SOPHOS
Cybersecurity delivered.

Rapport Sophos 2023 sur les menaces

Les marchés criminels en pleine maturité présentent de nouveaux défis pour les professionnels de la cybersécurité

Sophos X-Ops

Sommaire

Joe Levy
Sophos CTO

Lettre du CTO

Comme chaque année, l'industrie de la cybersécurité a tendance à dresser un bilan de l'année écoulée et déclare que les douze derniers mois ont été parmi les plus marquants de son histoire. Si l'année 2022 n'a pas connu d'événement marquant comme Aurora, Stuxnet, WannaCry ou la cyberattaque de Colonial Pipeline, elle s'inscrit malheureusement dans les annales de la cyber-histoire avec l'éclatement d'une guerre en Europe — la plus importante depuis un demi-siècle.

L'importance de cette guerre pour la cybersécurité tient au fait que l'agresseur, un pays connu pour être l'un des principaux promoteurs et refuges de l'activité cybercriminelle dans le monde et le précurseur du ransomware en tant qu'industrie nationale, a envahi son voisin.

Au lendemain de l'invasion de l'Ukraine par la Russie, il était inévitable que le gouvernement russe encourage fortement son réseau cybercriminel national à manipuler l'opinion mondiale en sa faveur, tout en tentant de saboter la popularité que le président ukrainien avait pu acquérir dans le monde. Et c'est exactement ce qui s'est passé lorsque des ransomwares, des malwares et des groupes de désinformation ont émergé pour soutenir l'agression russe.

Ces efforts, jusqu'à aujourd'hui, ont été un échec total. L'opinion mondiale sur les auteurs de ransomwares était déjà au plus bas lorsque, durant toute la pandémie, ces gangs n'ont cessé de viser les secteurs les plus vitaux pour la mise en œuvre d'une réponse à la crise : la santé, la recherche médicale, les entreprises essentielles au maintien des chaînes d'approvisionnement et des opérations alimentaires et énergétiques, et même les systèmes éducatifs. Continuant sur leur lancée, ils ont attisé la colère du monde entier en déclarant leur soutien indéfectible à l'invasion russe et en prenant pour cible tout pays ou organisation qui s'opposait à elle.

Mais d'autres membres de ces mêmes gangs, basés en Ukraine, ont vu les choses différemment. C'est ainsi qu'une guerre de divulgation a débuté, avec des fuites révélant certaines des informations les plus sensibles jamais dévoilées sur le mode de fonctionnement de ces groupes cybercriminels. La guerre semble avoir rompu les liens entre les cybercriminels ukrainiens et leurs homologues russes (et biélorusses), peut-être même de manière définitive.

Dans le même temps, alors que la Russie était occupée à sa guerre d'agression, la Chine s'est lancée dans des opérations cybercriminelles spectaculaires, ciblant non seulement ses voisins et les pays qu'elle considère comme essentiels dans le cadre de son projet « Nouvelle route de la soie », mais aussi le secteur de la sécurité lui-même. Dans une série d'attaques toujours plus audacieuses contre les sociétés spécialisées dans la protection des réseaux et des données, des groupes de cybercriminels basés en Chine (et probablement subventionnés) ont attaqué le matériel fabriqué par la quasi-totalité des entreprises des secteurs de la cybersécurité et des infrastructures.

En fait, on pourrait presque dire qu'en 2022, les masques sont tombés. Les deux plus grandes nations représentant une menace de cybersécurité pour le reste du monde ont décidé de rompre avec leur ancienne image prétendant n'avoir joué aucun rôle dans des fuites à grande échelle, des attaques majeures sur les infrastructures ou encore des dysfonctionnements dans bon nombre de domaines tels que l'éducation, la santé ou le commerce mondial. Elles pourraient tout aussi bien nous le brandir sous le nez, comme pour nous demander ce que nous allons bien pouvoir faire à ce sujet.

Ce que nous faisons — et ce que Sophos continuera de faire — c'est de renforcer les initiatives déjà en cours pour protéger à la fois nos clients et nous-mêmes. La société s'est engagée dans un processus pluriannuel d'amélioration progressive de la détection et de l'intervention automatisée face au comportement des ransomwares. Son succès à dérouter les attaquants est tel qu'ils n'ont pas d'autre choix que de redoubler leurs efforts afin de nous échapper s'ils veulent mettre à profit leurs menaces.

De plus, les attaques contre les infrastructures par des gangs basés en Chine et en Russie montrent qu'il est plus important que jamais de pouvoir faire confiance à son fournisseur de sécurité. Nous pensons que les fournisseurs doivent communiquer en toute transparence sur leurs investissements en matière de sécurité pour que cette confiance soit gagnée et maintenue, en particulier lorsque ceux-ci proposent des services et des produits de cybersécurité. Sophos a mis en place un Trust Center qui offre un aperçu du travail que nous effectuons autour des avis de sécurité et des signalisations de vulnérabilités, de nos tests de sécurité et de notre programme Bug Bounty, ainsi que de notre analyse des incidents et de nos plans d'intervention. Nous investissons continuellement dans la protection de notre propre infrastructure contre les attaques ciblées des APT et dans le renforcement du matériel et des logiciels qui opèrent dans les environnements de nos clients. Notre réussite à cet égard sera progressive, car les adversaires n'ont de cesse d'identifier et d'exploiter de nouvelles vulnérabilités, et semblent avoir intensifié leurs efforts pour contourner la sécurité des pare-feux, des switchs et des points d'accès réseau de chaque fournisseur. Nous continuons également à intégrer des configurations sécurisées par défaut dans nos offres et à introduire des outils tels que des diagnostics de sécurité et des mesures correctives de politiques dans nos produits et services afin d'améliorer les postures et l'hygiène de fonctionnement.

Les menaces continueront d'évoluer, et Sophos s'adaptera sans relâche pour continuer à garantir des résultats supérieurs en matière de cybersécurité.

Le ton est donné : la guerre en Ukraine

Si la guerre est la continuation de la politique par d'autres moyens et que le cyberconflit n'est qu'une branche de la guerre, il est logique que le conflit ukrainien se présente de la même manière en ligne et hors ligne. À l'heure où nous écrivons ces lignes, le paysage des menaces semble catastrophique à l'intérieur des frontières de l'Ukraine, tout en causant des dysfonctionnements certes moins profonds, mais néanmoins importants dans le reste du monde occidental — et un certain malaise, car le potentiel de conflit, de désinformation et de perturbation à plus grande échelle reste élevé.

Une zone de conflit qui a des répercussions dans le reste du monde

Comme on pouvait s'y attendre, l'escalade cinétique des attaques russes contre l'Ukraine, le 24 février, a profité aux escrocs qui cherchent à exploiter la peine et l'inquiétude au niveau mondial.

Début mars, nous avons observé une hausse des emails caritatifs frauduleux demandant des dons internationaux pour l'Ukraine. Dans les premiers jours de guerre, les responsables ukrainiens ont lancé des appels aux dons au monde entier pour les aider dans leurs efforts défensifs et ces appels comprenaient des demandes de dons en cryptomonnaies au trésor public. Les escrocs se sont immédiatement intéressés aux cryptomonnaies et ont envoyé des millions de messages de spam reprenant cette demande, mais en remplaçant les adresses de portefeuilles de cryptomonnaies par des adresses n'appartenant pas au gouvernement ou à toute autre organisation caritative ou non gouvernementale légitime. Lors du weekend du 5 et 6 mars, le nombre de spams sollicitant des dons à ces faux portefeuilles de cryptomonnaie a atteint un tel volume qu'il représentait la moitié de l'ensemble de spams que nous avons reçu dans cette période ! Heureusement, cette campagne n'a duré que quelques jours.

