actusécu

By xmco

ACTUALITÉ | VEILLE CYBER | PENTEST | CTI | ÉVÈNEMENT SÉCU

JANVIER 2024

HORS-SERIE

Dossier spécial Dark Web

Les activités cybercriminelles : entre Dark Web et réseaux sociaux

Les spyware commerciaux

61

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

xmco

We deliver cybersecurity expertise

xmco

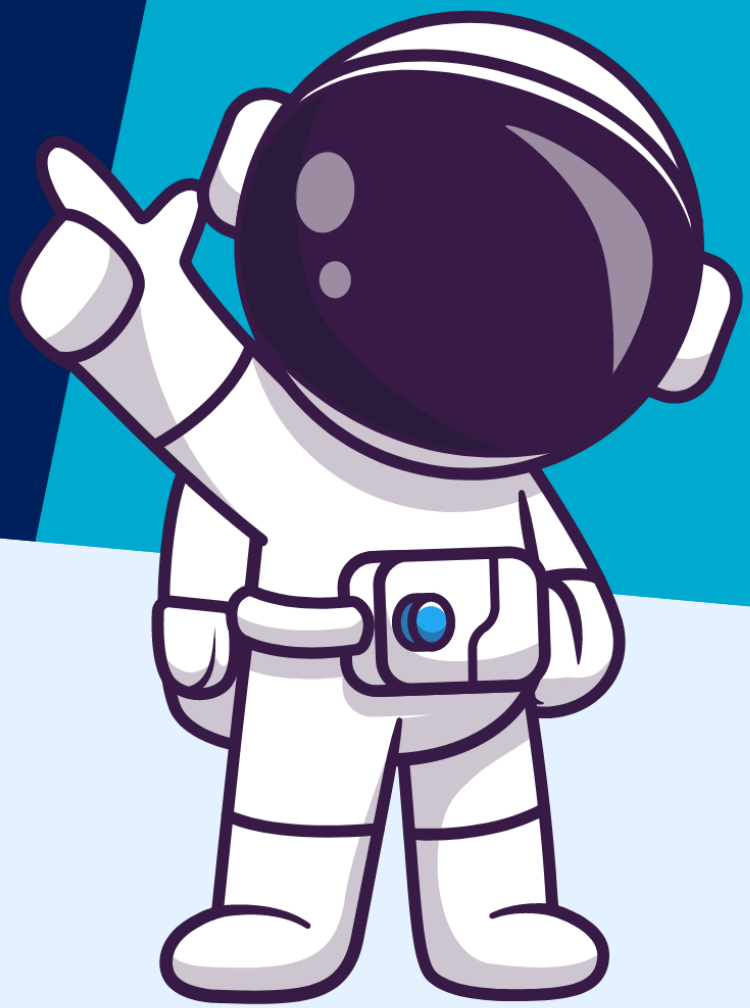
We deliver cybersecurity expertise

Vous recherchez un cabinet d'expertise en cybersécurité à taille humaine ?

Rejoignez l'équipe !

JOIN US!

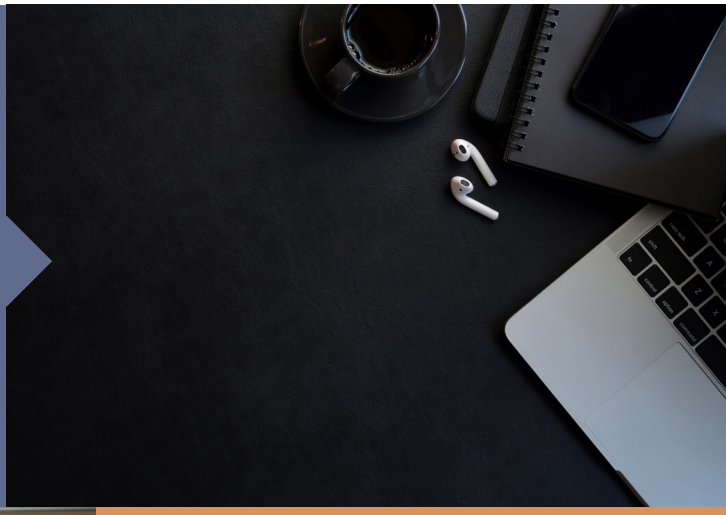
- **Pentesteur**
- **Consultant GRC**
- **Ingénieur / Analyste CTI**
- **Analyste Cybercriminalité**



Envoyez-nous votre CV ou postulez sur notre site

recrutement@xmco.fr
stages@xmco.fr
www.xmco.fr/rejoindre-xmco/

Sommaire



Contact Rédaction : actusecu@xmco.fr - Rédacteur en chef / Mise en page : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Johanna KUMRO, Ambroise DA SILVA, Vincent JEZEQUEL, Antoine AVET, Nicolas RAIGA CLEMENCEAU

Les activités cybercriminelles : entre Dark Web et réseaux sociaux

Par Johanna KUMRO et Ambroise DA SILVA

Executive Summary

Suite au premier dossier publié sur notre site web et abordant le sujet du Dark Web, notre équipe CTI a souhaité approfondir ce sujet et celui des réseaux sociaux afin de mettre en lumière plusieurs points :

- le Dark Web a toujours été perçu comme étant une communauté dans laquelle les cybercriminels peuvent échanger et se bâtir une réputation ;
- bien qu'il s'agisse d'un environnement instable, les arnaques qui y prolifèrent et l'omniprésence des autorités ont poussé les cybercriminels à étendre leurs présences sur d'autres canaux de communication ;
- l'utilisation des réseaux sociaux démocratise le cybercrime en restant anonyme et permet de promouvoir plus facilement les activités malveillantes ;
- chaque profil d'acteur de la menace bénéficie d'un avantage spécifique sur un ou plusieurs réseaux sociaux ;
- le recours aux réseaux sociaux favorise la démocratisation des activités, mais ouvre également la voie à des clients potentiels peu informés en matière de cybercriminalité ;
- malgré une montée en puissance de l'usage des réseaux sociaux, le Dark Web demeure un espace privilégié de la fréquentation des communautés cybercriminelles.

Note	*L'expression « réseaux sociaux » est utilisée dans ce dossier pour désigner à la fois les messageries comme Telegram ou WhatsApp, et les réseaux sociaux comme Snapchat, X (ex-Twitter) ou Facebook.*

Note	*L'expression « Dark Web » est utilisée dans ce dossier pour désigner l'espace cybercriminel traditionnel, constitué de forums et de marketplaces, disponibles depuis des darknets comme le réseau TOR, mais parfois aussi disponibles depuis le clearweb.*

Introduction

Comme souvent dans l'écosystème cyber, l'évolution du Dark Web est l'histoire d'un détournement d'un outil de son usage premier. Le Dark Web est à la base développé à travers le réseau Tor à la fin des années 90 par des organismes de recherches pour bâtir un réseau anonyme et chiffré qui servirait à protéger les communications sensibles des services de renseignements américains. Cependant, ses capacités d'anonymisation attirent des individus aux motivations variées : promotion de la liberté d'expression, résistance aux régimes autoritaires, lancement d'alertes et activités criminelles.

Les types de crimes qui prévalent sont la vente d'armes, la vente de drogues, le partage d'informations impliquant des images et vidéos violentes, pornographiques et pédopornographiques, mais aussi la vente de documents volés ou contrefaits comme des pièces d'identité, des cartes de crédit et des identifiants bancaires. On retrouve également la vente d'accès aux systèmes d'information de certaines entreprises et la vente d'outils destinés à mener des cyberattaques.

L'association de la cryptomonnaie aux ventes effectuées sur le Dark Web a d'autant plus renforcé la présence des cybercriminels en facilitant les transactions. Le Dark Web a permis aux cybercriminels de créer une communauté dans laquelle ils peuvent se retrouver et échanger.

Néanmoins, avec l'essor des réseaux sociaux et les multiplications des actions des forces de l'ordre sur le Dark Web, une nouvelle tendance s'est observée. Les activités des cybercriminels et des hacktivistes semblent s'être propagées sur les réseaux sociaux, notamment en ce qui concerne la vente d'identifiants de connexion, la vente de méthode de fraude et la quête de popularité.

De ce fait, les analystes CTI observent une recrudescence d'acteurs malveillants sur les différents réseaux sociaux. Cette observation nous amène à nous poser les questions suivantes :

- Cette nouvelle activité remplace-t-elle les activités traditionnelles du Dark Web ?
- Pourquoi les acteurs malveillants utilisent-ils davantage les réseaux sociaux dans le cadre de leurs activités criminelles ?

PARTIE 1

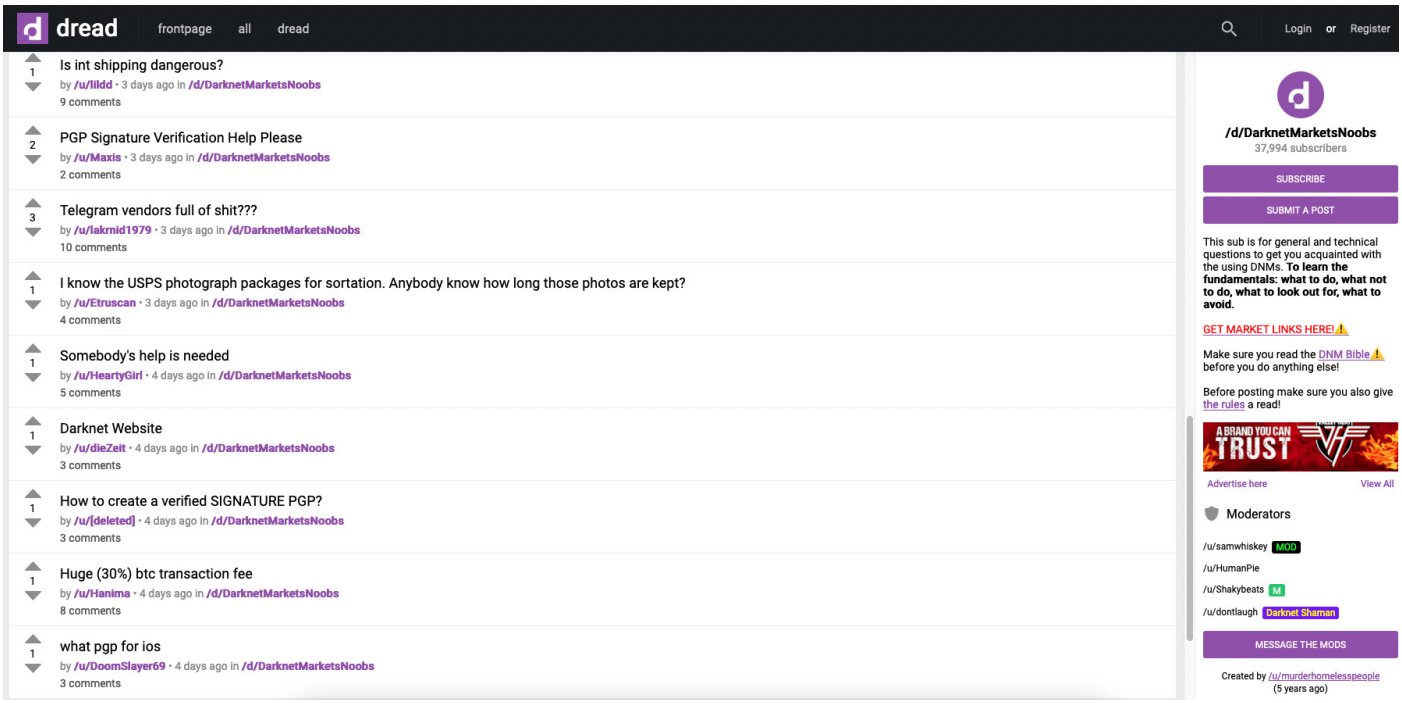
Le Dark Web : l'espace privilégié des activités cybercriminelles

Un espace communautaire et restreint

Une communauté d'entraide

Le Dark Web est aujourd'hui avant tout connu pour ses marketplaces et forums variés. Cette prolifération a permis aux utilisateurs qualifiés de créer des communautés dans lesquelles il est possible d'échanger de l'information, des bonnes pratiques, des recommandations sur les profils des acheteurs et des vendeurs, d'alerter sur les arnaques et les sites malveillants à éviter.

Ces communautés permettent aux débutants de se former techniquement. Par exemple, sur le site Dread, la section « d/darkwebmarketnoobs » permet aux nouveaux utilisateurs de bénéficier de recommandations sur les meilleurs outils et pratiques.



Section « d/darkwebmarketnoobs » de DREAD

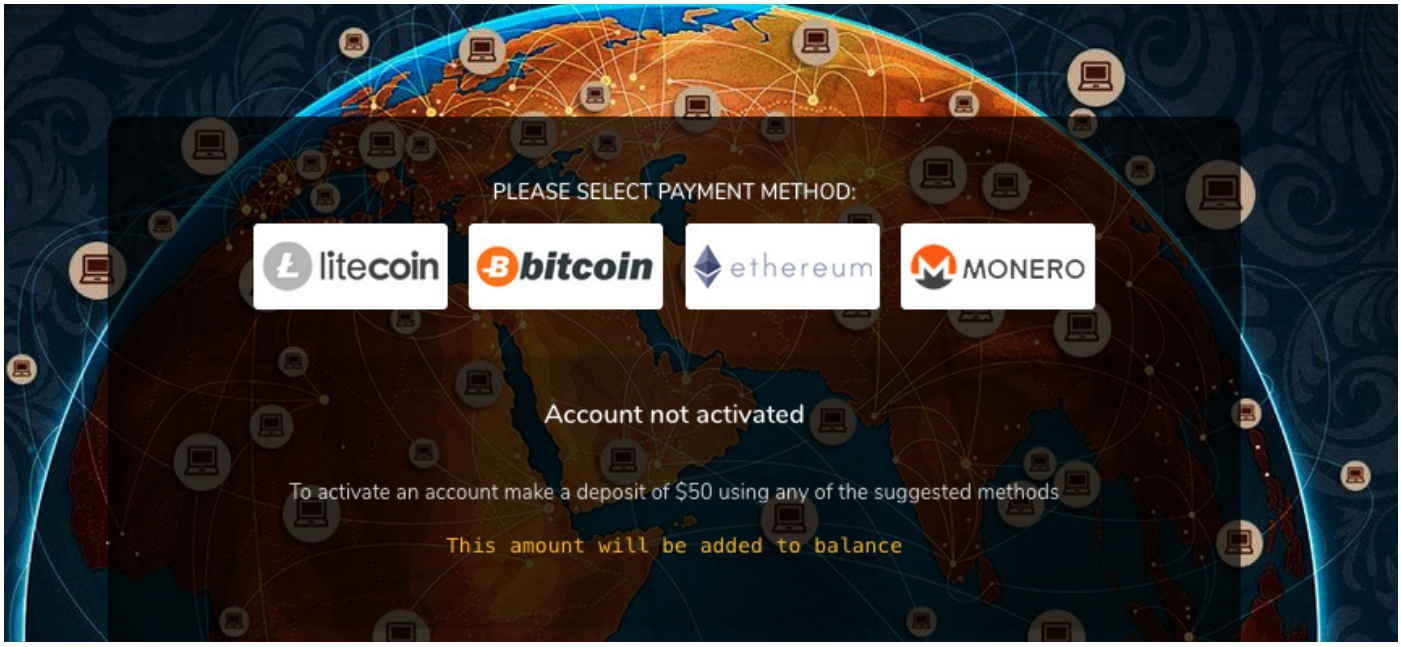
Les utilisateurs publient aussi des articles et des méthodes pour aider la communauté sur divers sujets tels que les dernières vulnérabilités, les discussions sur la programmation, sur la cryptographie, l'ingénierie sociale, l'OSINT, les fraudes comme le carding, etc.

Focus	*Le carding est une activité illégale qui consiste à utiliser frauduleusement des cartes de crédit ou de débit, généralement obtenues de manière illicite, pour effectuer des achats en ligne ou en personne sans l'autorisation du titulaire de la carte.*

De manière générale, les forums renforcent aussi le sentiment de communauté en mettant en place des politiques d'utilisation. Par exemple, ils peuvent bannir les utilisateurs qui ne participent pas à la vie de la communauté : le leeching (consommer du contenu sans en partager en retour) est banni. La création de chat rooms publics permet aussi aux utilisateurs de discuter et de collaborer sur des projets.

L'accès limité aux sites cybercriminels et le besoin de se bâtir une réputation

Le sentiment de communauté est d'autant plus renforcé que certains forums sont accessibles uniquement sur invitation et nécessitent un code d'invitation, une référence par un membre existant et parfois même l'abondement d'un solde en cryptomonnaie comme cela est le cas pour la marketplace Russian Market.



Processus d'inscription sur Russian Market

Certains d'entre eux sont entièrement privés, avec des adresses .onion dédiées au réseau Tor qui ne sont pas partagées publiquement et d'autres contiennent des discussions privées dans des sous-forums dont l'accès est restreint. Le principe est le même que pour les autres forums, ils permettent aux utilisateurs de traiter des sujets suivants : la vente de données volées, la planification d'attaques, la distribution de malwares, etc.

> « Les fermetures des forums Raidforums (2022) et Breached (2023) ont contribué à maintenir ce climat de suspicion… »

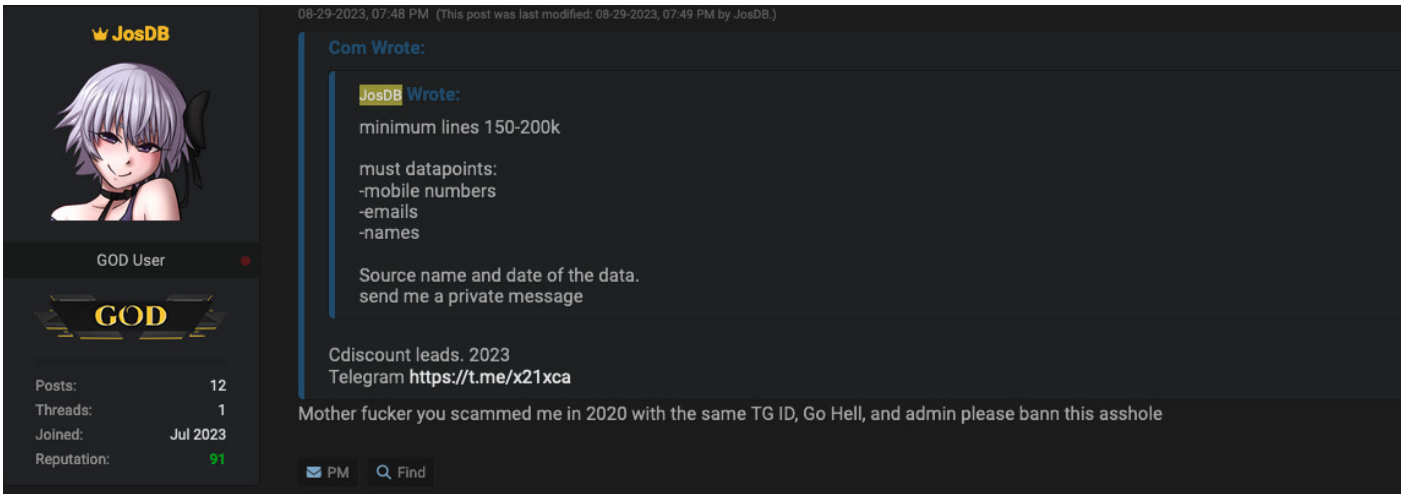
La mise en place de telles barrières peut s'expliquer pour plusieurs raisons :

- la volonté de tenir les non-initiés (noobs) à l'écart ;
- les analystes en sécurité et les forces de l'ordre sont très présents sur les sites cybercriminels. Cela peut susciter beaucoup de méfiance envers les profils n'ayant pas de réputation ou n'ayant effectué aucune transaction ;
- les marketplaces sont de plus en plus difficiles d'accès depuis la fermeture en 2017 par le FBI et Europol des marketplaces Alphabay et Hansa. Les nombreuses arrestations qui ont suivi ont suscité une certaine paranoïa parmi les utilisateurs. Les fermetures des forums Raidforums (2022) et Breached (2023) ont contribué à maintenir ce climat de suspicion…

BreachForums suite à la fermeture du site par les forces de l'ordre

De manière générale, et en particulier à cause de l'anonymat que permet cet environnement, toutes les transactions se basent sur la réputation des profils. La réputation est primordiale pour un acteur malveillant, c'est pour cela que l'on constate parfois l'utilisation du même pseudonyme sur différentes plateformes. Cela permet aux utilisateurs soucieux de leur réputation d'être reconnus à travers la communauté comme des personnes de confiance.

Le système de réputation mis en place par les forums ainsi que l'historique des publications sont donc de bons indicateurs de la crédibilité des acteurs. Ils renforcent la communauté en mettant en avant les acteurs connus et réputés tout en permettant de signaler les éventuels arnaqueurs.



Utilisateur dénonçant l'arnaque qu'il a subie

Un espace qui fait face à des limites structurelles

L'instabilité des infrastructures sur le Dark Web

Les infrastructures du Dark Web sont généralement considérées instables. Les raisons sont diverses et notamment dues à leur manque de moyens. Aussi, les sites sont plus exposés aux attaques diverses comme les attaques de déni de service (DoS), car leurs infrastructures étant moins robustes car souvent hébergées sur des serveurs privés. Les autorités fournissent un effort constant afin de perturber leurs activités, occasionnant de fréquentes fermetures de sites. La communauté est aussi considérée comme volatile, le nombre d'acteurs peut entraîner des disputes menant à la réalisation de campagne DDoS [2].

