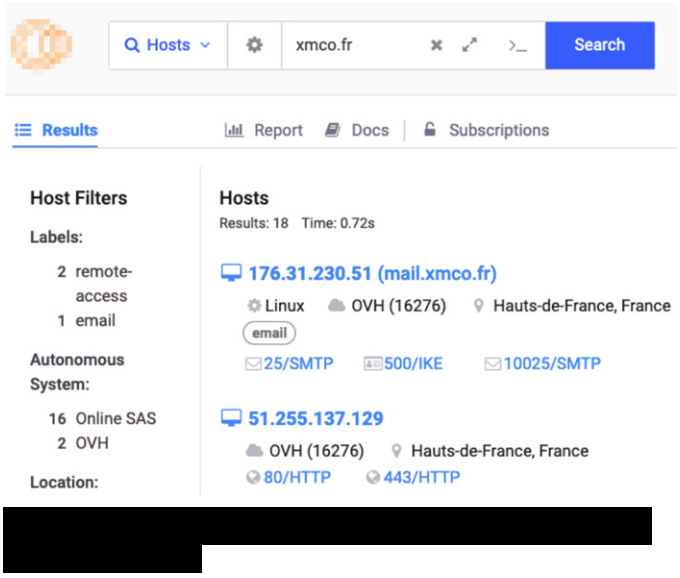
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
11885868176	2024-01-27	2024-01-27	2024-04-26	pentest-raw.xmco.fr	pentest-raw.xmco.fr
11885857623	2024-01-27	2024-01-27	2024-04-26	pentest-raw.xmco.fr	pentest-raw.xmco.fr
11810379077	2024-01-20	2024-01-20	2024-04-19	pentest-www.xmco.fr	pentest-www.xmco.fr
11810378702	2024-01-20	2024-01-20	2024-04-19	pentest-www.xmco.fr	pentest-www.xmco.fr
11798497840	2024-01-19	2024-01-19	2024-04-18	content.xmco.fr	content.xmco.fr
11798501909	2024-01-19	2024-01-19	2024-04-18	content.xmco.fr	content.xmco.fr
11616529899	2023-12-30	2023-12-30	2024-03-29	eye.marketing.xmco.fr	eye.marketing.xmco.fr forms.marketing.xmco.fr img.marketing.xmco.fr

Utilisation du service crt.sh pour la découverte de sous-domaines xmco.fr

Pour chaque domaine obtenu, il est nécessaire d'obtenir ses **configurations** [redacted] Ces protocoles interviennent sur trois

aspects de la sécurité relative aux courriers électroniques en provenance du domaine concerné. Une configuration trop permissive ou l'absence de configuration offrent aux auditeurs la possibilité d'usurper l'identité du domaine lors de campagnes de phishing.

Des services en ligne comme [redacted] scannent en permanence l'ensemble des adresses IP publiques afin de détecter des ports ouverts et par conséquent des services accessibles depuis Internet. En y recherchant des mots-clés, tels que le nom de la cible, ou les noms de domaine et adresses IP identifiées au préalable, ces applications retournent les services exposés ainsi que des détails dépendant du type de service. Par exemple, les services hébergeant une application web seront accompagnés d'informations sur les en-têtes HTTP et sur le certificat TLS.



[redacted]

De tels services pourront faire l'objet d'une phase d'exploitation active afin d'y identifier des vulnérabilités ayant un fort impact vis-à-vis des trophées définis ou permettant d'accéder au réseau interne.

Il est important de noter qu'aucun de ces outils d'OSINT n'est considéré comme préférable. Il est recommandé de combiner les sources d'informations afin de récolter le maximum de données sur la cible et d'éviter de passer à côté d'un actif potentiellement vulnérable.

Ainsi, il n'existe pas de méthode privilégiée pour la découverte des actifs informatiques d'une entreprise. Utiliser plusieurs sources d'informations diminue le risque de manquer un actif.

D'autres outils, fonctionnant pour certains de manière active, ne sont pas présentés dans cette section mais peuvent tout de même être utilisés durant la phase de reconnaissance logique : [redacted] **WHOIS**, [redacted] **tlsx**, ou encore [redacted] en mode actif.