Scams ukrainiens en pourcentage du volume quotidien de spam, mars 2022

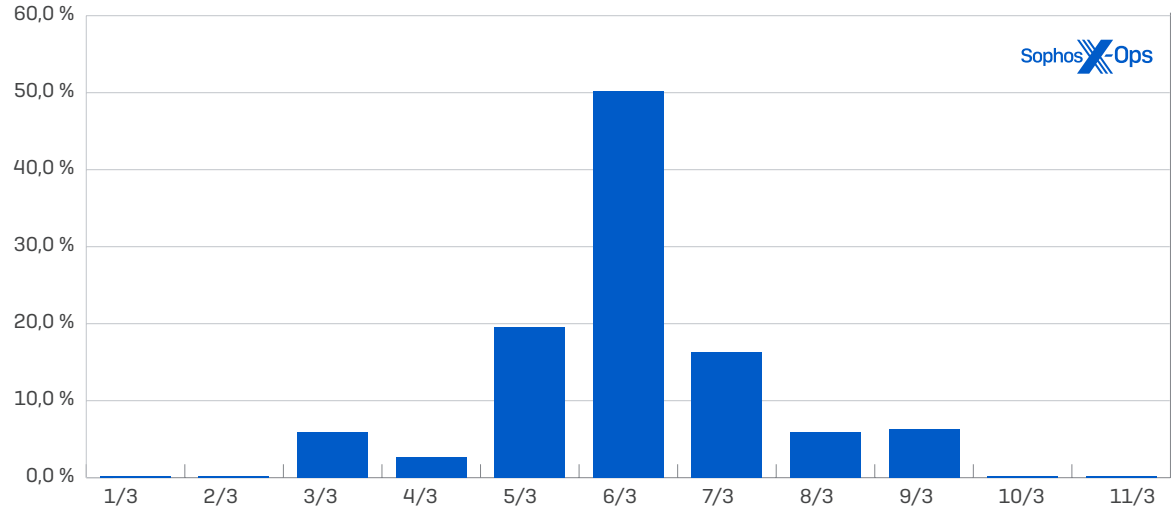


Fig.1. Le volume de spam sollicitant des dons à des adresses de cryptomonnaie frauduleuses brièvement en hausse.

Le mois de mai a également vu naître des centaines de sites frauduleux sollicitant des « dons », mais comme pour le spam initial, au vu des informations financières communes, ces sites étaient probablement gérés par un nombre relativement restreint d'entités. Dans tous les cas, ces attaques ne faisaient pas preuve d'une grande prouesse technique. En effet, elles consistaient notamment en des duperies d'ingénierie sociale qui invoquaient le nom du pays ou celui de ses dirigeants, et s'appuyaient sur des vulnérabilités et des exploits relativement obsolètes pour se déployer.

Par exemple, dans une campagne de spam notable ce même mois, le groupe Emotet a distribué un ensemble de documents Word malveillants avec des titres provocateurs imitant la propagande russe, tels que « Les États-Unis et leurs alliés fournissent des armes chimiques à l'armée ukrainienne.doc », dans le but de diffuser leur malware. Dans cette attaque, les documents malveillants ont utilisé l'exploit CVE-2021-40444 pour infecter les ordinateurs des victimes qui ouvraient les fichiers sur des machines qui n'avaient pas installé ce correctif Office publié à l'automne dernier.

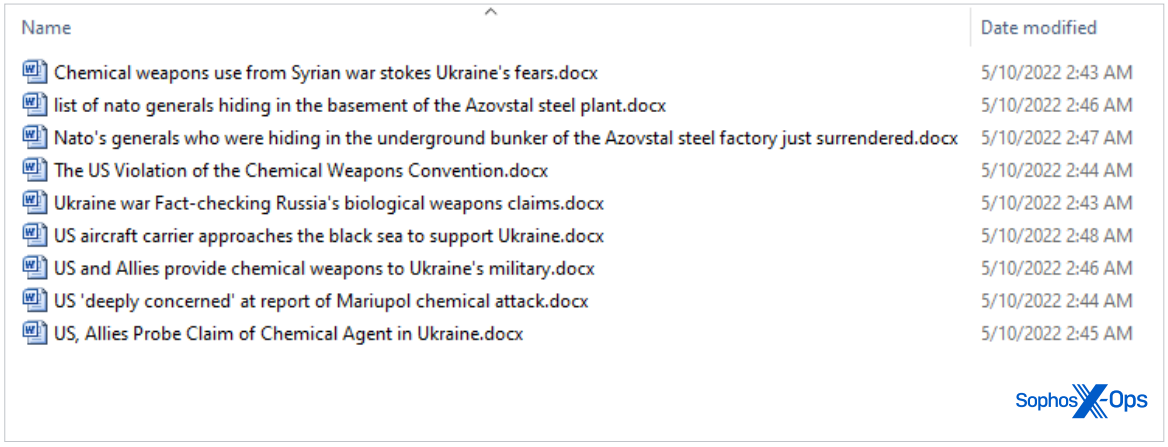


Fig. 2. Les noms de fichiers des emails de spam Emotet sur l'Ukraine faisaient l'objet d'affirmations fausses et effrayantes.

En ce qui concerne les cyberattaques entre états en dehors des frontières de l'Ukraine, notamment l'un des deux incidents les plus médiatisés, difficile de dire pour sûr qui est responsable à l'heure où nous écrivons ces lignes… L'attaque de ViaSat, qui a affecté les services satellites des Ukrainiens et d'autres clients en Europe quelques heures avant le début de l'invasion, est fermement qualifiée par les autorités comme étant l'œuvre de la Russie. Mais les piratages de sites Web d'aéroports occidentaux accessibles au public, survenus en octobre, sont plus difficiles à interpréter : s'agissait-il d'efforts d'un État-nation visant à intimider les alliés de l'Ukraine ou d'attaques indépendantes ?

En fait, la deuxième option semble le plus sensée. Les sabotages low-tech et DDoSing (y compris sur les sites aéroportuaires, sans parler de la tentative de perturber le vote de l'Eurovision) ont marqué les premiers jours de la guerre, mais alors que le conflit se poursuit cet hiver et que les tensions mondiales s'intensifient, certains observateurs non spécialistes ont constaté les facéties du groupe de hackers pro-russe, connu sous le nom de « Killnet » — rappelant que rien n'est encore résolu sur ce front.

Au cœur de l'action

En Ukraine, le tableau est plus sombre et plus déconcertant. Plusieurs attaques visant le gouvernement ukrainien ont suivi les mêmes schémas que les campagnes criminelles : utilisation d'emails d'ingénierie sociale, de malwares classiques et d'outils de sécurité détournés. À titre d'exemple, citons le cas d'un email frauduleux qui contenait un lien vers une « mise à jour antivirus », mais qui, en réalité, déposait une balise pour Cobalt Strike. Dans un autre cas (que nous examinerons plus loin dans ce rapport), un voleur d'informations prétendait vendre de grandes quantités de données sur des citoyens ukrainiens et des organisations gouvernementales. Il n'a fait aucune demande de rançon, mais simplement menacé d'exposer ces données.

Par ailleurs, l'Ukraine et la Russie, bien qu'étant des pays distincts, ont des citoyens qui sont depuis longtemps des partenaires dans la criminalité (au sens propre), avec de multiples gangs de ransomware utilisant des filiales basées dans les deux pays. Lorsque la guerre a éclaté, certains gangs semblent s'être dissolus dans un élan de nationalisme.

Plus surprenant encore, la scission entre membres russes et ukrainiens des gangs de ransomware et de leurs affiliés pourrait avoir donné naissance à Conti Leaks, une sorte de « dump » de journaux de chats du groupe de ransomware. Un compte Twitter éphémère appelé @TrickbotLeaks puis doxxed a révélé des informations personnelles ou privées sur les membres présumés des groupes criminels Trickbot, Conti, Mazo, Diavol, Ryuk et Wizard Spiders.

Quelles informations pouvons-nous tirer de toute cette tragédie ? Des preuves supplémentaires que, comme l'affirment de nombreux chercheurs occidentaux depuis des années, le FSB (Service fédéral de sécurité de la Fédération de Russie) est étroitement lié à un certain nombre de groupes de ransomware, et pourrait même avoir passé un contrat avec ces entités pour des incursions spécifiques de Conti.

Hélas, aucun de ces conflits fratricides n'a entraîné une baisse significative ou durable de l'activité des ransomwares dans le monde. Même si 2022 a débuté par de multiples arrestations par des agents du FSB de membres du groupe de ransomware-as-a-service REvil (en janvier) et d'un gang de carding anonyme (en février), allant jusqu'à l'extradition d'un membre de REvil vers les États-Unis pour y être jugé début mars ; en milieu d'année, ce type de collaboration internationale en matière de lutte contre la criminalité semblait impensable. Et certains signes indiquaient que REvil, ou un autre logiciel se faisant passer pour ce service, s'était déjà réveillé. Pendant ce temps, la guerre se poursuit…

L'économie des malwares

Si le paysage des menaces a beaucoup évolué ces douze derniers mois, le développement continu de l'économie cybercriminelle est sans doute la tendance la plus marquante. Cet écosystème s'est transformé en un secteur d'activité à part entière, avec un réseau de services connexes et des processus opérationnels bien établis et professionnalisés.