Plus spécifiquement, des instabilités s'expliquent aussi du fait que le protocole Tor n'a pas été créé dans le but d'optimiser la vitesse, mais pour anonymiser les communications de ses utilisateurs. Cela signifie concrètement que le temps de téléchargement sur Tor est lent. On constate notamment que télécharger des fichiers sur les sites vitrine des opérateurs de ransomwares peut être très lent sans les bons outils. Les crashs peuvent même être fréquents lorsqu'un grand nombre d'utilisateurs tentent de télécharger les fichiers en même temps (par exemple, lorsque les victimes de groupe de ransomwares sont d'un coup très nombreuses ou très connues).

Pour pallier ces limites, l'opérateur Clop a choisi de recourir à des torrents conjointement à l'emploi de sites sur le clear web lors de sa campagne d'exploitation d'une vulnérabilité dans MoveIT. Cela lui a permis de diffuser plus largement les données volées à ses victimes.

> « Le Dark Web est un écosystème dans lequel beaucoup d'arnaques ont lieu... On observe de plus en plus de cas de scam exit sur les marketplaces anglophones. »

À mesure que les activités criminelles se sont multipliées sur les sites Onion, les escroqueries et les attaques entre cybercriminels ont également proliféré. Les serveurs des sites Web en .onion sont mis hors service lorsqu'ils sont victimes d'attaques. Il arrive parfois que les sites soient indisponibles pendant des semaines, ce qui serait impensable pour des fournisseurs de services réputés. Toutes ces instabilités peuvent pousser certains attaquants à délaisser le Dark Web pour des alternatives plus fiables.

Focus	*Daniel's Hosting, l'un des plus importants fournisseurs de services d'hébergement de sites du Dark Web qui hébergeait environ 6 500 sites Web en .onion [3]. Ce site a été compromis en 2018, provoquant une panne massive des sites accessibles sur le Dark Web. L'infrastructure a été compromise à travers l'exploitation d'une vulnérabilité PHP zero-day qui a permis à l'attaquant d'accéder à la base de données complète des sites et de supprimer tous les comptes qu'elle contenait.*

Des arnaques omniprésentes et une perte de confiance générale

Le Dark Web est un écosystème dans lequel beaucoup d'arnaques ont lieu, mais pas uniquement envers les débutants. Les cybercriminels n'hésitent pas à s'attaquer entre eux. On observe de plus en plus de cas de scam exit sur les marketplaces anglophones.

Le terme de scam exit désigne la disparition des administrateurs d'un site après avoir récupéré tous les fonds des vendeurs. 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 [4] 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.

Les marketplaces, pour la plupart, fonctionnent sur le principe de dépôt de fonds. Cela signifie que les administrateurs exigent des vendeurs le dépôt d'une certaine somme, leur permettant ainsi de :

- générer des revenus en plus des frais d'inscriptions et commissions sur les ventes ;
- limiter les arnaques et assurer la qualité des vendeurs en dissuadant certaines populations (escrocs, analystes, noobs) de s'inscrire ;
- garantir la disponibilité des produits et services (il se peut que les vendeurs ne puissent pas respecter leurs engagements).

En général, un scam exit s'accompagne d'une inaccessibilité du site concerné, les administrateurs prétendant subir une attaque DDoS. Cela a notamment été le cas pour la marketplace Empire en 2020. Les incitations au calme et à ne pas répandre la nouvelle de cette prétendue attaque ont finalement eu pour effet de mettre au jour l'arnaque. Les escroqueries de ce type, souvent motivées par le gain financier, peuvent avoir un fort impact sur les utilisateurs qui accordaient leur confiance à la plateforme.

Focus

Le langage est également un facteur permettant de créer un sentiment de communauté sur le Dark Web et de différencier les internes (expérimentés) des externes (noob). Le niveau technique du langage de certains utilisateurs a ainsi tendance à exclure les non-initiés de certaines conversations. Cette technicité du langage est combinée à une forte évolutivité des mots et concepts au fil du temps. L'argot (slang) est par ailleurs souvent employé comme un jeu, permettant aux locuteurs de démontrer leur aisance à parler d'un sujet donné.

L'argot est aussi utilisé comme un outil de confiance. Une étude de l'université de Cambridge [5] s'est penchée sur la question de l'utilisation de l'argot sur les forums cybercriminels. Selon cette dernière, il y aurait une corrélation entre l'utilisation de l'argot et la réputation des profils. Plus un profil a une bonne réputation, moins il utilise de l'argot. C'est ce qu'ils appellent le « cold start problem ». Lorsqu'un nouvel utilisateur arrive sur un forum, il n'a aucun moyen de prouver sa crédibilité donc l'utilisation de l'argot peut être considérée comme étant un indicateur de confiance.

Ainsi, on observe une montée en puissance de la suspicion et de la méfiance au sein du Dark Web qui pousse les cybercriminels à se tourner vers d'autres canaux de communication et de partage.

Des forums et marketplaces de plus en plus surveillés par les autorités internationales

La croissance des transactions illicites sur le Dark Web a poussé les gouvernements à améliorer leurs capacités en termes d'application de la loi et en moyens pour s'attaquer aux cybercriminels. Les autorités travaillent activement pour surveiller, infiltrer, démanteler et poursuivre les opérateurs de marketplaces cybercriminelles. Ces activités s'inscrivent dans un effort global visant à lutter contre la cybercriminalité, la fraude en ligne, la vente de produits illicites et d'autres activités illégales sur Internet.

À cet égard, le dark web peut donc être considéré comme une sorte de honeypot géant, l'infiltration et la surveillance des sites par les autorités leur permettant de piéger les cybercriminels. Il est ainsi probable que certains forums ou marketplaces soient infiltrés voire même gérés par les autorités, comme ce fut notamment le cas de la marketplace Hansa. Les multiples infiltrations de la police sur ces différentes plateformes laissent de nombreux utilisateurs sceptiques sur les messages de sécurité et d'anonymat associés à l'utilisation de TOR.

> « Le Dark Web pourrait, sous forme de raccourci, être considéré comme un honeypot géant, puisque l'infiltration et la surveillance des sites par les autorités leur permettent de piéger les cybercriminels »

Dès 2016, l'acteur Ghostshell, connu pour avoir compromis plusieurs instances gouvernementales américaines, avait accordé une interview [5] à DataBreaches dans laquelle il affirmait que « le deep web (...) est le plus grand honeypot jamais créé par des agences internationales, sous la houlette des États-Unis et en collaboration avec le Royaume-Uni ». Il ajoutait que le forum Hell (le plus grand forum existant de l'époque) « est connu pour être rempli uniquement de fédéraux (FBI) et de chercheurs qui s'y rendent uniquement pour s'entraîner à attraper des pirates informatiques ».

Focus	*La saisie par les autorités d'un site criminel a en général pour seul effet de forcer la migration de ses utilisateurs malveillants vers d'autres plateformes. Conscientes de cette réalité, en 2016, les autorités néerlandaises ont donc choisi une nouvelle approche. Plutôt que de fermer le très populaire site Hansa, la décision fut prise de l'infiltrer.* *Deux agents de l'unité nationale néerlandaise de lutte contre la criminalité de haute technologie ont détaillé leur enquête de 10 mois, connue sous le nom d'Opération Bayonet, sur Hansa. Lors de cette opération, les deux agents ont réussi à identifier les deux administrateurs du site et à s'emparer de leurs profils pour avoir un contrôle complet sur la marketplace. Ils ont surveillé les acheteurs et les vendeurs de Hansa, modifié discrètement le code du site pour récupérer davantage d'informations d'identification de ces utilisateurs. Cela a mené à l'équivalent de millions de dollars en bitcoins confisqués, plus d'une douzaine d'arrestations et de comptages des principaux trafiquants de drogue du site et la récupération d'une vaste base de données d'informations sur les utilisateurs de Hansa qui, selon les autorités, devrait « hanter toute personne ayant acheté ou vendu sur le site au cours de son dernier mois de mise en ligne ».* *D'après Marinus Boekelo, l'un des deux investigateurs, le succès de cette opération a résidé en l'impact psychologique occasionné tant sur les acheteurs que les vendeurs, nuisant globalement à la confiance accordée à la plateforme par ses utliisateurs.*

La communauté cybercriminelle est bien informée de la présence des autorités sur certains forums, comme elle sait également que certains forums sont toujours en activité, car ils permettent à la police de rassembler des preuves et piéger les utilisateurs. C'est notamment pour cette raison que les cybercriminels ont tendance à utiliser des alternatives, comme les réseaux sociaux pour se discuter entre eux. Néanmoins, même si beaucoup préfèrent utiliser d'autres plateformes, les forums cybercriminels restent populaires et cela se remarque notamment par la création continue de nouveaux forums.

Le besoin de répondre aux nouveaux profils cybercriminels et de s'adresser à un public plus large

Les arrestations médiatisées de criminels ou les fermetures de certains sites du Dark Web contribuent à dissiper l'illusion selon laquelle l'utilisation de TOR offre un anonymat et une stabilité à toute épreuve. En conséquence de quoi, les attaquants seraient poussés à utiliser davantage d'autres espaces comme les réseaux sociaux pour préserver leur anonymat.

Une opération de l'envergure de l'opération Bayonet, ayant permis de fermer les marketplaces Alpha Bay et Hansa, serait beaucoup plus difficile à mettre en place aujourd'hui. En effet, une tendance à la décentralisation des activités cybercriminelles émerge. Ainsi, il est courant que si les transactions s'effectuent toujours sur les plateformes du darkweb, les échanges préalables passent par d'autres canaux (principalement Telegram, mais également Jabber ou Tox).

> « En d'autres termes, il est probable que certains forums ou marketplaces soient infiltrés, et même gérés par les autorités comme ce fut le cas de la marketplace Hansa »

En réalité, l'usage des réseaux sociaux a permis de démocratiser le cybercrime à plusieurs niveaux :

- **Technique :** des personnes moins qualifiées peuvent suivre ou se lancer dans des activités cybercriminelles. Les utilisateurs trouvent plus facilement ce qu'ils souhaitent acheter contrairement aux plateformes hébergées sur TOR, car cela demande moins d'expertise technique. Ils n'ont pas besoin de trouver les sites en .onion, de faire une demande ou de payer pour se créer un profil, etc.

- **Quantitatif :** les plateformes de messagerie ont permis aux vendeurs de cibler un public incomparablement plus large. En effet, les réseaux sociaux sont beaucoup plus accessibles par les internautes que les marketplaces ou forums du Dark Web. Elles ont aussi permis aux acheteurs d'interagir directement avec leurs clients, contrairement aux transactions sur le Dark Web qui nécessitent souvent un escrow (tiers de confiance transactionnel).

- **Réputationnel :** sur les plateformes de messagerie et les réseaux sociaux en général, les attaquants n'ont plus besoin de se forger une réputation. Il est courant que les profils et les canaux apparaissent puis disparaissent du jour au lendemain ou soient abandonnés rapidement. Il y a peu ou pas de section commentaires ou avis, peu d'éléments permettent de témoigner de la crédibilité d'un profil. Il est possible de demander des samples, mais ce qui est envoyé n'est pas forcément un gage d'authenticité.

PARTIE 2

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

Les profils cybercriminels et le déploiement de la fraude sur les réseaux sociaux

Les catégories d'acteurs

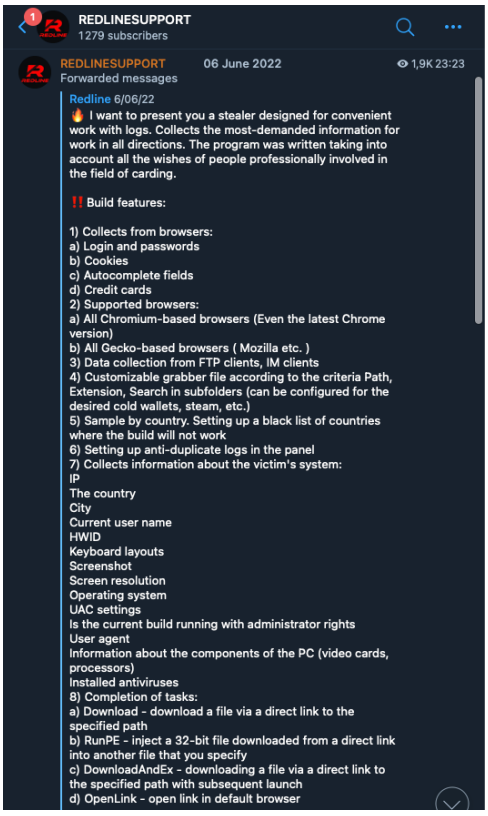
Le CERT-XMCO a distingué 4 principales catégories de profils d'acteurs de la menace pour mettre en évidence l'avantage comparatif offert par l'utilisation des réseaux sociaux tels que Telegram, X (précédemment connu sous le nom de Twitter), Snapchat, Instagram pour chaque profil cybercriminel :

- les Opérateurs de Malware-as-a-Service (MaaS) ;
- les Telegram Cloud of Logs (TCLs) ;
- les facilitateurs ;
- les fraudsters.

Les Opérateurs de Malware-as-a-Service (MaaS)

Certains développeurs (aussi appelés opérateurs dans le cadre du modèle MaaS) de logiciels malveillants exploitent un modèle de service appelé « Malware as-a-Service ».
Ce système permet à des clients potentiels d'acquérir une licence d'utilisation de logiciels malveillants pour une durée déterminée, renouvelable par abonnement. À titre d'exemple, les fonctionnalités de nombreux malwares de type « infostealer » – des malwares conçus pour dérober des données d'authentification sur des machines compromises – sont vendues sur Telegram. Parmi les infostealer les plus célèbres figurent Meta, Raccoon, Redline, Aurora et Vidar.

Telegram est principalement utilisé par ces opérateurs comme une interface pour la gestion des abonnements et la mise à disposition des données volées. La simplicité d'utilisation de Telegram permet à un acheteur de consulter facilement les données nouvellement volées depuis l'application. Ainsi, Telegram, en parallèle de l'utilisation du modèle MaaS, facilite l'utilisation de malwares par des profils peu expérimentés et contribue à élargir leurs bases utilisateurs. Plus généralement, le modèle MaaS permet une division du travail, où chacun se spécialise et bénéficie de l'expertise des autres.



Redline promouvant son infostealer éponyme sur Telegram

PARTIE 2

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

Les Telegram Cloud of Logs (TCLs)

Les TCLs désignent des canaux Telegram qui facilitent la mise à disposition d'informations d'authentification dérobées provenant de machines compromises par des infostealers. Le terme « logs » est utilisé pour décrire ces données volées qui sont ensuite distribuées gratuitement ou sous forme d'abonnements payants sur des canaux détenus par des attaquants. Parfois un attaquant mettra en place deux canaux Telegram : l'un gratuit, servant de démonstration de ses capacités et ne contenant qu'une infime partie des logs recueillis par l'infostealer ; et l'autre payant, regroupant l'ensemble des logs récupérés. Les clients ont alors la possibilité d'acquérir des logs permettant de se connecter à divers services, tels que des comptes de réseaux sociaux ou encore des ressources plus sensibles comme des portefeuilles de cryptomonnaies et des comptes d'employés d'entreprises. La compromission d'un compte employé peut entraîner des conséquences graves pour les entreprises concernées, telles que l'exfiltration de données confidentielles ou le déploiement de ransomwares. Le cas de l'attaque de EA Games par Lapsus$ en 2022 est un bon exemple d'entreprise victime de compromission, dont l'accès initial a été facilité par l'achat de logs sur des marketplaces spécialisées [6].

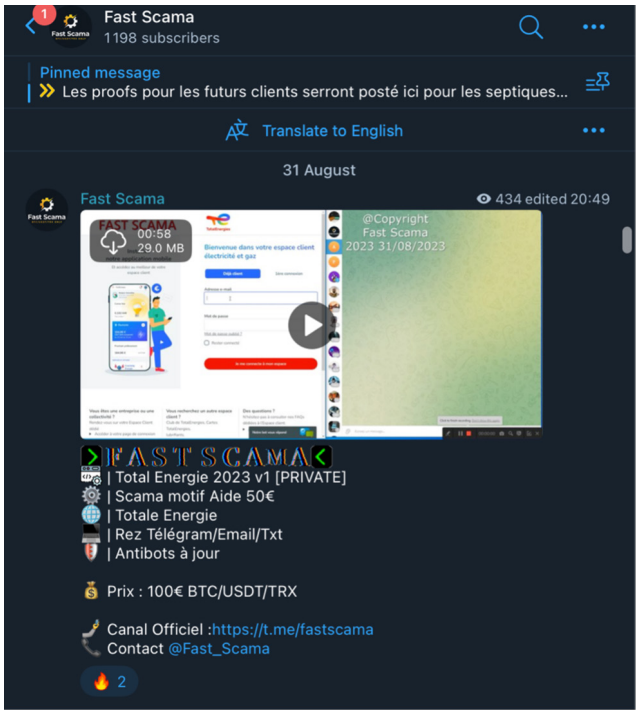
Le choix des réseaux sociaux tels que Telegram, par opposition aux forums et marketplaces du Dark Web, facilite l'acquisition de logs pour des acteurs malveillants moins expérimentés sur le plan technique. Bien que le nombre exact de TCLs actifs soit difficile à évaluer, un rapport publié par l'entreprise Kela en août 2023 témoigne d'une chute significative des prix des logs depuis le recours par les attaquants à Telegram et au modèle TCL. Selon ce rapport [7], en juillet 2023, environ 180 000 logs étaient disponibles sur la plateforme Russian Market (une des marketplaces les plus prisées pour l'achat de logs). En parallèle, d'après le rapport de Kela, un abonnement à 5 TCLs permettrait à un attaquant d'obtenir l'accès à près de 500 000 logs au cours du même mois. Le coût constitue également un avantage majeur. Sur Russian Market, le prix moyen d'un seul log s'élève à environ 13 dollars, tandis qu'un abonnement à une chaîne privée de TCL peut coûter entre 90 et 150 dollars, offrant un accès allant de 9 000 à 300 000 nouveaux logs par mois.

Les facilitateurs

S'il n'existe pas de terme officiel pour les désigner, nous appelons ici « facilitateurs » l'ensemble des services qui facilitent la fraude, le vol d'identifiants et la diffusion de secrets de connexion volés. À cette fin, les facilitateurs proposent divers produits et services. Par exemple :

Scama : un template de phishing sous forme de code source qui imite graphiquement un site officiel afin de tromper une victime. L'objectif est de faire en sorte que la victime saisisse ses secrets de connexion ou des informations personnelles comme des informations bancaires sur ce qu'elle pense être le site légitime, permettant à l'attaquant de les voler par la suite.

Combolist : une combolist est une liste de couples de noms d'utilisateur et de mots de passe. Ces listes peuvent être utilisées par les cybercriminels pour mener des attaques par énumération et de password spraying dans des systèmes informatiques, des comptes en ligne, ou des réseaux, dans le but d'accéder illégalement à des informations sensibles.



Boucle Telegram vendant des scamas

On peut aussi mentionner dans cette catégorie les leads qui sont des bases de données comprenant des adresses e-mail d'employés d'entreprises. Ces adresses seront généralement massivement exploitées dans le cadre de campagnes de phishing.

Config : les configs (ou configurations) sont des templates qui contiennent les réglages et paramètres nécessaires au lancement d'attaques à l'aide de logiciel open-source type OpenBullet, un outil permettant entre autres le scraping, l'analyse ou le pentesting automatisé. Comme souvent, OpenBullet a été largement réapproprié par les attaquants pour lancer une variété d'attaques automatisées :

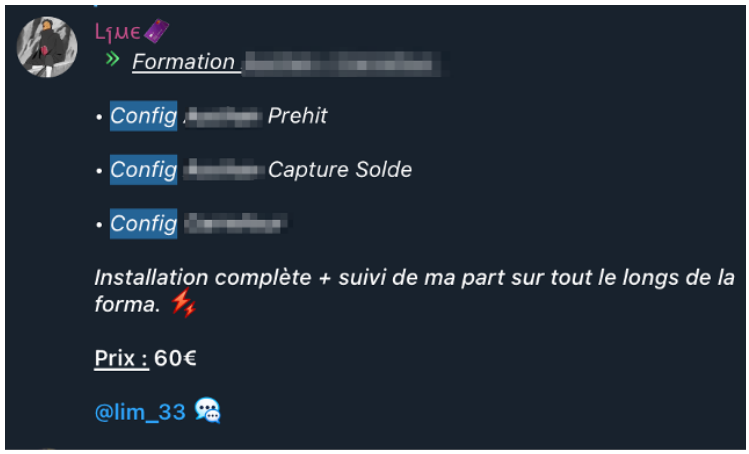
- Numération (ou brute force) ;
- Injection SQL ;
- Password spraying ;
- Account takeover ;
- Account verification ;
- CAPTCHA cracking.

Chaine Telegram proposant gratuitement des combolist

Il est possible de trouver de nombreuses configurations sur les forums du Dark Web. Les cybercriminels peuvent distribuer ou vendre ces configurations, ce qui en fait une ressource précieuse dans le monde des attaques automatisées. Les configurations sont importantes, car elles permettent aux attaquants de gagner du temps et de l'argent. Elles permettent aux utilisateurs de lancer des attaques sophistiquées sans avoir à créer leurs propres scripts à partir de zéro.

Les configurations doivent être adaptées aux cibles visées ; c'est pourquoi les configurations les plus récentes et les plus sophistiquées ont le plus de valeur et sont généralement mises en vente.