Sources d'informations
Services de scans automatiques, Certificate Transparency, registrars
Informations collectées
Nom d'hôtes, adresses IP, services exposés, solutions externes, configuration mail

ÉNUMÉRATION DES FUITES DE DONNÉES APPARTENANT À L'ENTREPRISE

L'étape d'énumération des fuites de données vise à identifier les éléments sensibles appartenant à l'entreprise et rendus publics, soit par erreur de la part d'employés, soit la publication de bases de données ayant fuité. L'objectif pour les auditeurs est d'obtenir des adresses électroniques exploitables dans des scénarios d'hameçonnage, des numéros de téléphone pour de l'hameçonnage par téléphone, des combinaisons d'identifiants / mots de passe afin d'envisager une connexion sur un serveur VPN, ou encore des clés AWS permettant d'accéder à des services hébergés dans le *cloud*. Les plateformes d'échange telles que [redacted] ou **Pastebin** constituent des sources d'informations intéressantes.

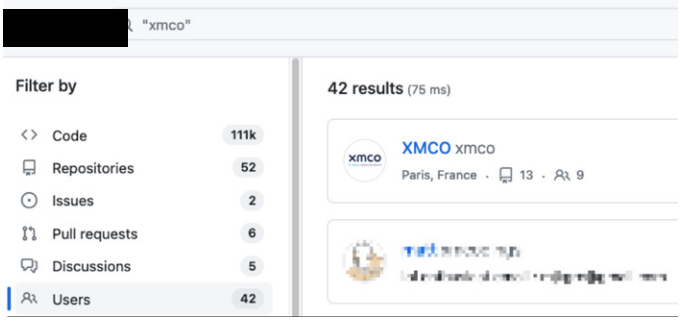
Il convient de s'intéresser au contenu public hébergé sur des services tiers mentionnant la cible. Par exemple, les plateformes collaboratives de code basées sur le protocole Git telles que GitHub, GitLab ou Bitbucket s'avèrent être des sources d'informations pertinentes.

En effet, elles peuvent contenir des identifiants de connexion ou des jetons d'accès à d'autres services (rôles dans AWS, *service principals* dans Entra), mais également d'autres types d'informations à valoriser, comme des fichiers pouvant contenir des adresses IP et des URL externes ou internes.

Pour repérer rapidement des pages contenant un mot clé spécifique sur ces plateformes, il est possible de tirer parti du **Google Dorking**. Il s'agit d'une technique de recherche reposant sur des opérateurs logiques. Les recherches effectuées à l'aide de ces opérateurs sont plus fines. Il est ainsi possible d'orienter la recherche sur un site Internet spécifique avec l'opérateur [redacted] et de n'obtenir que les pages contenant une chaîne particulière de caractères en précisant cette chaîne entre guillemets.
La **Google** [redacted] regroupe des requêtes Google Dorks utiles pour le renseignement d'origine sources ouvertes.

Utilisation de Google [redacted] afin d'identifier du contenu lié à XMCO sur le service [redacted]

La recherche ci-dessus permet d'obtenir du contenu mentionnant la chaîne de caractère « xmco ». Cette recherche peut également être effectuée directement sur [redacted]



Recherche du mot clé « xmco » sur la plateforme d'échange de code source [redacted]

Au total, 52 dépôts contiennent la chaîne de caractère « xmco » dans leur code et 40 utilisateurs contiennent cette même chaîne dans leur nom ou leur description. Il s'agit ensuite d'effectuer un tri dans les résultats afin de ne garder que le contenu pertinent et en lien avec l'entreprise ciblée.

Il arrive de tomber sur des "repo" contenant un grand nombre de fichiers. L'outil [redacted] permet de parcourir ces derniers à la recherche de secrets et autres données sensibles.
On peut également mentionner les applications web SourceGraph (https://sourcegraph.com/search) et Grep.app (https://grep.app/) qui permettent d'effectuer des recherches similaires à partir de mots clés.

De manière générale, tous les services externes utilisés par les employés de l'entreprise cliente sont susceptibles d'être exploités durant cette phase. Cette recherche de secrets et de données intéressantes pour la préparation d'attaques peut s'étendre à d'autres types de plateformes, comme par exemple Trello, Pastebin ou encore aux buckets S3 dans AWS. L'outil [redacted] agrège des données publiques et propose une fonctionnalité de recherche par mot clé.

Il est également intéressant de consulter les archives d'Internet disponibles auprès de services tels que la [redacted] Ce projet réalise des sauvegardes régulières de tous les sites Internet publics, rendant possible l'accès aux versions précédentes des sites d'intérêt pour l'opération.