Ce marché de la cybercriminalité a suivi le même modèle que les groupes informatiques, qui proposent des offres « as-a-service ». Les courtiers en accès (IAB), les ransomwares, les malwares voleurs d'informations, la diffusion de logiciels malveillants et d'autres éléments de cybercriminalité ont permis l'entrée sur le marché d'aspirants cybercriminels.

Cette tendance s'explique en partie par l'émergence de l'économie de la cybercriminalité. Les marchés criminels tels que Genesis permettent aux cybercriminels novices d'acheter des malwares et des services de déploiement, puis de vendre en masse des identifiants volés et d'autres données. Les courtiers en accès exploitent les logiciels vulnérables pour s'introduire sur des centaines de réseaux, puis les vendre à d'autres criminels, en monnayant souvent le même accès exploité plusieurs fois. Quant aux groupes affiliés de ransomware et autres attaquants, ils achètent des identifiants et l'accès pour effectuer des activités criminelles à plus haut risque et à plus haute récompense.

L'industrialisation des ransomwares a permis de transformer les groupes affiliés en entreprises plus professionnelles spécialisées dans l'exploitation. À travers l'utilisation d'outils professionnels de sécurité offensive, de logiciels légitimes pour l'administration et le support technique, de malware as-a-service et d'autres exploits et logiciels malveillants accessibles sur le marché, nous assistons à une convergence des acteurs autour d'ensembles d'outils, de tactiques et de pratiques qui ne peuvent plus être associés à des opérations de ransomware spécifiques, à de l'espionnage d'État ou à d'autres motifs spécifiques. Ces groupes professionnalisés se spécialisent dans l'obtention (ou l'achat) d'accès pour le compte de tout acteur motivé et prêt à payer — ou, dans certains cas, pour plusieurs acteurs aux motivations multiples.

À bien des égards, ces groupes ont imité l'industrie du cloud et des services web dans leurs business models. Comme le secteur de l'informatique a adopté le modèle « as-a-service » pour une grande partie de ses opérations, presque tous les composants du toolkit de la cybercriminalité peuvent être confiés à des fournisseurs de « crime-as-a-service » qui font leur promotion sur les sites Web clandestins. Nous présenterons brièvement ces neuf composants et réserverons le dixième pour une discussion plus approfondie.

Les neuf vilains petits canards

Accès 'as-a-service' : Les accès aux comptes et aux systèmes compromis sont vendus à l'unité ou en gros par le biais de services clandestins, notamment le protocole RDP (Remote Desktop Protocol) et les identifiants VPN, les comptes, les bases de données, les web shells et les vulnérabilités exploitables.

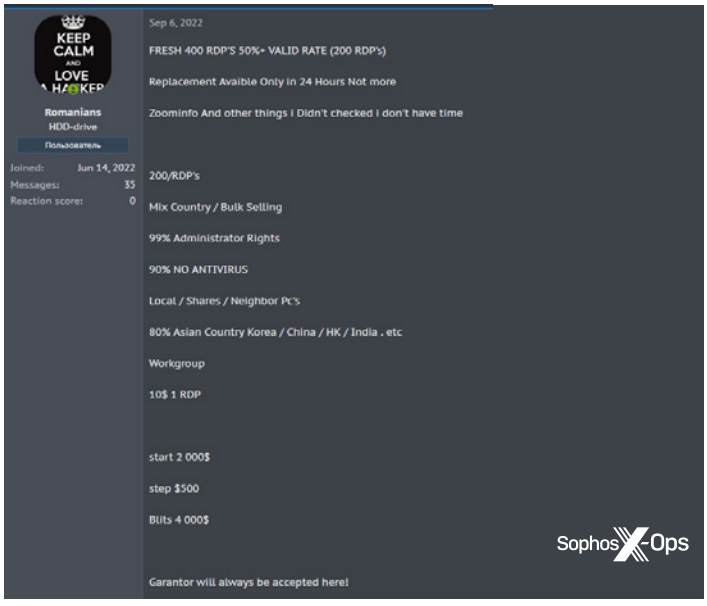


Fig. 3. Un courtier en accès, cherchant une vente rapide, vante ses mérites.

Fig. 4. Données d'une société européenne en vente aux enchères

Distribution/diffusion de malwares « as-a-service » : Faciliter la distribution de malwares dans des zones géographiques ou des secteurs spécifiques, voire plus largement. Dans les annonces que nous avons vues pour ces services, le mode opératoire n'est pas clairement identifiable pour chaque cas, mais, parmi les vecteurs possibles, on peut citer les attaques par « point d'eau », l'exploitation de vulnérabilités ou les croisements avec les listes AaaS (Access-as-a-service).

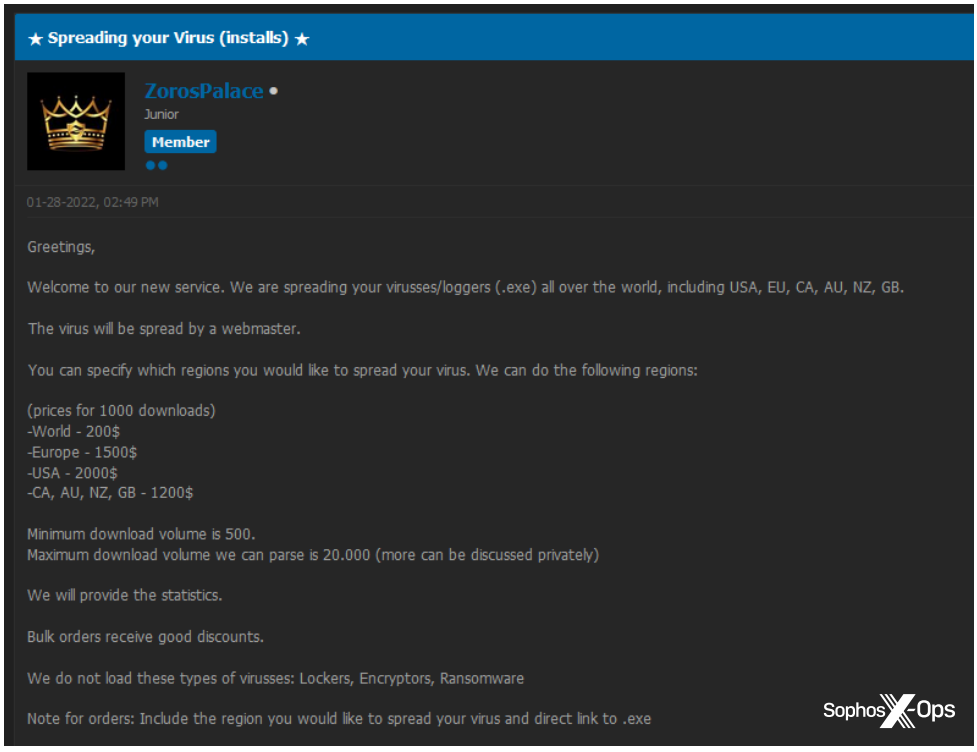
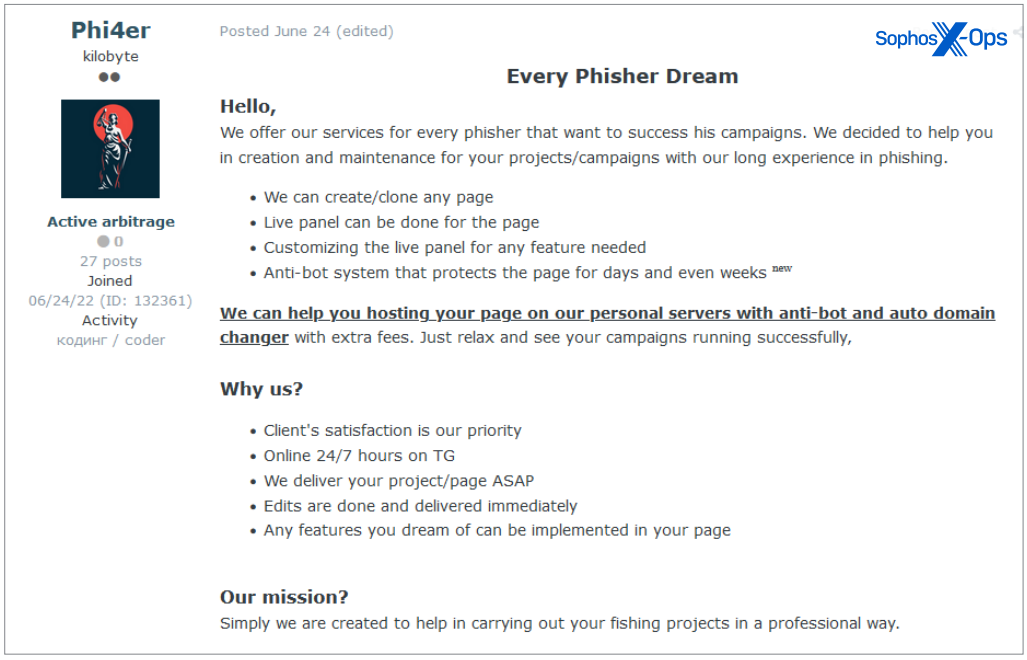


Fig. 5. Un service naissant propose des services de diffusion de logiciels malveillants.