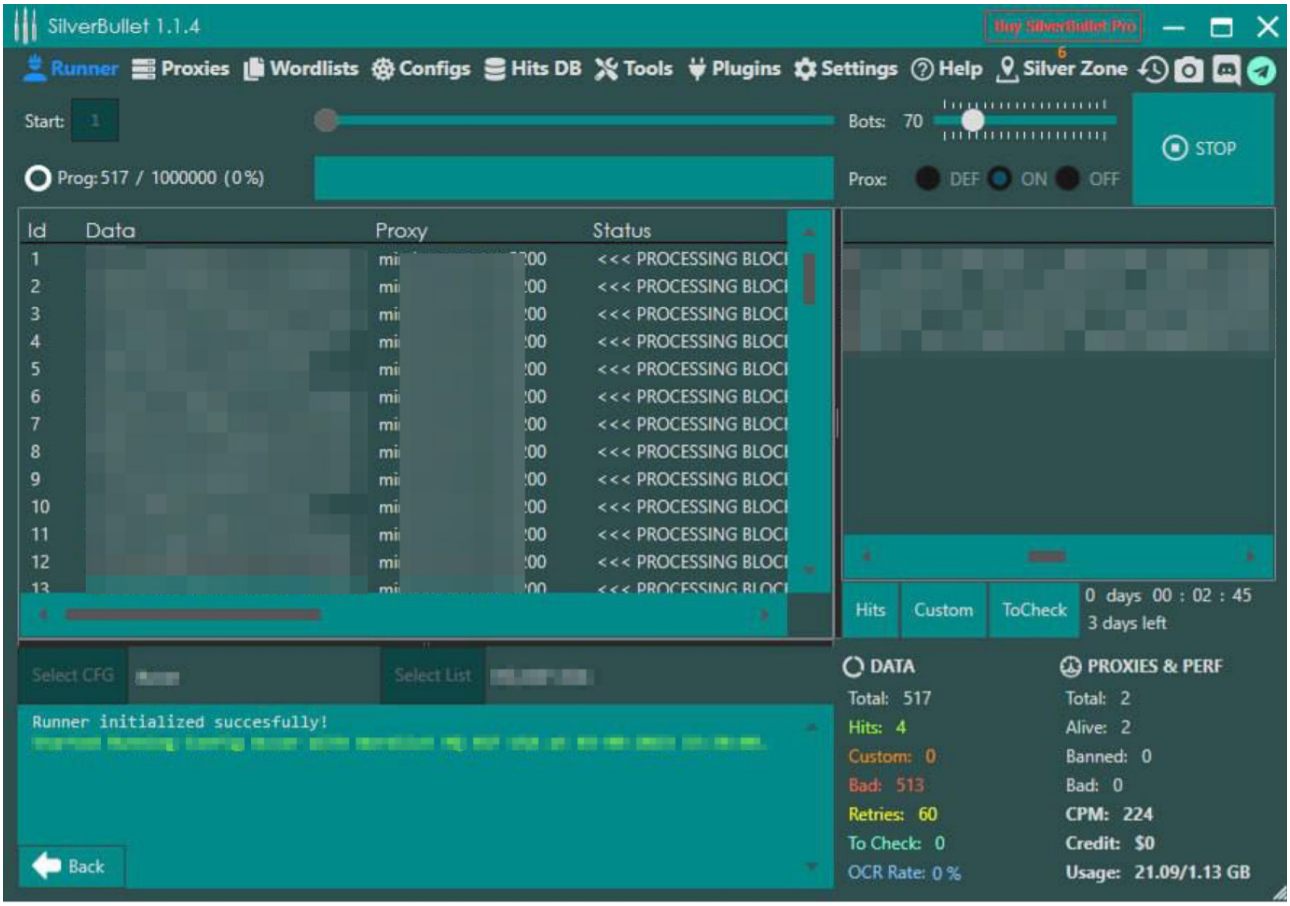
OpenBullet est généralement utilisé par les personnes qui n'ont pas de connaissances approfondies en programmation. En effet, les configurations sont le plus souvent prêtes à l'emploi, et leur usage repose avant tout sur les compétences techniques de ceux qui les ont élaborées puis vendues. Une fois qu'un attaquant obtient la configuration souhaitée, le lancement de l'attaque peut être immédiat. Le logiciel lit la configuration, analyse ses composants et crée une interface graphique permettant à l'utilisateur de mettre en place son attaque.



Aperçu de la vente de config sur Telegram, ciblant de grandes entreprises françaises accompagnées d'une formation à l'utilisation de celles-ci

Les configurations OpenBullet développées visent le plus souvent à tenter de se connecter sur un maximum de comptes clients qui disposeraient d'un solde sur les sites visés (vente de détails, assurances, carte-restaurant, etc.), pour ensuite les siphonner.

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

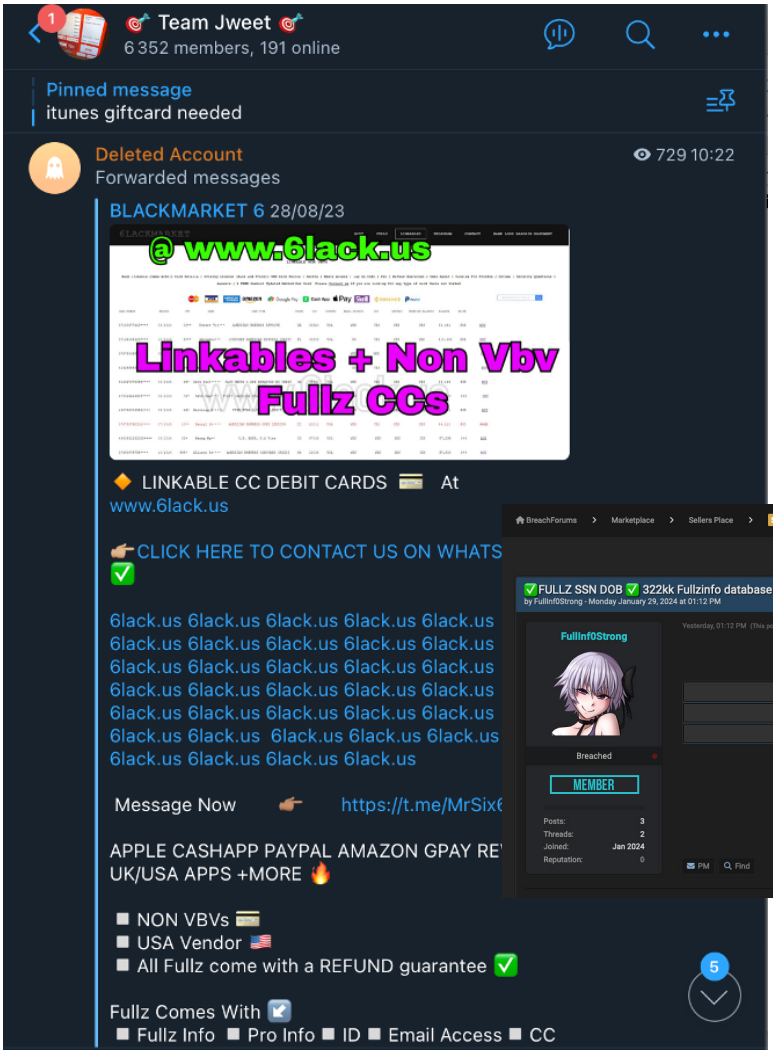


Aperçu de l'interface de SilverBullet, un dérivé du logiciel open source OpenBullet

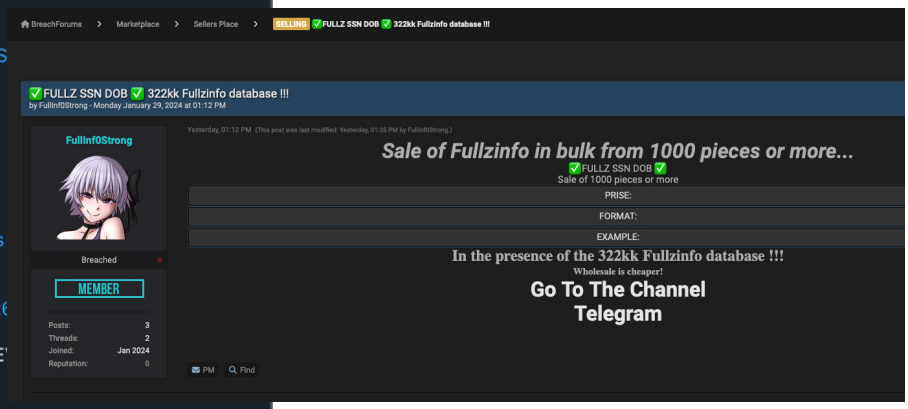
Fullz : ensemble d'informations personnelles appartenant à un individu. Ces informations sont généralement obtenues par le biais de fuites de données ou d'attaques par phishing. Un paquet « fullz » comprend généralement le nom complet d'une personne, sa date de naissance, son numéro de sécurité sociale, les détails de son compte financier (comme les informations relatives à son compte bancaire ou à sa carte de crédit), son adresse, son numéro de téléphone et parfois même des informations supplémentaires telles que les détails de son permis de conduire ou son dossier médical. Ces informations seront utilisées afin de perfectionner une attaque de spear-phishing ou pour procéder à des achats en ligne.

Facilement accessibles à l'achat sur des chaînes Telegram, ces services et produits frauduleux sont promus auprès de publics peu expérimentés en fournissant des manuels d'utilisation pour les accompagner, comme illustrés dans la capture d'écran ci-dessous.

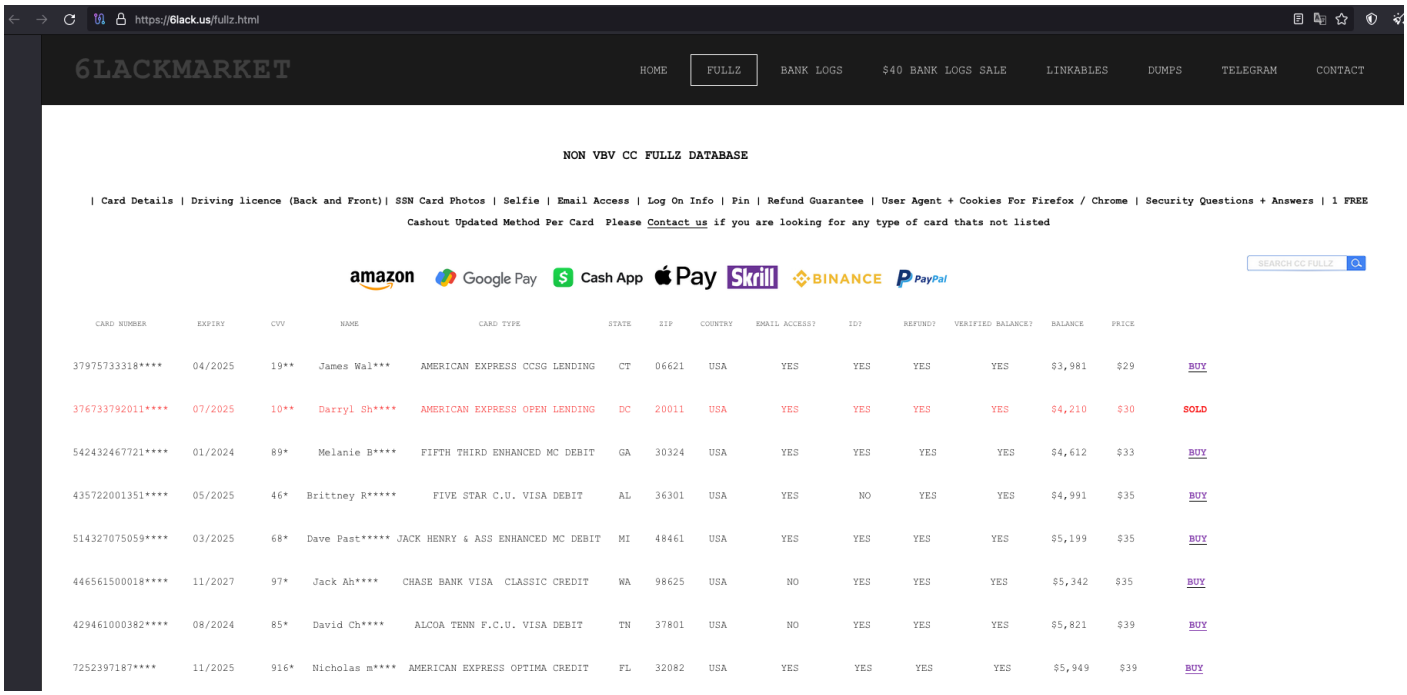
> « Les configurations OpenBullet développées visent le plus souvent à tenter de se connecter sur un maximum de comptes clients qui disposeraient d'un solde sur les sites visés (vente de détails, assurances, carte-restaurants, etc.), pour ensuite les siphonner. »



Vendeur promouvant via Telegram son site de vente de fullz et cc (carte de crédit)



Aperçu d'un utilisateur prétendant vendre des fullz sur le forum cybercriminel BreachForums



Aperçu d'une marketplace nommée 6lacmarket vendant des fullz et cc

Cependant, la fiabilité des combolists, fullz, configurations, leads et scamas peut être incertaine et des vendeurs profitent de l'inexpérience des acheteurs en leur proposant des produits souvent obsolètes pour les combolists ou dysfonctionnels pour les scamas.

PARTIE 2

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

Les fraudsters

Cette catégorie regroupe les acteurs qui utilisent le cyberespace pour mener leurs activités frauduleuses (ex. interagir avec des acheteurs), mais ne proposent pas de produits de nature cyber. Leur cible privilégiée est souvent constituée de produits contrefaits tels que des faux billets, des yescards (cartes censées permettre des retraits illimités d'argent aux distributeurs), des chèques cadeaux ou tickets restaurant. Les annonces associées à ces produits sont souvent trompeuses (yescards non fonctionnelles par exemple), et dans certains cas, les commandes ne sont jamais expédiées. Dans ce contexte, la principale victime est l'acheteur qui cherchait à tirer bénéfice de schémas frauduleux. Les entreprises peuvent également être victimes de préjudices réputationnels ou financiers liés à ces fraudes.

Les fraudsters sont des acteurs malveillants présents sur de nombreux réseaux sociaux et notamment Telegram qui peut être utilisé pour promouvoir des biens frauduleux. Le CERT-XMCO a également constaté de multiples cas de promotions de fraudes sur des plateformes telles que Facebook, X, Snapchat et Instagram. Une fois qu'un produit est promu sur l'un de ces réseaux, le vendeur cherchera souvent à entrer en contact via une application de messagerie tierce.

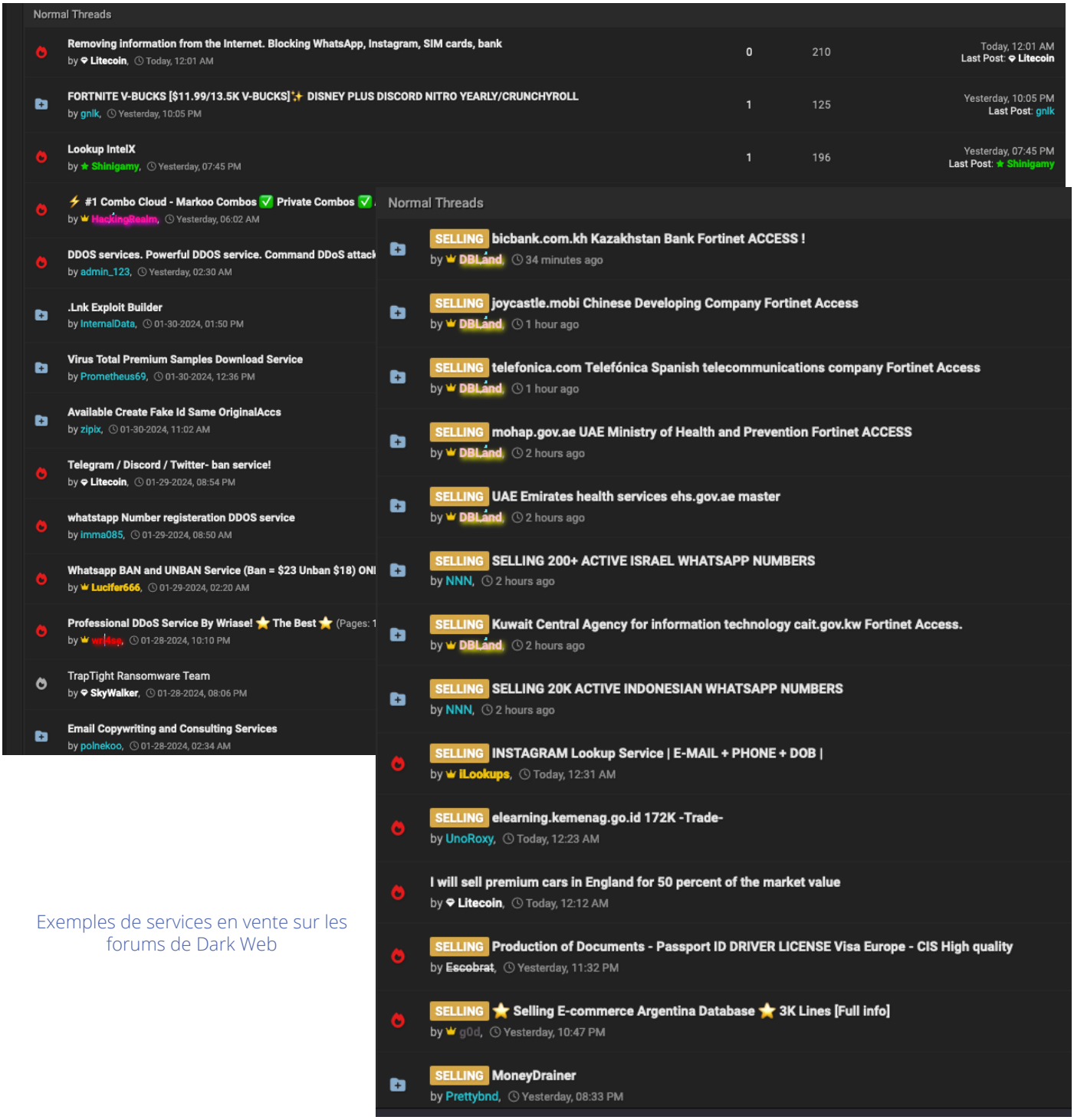
Aperçu d'une publication d'un fraudster promouvant sur X un service de yescard et renvoyant les acheteurs sur Telegram

Cybercriminel faisant de la publicité pour ses services de faux billets sur X et incitant les acheteurs à le contacter sur Telegram et Snapchat

Dans la plupart des cas, les utilisateurs sont redirigés vers Telegram ou Snapchat. La redirection vers d'autres applications permet aux fraudsters d'acquérir davantage d'agilité et de persistance sur les réseaux, notamment si l'un des comptes employés dans la fraude est supprimé par les entreprises qui possèdent les applications de communication ou par les forces de l'ordre.

Comme illustré dans les captures d'écran, les fraudsters représentent des profils cybercriminels polyvalents, utilisant une multitude de plateformes pour vendre leurs produits malveillants. Cette tendance s'explique par le caractère souvent frauduleux de leurs marchandises, reposant sur leur capacité à arnaquer leurs clients afin de générer des profits.

Ainsi, leur présence sur de multiples réseaux sociaux tels que Telegram, X, Snapchat et WhatsApp leur permet d'attirer un nombre accru de victimes potentielles qui ne fréquentent pas habituellement des réseaux sociaux de niches comme Telegram. De plus, en diversifiant leurs réseaux, ils évitent de tout miser sur une seule plateforme, au cas où un réseau serait banni par les autorités ou les entreprises qui les contrôlent.



Exemples de services en vente sur les forums de Dark Web

L'utilisation des réseaux sociaux par les groupes hacktivistes et les groupes d'extorsion

Cette partie traite conjointement des groupes hacktivistes et des groupes d'extorsion.

Nous favorisons le terme « groupe d'extorsion » pour désigner l'ensemble des groupes qui cherchent à exercer une pression sur leurs victimes pour qu'elles payent une rançon. En effet, des groupes tels que Stormous optent pour une approche différente des groupes ransomware classiques en ne recourant pas à une phase de chiffrement pour verrouiller les systèmes de leurs victimes. Au lieu de cela, ils se contentent d'extraire les données confidentielles et menacent de les divulguer.

Les groupes hacktivistes sont examinés conjointement en raison de leur usage massif des réseaux sociaux pour donner de la résonance aux attaques qu'ils revendiquent. De plus, la frontière entre ces types d'acteurs est souvent poreuse. Certains groupes d'extorsion mènent des actions d'hacktivisme pour porter des messages politiques, d'autres passent de l'hacktivisme à l'extorsion comme GhostSec, un groupe hacktiviste qui a récemment franchi une étape en créant sa propre licence de RaaS (Ransomware en tant que Service) nommée GhostLocker [8].

Telegram, un canal de choix pour les campagnes d'influence des groupes hacktivistes

Un groupe hacktiviste est constitué d'un ensemble d'individus engagés dans la promotion d'une cause politique à travers l'utilisation de moyens cyber. Les méthodes employées pour défendre la cause varient : le vol et la divulgation de données, l'influence, la désinformation ou des attaques DDoS (déni de service distribué).

Une composante essentielle de tout groupe hacktiviste réside dans la diffusion de ses revendications. Cette propagation se réalise à travers divers moyens présents dans le cyberespace (clear, deep et Dark Web confondus), tels que des blogs, des forums ou encore des réseaux sociaux. Nos investigations révèlent une tendance croissante des hacktivistes à privilégier les réseaux sociaux par rapport à d'autres canaux de communication. Cette préférence peut s'expliquer de plusieurs manières :

- Telegram présente un avantage par rapport au darkweb en termes de stabilité et de simplicité, permettant à n'importe qui d'aisément créer une nouvelle chaîne ou en rejoindre une existante ;
- Une chaîne Télégram est gratuite et ne nécessite pas, comme un blog, des coûts d'hébergements, des compétences techniques spécifiques, ou encore du temps dédié à la modération ;
- Telegram, et désormais X depuis son rachat par Elon Musk, ne semblent pas prendre d'actions décisives en ce qui concerne la nature des informations partagées sur ces réseaux. De plus, comme l'illustre la publication de SiegedSec sur X, si une chaîne Telegram est fermée, un acteur peut utiliser un réseau tiers pour promouvoir une nouvelle chaîne Telegram et ainsi maintenir une plateforme pour s'exprimer.