Des pages contenant des données sensibles peuvent également avoir été supprimées. Si de telles pages ont été archivées à un instant t, il est toujours possible d'y accéder. L'outil en ligne de commande [redacted] agrège les données depuis l'Open Threat Exchange d'AlienVault, de la Wayback Machine, de [redacted] et [redacted] à partir d'un nom de domaine donné.

Ensuite, les auditeurs consultent les bases de données ayant fuité à la recherche d'accès initiaux. Des agrégats de "leaks" d'identifiants (avec le mot de passe parfois en texte clair

mais souvent sous forme d'empreinte cryptographique) sont publiés de temps à autre sur le dark web. On peut notamment référencer [redacted] ou la liste [redacted]

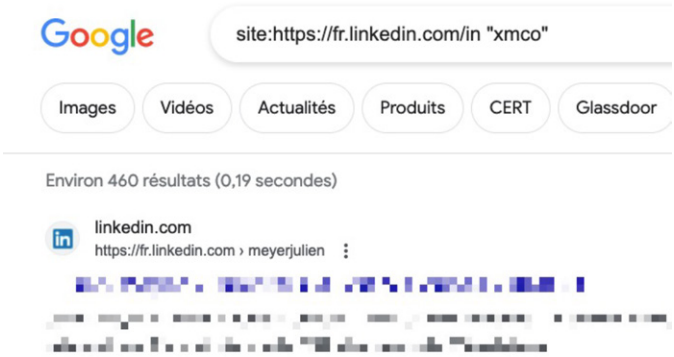
De tels accès sont précieux pour les phases d'intrusion après la phase de reconnaissance, et pourront être éprouvés sur les différents services identifiés (pages d'administration, appliance VPN, bases de données et services d'administration exposés, etc.).

Sources d'informations
Plateforme d'échange, archives d'Internet, bases de données compromises
Informations collectées
Secrets d'authentification, adresses électroniques, code source,

Ingénierie sociale

L'ingénierie sociale vise à exploiter l'écosystème humain et économique de la cible. L'objectif de cet axe de l'exercice Red Team est d'acquérir le maximum de connaissances sur les employés, les personnes clés de l'entreprise, mais également les relations entre les différentes équipes, tout en s'imprégnant du contexte dans lequel ces personnes travaillent au quotidien. L'obtention de telles informations permettra de mieux appréhender la préparation de scénarios de phishing / spear-phishing / vishing pertinents ainsi que la phase d'intrusion physique et les scénarios d'attaques qui en découlent. En particulier, l'analyse des profils techniques de l'entreprise ciblée permet souvent de récupérer les technologies employées en interne (EDR, mécanismes de SSO…).

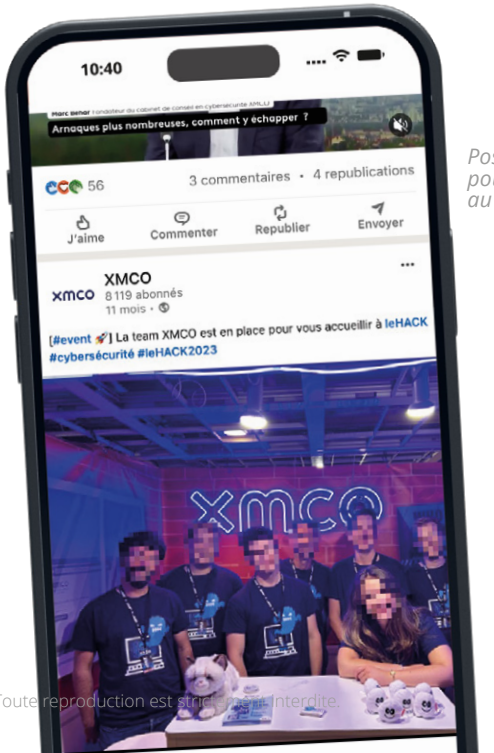
Pour commencer, une simple recherche utilisant des opérateurs Google Dorks permet d'identifier des employés de l'entreprise. La capture ci-dessous illustre une recherche permettant d'obtenir des pages contenant la chaîne « xmco » et ciblant le réseau social professionnel **LinkedIn**. Ceci permet aux auditeurs de repérer des profils en lien avec l'entreprise cible, appartenant potentiellement à des employés ou à des prestataires :



Google Dorks permettant d'identifier des employés d'XMCO

Des recherches sur le site vitrine de l'entreprise peuvent également mener à l'identification de personnes clés de l'entreprise. Les auditeurs établissent alors une liste d'employés en renseignant si possible leur poste au sein de l'entreprise et leurs adresses électroniques si elles sont publiques.