Phishing 'as-a-service' : Les cybercriminels offrent des services de bout en bout pour les campagnes de phishing, comprenant sites clonés, hébergement, emails conçus pour contourner les filtres antispam et tableaux de bord pour surveiller les résultats.



Phi4er
kilobyte
●●

Active arbitrage
● 0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

Sophos X-Ops

Every Phisher Dream

Hello,

We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks new

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

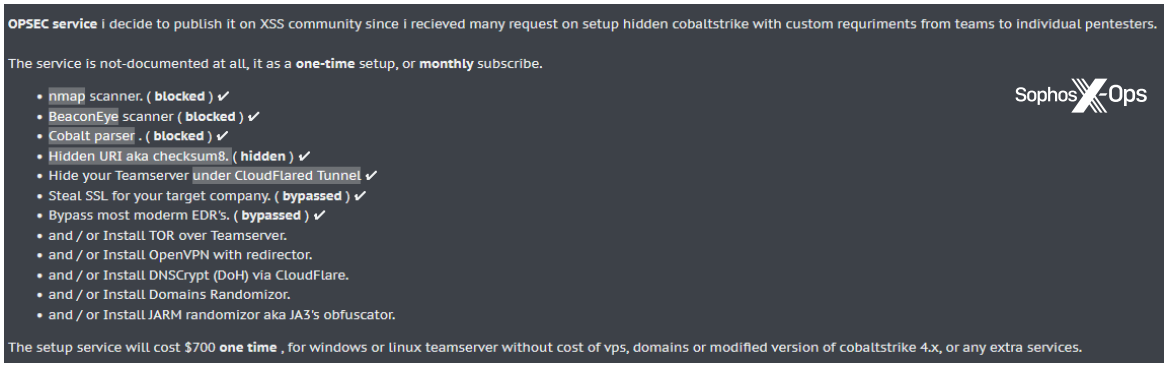
- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?

Simply we are created to help in carrying out your fishing projects in a professional way.

Fig. 6. Suite de services de phishing proposée avec une garantie de service après-vente.

OPSEC 'as-a-service' : Un service particulièrement intéressant, que nous avons vu regroupé avec Cobalt Strike sur un forum criminel. Le vendeur propose d'aider les acheteurs en fournissant un service OPSEC, en usage unique ou en abonnement mensuel, conçu pour cacher les infections de Cobalt Strike et minimiser le risque de détection et d'attribution.



OPSEC service i decide to publish it on XSS community since i recieved many request on setup hidden cobaltstrike with custom requriments from teams to individual pentesters.

The service is not-documented at all, it as a **one-time** setup, or **monthly** subscribe.

Sophos X-Ops

- nmap scanner. (**blocked**) ✔
- BeaconEye scanner (**blocked**) ✔
- Cobalt parser . (**blocked**) ✔
- Hidden URI aka checksum8. (**hidden**) ✔
- Hide your Teamserver under CloudFlared Tunnel ✔
- Steal SSL for your target company. (**bypassed**) ✔
- Bypass most moderm EDR's. (**bypassed**) ✔
- and / or Install TOR over Teamserver.
- and / or Install OpenVPN with redirector.
- and / or Install DNSCrypt (DoH) via CloudFlare.
- and / or Install Domains Randomizor.
- and / or Install JARM randomizor aka JA3's obfuscator.

The setup service will cost $700 **one time** , for windows or linux teamserver without cost of vps, domains or modified version of cobaltstrike 4.x, or any extra services.

Fig. 7. Des fournisseurs de services spécialisés aidant les attaquants à effacer leurs traces.

Chiffrement 'as-a-service' : Service couramment proposé à la vente sur de nombreux forums, le chiffrement en tant que service permet de chiffrer les malwares pour éviter la détection, notamment par Windows Defender et SmartScreen — et par les autres antivirus dans une moindre mesure. Dans l'exemple ci-dessous, le service était proposé à 75 $ pour un achat ponctuel et à 300 $ pour un abonnement d'un mois, avec utilisation illimitée du service.

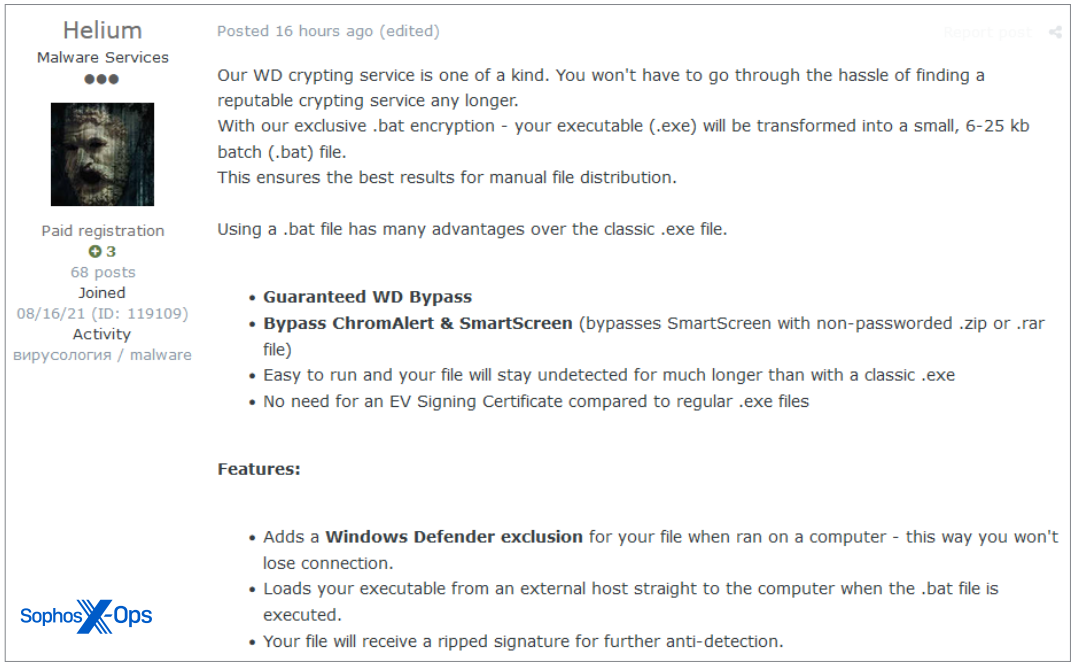


Fig. 8. Pour échapper à la détection, un service spécialisé propose de transformer des fichiers .exe en fichiers .bat.

Scamming 'as-a-service' : Autre exemple de publicité que l'on peut voir sur les forums criminels : les « scamming kits » ou kits pour arnaque, particulièrement liés aux escroqueries de cryptomonnaie. Il n'est pas toujours évident de savoir exactement ce qu'ils contiennent, mais l'un d'entre eux proposait notamment une « Elon Musk Giveaway BTC Scampage » pour 450 $. Il s'agit d'une arnaque en vogue depuis au moins 2018, qui a fait le tour de Twitter, Medium et même l'objet d'une vidéo de deepfake.

Vishing 'as-a-service' : Un vishing est un service de phishing vocal qui consiste pour le cybercriminel à louer un système vocal pour recevoir des appels, avec un « système d'intelligence artificielle », qui permet au locataire de faire parler les victimes à un bot plutôt qu'à un humain.