Publication par SiegedSec promouvant le lancement d'une nouvelle chaîne Telegram, suite à la fermeture de la précédente

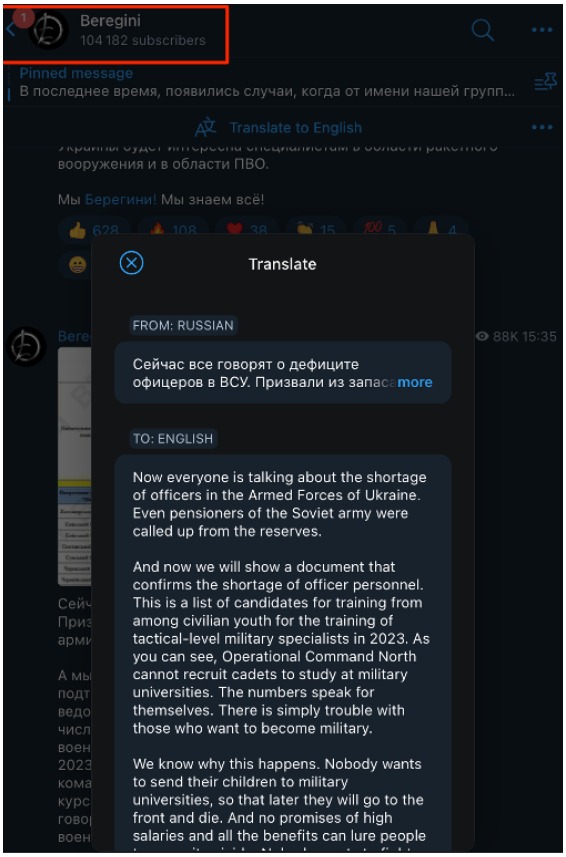
Facilitation des campagnes d'influence via les réseaux sociaux

Les réseaux sociaux, et Telegram en particulier, sont donc d'efficaces vecteurs permettant notamment la diffusion de campagnes d'influence, voire de désinformation. Celles-ci peuvent prendre plusieurs formes, les trois principales étant :

Appropriation d'attaques : dans un rapport publié par Radware [9] en avril 2023, des chercheurs ont constaté que de nombreux groupes hacktivistes s'approprient les attaques d'autres groupes. Un exemple flagrant de cette appropriation d'attaques se retrouve dans le groupe Telegram de Killnet. Ce groupe hacktiviste a republié plusieurs attaques menées par un autre groupe, NoName057(16), sans mentionner explicitement qu'il en était à l'origine. Certains groupes peuvent exploiter la possibilité offerte par Telegram de repartager du contenu provenant d'un autre groupe sans mentionner qu'ils n'ont pas participé à l'opération initiale. Bien qu'ils ne revendiquent pas directement l'attaque, cela peut semer le doute quant à la participation effective du groupe qui republie le contenu.

Désinformation politique : les attaques sous faux drapeaux visent à se faire passer pour un groupe considéré comme ennemi pour promouvoir des objectifs idéologiques spécifiques. C'est notamment le cas du groupe Beregini. Celui-ci se présente comme un groupe de type « compromission et divulgation » prétendument ukrainien, et diffuse des documents officiels qui soutiennent la propagande russe [10]. La généralisation de l'utilisation de Telegram facilite la diffusion rapide et étendue de fausses informations, renforçant ainsi leur impact. Actuellement, la chaîne de Beregini compte plus de 100 000 abonnés qui persistent à remettre en question la ligne politique et les décisions militaires de l'Ukraine dans le contexte du conflit avec la Russie.

> « Certains groupes d'extorsion font de l'hacktivisme pour porter des messages politiques qu'ils défendent, d'autres passent de l'hacktivisme à l'extorsion »



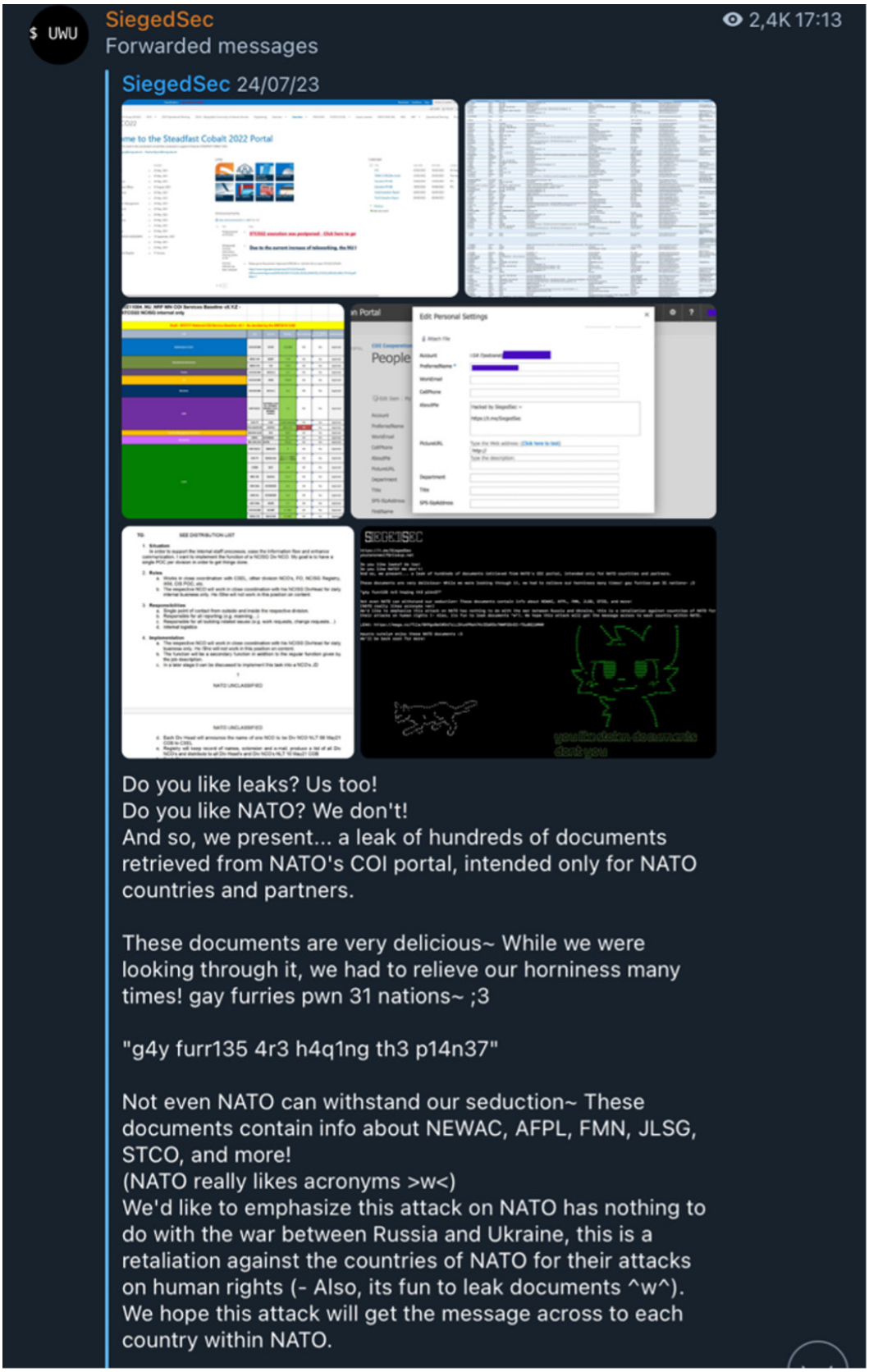
Aperçu de la boucle Telegram Beregini

Surestimation des attaques : ce type de désinformation constitue l'un des cas les plus récurrents. De nombreux groupes hacktivistes, animés par le besoin de créer un sensationnalisme, amplifient délibérément l'impact de leurs attaques, tirant parti de la visibilité offerte par les réseaux sociaux. Ce sensationnalisme est nécessaire à leur existence, car de nombreux groupes survivent uniquement de dons de leurs bases partisanes.

Une note du FBI [11] souligne que cette surestimation est particulièrement frappante en ce qui concerne les attaques par déni de service distribué (DDoS). Celles-ci ne causeraient que des dommages mineurs contrastant avec ce que rapportent communément les hacktivistes."

En ce qui concerne le vol de données, la criticité des documents obtenus à la suite d'une compromission est souvent exagérée afin de satisfaire les partisans du groupe ransomware ou hacktiviste. Un exemple illustrant cela est la prétendue compromission de l'OTAN, annoncée par SiegedSec. Celui-ci n'a en réalité eu accès qu'à un portail collaboratif contenant des documents non classifiés en matière de défense, dont la plupart étaient déjà accessibles au public.

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

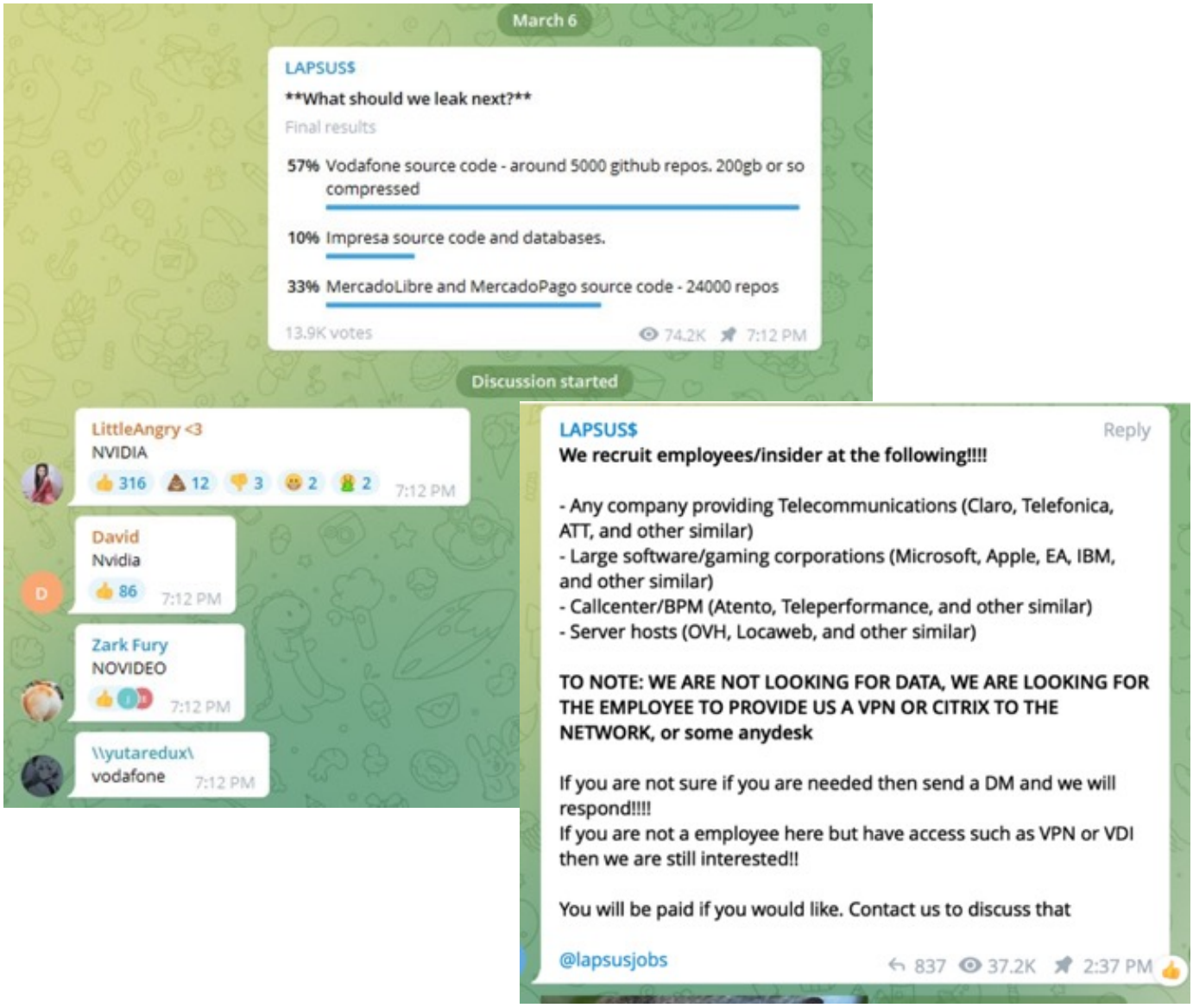


SiegedSec publiant des documents volés d'un portail collaboratif de l'OTAN ne contenant aucun document secret défense

Facilitation des campagnes de communication via les réseaux sociaux

Les réseaux sociaux constituent également des outils de communication extrêmement efficaces. Etant largement plus accessibles par les internautes, ils offrent une visibilité accrue dont les acteurs malveillants savent profiter. On peut constater deux types d'utilisation :

- Les acteurs malveillants, qu'ils soient cybercriminels ou hacktivistes, promeuvent généralement leurs groupes sur Telegram afin de se faire connaître. Ce fut notamment le cas pour Mysterious Bangladesh et IT Army of Ukraine, dont la visibilité des revendications a souvent largement outrepassé l'impact réel des attaques DDoS ;
- les attaquants peuvent aussi utiliser les réseaux sociaux pour se vanter de leurs exploits comme l'a démontré le groupe LAPSUS$ en 2022, caractérisé par son fort désir de notoriété. Ses nombreux messages publiés sur sa chaine Telegram comptaient souvent plusieurs dizaines de milliers de vues et des centaines de commentaires d'autres utilisateurs.



Compte Telegram de LAPSUS$ en 2022

PARTIE 2

Le recours aux réseaux sociaux pour étendre les activités cybercriminelles

Les groupes d'extorsion se maintiennent sur le Dark Web

Pour contraindre les entreprises à verser une rançon, les groupes d'extorsion ont recours à la divulgation progressive de documents confidentiels, échantillon après échantillon. Ces fuites sont régulièrement mises en lumière sur leurs canaux de communication, notamment sur la plateforme Telegram.

Il apparaît que les réseaux sociaux, tel que Telegram, servent principalement à diffuser des annonces, à revendiquer des attaques et à accroître la visibilité de leurs sites vitrine. Ces sites hébergés sur le Dark Web incarnent l'identité des groupes d'extorsion où ils se présentent, revendiquent leurs actes et font fuiter les donner de leurs victimes. Ainsi, le recours aux réseaux sociaux est limité à la diffusion de messages.

Cette approche offre un contrôle accru sur leurs moyens de communication tout en permettant le partage d'ne quantité plus importante de documents et données volées (se chiffrant en centaines de gigaoctets, voire en téraoctets), ceci n'étant pas réalisable sur Telegram.

STORMOUS annonce la fuite de 25% des données volées et pousse la victime à payer la rançon

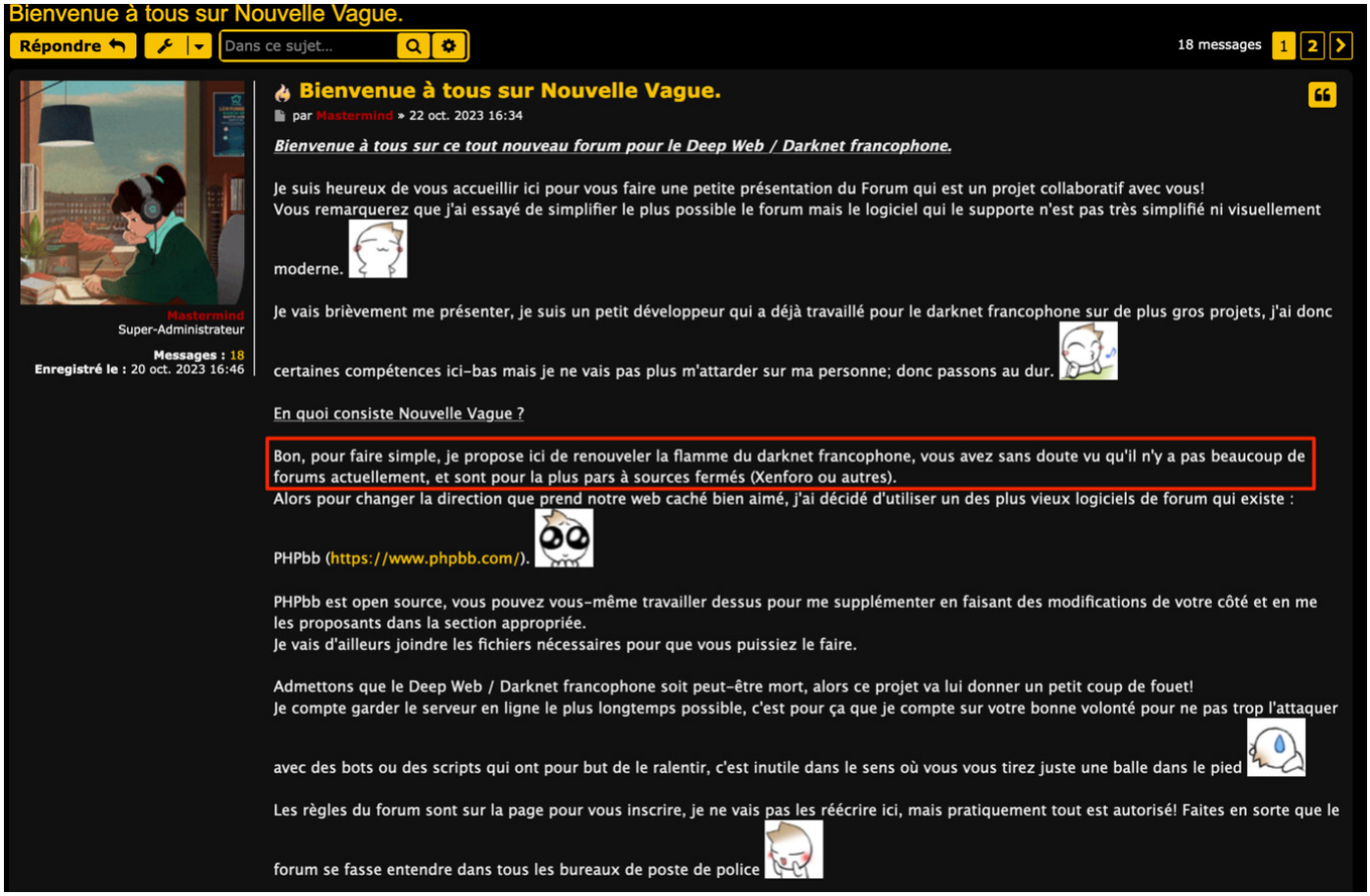
Plus globalement la quasi-totalité des groupes ransomware et autres groupes d'extorsion recourent encore à des sites vitrine accessibles sur Tor pour faire fuiter les données de leurs victimes.

Conclusion

Cette analyse met en évidence la montée en puissance du recours aux réseaux sociaux par divers profils de cybercriminels. Chaque plateforme offre des avantages comparatifs, permettant à certains acteurs malveillants de mener leurs activités de manière plus efficace, comme illustré par l'exemple des TCLs.

Les réseaux sociaux ont également contribué à simplifier les schémas de fraude en les rendant plus accessibles. Cette accessibilité accrue a entraîné une diminution du niveau de compétence technique requis pour s'impliquer dans le cybercrime, observable notamment chez les facilitateurs qui proposent des produits techniques, tels que des configs vendues avec des guides de formation, facilitant l'entrée des nouveaux venus dans le monde de la cybercriminalité.

Cependant, cette dynamique n'a pas pour autant rendu le Dark Web obsolète. La vente de logs reste par exemple monnaie courante sur le Dark Web comme en témoigne l'importance de la marketplace Russian Market, qui propose en moyenne quelque 180 000 nouveaux logs par mois. Par ailleurs, de nombreux forums cybercriminels demeurent les principaux espaces de fréquentation d'importantes communautés cybercriminelles. De surcroit, de nouveaux forums émergent de manière continue (avec plus ou moins de succès en fonction des situations), comme c'est le cas avec Nouvelle Vague dans l'écosystème francophone.



Mastermind, administrateur de Nouvelle Vague, annonçant l'ouverture du forum

En conclusion, le CERT-XMCO observe un recours accru aux réseaux sociaux en complément de l'usage existant du Dark Web, plutôt qu'une substitution des activités du Dark Web vers les réseaux sociaux ?

Le CERT-XMCO estime que la tendance actuelle d'utilisation croissante des réseaux sociaux perdurera dans le temps. Les réseaux sociaux offrent divers avantages techniques, communautaires, de simplification et d'évasion des autorités, ce qui les rendra complémentaires au Dark Web.

Bibliographie

[1] https://weis2023.econinfosec.org/wp-content/uploads/sites/11/2023/06/weis23-hughes.pdf

[2] http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/9d555ad9f2076776b532

[3] Pierlugi Paganini, "6,500+ sites deleted after Dark web hosting provider Daniel's Hosting Hack", Security Affairs, 18 nov 2018.

[4] Louise Ferret, "Tor2(run out the back)Door: Exit, Scam or Seizure?", Searchlight Cyber, Septembre 2023.
https://www.slcyber.io/tor2run-out-the-backdoor-exit-scam-or-seizure/

[5] Dissent, "GhostShell, On the Record – Snitches, Feds, and the Scene, 15 mars 2016.