De plus, cette étape est l'occasion de découvrir le contexte actuel de l'entreprise. Une étude de la communication de l'entreprise sur les réseaux sociaux permet d'obtenir des informations utiles pour l'élaboration de scénarios d'hameçonnage. Par exemple, en parcourant la page LinkedIn d'XMCO, on peut découvrir que les employés étaient présents au forum de cybersécurité **leHACK**.



Post LinkedIn d'XMCO pour sa participation au forum leHACK

L'exemple du post précédent fournit un prétexte d'hameçonnage aux auditeurs. En effet, un courrier électronique annonçant la publication des photos de cet événement sur une plateforme interne pourrait tromper des employés et les forcer à rentrer leurs identifiants de connexion sur une mire d'authentification malveillante.

Sources d'informations

LinkedIn,
Site vitrine

Informations collectées

Liste d'employés,
personnes clés,
environnement humain de l'entreprise,
données financières,
Contexte actuel

Préparation de l'intrusion physique

La préparation des intrusions physiques nécessite de réaliser une reconnaissance du périmètre afin d'identifier :

- Les locaux pertinents à inclure aux scénarios d'attaque (par exemple, un bâtiment regroupant les infrastructures et métiers IT) ;

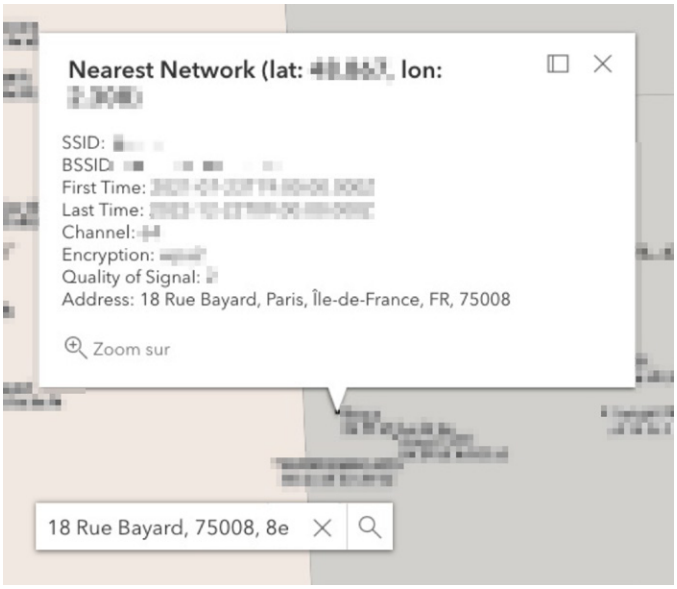
- Les mesures de sécurité physique déployées à l'extérieur et si possible à l'intérieur de ces locaux.

Pour ce faire, il convient de chercher et d'étudier les plans des locaux de l'entreprise, les images dévoilant l'intérieur des bâtiments, mais également les photographies des employés afin d'adapter le discours (la « légende ») dans le cas où nous les croiserions.

Le repérage des locaux peut être réalisé à l'aide de services publics comme [redacted] ou [redacted]. En naviguant avec [redacted] les auditeurs peuvent repérer les entrées possibles des locaux, les bâtiments environnants, les caméras de surveillance, la présence de badgeuses ou de vigiles, le type de portique de sécurité (anti-tailgate ou non), etc.

Une fois sur site, avant de tenter de réaliser l'intrusion physique, un repérage des alentours permet également d'initier la phase d'attaques sur les points d'accès Wi-Fi appartenant à la cible.

Le service [redacted] maintient une base de données de la localisation de points d'accès Wi-Fi et d'antennes. Il fournit le réseau Wi-Fi le plus proche pour une localisation donnée. Il est alors possible d'obtenir le nom du réseau sans fil de l'entreprise ainsi que certains éléments de sa configuration.



dentification des réseaux sans fil accessibles depuis les locaux de l'entreprise XMCO à l'aide de l'outil [redacted]

L'identification du style vestimentaire des employés peut également faciliter l'intrusion physique des auditeurs. Il arrive que des employés publient des photographies des bureaux ou des espaces de coworking. Ainsi, s'adapter au style des employés permet d'être moins suspect que si nous nous rendions en costume/cravate

La tenue et les badges des employés peuvent être identifiés sur ce type de photo. Les auditeurs ont alors la capacité de créer un badge factice et d'adopter une tenue conforme à la politique de l'entreprise. Ceci aura pour effet de les rendre moins suspicieux lors de l'intrusion physique.