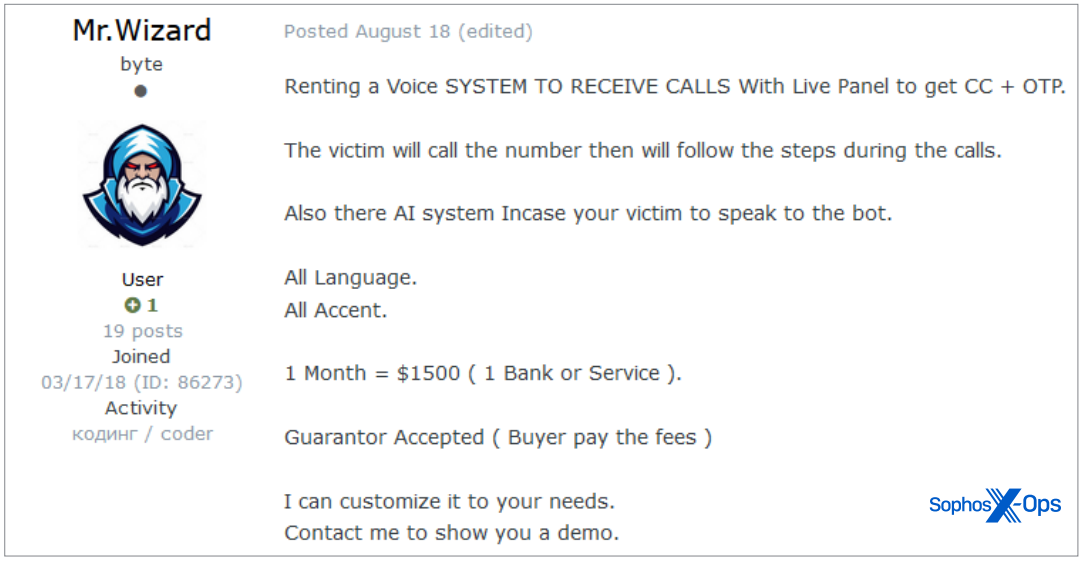


Fig. 9. Offre de type vishing-as-a-service qui comprend « toutes les langues, tous les accents ».

Spamming 'as-a-service' : Un vieux classique, mais toujours prévalent sur les forums criminels, le spamming as-a-service propose l'envoi de spam en masse via divers mécanismes, dont le SMS et l'email. Dans certains cas, le cybercriminel propose de mettre en place toute l'infrastructure à partir de zéro ; dans d'autres, il exploite l'infrastructure existante pour envoyer des messages indésirables personnalisés.

Scanning 'as-a-service' : Pour finir, un service particulièrement intéressant proposé sur un forum criminel, qui offre aux utilisateurs l'accès à une série d'outils commerciaux légitimes — tels que Metasploit, Invikti, Burp Suite, Cobalt Strike et Brute Ratel — afin d'identifier (et, vraisemblablement, exploiter) les vulnérabilités. Comme le montre la figure 10, les acheteurs peuvent bénéficier de remises importantes. Toute l'infrastructure est apparemment créée et maintenue par le vendeur, qui ajoute par ailleurs « qu'il ne reste plus qu'à attendre le résultat du scan dans sa boîte de réception ».

Fig. 10. Fournisseur de scanning as-a-service donne accès à diverses suites d'outils commerciaux populaires.

Une professionnalisation sophistiquée

À mesure que l'industrie du « as-a-service » se développe et que le commerce de la cybercriminalité se banalise, l'interface de ces marchés évolue. Sur un forum dominant par exemple, les utilisateurs peuvent payer un espace publicitaire et afficher des bannières animées pour les milliers d'autres utilisateurs du forum. Notez que l'une des publicités de l'exemple ci-dessous porte sur Genesis, le marcketplace populaire dont nous avons déjà parlé.

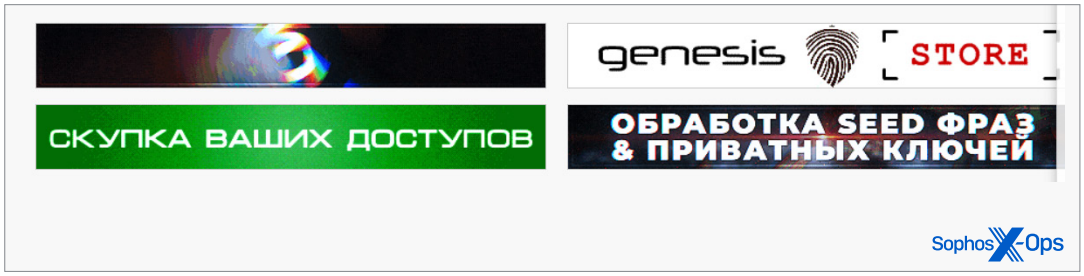


Fig. 11. Un forum criminel héberge des publicités pour divers marketplaces et services.

De plus, les cybercriminels s'aperçoivent de plus en plus des bénéfices d'une mise en page et d'une conception graphique professionnelles. S'il y a quelques années, les offres de malwares et de services se faisaient généralement sous la forme de messages simples, avec beaucoup de texte contenant la liste des fonctionnalités et caractéristiques, les offres d'aujourd'hui sont souvent accompagnées d'images accrocheuses conçues pour apporter aux produits professionnalisme et légitimité pour les aider à sortir du lot.

Fig. 12. Le service Zed Point promet de fournir des informations pour faciliter la modification ou le vol d'identité.

Fig. 13. NoCryi collecte et maintient l'accès aux cookies de session volés.

Les marketplaces ne font pas seulement la publicité de produits et de services. Avec l'économie criminelle qui continue de croître et de se professionnaliser, les offres d'emploi et de recrutement sont devenues monnaie courante. Plusieurs marketplaces de premier plan disposent de pages d'aide dédiées, aussi bien pour ceux qui cherchent un emploi (habituellement en tant que « pen-testers », un euphémisme souvent employé pour les affiliés de ransomware) que pour ceux qui recrutent du personnel.

0

[JOB - BTC/XMR] I operate dozens of phishing websites of all kinds. Looking for some "marketers" who can bring people in for a 50/50 split

by **/u/carderman** • 1 week ago in **/d/Jobs4Crypto**

Like the title states, I've got a bunch of different custom-built phishing websites, ranging from fake darknet markets, fake crypto exchanges, email templates with fake giveaways & crypto promos, fake carding sites, simple landing pages, and so on.

I'm looking for someone or someones who'd like to bring people in, via spamming, social engineering, whatever method works for you... and if they take the bait, we split their generous donations 50/50.

I've had some of these up for anywhere from over a year to some I just created this week. These sites bring in a decent chunk of change as they are, but I've never been opposed to more money.

If interested in getting started, or simply learning more about them, just DM me and I can send you some links and you can choose which ones you think you might be able to do something with.

We can keep track of which ones are yours using a coupon code or custom "referral" url. I have a couple ideas for making sure we're on the same page when it comes to keeping track of which "sales" are yours. I'm keen to ensure you're compensated fairly for the hits you bring in because that's just good business - this shit is already passive AF and basically free money for me at the end of the day. But If you can bring in more free money then I'm more than happy to keep you happy if that means you'll keep selling.

Hell, if you're really good, I'd be more than happy to give you the lions share.

Let's make some money, ladies!

SophosX-Ops

Fig. 14. Les alliances entre entités ayant des compétences différentes permettent d'accroître l'efficacité.

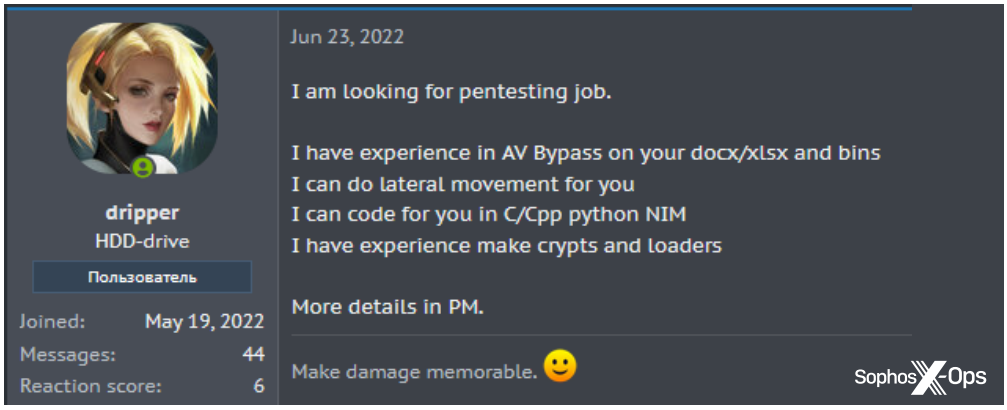


Fig. 15. Un « pen-tester » expérimenté cherche à travailler avec une entité établie.