[6] https://www.xmco.fr/wp-content/uploads/2022/12/XMCO-ActuSecu-58-Conti-Lapsus-WiFi.pdf

[7] https://www.kelacyber.com/telegram-clouds-of-logs-the-fastest-gateway-to-your-network/

[8] https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec

[9] https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/

[10] https://www.activefence.com/research/russias-disinformation-game/

[11] https://www.ic3.gov/Media/News/2022/221104.pdf

La prolifération des spyware commerciaux

Par Vicent JEZEQUEL et Antoine AVET

Executive Summary

Le terme spyware commercial désigne des outils d'interception de données proposés à la vente par des sociétés légitimes. Il a été popularisé en particulier depuis juillet 2021 et la mise au jour de l'affaire Pegasus, du nom d'un spyware fourni par la société israélienne NSO Group. Ces révélations ont mis en lumière l'exploitation de ces outils offensifs par divers gouvernements à des fins de surveillance et souligné les fragilités du cadre légal encadrant leur utilisation.

Ces spyware sont essentiellement distribués à leurs cibles par l'exploitation de vulnérabilités 0-day et la conduite de campagnes de phishing ciblées plus ou moins sophistiquées. Certaines des vulnérabilités exploitées ont pour caractéristique de ne nécessiter aucune interaction avec les utilisateurs (0-click), exposant en conséquence même les plus avertis d'entre eux.

Afin d'assurer leur persistance sur les appareils compromis et échapper à la détection, plusieurs techniques d'obfuscation ont été utilisées par les fournisseurs de spyware. L'objectif est de dissimuler leurs fonctionnalités malveillantes en les masquant au sein de processus légitimes ou via le téléchargement ultérieur des modules de surveillance.

En dépit de leur couverture médiatique et des mesures prises par les États pour limiter leur utilisation et leur diffusion, les spyware commerciaux continuent d'être largement utilisés par des « sociétés d'interception légale ». Leur prolifération s'appuie notamment sur la commercialisation et la fuite de codes malveillants sur des marketplaces criminelles, ainsi qu'en sources ouvertes.

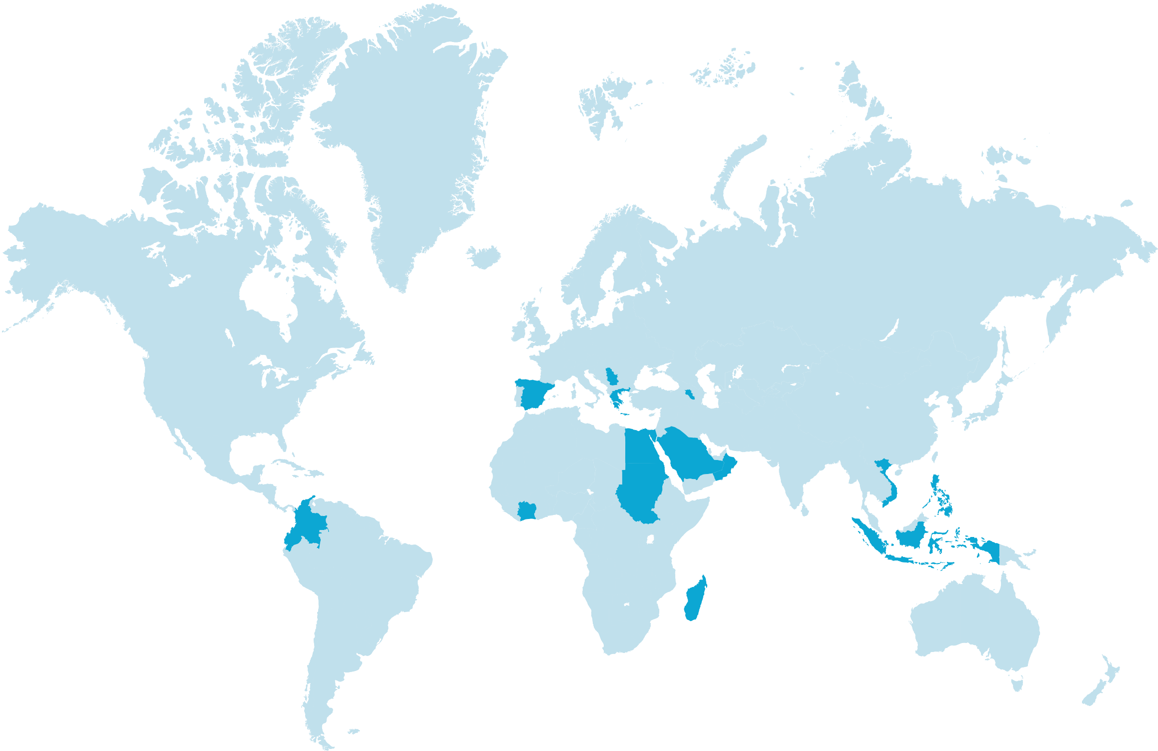
Cette prolifération s'explique également par la manne financière que représente le marché des spyware, qui s'élèverait à près de 12 milliards de dollars. La régulation de ce marché présente ainsi une certaine ambivalence, caractérisée par des cadres juridiques variés et le double discours des États qui les emploient, à des fins de surveillance, mais également comme outils de leur politique étrangère.

Le CERT-XMCO vous propose en fin de rapport des recommandations permettant de limiter votre surface d'exposition aux spyware commerciaux. Elles ont pour objectif de répondre aux risques liés aux deux principaux vecteurs de compromission observés par nos consultants : l'exploitation de vulnérabilités et les campagnes de spear-phishing.

La prolifération des spyware commerciaux

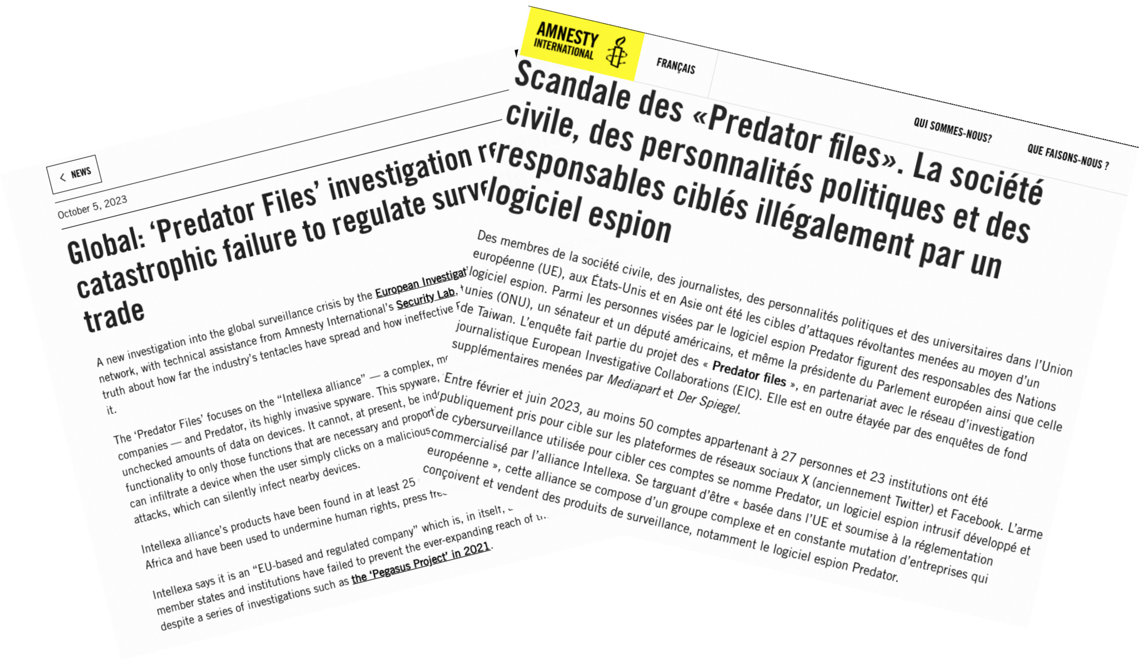
Introduction

La publication des « Predator Files » [1] en octobre 2023 est venue remettre sur le devant de la scène le phénomène de prolifération des spyware commerciaux observés par les consultants du CERT-XMCO.



Pays accusés d'avoir déployé le spyware Predator - Source : Carnegie [2]

Entre 2011 et 2023, au moins 74 gouvernements ont conclu des contrats avec des entreprises commerciales pour acquérir et déployer des outils de surveillance disposant de capacités d'écoute, de géolocalisation et d'interception de données, principalement auprès de journalistes, activistes et personnalités politiques [3].



NEWS

October 5, 2023

Global: 'Predator Files' investigation r… catastrophic failure to regulate surv… trade

A new investigation into the global surveillance crisis by the European Investigat… network, with technical assistance from Amnesty International's Security Lab, … truth about how far the industry's tentacles have spread and how ineffective … it.

The 'Predator Files' focuses on the "Intellexa alliance" — a complex, m… companies — and Predator, its highly invasive spyware. This spyware, … unchecked amounts of data on devices. It cannot, at present, be ind… functionality to only those functions that are necessary and proport… can infiltrate a device when the user simply clicks on a malicious… attacks, which can silently infect nearby devices.

Intellexa alliance's products have been found in at least 25 … Africa and have been used to undermine human rights, press fre…

Intellexa says it is an "EU-based and regulated company" which is, in itself, … member states and institutions have failed to prevent the ever-expanding reach of t… despite a series of investigations such as the 'Pegasus Project' in 2021.

AMNESTY INTERNATIONAL

FRANÇAIS

QUI SOMMES-NOUS?

QUE FAISONS-NOUS ?

Scandale des «Predator files». La société civile, des personnalités politiques et des responsables ciblés illégalement par un logiciel espion

Des membres de la société civile, des journalistes, des personnalités politiques et des universitaires dans l'Union européenne (UE), aux États-Unis et en Asie ont été les cibles d'attaques révoltantes menées au moyen d'un logiciel espion. Parmi les personnes visées par le logiciel espion Predator figurent des responsables des Nations unies (ONU), un sénateur et un député américains, et même la présidente du Parlement européen ainsi que celle de Taiwan. L'enquête fait partie du projet des « **Predator files** », en partenariat avec le réseau d'investigation journalistique European Investigative Collaborations (EIC). Elle est en outre étayée par des enquêtes de fond supplémentaires menées par *Mediapart* et *Der Spiegel*.

Entre février et juin 2023, au moins 50 comptes appartenant à 27 personnes et 23 institutions ont été publiquement pris pour cible sur les plateformes de réseaux sociaux X (anciennement Twitter) et Facebook. L'arme de cybersurveillance utilisée pour cibler ces comptes se nomme Predator, un logiciel espion intrusif développé et commercialisé par l'alliance Intellexa. Se targuant d'être « basée dans l'UE et soumise à la réglementation européenne », cette alliance se compose d'un groupe complexe et en constante mutation d'entreprises qui conçoivent et vendent des produits de surveillance, notamment le logiciel espion Predator.

Collectivement qualifiés de « sociétés d'interception légale », les fournisseurs de spyware prétendent les vendre uniquement à des clients gouvernementaux ayant un usage légitime de ces outils de surveillance, tels que les services de renseignement et les forces de l'ordre [4]. Pourtant, leur exploitation s'est bien souvent émancipée du cadre légal, s'apparentant selon le Citizen Lab à du « Despotism-as-a-Service » [5].

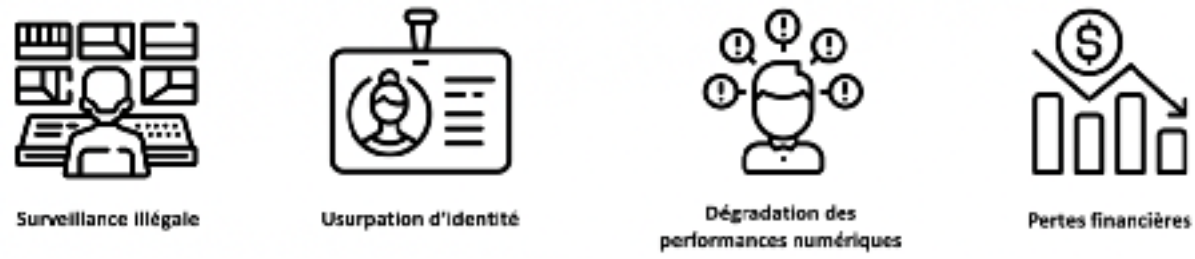
L'affaire Pegasus, mise au jour en juillet 2021, a participé à la prise de conscience des autorités politiques européennes et des entreprises spécialisées dans le secteur des télécommunications face au risque de dérive autoritaire [6]. En février 2022, le Contrôleur européen de la protection des données (CEPD) a appelé à une interdiction du développement et de la commercialisation de ces logiciels de surveillance dans l'Union européenne [7].

Outre-Atlantique, la mise en place de sanctions économiques sous l'administration Biden est venue bousculer les parties prenantes au sein de cet écosystème résilient, sans pour autant changer la donne sur la régulation de ces outils [8] [9] [10]. Aujourd'hui, les outils d'interception numérique occupent une place prépondérante dans la stratégie de défense et d'influence de certains États et représentent une source de revenus non négligeable [11].

Enfin, la tendance au Bring Your Own Device (BYOD), qui consiste à utiliser des appareils personnels dans un contexte professionnel, augmente la surface d'attaques exploitable pour les clients de spyware. Zimperium, qui faisait état d'une augmentation de 466 % des attaques de type 0-day contre les appareils mobiles en 2021, démontre la proactivité des acteurs qui les exploitent et souligne les risques associés à cette pratique en plein essor [12] [13].

Les données collectées à l'issue de la surveillance de l'activité numérique :

Les conséquences liées à la collecte des données :



Une sophistication reflétée par les modes de distribution

Les campagnes de distribution de spyware commerciaux observées par le CERT-XMCO se sont généralement appuyées sur des chaînes d'infection combinant l'exploitation de vulnérabilités et la conduite de campagnes de phishing plus ou moins sophistiquées comme vecteurs d'accès initial [14] [15] [16].

Certains fournisseurs de spyware ont en outre démontré une capacité à exploiter des outils et méthodes supplémentaires leur permettant d'optimiser leurs opportunités de compromission, témoignant d'un degré de sophistication rivalisant avec des groupes d'attaquants attribués à des États [17].

Vulnérabilités 0-day

La majeure partie des vulnérabilités exploitées pour distribuer des spyware commerciaux sont des vulnérabilités dites 0-day. Il s'agit de vulnérabilités activement exploitées avant qu'elles ne soient corrigées ou même identifiées par les éditeurs [18]. 41 vulnérabilités de ce type ont été détectées et divulguées en 2022 par Google Project Zero, soit le deuxième plus grand nombre jamais enregistré depuis 2014 [19]. Le CERT-XMCO souligne l'exploitation de 3 d'entre elles par des sociétés privées :

Exploitation de la CVE-2022-2294 par la société israélienne Candiru
La vulnérabilité affectant Google Chrome consistait en un dépassement de tampon sur le tas (heap buffer overflow) dans le logiciel open-source WebRTC (Web Real-Time Communications). Ce dernier offre une interface de programmation JavaScript permettant une communication en temps réel entre les navigateurs web et la machine [20].

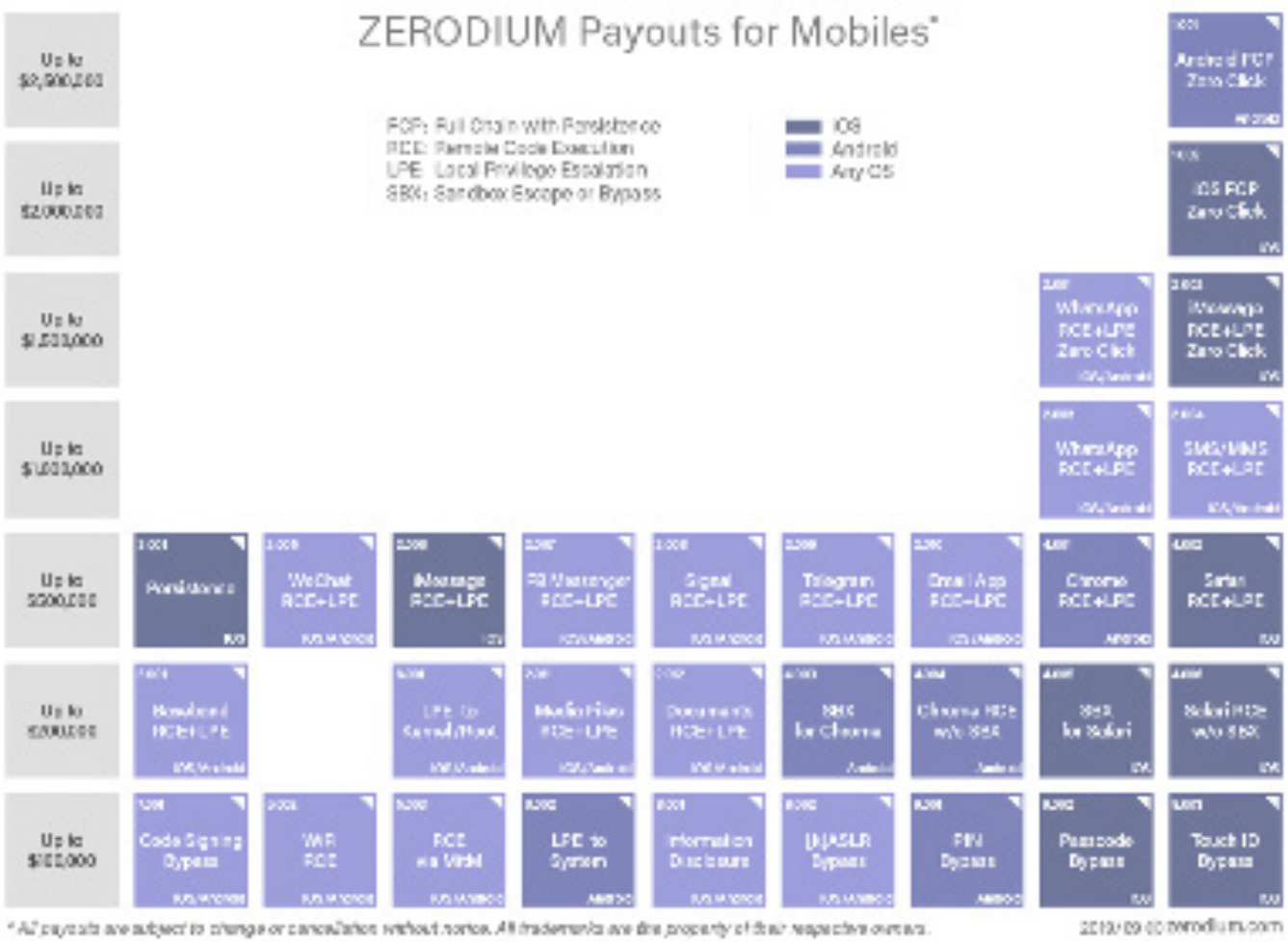
Exploitation de la CVE-2022-26485 par la société espagnole Variston
La vulnérabilité affectant Mozilla Firefox était issue d'une utilisation de la mémoire après libération (use-after-free) lors du traitement des données XSLT et permettait de mener une attaque par XSS (cross-site scripting). L'attaquant pouvait ainsi provoquer un déni de service ou exécuter du code arbitraire sur le système ciblé [21].

Exploitation de la CVE-2022-22047 par la société autrichienne DSIRF
Selon Microsoft, cette vulnérabilité était liée à un problème de mise en cache du contexte d'activation dans le sous-système d'exécution Client-Server (CSRSS) sous Windows et Windows Server. La société DSIRF, basée à Vienne, l'aurait exploitée dans le cadre de son offre commerciale d'interception numérique [22] [23].

Vulnérabilités 0-click

Parmi les vulnérabilités exploitées par les fournisseurs de spyware, certaines ont pour caractéristique de ne pas nécessiter d'interaction de la part des utilisateurs (0-click) [24]. Ces dernières sont très recherchées sur le marché concurrentiel de la vente de codes d'exploitation. À titre d'exemple, le broker américain Zerodium est prêt à débourser 2,5 millions de dollars, pour la découverte d'une chaîne d'exploitation de type 0-click (FCP) sur Android [25].

Selon Citizen Lab, la chaîne d'exploitation BLASTPASS, tirant parti des vulnérabilités CVE-2023-41064 et CVE-2023-41061, a été exploitée par le fournisseur israélien NSO Group pour prendre le contrôle d'appareils mobiles fonctionnant avec la dernière version d'iOS (16.6). Elle ne nécessitait aucune interaction de la part de la victime et reposait sur l'envoi par iMessage de pièces jointes PassKit contenant des images malveillantes [26].



Récompenses proposées pour la découverte de vulnérabilités sur iOS et Android - Source : Zerodium [25]

Dans une seconde campagne, le spyware Pegasus de NSO Group aurait compromis 1 400 utilisateurs de WhatsApp entre le 29 avril et le 10 mai 2019, parmi lesquels des diplomates, dissidents politiques, journalistes et hauts représentants du gouvernement. En envoyant des paquets SRTCP spécialement conçus, un attaquant était en mesure d'exploiter la vulnérabilité 0-click CVE-2019-3568 et d'exécuter du code arbitraire sur l'appareil ciblé. Pegasus pouvait être installé via un simple appel, sans que la victime n'y réponde [27] [28].

Une troisième chaine d'infection marquante a été identifiée en avril 2023 et attribuée à l'entreprise israélienne QuaDream. Référencée sous le nom ENDOFDAYS et ciblant les versions 14.4.0 et 14.4.2 d'iOS, cette dernière exploitait des invitations dans iCloud Calendar pour distribuer le code malveillant du spyware Reign [29].