Sources d'informations
Services de navigation virtuelle, Wilge
Informations collectées
Emplacement des locaux, style vestimentaire des employés, Configuration des réseaux sans fil

Conclusion

La phase de renseignement d'origine sources ouvertes est cruciale pour la réussite d'une mission Red Team. Elle permet aux auditeurs d'acquérir un haut niveau de connaissance sur l'entreprise cible. La compréhension de l'environnement humain et économique est tout aussi importante que la connaissance de données techniques concernant l'infrastructure informatique de l'entreprise.

Toute donnée collectée est susceptible d'être exploitée durant la mission Red Team.

Une fois la phase OSINT terminée, les auditeurs tirent parti des informations collectées afin de mener des attaques contre les services exposés, d'élaborer des scénarios de phishing, ou encore de parvenir à s'introduire physiquement dans les locaux de l'entreprise.

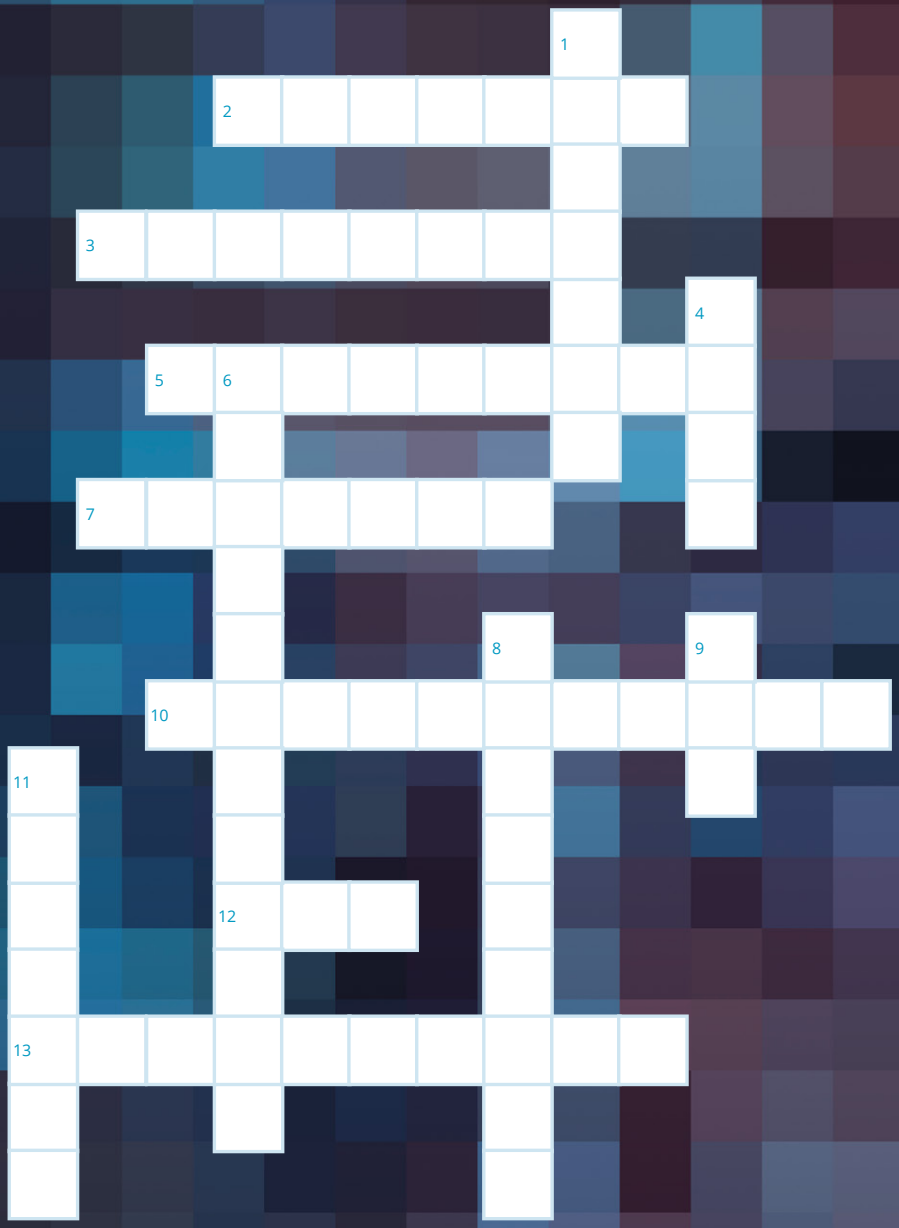
Sources

• *https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043974282*
• *https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047052655*
• *https://www.lemondedudroit.fr/decryptages/88174-quel-est-cadre-legal-osint.html*
• *https://fr.wikipedia.org/wiki/Open_Source_Center*
• *https://fr.wikipedia.org/wiki/Bellingcat*
• *https://[redacted]/fr/accueil/*
• *https://[redacted]/fr/faq-items/2-quels-sont-les-autres-domaines-de-losint/*
• *https://[redacted]*
• *https://www.exploit-db.com/google-[redacted]*
• *https://mermaid.live/*

Illustrations

• *https://assets.website-files.com/5f22271f4a92a90a8198c6ef/5f581f61563c688743b41aff_best-social-networking-sites.jpg*
• *https://blog.idrsolutions.com/app/uploads/2017/03/PNG.png*
• *https://media.istockphoto.com/id/505626040/fr/vectoriel/carte-du-monde-monde-croquis-vectoriels.jpg?s=612x612&w=0&k=20&c=_-oyEfwzb4lu7JtZopoeX8xlKBBtYgjPnrr5V98nrvw=*
• *https://cdn2.iconfinder.com/data/icons/education-46/100/antenna-512.png*
• *https://img.freepik.com/vecteurs-premium/icone-loupe-dessin-anime-fond-blanc-illustration-vectorielle-plane_693602-14.jpg?w=2000*
• *https://www.universite-paris-saclay.fr/sites/default/files/2021-02/informatique.jpg*