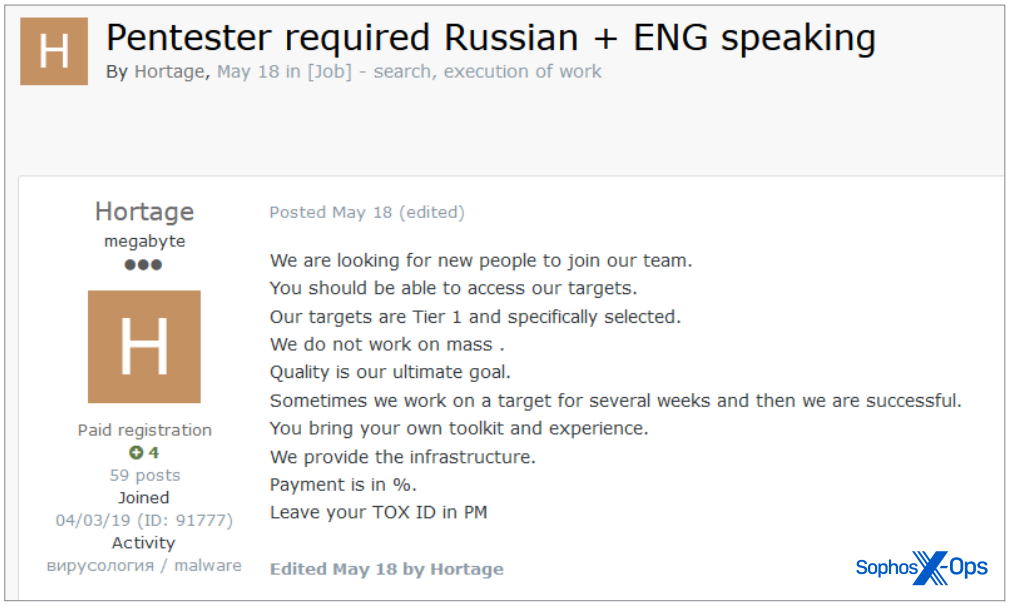


Fig. 16. Un gang criminel établi cherche des membres supplémentaires.

Infostealers ou voleurs d'informations

Les services spécialisés dans le vol de données font partie intégrante de cette infrastructure de soutien à l'économie des malwares et s'apparentent aux offres « as-a-service » que nous venons de voir, mais de manière plus généralisée. Grâce aux offres de malwares as-a-service et de déploiement de malwares as-a-service, les cybercriminels novices peuvent commencer avec un faible investissement et peu de compétences — si ce n'est la capacité à ouvrir une session dans les panneaux de commande Web — pour accéder aux marketplaces des identifiants.

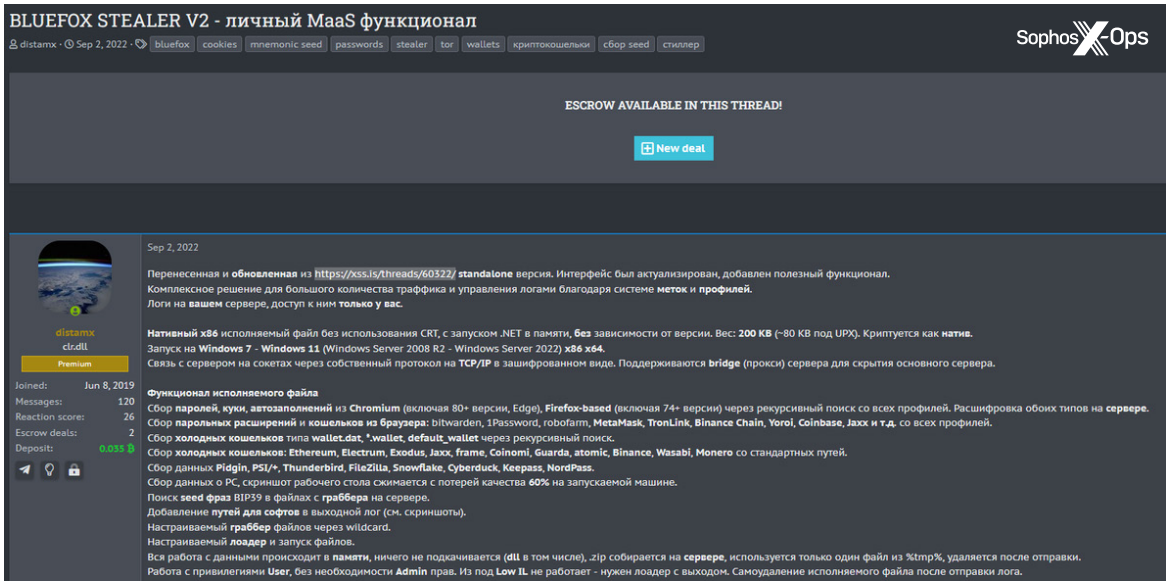


Fig. 17. Les services de vol de données prospèrent dans l'écosystème de la cybercriminalité spécialisée.

Ils peuvent alors revendre ces identifiants volés dans différents marketplaces souterrains. Dans certains cas, ces identifiants ne sont que des collectes accessoires d'informations, recueillies via des transactions de cryptomonnaie volées et d'autres méthodes de monétisation de malwares.

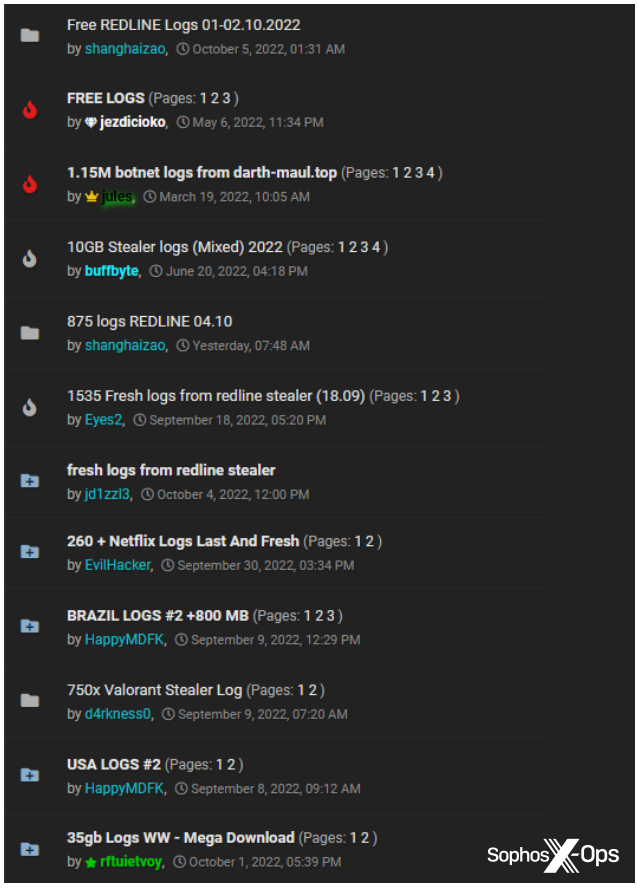


Fig. 18. « Journaux » volés à vendre comprenant mots de passe et autres identifiants

Les opérateurs des infostealers savent très bien que les spécialistes de la cybersécurité s'intéressent à leurs agissements et, fidèles à eux-mêmes, y voient une opportunité d'en tirer profit. XSS, un forum clandestin, a récemment cherchéà monétiser les efforts de « white-hat » ou hackers éthiques de retirer ses forums en proposant un abonnement annuel de 2 000 $ pour un accès sans entrave à la collecte de données.