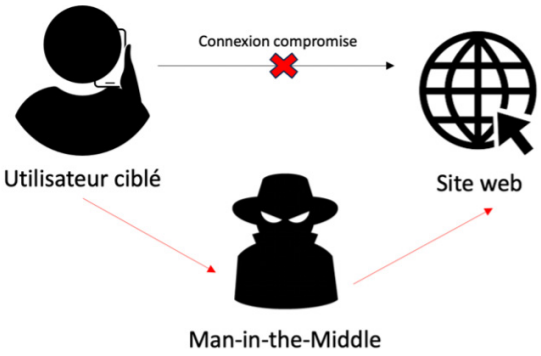
En complément, d'autres vulnérabilités 0-click ont récemment été identifiées. Bien qu'étant originellement exploitées par des acteurs malveillants attribués à des états, il n'est pas à exclure que ces dernières soient utilisées à l'avenir par des fournisseurs de spyware commerciaux, malgré les mesures d'atténuation publiées par les éditeurs des produits affectés.

À ce titre, en juillet 2023, Apple a corrigé plusieurs vulnérabilités découvertes par les chercheurs de Kaspersky, en particulier une vulnérabilité critique référencée sous le nom de CVE-2023-38606 affectant iMessage et exploitée dans le cadre d'une campagne d'attaques que les services de renseignement russes ont attribuée à la NSA [30] [31] [32]. Cette vulnérabilité de type 0-click ne nécessitait aucune interaction avec l'utilisateur ciblé pour rendre l'infection effective et ciblait des appareils fonctionnant sur des versions d'iOS antérieures à 15.7.1.

Le recours au spear-phishing

Cette méthode largement éprouvée par les attaquants s'appuie sur une connaissance préalable de l'environnement de l'utilisateur ciblé pour gagner en crédibilité lors de la distribution du leurre de phishing (courriel, SMS, fichier, application) [33].

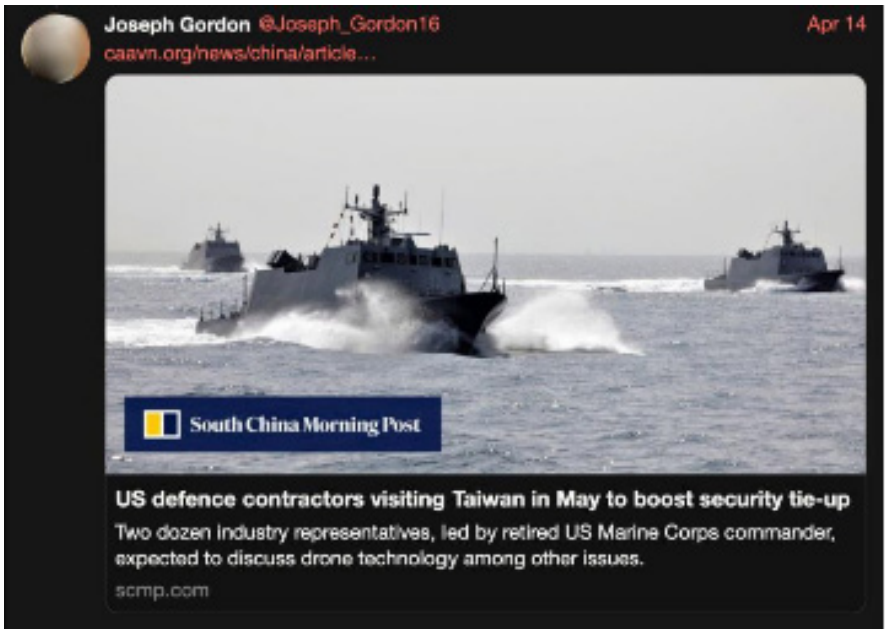
En septembre 2022, les chercheurs de Citizen Lab ont identifié la compromission du smartphone d'une personnalité politique égyptienne via la distribution du spyware Predator développé par Cytrox. Ce dernier avait été la cible de SMS l'invitant à cliquer sur un lien de phishing redirigeant vers des sites web n'utilisant pas le protocole HTTPS. Une fois ces liens ouverts, la chaîne d'exploitation se déclenchait automatiquement et déployait un binaire malveillant conçu pour choisir si l'implant du spyware devait être installé sur l'appareil compromis [16].



Le malware s'appuie sur le loader Alien au sein du processus central zygote64 et exploite ensuite 5 vulnérabilités de type 0-day. Le loader récupérait ensuite le spyware Predator sous la forme de fichier ELF à partir d'adresses contrôlées par les attaquants, puis mettait en place un environnement d'exécution Python pour faciliter l'emploi des diverses fonctionnalités du spyware [34].

L'exploitation de plateformes de marketing et d'OSINT

La distribution de code malveillant peut également s'appuyer sur une reconnaissance approfondie des utilisateurs ciblés sur les réseaux sociaux afin d'opérer des attaques par ingénierie sociale [35]. Plusieurs fournisseurs de spyware sont soupçonnés d'utiliser de faux comptes lors de la phase de compromission initiale. En décembre 2022, Meta alertait déjà au sujet de cette pratique, en supprimant plus de 300 comptes Facebook et Instagram opérés par Cytrox [36].



Compte Twitter utilisé pour distribuer le spyware Predator hébergé sur un domaine malveillant caavn.com
Source : Amnesty International [37]

Les fournisseurs de spyware pourraient en outre s'appuyer sur des outils de reconnaissance en source ouverte et sur les réseaux sociaux comme ceux proposés par les firmes Cobwebs, CyberRoot Risk Advisory Private et Cognyte. La société israélienne Cobwebs, spécialisée dans le renseignement d'origine sources ouvertes (OSINT), propose une technologie capable de localiser un appareil mobile [38]. Une fois fusionnées, les données d'utilisateurs disponibles en accès libre sur Internet peuvent devenir des renseignements actionnables lors de la phase de compromission initiale.

Une autre entreprise nommée Bsightful proposerait une solution similaire basée sur le croisement des données de navigation et d'autres sources d'informations disponibles sur le web ou achetées auprès de revendeurs [39]. Bsightful a depuis été racheté par Cognyte pour ses clients régaliens. S'appuyant sur l'expérience de Bsightful, Cognyte a développé une solution baptisée Sherlock, exploitant des publicités pour le suivi des utilisateurs ciblés, puis pour la distribution de code malveillant [40].

« En septembre 2022, les chercheurs de Citizen Lab ont identifié la compromission du smartphone d'une personnalité politique égyptienne via la distribution du spyware Predator développé par Cytrox »

Par ailleurs, les activités de surveillance ont pu être facilitées par le recours à des outils de marketing digital permettant de gérer la conduite des campagnes de spear-phishing à grande échelle. C'est le cas de société indienne CyberRoot, qui a utilisé l'outil de marketing Branch pour créer, gérer et suivre l'envoi de liens de phishing [36].

Prenant l'apparence de services publicitaires, ces outils de reconnaissance et de marketing digital ne sont pas considérés comme collectant des informations en vue d'activités offensives ultérieures et ne sont donc pas, ou peu réglementés. C'est aussi le cas de Rayzone, dont le produit Echo, n'est pas soumis à la supervision de l'État israélien, car il utilise des informations issues de sources ouvertes [41] [42].

L'appui d'entreprises de télécommunications

Enfin, les fournisseurs de spyware se seraient appuyés sur la collaboration avec des entreprises du secteur des télécommunications. Rayzone, en particulier, est soupçonné d'avoir fait appel à l'opérateur anglo-normand Sure Guernsey, suggérant qu'il exploitait son réseau pour avoir accès aux capacités de localisation de l'opérateur [43].

En 2021, les chercheurs du Threat Analysis Group (TAG) de Google ont observé une campagne d'attaques lors de laquelle le fournisseur du spyware Hermit collaborait avec des Fournisseurs d'Accès à Internet (FAI) pour désactiver la connectivité des appareils mobiles ciblés. Une fois la connexion désactivée, les opérateurs envoyaient un lien malveillant par SMS demandant à la cible d'installer une application en apparence légitime pour rétablir sa connexion [44].

L’usage de techniques d’obfuscation pour échapper à la détection

Le contournement des outils de sécurité constitue un élément décisif lors de la distribution de code malveillant sur les appareils mobiles. Dans le cadre de ses activités de veille, le CERT-XMCO a observé plusieurs techniques d'obfuscation utilisées par les fournisseurs de spyware.

Évasion des outils d’analyse de code

En novembre 2022, le TAG de Google a identifié des mécanismes d’obfuscation utilisés par l'entreprise espagnole Variston IT pour son framework Heliconia, composé de fonctionnalités visant à contourner les environnements d’analyse de type sandbox [21]. D'autres spyware commerciaux, comme FinFisher [45] et Pegasus [46], se sont également appuyés sur des mécanismes d'évasion de sandbox pour limiter le potentiel de détection.

Modularité de code

Certains des spyware observés par le CERT-XMCO ont été conçus de manière modulaire, de sorte à dissimuler leurs fonctionnalités malveillantes dans des payloads distribuées de manière choisie en fonction des objectifs visés. Le spyware Hermit a ainsi été distribué par le biais de fichiers APK ne contenant aucun code malveillant mais ayant la capacité de télécharger des modules aux fonctionnalités de surveillance variées depuis un serveur opéré par les attaquants, une fois le malware installé sur l’appareil ciblé [14] [44].

> « En juin 2023, les chercheurs de Cisco Talos précisaient que le spyware Predator n'installait pas les certificats au niveau du système pour éviter toute interférence au niveau de l’utilisation de l'appareil compromis qui pourrait alerter l’utilisateur ciblé »

Dissimulation des communications via des processus légitimes

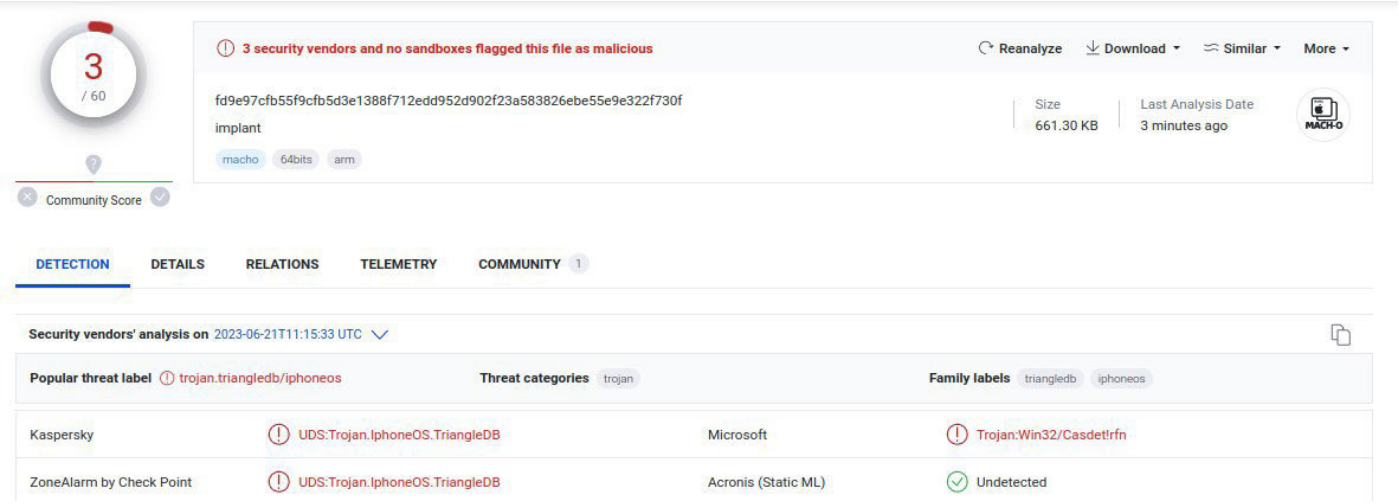
Le contournement des outils de sécurité peut également être effectué lors de l’établissement des communications avec les serveurs de commande et de contrôle (C2). En juin 2023, les chercheurs de Cisco Talos précisaient que le spyware Predator n'installait pas les certificats au niveau du système pour éviter toute interférence au niveau de l’utilisation de l'appareil compromis qui pourrait alerter l’utilisateur ciblé [34].

Celui-ci dissimule en outre ses communications au sein des processus légitimes pour contourner le module de sécurité d'Android (SELinux). Selon les chercheurs, la spécificité du loader Alien résidait dans sa capacité à abuser de l'architecture de sécurité SELinux pour lever les restrictions existantes sur les autorisations d'accès aux processus du système et lui permettre de communiquer avec des serveurs de C2 non autorisés.

Dans certains cas, des fournisseurs de spyware ont astucieusement usurpé le nom de processus légitimes pour leur payload. C'est notamment le cas de Pegasus qui modifie le nom du processus CommCenterRootHelper qui devient ainsi CommsCenterRootHelper et n'attire pas l'attention lors de l'analyse statique des appareils compromis [47].

Des algorithmes de compression

Les fournisseurs de spyware ont aussi recours à la compression des fichiers de package d'applications APK pour contourner la détection des outils de sécurité. Cette méthode a été identifiée en août 2023 par les chercheurs du zLab de Zimperium pour distribuer un spyware non référencé. Pour ce faire, le fichier APK malveillant utilise volontairement une méthode de décompression non supportée permettant d'entraver l'analyse statique par les outils de sécurité [48].

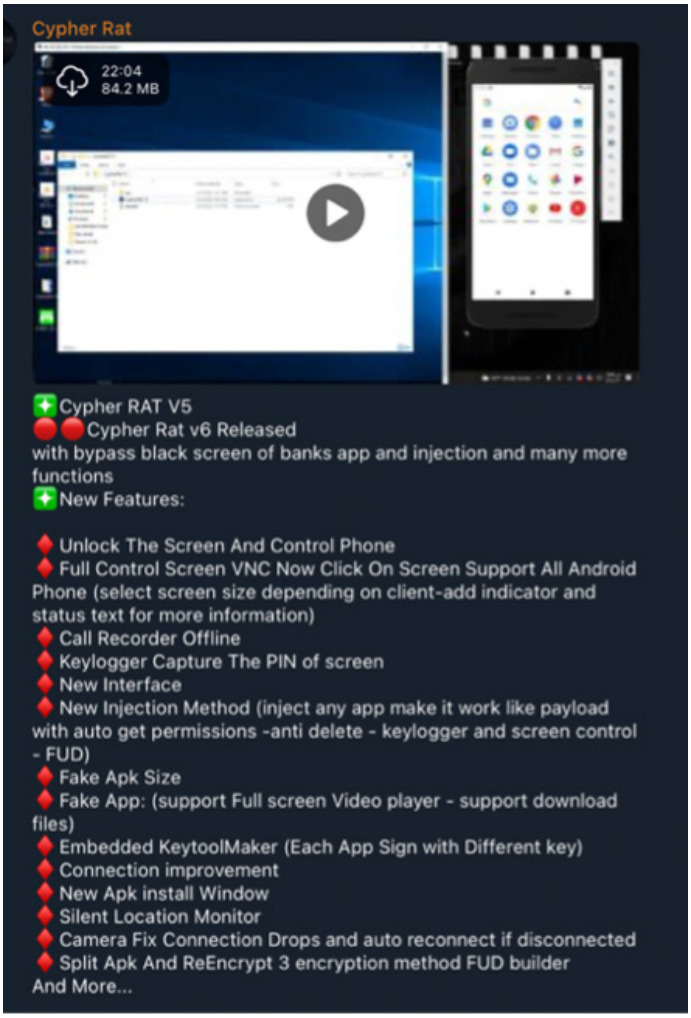


Résultats de l'analyse du spyware TriangleDB par VirusTotal

Une prolifération s'appuyant sur l'écosystème cybercriminel

La divulgation de code source des spyware, bien loin d'endiguer leur utilisation, permet à des acteurs malveillants novices d'accéder à du code sophistiqué servant de base pour développer de nouvelles variantes. En 2020, la société allemande Wolf Intelligence proposait la solution d'interception numérique WolfRAT dont une partie du code source était basée sur DenDroid, ayant fait l'objet d'une divulgation publique en 2014 [49].

Les fournisseurs et clients de spyware pourraient aussi s'appuyer sur la commercialisation de codes malveillants sur des marketplaces criminelles. Des acteurs de la menace ont proposé à la vente des spyware aux fonctionnalités avancées et de codes d'exploitation pour Android et iOS, proposant même des comparatifs avec les fournisseurs traditionnels, des services sur mesure et des prix de location attractifs, participant à la popularisation des services.

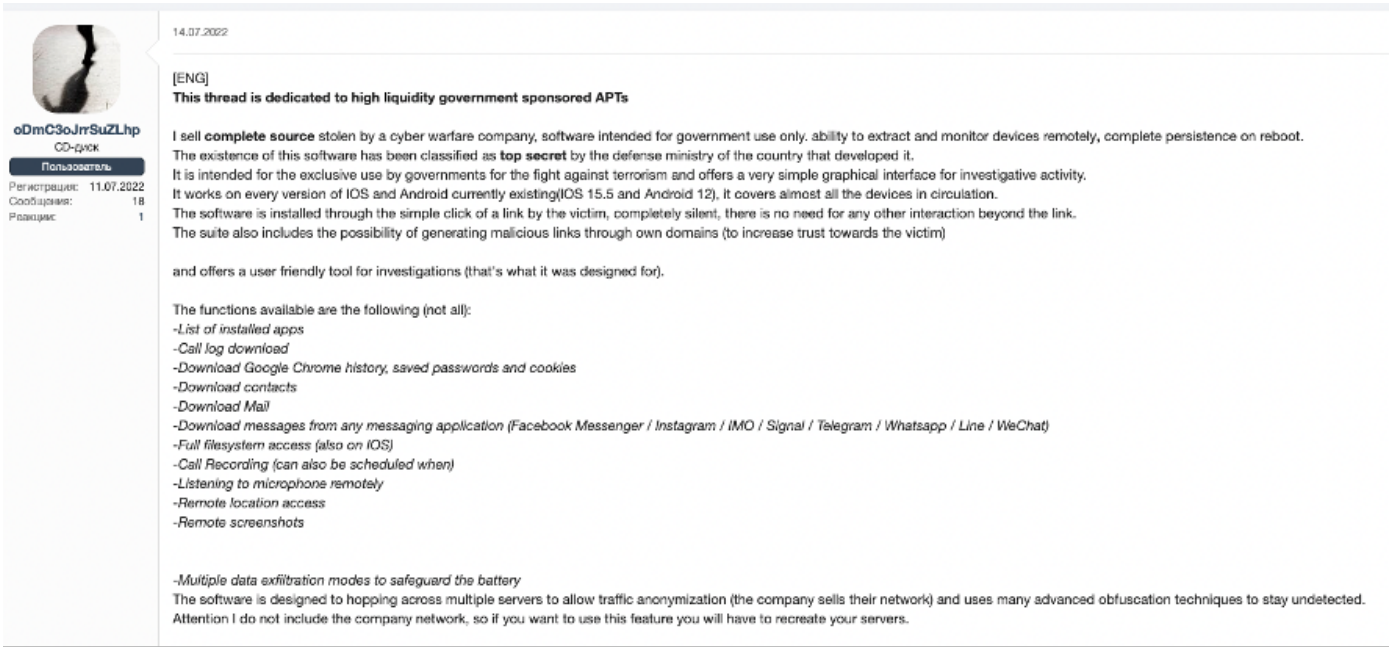


Promotion du spyware Cypher RAT sur Telegram
Source : CERT-XMCO

À titre d'exemple, le CERT-XMCO a identifié la commercialisation sur Telegram et sur des marketplaces populaires du spyware SpyNote. Ce dernier distribuait son code malveillant lors de la réception d'un appel téléphonique sortant ou lors d'une navigation sur Internet. Lors de son exécution, SpyNote demande l'autorisation BIND_ACCESSIBILITY_SERVICE accordée par l'utilisateur de l'appareil ciblé [50]. D'après un rapport de ThreatFabric publié en janvier 2023, les détections de SpyNote ont augmenté à la suite de la fuite du code source de l'une de ses variantes, référencée sous le nom de CypherRat.

Par ailleurs, il n'est pas rare que des fournisseurs de spyware recyclent les codes de leurs homologues. FinFisher a notamment été accusé de plagier le code FlexiSpy développé par une entreprise thaïlandaise [2]. Le code source des spyware est facilement duplicable dès lors qu'il est publié en open source.

Dans la mesure où certaines de ces firmes font aussi l'objet d'attaques de type Hack&Leak visant à divulguer publiquement leurs outils et méthodes, le risque de prolifération des spyware est démultiplié. Ce fut notamment le cas de la société italienne Hacking Team en juillet 2015 [51].