Mots croisés



- 1 : Dispositif ou logiciel qui filtre les connexions réseau entrantes et sortantes
- 2 : Outil réputé pour le cassage de mots de passe, et ami des félins
- 3 : Configuration d'une adresse IP permettant d'être figée sur un système
- 4 : Équipe spécialisée en cybersécurité dédiée à la gestion des incidents de sécurité informatique à grande échelle
- 5 : Niveau d'autorisation accordé à un utilisateur ou à un processus qui détermine les actions qu'il peut effectuer sur un système
- 6 : Type de malware qui chiffre les données et demande une rançon pour les récupérer
- 7 : Gestionnaire de base de données ayant souffert d'une vulnérabilité publique majeure en décembre 2025...
- 8 : Technique d'attaque qui consiste à insérer du code malveillant dans une application
- 9 : Équipement de sécurité ou aboiement de toutou ?
- 10 : Adepte des nuits blanches ou conférence réputée en cybersécurité qui se tiendra en mars prochain
- 11 : (pipeline): Chaîne automatisée de processus qui permet d'intégrer, tester et déployer du code en continu
- 12 : Évènement permettant de challenger ses compétences en hacking dans diverses catégories
- 13 : Autorisation pour un service à accéder à un autre au nom de l'utilisateur, ce mécanisme a été implémenté par Microsoft à partir de Windows Server 2000

Notes

Notes

xmco

We deliver cybersecurity expertise

Nos consultants pensent comme les attaquants pour mieux les contrer, puis vérifient manuellement chaque vulnérabilité potentielle afin de livrer une vision claire et exploitable des risques Cyber. Audits, pentests, réponse à incident, conformité PCI DSS, veille CERT et CTI : nous couvrons tout le cycle de vie de la cybersécurité. **Cette exigence transforme la sécurité en levier de performance mesurable.** Certifiés PASSI et PCI QSA, nous demeurons indépendants et engagés pour la réussite numérique de nos clients.

Date de création :	2002
Effectif salariés :	plus de 100
Qualifications :	PASSI, QSA et CERT officiel
Clients actifs :	plus de 450
dont clients CERT :	plus de 100
Secteurs :	Banque, Assurance, Industrie, Institutions, Transports, Médias, Luxe, etc.

Renseignement :

info@xmco.fr

01 79 35 29 30

www.xmco.fr