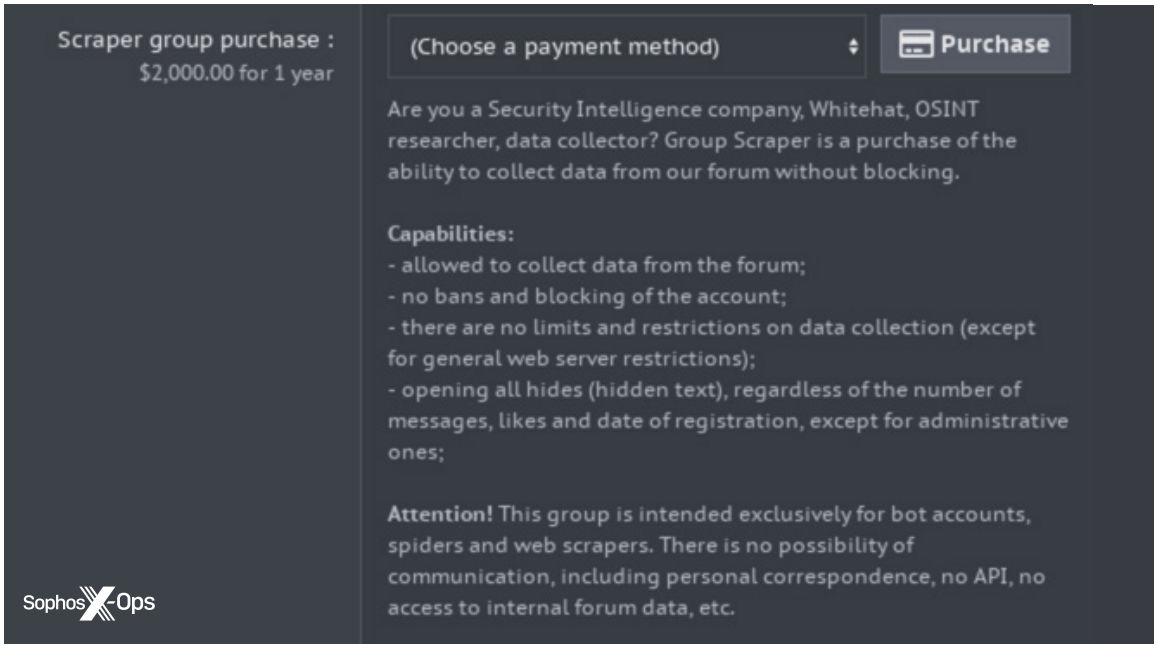


Fig. 19. Un forum offre un accès payant aux consultants désignés comme « blue-hat scrapers » qui tentent de garder un œil sur les activités criminelles. (La deuxième image présente le texte traduit du russe à l'anglais).

Le terme « Infostealer » est très général. Il englobe divers types de malwares évoqués dans d'autres chapitres de ce rapport, notamment les outils d'accès à distance (RAT), les enregistreurs de frappe, les « clippers » axés sur les cryptomonnaies ainsi que d'autres logiciels malveillants qui s'emparent des identifiants, des cookies de navigateurs, des transactions en cryptomonnaies ou de toute autre donnée pouvant être rapidement volée et vendue, ou réutilisée à d'autres fins malveillantes.

Les infostealers ont fourni les cookies Slack utilisés par le gang Lapsus$ pour accéder au réseau d'entreprise d'Electronic Arts en 2021. Ils ont également été impliqués dans d'autres activités malveillantes plus récentes qui ont exploité des jetons de session volés pour des applications Web en vue d'obtenir un accès plus persistant et plus étendu, allant de la compromission de la messagerie professionnelle aux attaques par ransomware.

Infostealers classés en fonction du pourcentage de machines individuelles

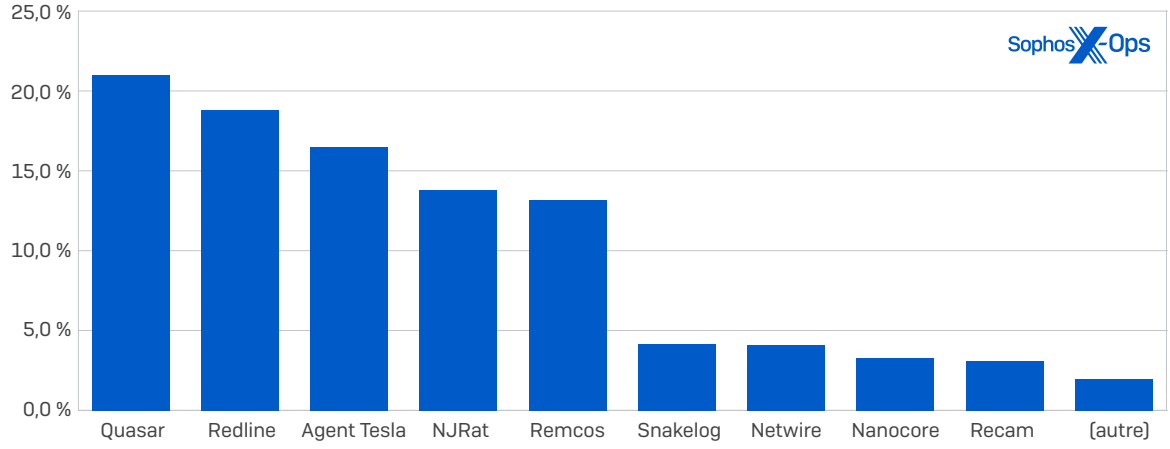


Fig. 20. Quasar, Redline et Agent Tesla sont responsables de la majeure partie des malwares voleurs d'informations ayant été découverts ; Quasar ayant été trouvé sur plus d'un cinquième des machines infectées sur une période de six mois.

Les plus aguerris en matière d'infostealers remarqueront certainement l'absence dans la figure ci-dessus du célèbre Raccoon Stealer. Après une entrée en scène en 2019, les malwares basés en Ukraine et axés sur Windows ont temporairement disparu du paysage au début de 2022 suite à l'action du FBI en collaboration avec les autorités néerlandaises et italiennes, pour revenir ensuite avec une nouvelle équipe dirigeante. En juin a débuté le développement d'une nouvelle version, et en septembre, la version finalisée a été annoncée sur le canal Telegram des auteurs. Mais malgré cette annonce, nous avons vu jusqu'à présent très peu de cas récents du nouveau Raccoon Stealer. Fin octobre, le ministère de la Justice américain a dévoilé un acte d'accusation qui incrimine un ressortissant ukrainien actuellement détenu par les Pays-Bas pour conspiration en vue d'exploiter ce service.

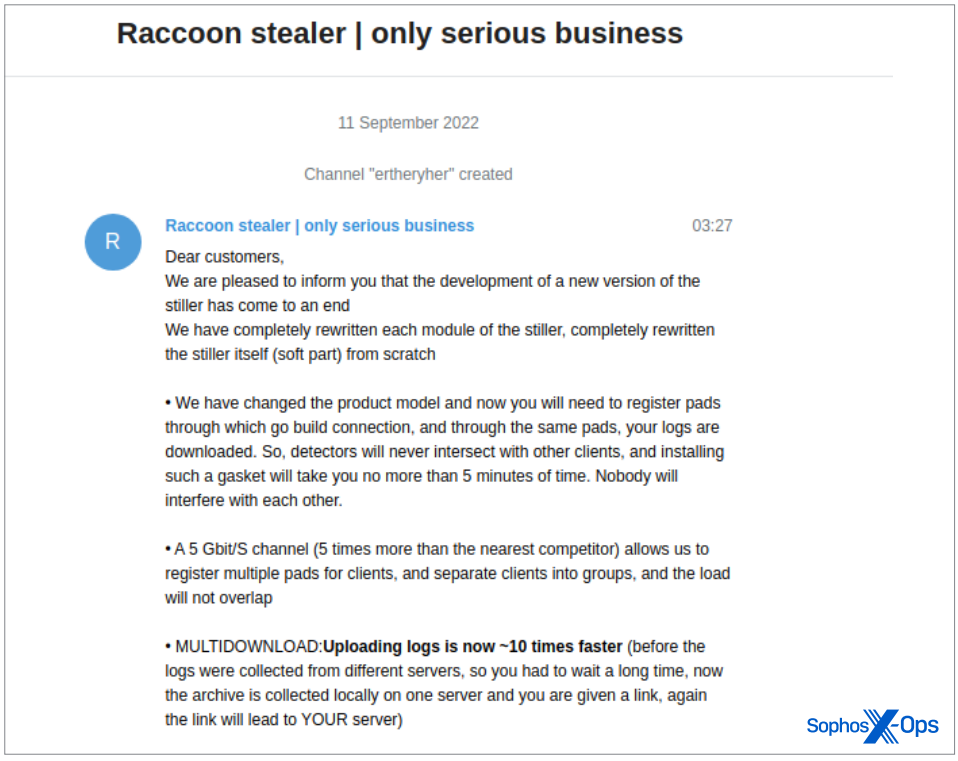


Fig. 21. Raccoon Stealer a annoncé sa dernière version sur la chaîne Telegram du groupe en septembre.