14.07.2022

oDmC3oJrrSuZLhp
CD-диск
Пользователь
Регистрация: 11.07.2022
Сообщения: 18
Реакции: 1

[ENG]
This thread is dedicated to high liquidity government sponsored APTs

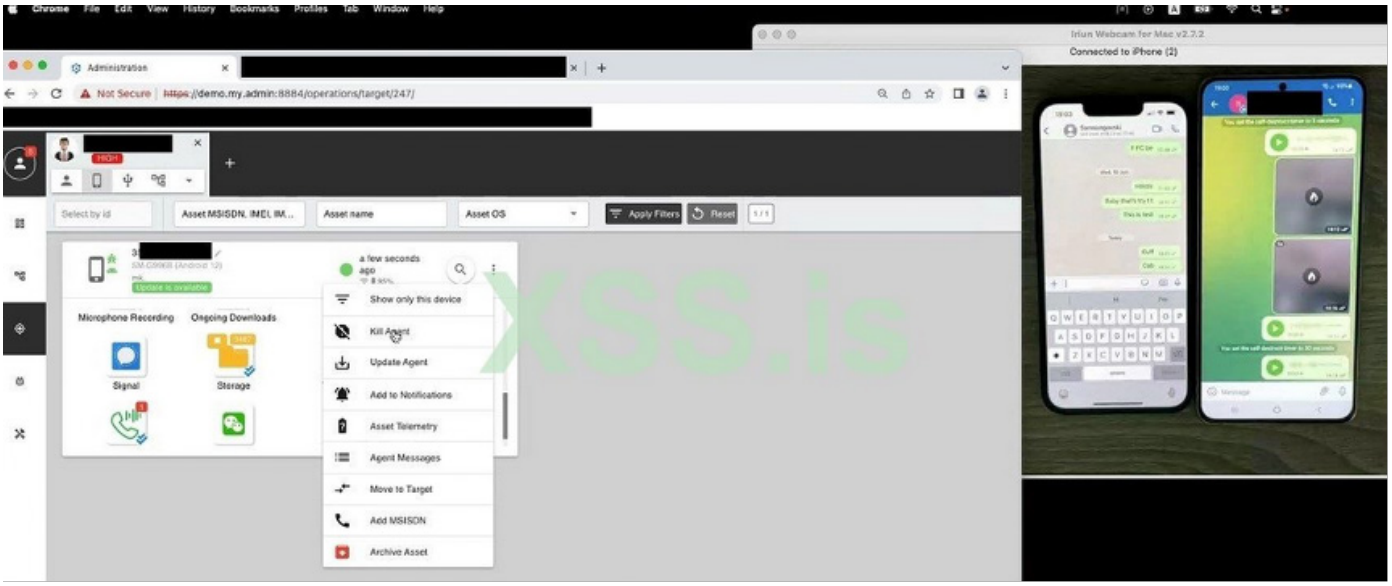
I sell **complete source** stolen by a cyber warfare company, software intended for government use only. ability to extract and monitor devices remotely, complete persistence on reboot.
The existence of this software has been classified as **top secret** by the defense ministry of the country that developed it.
It is intended for the exclusive use by governments for the fight against terrorism and offers a very simple graphical interface for investigative activity.
It works on every version of IOS and Android currently existing(IOS 15.5 and Android 12). It covers almost all the devices in circulation.
The software is installed through the simple click of a link by the victim, completely silent, there is no need for any other interaction beyond the link.
The suite also includes the possibility of generating malicious links through own domains (to increase trust towards the victim)

and offers a user friendly tool for investigations (that's what it was designed for).

The functions available are the following (not all):
-List of installed apps
-Call log download
-Download Google Chrome history, saved passwords and cookies
-Download contacts
-Download Mail
-Download messages from any messaging application (Facebook Messenger / Instagram / IMO / Signal / Telegram / Whatsapp / Line / WeChat)
-Full filesystem access (also on iOS)
-Call Recording (can also be scheduled when)
-Listening to microphone remotely
-Remote location access
-Remote screenshots

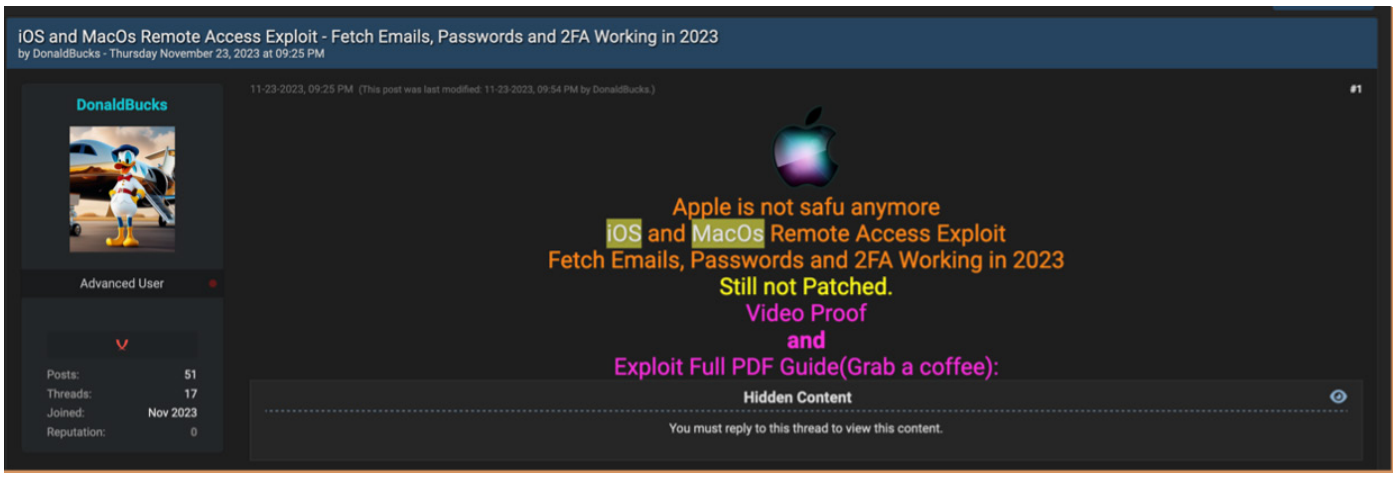
-Multiple data exfiltration modes to safeguard the battery
The software is designed to hopping across multiple servers to allow traffic anonymization (the company sells their network) and uses many advanced obfuscation techniques to stay undetected.
Attention I do not include the company network, so if you want to use this feature you will have to recreate your servers.

Vente du code source complet d'un spyware - Source : CERT-XMCO



Panel de contrôle utilisé par les opérateurs du spyware en vente - Source : CERT-XMCO

Le CERT-XMCO a en outre détecté la vente de plusieurs vulnérabilités de type 0-day iOS et Android sur des marketplaces criminelles par des Initial Access Brokers (IAB). Motivés par la recherche du gain financier, ces acteurs participent à la prolifération des outils d'interception de type spyware et à leur exploitation dans le cadre d'activités illégales.



Un outil au service de politiques étrangères

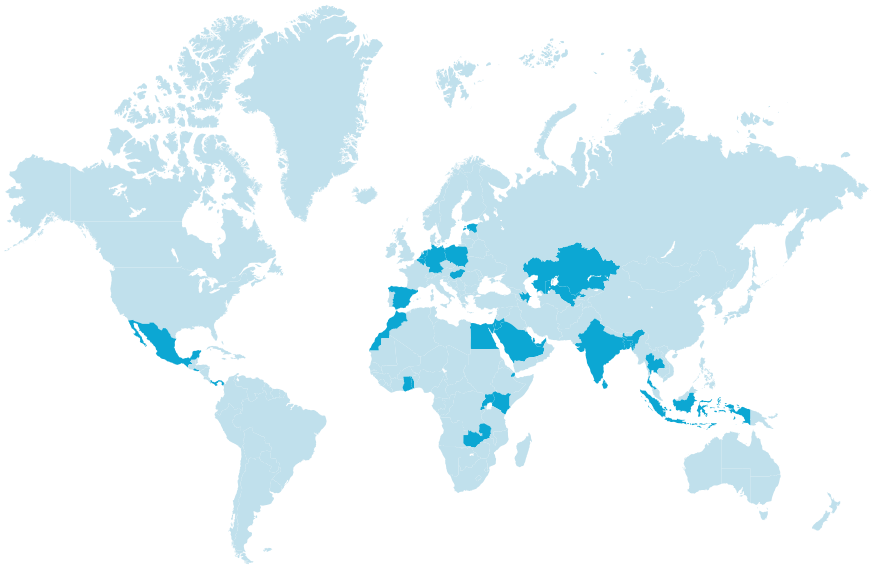
Le marché des spyware représenterait près de 12 milliards de dollars [11]. Entre 2011 et 2023, au moins 74 gouvernements ont conclu des contrats avec des sociétés commerciales pour obtenir des outils d'interception numérique, dont 44 sont considérés comme des autocraties. Ces chiffres illustrent la montée en puissance des solutions de Spyware-as-a-Service [52].

L'hégémonie d'Israël en matière de fourniture de spyware

L'hégémonie des entreprises israéliennes sur le marché des outils d'interception s'explique par la place que ces outils occupent dans la doctrine de sécurité de Tel-Aviv. Dès 2010, Benjamin Netanyahu a introduit une série de mesures permettant aux vétérans de l'Unité 8200 de fonder des entreprises privées pour participer à l'élaboration d'un complexe militaro-industriel [53].

Une étude du journal Haaretz affirme que 80% des 2 300 personnes ayant fondé des entreprises en lien avec la cybersécurité ont préalablement servi au sein des unités de guerre électronique des Forces de défense israéliennes (FDI), notamment l'Unité 8200 [54]. À titre d'exemple, le New York Times rapporte que presque tous les membres de l'équipe de recherche du NSO Group ont travaillé au sein de la Direction du renseignement militaire israélien [55]. En plus de ces liens étroits, les fournisseurs de spyware doivent obtenir des licences d'exportation du ministère israélien de la Défense pour vendre leurs outils à l'étranger, permettant au gouvernement d'influencer les entreprises et, dans certains cas, les pays qui leur achètent ces produits. Le commerce des outils offensifs cyber a été placé au cœur de la stratégie de Défense nationale israélienne et représente un moteur de la croissance économique du pays ainsi qu'un levier précieux de financement de la R&D à des fins militaires [56].

Encore aujourd'hui, ces outils occupent une place centrale dans les aspirations politiques israéliennes au Moyen-Orient et en Afrique. La fourniture de Pegasus à plusieurs pays africains aurait été utilisée comme monnaie d'échange par Tel-Aviv pour obtenir un soutien à sa candidature au statut d'observateur auprès de l'Union africaine, obtenue en juillet 2021 [57]. Par ailleurs, il est notamment intéressant d'observer qu'après l'annonce de la normalisation des relations israélo-marocaines, le Royaume du Maroc est devenu client de la société NSO Group [58].



Allemagne
Arabie Saoudite
Azerbaïdjan
Bahreïn
Bangladesh
Belgique
Djibouti
Egypte
Emirats Arabes Unis
Espagne
Estonie
Ghana
Hongrie
Inde
Indonésie
Israël
Jordanie
Jordanie
Kazakhstan
Kenya
Le Salvador
Mexique
Maroc
Ouganda
Ouzbékistan
Pays-Bas
Panama
Pologne
Rwanda
Thaïlande
Togo
Zambie

Pays accusés d'avoir déployé le spyware Pegasus - Source : Carnegie [2]

En mars 2022, l'Agence israélienne de contrôle des exportations de défense a interdit la vente du spyware Pegasus aux autorités ukrainiennes [59]. En adoptant cette posture, Israël cherchait vraisemblablement à éviter un incident diplomatique avec la Russie, qui a généralement permis à Tel-Aviv de frapper des cibles iraniennes et libanaises en Syrie. Le journal Haaretz a enfin rapporté qu'Israël avait refusé d'accorder des licences au Bangladesh, craignant que l'outil ne tombe entre les mains du Pakistan, fervent défenseur de la cause palestinienne [60].

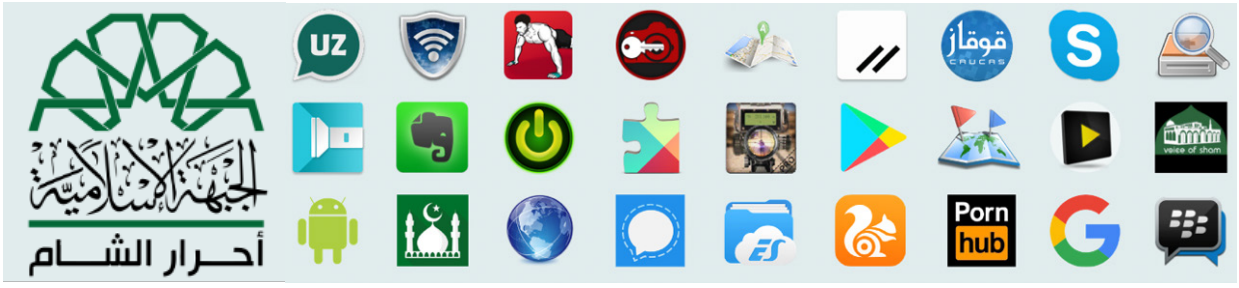
Des spyware au service de la politique étrangère du Kremlin

En mars 2023, le Wall Street Journal a rendu public un rapport indiquant que les autorités russes, agissant au travers d'un contrat établi entre la société russe PROTEI et l'opérateur de réseau mobile iranien Ariantel, avaient fourni une solution d'interception téléphonique à l'Iran. PROTEI aurait livré un logiciel de censure Internet, intégré à un système de téléphonie mobile en cours de développement, permettant de surveiller, intercepter, rediriger ou dégrader l'ensemble des communications mobiles des utilisateurs iraniens. Cette fourniture aurait été effectuée en échange de drones fournis par Téhéran, utilisés par les forces armées russes dans le cadre de la guerre en Ukraine [61].

Ce ne serait pas la première fois qu'une entreprise russe commercialise un spyware en soutien à la politique étrangère du Kremlin. En 2018, les chercheurs de Lookout avaient identifié un Remote Access Trojan (RAT) Android nommé Monokle et développé par la société Special Technology Centre (en russe : Специальный Технологический Центр). Cette dernière avait été sanctionnée par le gouvernement américain pour son implication dans l'ingérence de Moscou lors des élections présidentielles américaines de 2016 et ses liens supposés avec le renseignement militaire russe (GRU).

« ... les autorités russes, agissant au travers d'un contrat établi entre la société russe PROTEI et l'opérateur de réseau mobile iranien Ariantel, avaient fourni une solution d'interception téléphonique à l'Iran »

Monokle s'appuyait sur des techniques avancées d'exfiltration de données et installait un certificat spécifié par l'attaquant, facilitant les attaques de type Man-in-the-Middle. Le RAT utilisait également des dictionnaires de texte prédictifs définis par le client du spyware pour isoler les sujets d'intérêt à surveiller sur les appareils ciblés [62].



Applications trojanisées par Monokle - Source : Lookout [62]

Les chercheurs ont établi que Monokle avait été essentiellement utilisé pour cibler en 2017 des appareils mobiles d'individus en lien avec des groupes militants et religieux au Moyen-Orient, en Europe de l'Est et dans le Caucase. Monokle pourrait avoir été proposé aux autorités syriennes pour lutter contre le groupe Ahrar al-Sham, une faction rebelle ayant prêté allégeance au Front islamique syrien, qui a pour objectif de lutter contre le gouvernement de Bachar el-Assad.

La régulation du marché par les États-Unis et l'Union européenne

La régulation du marché des spyware commerciaux par les États-Unis et l'Union européenne présente une ambivalence frappante, illustrée par des actions réglementaires juxtaposées à des pratiques de fourniture de ces outils à des puissances étrangères. En juillet 2023, le Bureau de l'Industrie et de la Sécurité (BIS) du département du Commerce américain a ajouté deux fournisseurs étrangers de spyware à sa liste de blocage économique, soulignant leur utilisation d'exploits pour accéder de manière non autorisée à des appareils téléphoniques et menacer la vie privée d'utilisateurs à l'échelle mondiale [63] [9] [10].

Pour autant, le gouvernement américain ne promulgue pas l'interdiction totale des spyware commerciaux. Le décret signé par l'administration Biden permet aux entreprises américaines, respectant certains critères, de continuer à développer et commercialiser ces outils. Pour échapper aux sanctions, les autres fournisseurs adoptent des stratégies complexes de création de structures de sociétés-écrans, changeant de nom lorsque des scandales éclatent [64].

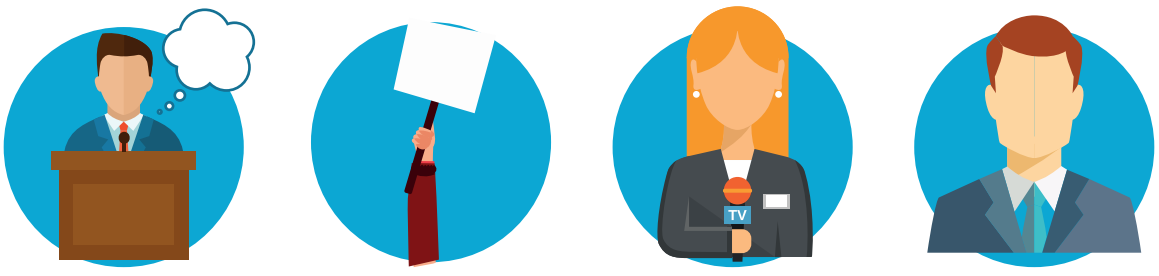
En parallèle, au sein de l'Union européenne, les réglementations sur l'octroi de licences pour la commercialisation de spyware varient entre les États membres. Certains, comme la Bulgarie, Chypre, la Grèce, la Hongrie, l'Italie, et Malte, disposent de cadres juridiques non contraignants. Des députés européens ont ainsi appelé plusieurs pays membres à se conformer aux arrêts de la Cour européenne des droits de l'homme [65].

Malgré ces appels, des acteurs privés européens, tels que l'italien Data Flow, le français Nexa Technologies et l'espagnol Variston ont été accusées de fournir des technologies de surveillance numérique à des autocraties [66] [67] [68]. Dans certains cas, la vente de ces outils aurait également été exploitée comme instrument de la politique étrangère, Nexa Technologies (anciennement Amesys) ayant par exemple reconnu en 2011 que la signature de contrats avec la Libye de Mouammar Kadhafi avait été encouragée par la présidence française afin de poursuivre des objectifs diplomatiques [69].

Même si des mesures régulatrices sont prises, la prolifération continue des spyware commerciaux souligne le défi persistant de concilier les préoccupations éthiques et sécuritaires avec les intérêts commerciaux et géopolitiques.

Recommandations

Les campagnes de distribution de spyware commerciaux observées par le CERT-XMCO se sont principalement basées sur la combinaison de campagnes de spear-phishing avec l'exploitation de vulnérabilités 0-day, voire 0-click pour certaines d'entre elles.



Réduire son exposition aux vulnérabilités

Bien qu'il soit difficile de prévenir une compromission via l'exploitation de vulnérabilité de type 0-click, il reste néanmoins nécessaire de réduire autant que possible la surface d'attaque. À ce titre, il est hautement recommandé d'appliquer les correctifs des vulnérabilités connues ayant été activement exploitées à des fins de surveillance et susceptibles d'être utilisées de nouveau.

Par ailleurs, il est également important de rester alerte quant aux signes d'une infection par spyware et de se rapprocher des autorités compétentes le cas échéant. D'une manière générale, les traces d'une telle infection peuvent prendre les formes suivantes :

- Votre téléphone devient soudainement plus lent que d'habitude et s'éteint parfois de lui-même.
- Vous identifiez des dossiers, applications ou fichiers inhabituels et/ou inconnus sur votre appareil mobile.

Ces signes n'en restent pas moins difficilement attribuables et un code malveillant sophistiqué peut être indétectable sur une période prolongée.

Adopter une posture de vigilance face au phishing

Quant aux campagnes de spear-phishing, le CERT-XMCO recommande d'adopter les comportements suivants pour limiter les risques d'infection.

- Ne pas cliquer sur des liens non vérifiés et y renseigner vos informations personnelles d'identification (PII). Même s'ils sont en apparence légitimes, les sites de phishing demeurent le principal vecteur de compromission initiale exploitée par les acteurs de la menace cyber. En 2023, plusieurs kits de Phishing-as-a-Service ont été identifiés par le CERT-XMCO sur des marketplaces criminelles. Ces derniers automatisent le processus de création des sites de phishing pour des acteurs novices [70].

- Ne pas exécuter de fichiers ou installer d'applications mobiles provenant de sites non officiels ou à l'issue d'une phase d'approche sur les réseaux sociaux. Ce type de vecteur d'attaque est d'autant plus exacerbé par l'utilisation d'appareils mobiles professionnels à des fins personnelles et inversement. Il est donc hautement recommandé de séparer les usages de ces derniers pour limiter l'impact d'une compromission.

Lors de déplacements à l'étranger

- Rester en possession de votre appareil mobile à tout moment. Dans le cas contraire, il est recommandé de retirer la batterie et la carte SIM de l'appareil mobile. Gardez aussi un œil sur vos câbles, chargeurs et périphériques.
- Éteigner votre appareil mobile lorsque vous passez la douane ou d'autres points d'inspection.
- Il est recommandé de ne pas utiliser la fonction "Se souvenir de moi" lors des authentifications sur des sites web.
- Ne pas utiliser de réseaux Wi-Fi inconnus, ni les bornes de recharge dans les lieux publics.

CVEs exploitées par les fournisseurs de spyware commerciaux

Note	Note
Pegasus de NSO Group	CVE-2021-30860 CVE-2023-41064 CVE-2023-41061 CVE-2019-3568 CVE-2016-4655 CVE-2016-4656
Heliconia de Variston IT	CVE-2022-26485 CVE-2021-42298 CVE-2022-4262 CVE-2022-3038 CVE-2022-22706 CVE-2023-0266
Hermit de RCS Labs	CVE-2021-30883 CVE-2021-30983 CVE-2020-3837 CVE-2020-9907 CVE-2019-8605 CVE-2018-4344
Predator de Cytrox	CVE-2021-37973 CVE-2021-37976 CVE-2021-38000 CVE-2021-38003
KingsPawn de Quadream	CVE-2021-30860 CVE-2021-30858
Sherlock de Candiru	CVE-2021-21166 CVE-2021-30551 CVE-2021-33742 CVE-2022-2294 CVE-2021-31979 CVE-2021-33771
FinSpy (aussi connu comme FinFisher) de FinFisher Labs	CVE-2017-0199

Bibliographie

[1] Amnesty, «Global: 'Predator Files' investigation reveals catastrophic failure to regulate surveillance trade,» 5 Octobre 2023. [En ligne]. Available: https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/.

[2] Carnegie, «Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses,» 14 Mars 2023. [En ligne]. Available: https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

[3] Feldstein, Steven, «Global Inventory of Commercial Spyware & Digital Forensics,» 2 Mars 2023. [En ligne]. Available: https://data.mendeley.com/datasets/csvhpkt8tm/10.

[4] Mediapart, «« Projet Pegasus » : des révélations d'une ampleur mondiale sur la surveillance,» 19 Juillet 2021. [En ligne]. Available: https://www.mediapart.fr/journal/international/190721/projet-pegasus-des-revelations-d-une-ampleur-mondiale-sur-la-surveillance.

[5] Citizen Lab, «NSO Group iMessage Zero-Click Exploit Captured in the Wild,» 13 Septembre 2021. [En ligne]. Available: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.

[6] European Parliament, «The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware,» 5 Décembre 2022. [En ligne]. Available: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740151.

[7] European Data Protection Supervisor, «EDPS Preliminary Remarks on Modern Spyware,» 15 Février 2022. [En ligne]. Available: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.

[8] The White House, «FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security,» 27 Mars 2023. [En ligne]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/.

[9] US Department of State, «The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities,» 18 Juillet 2023. [En ligne]. Available: https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/.

[10] US Department of State, «The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities,» 3 Novembre 2021. [En ligne]. Available: https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/.

[11] The New Yorker, «How Democracies Spy on Their Citizens,» 18 Avril 2022. [En ligne]. Available: https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

[12] Zimperium, «2023 Global Mobile Threat Report: Key Insights on the State of Mobile Security,» 28 Juin 2023. [En ligne]. Available: https://www.zimperium.com/blog/key-insights-from-2023-global-mobile-threat-report/.

[13] Mordor Intelligence, «BYOD Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028) Source: https://www.mordorintelligence.com/industry-reports/byod-market,» [En ligne]. Available: https://www.mordorintelligence.com/industry-reports/byod-market.

[14] Lookout, «Lookout Uncovers Hermit Spyware Deployed in Kazakhstan,» 16 Juin 2022. [En ligne]. Available: https://www.lookout.com/threat-intelligence/article/hermit-spyware-discovery.

[15] Citizen Lab, «Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware,» 30 Août 2017. [En ligne]. Available: https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/.

[16] Citizen Lab, «PREDATOR IN THE WIRES - Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions,» Zimperium & Citizen Lab, 22 Septembre 2023. [En ligne]. Available: https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/.

[17] NCSC, «The threat from commercial cyber proliferation,» 19 Avril 2023. [En ligne]. Available: https://www.ncsc.gov.uk/report/commercial-cyber-proliferation-assessment.

[18] ESET, «Faille Zero-Day,» ESET, [En ligne]. Available: https://www.eset.com/fr/cybermenaces/faille-zero-day/.

[19] Google, «2022 0-day In-the-Wild Exploitation...so far,» 30 Juin 2022. [En ligne]. Available: https://googleprojectzero.blogspot.com/2022/06/2022-0-day-in-wild-exploitationso-far.html.

[20] Avast, «The Return of Candiru: Zero-days in the Middle East,» 21 Juillet 2022. [En ligne]. Available: https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/.

[21] Google, «New details on commercial spyware vendor Variston,» 30 Novembre 2022. [En ligne]. Available: https://blog.google/threat-analysis-group/new-details-on-commercial-spyware-vendor-variston/.

[22] Mandiant, «Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace,» 20 Mars 2023. [En ligne]. Available: https://www.mandiant.com/resources/blog/zero-days-exploited-2022.

[23] «Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits,» 27 Juillet 2022. [En ligne]. Available: https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/.

[24] Kaspersky, «Qu'est-ce qu'un programme malveillant sans clic et comment fonctionnent les attaques sans clic ?,» Kaspersky, [En ligne]. Available: https://www.kaspersky.fr/resource-center/definitions/what-is-zero-click-malware.

[25] Zerodium, «Zerodium Exploit Acquisition Program,» Zerodium, [En ligne]. Available: https://zerodium.com/program.html.

[26] Citizen Lab, «BLASTPASS - NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild,» 7 Septembre 2023. [En ligne]. Available: https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

[27] Security Affairs, «WhatsApp sued Israeli surveillance firm NSO Group and its parent Q Cyber Technologies,» 30 Octobre 2019. [En ligne]. Available: https://securityaffairs.com/93162/malware/whatsapp-lawsuit-nso-group.html.

[28] Citizen Lab, «CatalanGate - Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru,» 18 Avril 2022. [En ligne]. Available: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

[29] Citizen Lab, «Sweet QuaDreams - A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers,» Citizen Lab, 11 Avril 2023. [En ligne]. Available: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[30] Kaspersky, «Kaspersky révèle des informations complémentaires sur l'opération Triangulation,» Kaspersky, 26 Octobre 2023. [En ligne]. Available: https://www.kaspersky.fr/about/press-releases/2023_kaspersky-revele-des-informations-complementaires-sur-loperation-triangulation.

[31] Kaspersky, «A Matter of Triangulation,» 1 Juin 2023. [En ligne]. Available: https://eugene.kaspersky.com/2023/06/01/a-matter-of-triangulation/.

[32] The Register, «Kremlin claims Apple helped NSA spy on diplomats via iPhone backdoor,» 1 Juin 2023. [En ligne]. Available: https://www.theregister.com/2023/06/01/fsb_apple_nsa_spyware_kaspersky/.

[33] Ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique, «Sécurité de vos données : qu'est-ce que l'attaque par hameçonnage ciblé (spearphishing) ?,» 15 Septembre 2023. [En ligne]. Available: https://www.economie.gouv.fr/entreprises/hameconnage-spearphishing.

[34] Cisco Talos, «Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware,» 25 Mai 2023. [En ligne]. Available: https://blog.talosintelligence.com/mercenary-intellexa-predator/.

[35] Kaspersky, «What is Social Engineering?,» Kaspersky, [En ligne]. Available: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

[36] Meta, «Threat Report on the Surveillance-for-Hire Industry,» 15 Décembre 2022. [En ligne]. Available: https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

[37] Amnesty International, «The Predator Files: Caught in the Net,» 9 Octobre 2023. [En ligne]. Available: https://www.amnesty.org/en/documents/act10/7245/2023/en/.

[38] Haaretz, «'Cyber Mercenaries': Israel's Spyware Industry Is Getting Slammed Around the World,» 21 Décembre 2021. [En ligne]. Available: https://www.haaretz.com/israel-news/2021-12-21/ty-article/.premium/cyber-mercenaries-how-israels-spyware-industry-is-getting-slammed/0000017f-dbef-d3a5-af7f-fbef60bb0000.

[39] Vice, «The Company Helping the IRS Go Undercover Online,» 16 Février 2023. [En ligne]. Available: https://www.vice.com/en/article/xgynn4/company-helping-irs-go-undercover-cobwebs-technologies.

[40] The Register, «Probe reveals previously secret Israeli spyware that infects targets via ads,» 16 Septembre 2023. [En ligne]. Available: https://www.theregister.com/2023/09/16/insanet_spyware/.

[41] Calcalist, «Israel Police purchased new surveillance software without AG approval,» 29 Mai 2023. [En ligne]. Available: https://www.calcalistech.com/ctechnews/article/bkq6eef8h.

[42] The Guardian, «Israeli spy firm suspected of accessing global telecoms via Channel Islands,» The Guardian, 16 Décembre 2020. [En ligne]. Available: https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands.

[43] ANSSI, «État de la menace ciblant le secteur des télécommunications,» 18 Décembre 2023. [En ligne]. Available: https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/.

[44] Google, «Spyware vendor targets users in Italy and Kazakhstan,» 23 Juin 2022. [En ligne]. Available: https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/.

La prolifération des spyware commerciaux

[45] Microsoft, «FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines,» 1 Mars 2018. [En ligne]. Available: https://www.microsoft.com/en-us/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/.

[46] Cyble, «Israeli Spyware Pegasus Spying on Journalists and Activists,» 19 Juillet 2021. [En ligne]. Available: https://cyble.com/blog/israeli-spyware-pegasus-spying-on-journalists-and-activists/.

[47] Amnesty, «Rapport concernant la méthodologie technique employée pour détecter le logiciel Pegasus de NSO Group,» 18 Juillet 2021. [En ligne]. Available: https://www.amnesty.org/fr/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

[48] Zimperium, «Over 3,000 Android Malware Samples Using Multiple Techniques to Bypass Detection,» 16 Août 2023. [En ligne]. Available: https://www.zimperium.com/blog/over-3000-android-malware-samples-using-multiple-techniques-to-bypass-detection/.

[49] Cisco Talos, «The wolf is back...,» 19 Mai 2020. [En ligne]. Available: https://blog.talosintelligence.com/the-wolf-is-back/.

[50] Threat Fabric, «SpyNote: Spyware with RAT capabilities targeting Financial Institutions,» 5 Janvier 2023. [En ligne]. Available: https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.

[51] Softpedia, «Phineas Fisher's Account of How He Broke Into Hacking Team Servers,» 17 Avril 2016. [En ligne]. Available: https://news.softpedia.com/news/finfisher-s-account-of-how-he-broke-into-hackingteam-servers-503078.shtml.

[52] Kaspersky, «Les cybercriminels utilisent de nouvelles tactiques pour attaquer les entreprises industrielles et s'emparer de leurs données,» 3 Février 2022. [En ligne]. Available: https://www.kaspersky.fr/about/press-releases/2022_les-cybercriminels-utilisent-de-nouvelles-tactiques-pour-attaquer-les-entreprises-industrielles-et-semparer-de-leurs-donnees.

[53] L'Express, «Israël : l'unité 8200, nid d'espions, pépinière d'entrepreneurs,» 10 Juillet 2019. [En ligne]. Available: https://www.lexpress.fr/economie/high-tech/israel-l-unite-8200-nid-d-espions-pepiniere-d-entrepreneurs_2087731.html.

[54] Haaretz, «Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays,» 20 Octobre 2018. [En ligne]. Available: https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.

[55] The New York Times, «The Battle for the World's Most Powerful Cyberweapon,» 28 Janvier 2022. [En ligne]. Available: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[56] S. R. Laurent Richard, Pegasus: The Story of the World's Most Dangerous Spyware, 2023.

[57] Orient XXI, «Israel's Spyware Diplomacy in Africa,» 12 Septembre 2022. [En ligne]. Available: http://orientxxi.info/magazine/israel-s-spyware-diplomacy-in-africa,5859.

[58] Le Monde, «Après l'affaire NSO, Israël et le Maroc poursuivent leur rapprochement,» 11 Août 2021. [En ligne]. Available: https://www.lemonde.fr/international/article/2021/08/11/apres-le-scandale-nso-israel-et-le-maroc-poursuivent-leur-rapprochement_6091204_3210.html.

[59] Numerama, «Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia,» 23 Mars 2022. [En ligne]. Available: https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html.

[60] Haaretz, «In Response to Haaretz Investigation, Bangladesh Says It Made No 'Direct' Purchases of Spytech From Israel,» 11 Janvier 2023. [En ligne]. Available: https://www.haaretz.com/israel-news/security-aviation/2023-01-11/ty-article/.premium/bangladesh-says-it-made-no-direct-purchases-of-cybersecurity-from-israel/00000185-a153-d69c-abc5-b55b77070000.

[61] The Wall Street Journal, «Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows,» 27 Mars 2023. [En ligne]. Available: https://www.wsj.com/articles/russia-supplies-iran-with-cyber-weapons-as-military-cooperation-grows-b14b94cd.

[62] Lookout, «New Surveillanceware Developed by Russian Defence Contractor,» 24 Juillet 2019. [En ligne]. Available: https://www.lookout.com/threat-intelligence/article/monokle.

[63] Institut Montaigne, «De la prolifération à la déstabilisation : l'industrie spyware, une spirale centrifuge,» 6 Juillet 2023. [En ligne]. Available: https://www.institutmontaigne.org/expressions/de-la-proliferation-la-destabilisation-lindustrie-spyware-une-spirale-centrifuge.

[64] Le Monde, «A Chypre, un conglomérat de cybersurveillance entre opacité juridique et optimisation fiscale,» 16 Novembre 2023. [En ligne]. Available: https://www.lemonde.fr/les-decodeurs/article/2023/11/16/a-chypre-un-conglomerat-de-cybersurveillance-entre-opacite-juridique-et-optimisation-fiscale_6200486_4355770.html.

[65] Conseil de l'Europe, «Le logiciel espion Pegasus et ses répercussions sur les droits de l'homme,» 2022. [En ligne]. Available: https://www.coe.int/fr/web/freedom-expression/-/pegasus-spyware-and-its-impacts-on-human-rights.

[66] Intelligence Online, «Dataflow Security et Rayzone se servent dans un NSO en cours de rachat,» 16 Juin 2022. [En ligne]. Available: https://www.intelligenceonline.fr/surveillance--interception/2022/06/16/dataflow-security-et-rayzone-se-servent-dans-un-nso-en-cours-de-rachat,109792243-eve.

[67] La Tribune, «Nexa Technologies mise en examen pour « complicité d'actes de torture » suite à la vente de son logiciel Cerebro en Egypte,» La Tribune, 28 Novembre 2021. [En ligne]. Available: https://www.latribune.fr/economie/international/nexa-technologies-mise-en-examen-pour-complicite-d-actes-de-torture-pour-la-vente-de-son-logiciel-cerebro-en-egypte-897348.html.

[68] Google, «Spyware vendors use 0-days and n-days against popular platforms,» 29 Mars 2023. [En ligne]. Available: https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/.

[69] France Info, «Cybersurveillance en Libye et en Egypte : ce que l'on sait de l'affaire qui a conduit des patrons d'entreprises français devant la justice,» 22 Juin 2021. [En ligne]. Available: https://www.francetvinfo.fr/monde/afrique/egypte/cybersurveillance-en-libye-et-en-egypte-ce-que-l-on-sait-de-l-affaire-qui-a-conduit-des-patrons-dentreprises-francais-devant-la-justice_4673911.html.

[70] ESET, «Telekopye: Hunting Mammoths using Telegram bot,» 24 Août 2023. [En ligne]. Available: https://www.welivesecurity.com/en/eset-research/telekopye-hunting-mammoths-using-telegram-bot/.

Revue du web

Des infos techs et cybers diverses

Extension VSCode pour visualiser facilement les fichiers XML Nmap

#Pentest

https://marketplace.visualstudio.com/items?itemName=marduc812.nmap-peek

Outil pour interagir avec l'API BloodHound CE

#Pentest #Audit #Tool

https://github.com/deletehead/ReleaseTheHounds

Les fondamentaux de la sécurité Kubernetes (Partie 1 et 2)

#DevOps #Kubernetes

https://securitylabs.datadoghq.com/articles/kubernetes-security-fundamentals-part-1/

https://securitylabs.datadoghq.com/articles/kubernetes-security-fundamentals-part-2/

Interface web qui propose plusieurs décompilateurs de binaire permettant une comparaison rapide des résultats

#Reverse #Forensics

https://github.com/decompiler-explorer/decompiler-explorer

Petit outil rapide et simple pour effectuer des recherches DNS inversées en masse

#OSINT #Pentest #Tool

https://t.co/cKJVHtRAk2

Kubehound : outil pour trouver les chemins d'attaques dans les clusters Kubernetes

#Pentest #Kubernetes #Tool

https://kubehound.io/

IceKube : Un autre outil pour trouver les chemins d'attaques dans les clusters Kubernetes

#Pentest #Kubernetes #Tool

https://labs.withsecure.com/tools/icekube--finding-complex-attack-paths-in-kubernetes-clusters

Outil en cli codé en Go pour tester les injections de template (SSTI)

#Pentest #Tool

https://github.com/Hackmanit/TInjA

Ensemble d'entreprises qui divulguent les tactiques, techniques et procédures (TTP) des attaquants après avoir été victimes d'une intrusion

#Blueteam

https://github.com/BushidoUK/Breach-Report-Collection

Outil qui scanne les dépôts publics de Github pour identifier d'éventuelles CVE

#OSINT #Tool

https://github.com/Aqua-Nautilus/CVE-Half-Day-Watchers

Construire un agent d'IA capable d'automatiser une partie des tâches de test d'intrusion

#Pentest #IA

https://github.com/pentestmuse-ai/PentestMuse

Article qui explique comment exploiter les injections XPath

#Pentest #XPath

https://www.netspi.com/blog/technical/web-application-penetration-testing/exploiting-xpath-injection-weaknesses/

Scanner qui en combine plusieurs (Nikto Scanner, OWASP ZAP, Nuclei, SkipFish, Wapiti)

#Pentest #Tool

https://www.netspi.com/blog/technical/web-application-penetration-testing/exploiting-xpath-injection-weaknesses/

Article sur la construction d'une crackstation pour les mots de passe

#Pentest #Tool

https://www.sevnx.com/blog/post/building-a-password-cracker

Dernières infos issues de la veille CTI de notre service YUNO

Ransomware

Une opération internationale a saisi le site d'extorsion du ransomware RagnarLocker
19/10/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-5752
https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomwares-dark-web-extortion-sites-seized-by-police/

LockBit publie des données volées à Boeing
10/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6228
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

Le ransomware Qilin revendique la compromission de Yanfeng Automotive Interiors perturbant la production des usines de Stellantis
27/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6592
https://www.carscoops.com/2023/11/stellantis-production-disrupted-after-cyberattack-on-chinese-interior-supplier/

Les autorités américaines saisissent l'infrastructure du ransomware ALPHV/BlackCat
19/12/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-7039
https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

Publication d'un outil de déchiffrement pour le ransomware Black Basta
30/12/2023

https://leportail.xmco.fr/watch/advisory/CXN-2024-0017
https://github.com/srlabs/black-basta-buster

Infostealers & Malware-as-a-Service (MaaS)

Analyse du Malware-as-a-Service DarkGate
20/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6493
https://blog.sekoia.io/darkgate-internals/

Atomic Stealer distribué aux utilisateurs Mac dans le cadre de la campagne de phishing ClearFake
24/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6496
https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates

Détection du nouvel Infostealer-as-a-Service Nova, opéré par le groupe Sordeal
29/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6689
https://www.cyfirma.com/outofband/emerging-maas-operator-sordeal-releases-nova-infostealer/

Exploitation par des infostealers d'une vulnérabilité visant le protocole de sécurité OAuth2 de Google
29/12/2023

https://leportail.xmco.fr/watch/advisory/CXN-2024-0011
https://www.cloudsek.com/blog/compromising-google-accounts-malwares-exploiting-undocumented-oauth2-functionality-for-session-hijacking

Écosystème Dark Web

Le FBI saisit l'infrastructure du Botnet-as-a-Service IPStorm
14/11/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6309
https://www.justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service

Rapport sur le fonctionnement interne du kit de Scamming-as-a-Service Telekopye
23/11/2023

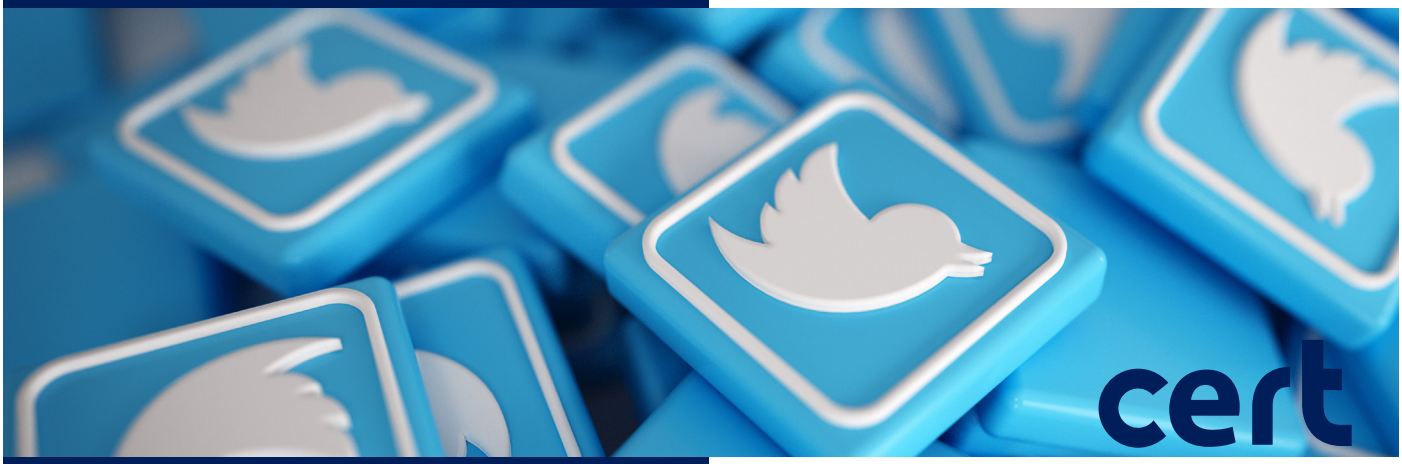
https://leportail.xmco.fr/watch/advisory/CXN-2023-6553
https://www.welivesecurity.com/en/eset-research/telekopye-chamber-neanderthals-secrets/

Arrestation d'un opérateur du groupe Kelvin Security par la police espagnole
10/12/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-6840
https://www.bleepingcomputer.com/news/security/kelvin-security-hacking-group-leader-arrested-in-spain/

Saisie de la marketplace criminelle Kingdom Market par les autorités fédérales allemandes
19/12/2023

https://leportail.xmco.fr/watch/advisory/CXN-2023-7083



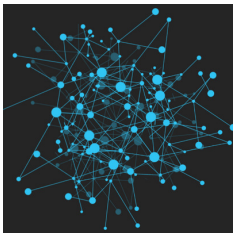
Découvrez notre sélection des comptes 8 (Twitter) incontournables !

Jean_Maes_1994
https://twitter.com/Jean_Maes_1994

disclosedh1
https://twitter.com/disclosedh1

Jhaddix
https://twitter.com/Jhaddix

SkelSec
https://twitter.com/SkelSec



tomnomnom
https://twitter.com/TomNomNom

hakluke
https://twitter.com/hakluke

ly4k_
https://twitter.com/ly4k_

ShitSecure
https://twitter.com/ShitSecure

actusécu

By xmco

xmco

We deliver cybersecurity expertise