Les infostealers se propagent par le biais de plusieurs méthodes. L'une des plus courantes est l'offre téléchargeable as-a-service basée sur l'ingénierie sociale. Son principe : inciter les utilisateurs à se procurer des fichiers d'archives ou des images disque censés contenir des programmes d'installation de logiciels légitimes, généralement vantés comme des versions « craquées » contournant les schémas de licences. Les téléchargements contiennent également des programmes d'installation de plusieurs malwares. Ces sites de téléchargement utilisent des techniques d'optimisation des moteurs de recherche pour se hisser en tête de toute recherche de logiciels « piratés ». D'autres méthodes de distribution se monnayent via des réseaux zombies tels qu'Emotet ou Qakbot/Qbot.

Certains infostealers, comme Agent Tesla, recourent généralement à des approches plus ciblées, en créant des emails malveillants destinés à un groupe spécifique de victimes. Ceux-ci contiennent des pièces jointes déguisées en documents urgents, qui sont en réalité des programmes d'installation de malwares.

Mais les infostealers peuvent être déployés de manière encore plus ciblée. Sophos a pu observer des cas où des intrus sur un réseau ont utilisé une porte dérobée déployée via Cobalt Strike pour lancer des malwares voleurs de cookies ainsi que d'autres malwares voleurs d'identifiants depuis le réseau. Le but était de recueillir des cookies de navigateur provenant de systèmes comprenant un serveur, qui pourraient ensuite être utilisés pour obtenir un accès en tant qu'utilisateur légitime aux ressources en ligne de l'organisation en vue de se déplacer ultérieurement sur le réseau.

Sophos a déployé un certain nombre de mesures pour bloquer les infostealers et a ajouté une protection contre le vol de cookies pour empêcher ces programmes malveillants de collecter des cookies de session.

L'évolution des ransomwares

Bien que les groupes de ransomware aient été quelque peu perturbés au cours des douze derniers mois en raison (entre autres) de l'agitation géopolitique et des poursuites judiciaires occasionnelles, de nouveaux groupes sont nés à partir des anciens, et les ransomwares demeurent l'une des menaces cybercriminelles les plus répandues pour les organisations. Les opérateurs de ransomware continuent de faire évoluer leurs activités et leurs modes d'action, à la fois pour échapper à la détection et pour intégrer de nouvelles techniques.

Certains groupes de ransomwares ont adopté de nouveaux langages de programmation dans le but de rendre la détection plus difficile, de faciliter la compilation de l'exécutable du ransomware pour qu'il fonctionne sous différents systèmes d'exploitation ou plateformes, ou simplement du fait que les personnes qui développent les charges utiles des malwares apportent leurs outils et leurs compétences. Le langage de programmation Rust a été adopté par les développeurs des ransomwares BlackCat et Hive, tandis que le malware de BlackByte a été écrit avec Go (alias GoLang).

Le ransomware le plus répandu observé lors des interventions de Sophos Rapid Response au cours des dix premiers mois de 2022 a été LockBit, suivi de près par BlackCat et Phobos. (Notons toutefois que la catégorie « Autres » englobe plus du cinquième des familles identifiées, indiquant que le spectre des ransomwares ne se limite pas à quelques familles connues.) La distribution est sans doute assez proche de la distribution globale réelle des attaques de ransomware dans le monde entier.

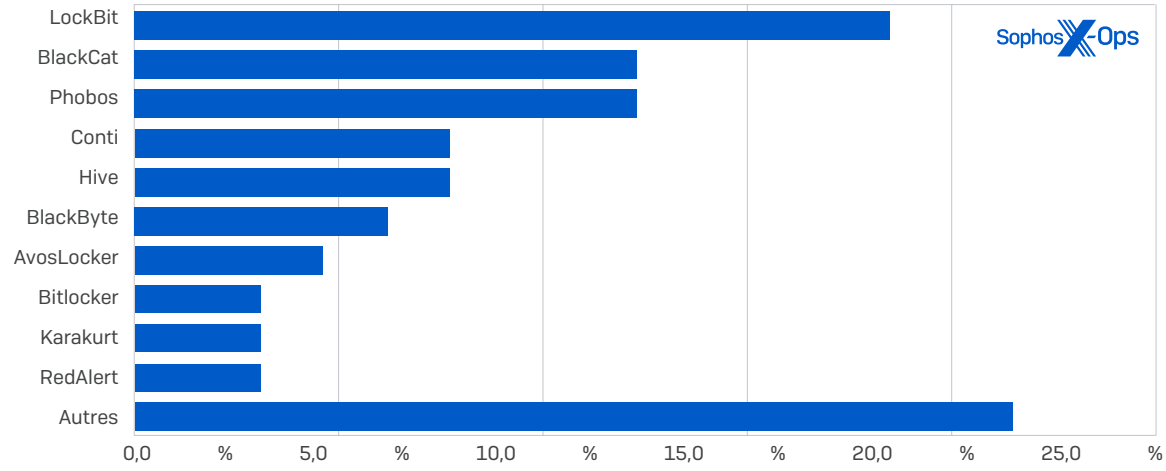


Fig. 22. Des menaces de premier plan comme LockBit, BlackCat et Phobos sont courantes, mais le spectre de menaces varie grandement.

En plus de diversifier les langues utilisées, les ransomwares ont également changé de cible, ne se concentrant plus uniquement sur Windows. RedAlert ou N13V, chiffrent les serveurs Windows et Linux ESXi, tout comme Luna (une autre souche de ransomware basée sur Rust). Mais il ne s'agit pas seulement des joueurs de seconde zone : les chercheurs ont aussi repéré une variante Linux-ESXi de LockBit en début d'année. L'évolution dans les plateformes ciblées signifie plus d'opportunités pour les cybercriminels : une surface d'attaque plus vaste, plus de pression sur les victimes et potentiellement moins de risque de détection, car la majorité des mesures anti-ransomware se concentrent sur Windows. Nous examinerons plus loin dans ce rapport les menaces qui pèsent sur Linux, Mac et les plateformes mobiles.

Nous avons également observé certains progrès dans la façon dont les ransomwares sont déployés sur les systèmes compromis. En effet, deux incidents de ransomware que les SophosLabs ont analysés plus tôt cette année — l'un impliquant Darkside, l'autre le ransomware Exx — concernaient l'utilisation détournée d'applications par ailleurs bénignes pour le chargement latéral de DLL. Dans le cas de Darkside, le cybercriminel a utilisé un logiciel antivirus sain ; avec Exx, c'était une mise à jour de Google. Après des années de succès avec certains attaquants de cibles niches, le chargement latéral de DLL est en train de gagner en popularité auprès des cybercriminels, car il peut leur permettre d'échapper à la détection en exécutant des charges utiles malveillantes se faisant passer pour des processus légitimes.

Pour ce qui concerne les méthodes de livraison et de propagation des ransomwares, les cybercriminels continuent d'improviser et de s'adapter. Nous avons pu notamment observer Impacket, un ensemble de modules Python open-source fonctionnant avec des protocoles réseau, être exploité pour un mouvement latéral sur des réseaux compromis. Les outils d'Impacket comprennent des fonctionnalités d'exécution à distance, des scripts de reniflage (« sniffing » en anglais) ou de dumping d'identifiants, des exploits pour des vulnérabilités connues et des modules d'énumération, ce

qui en fait un package très attrayant pour les opérateurs de ransomwares. Bien que destiné à être un outil de test de sécurité légitime, tout comme Metasploit et Cobalt Strike, ses caractéristiques et fonctionnalités attirent des utilisateurs peu scrupuleux. Dans le même style, nous avons également vu Brute Ratel être utilisé pour propager des charges utiles, comme mentionné plus haut. L'utilisation croissante d'outils de sécurité légitimes (« double usage ») par les attaquants exige que les défenseurs soient scrupuleusement au courant de tout ce qui opère sur leur réseau (et à quelles fins), et de qui a le droit de le faire.

Les groupes de ransomwares semblent également explorer des possibilités plus générales pour diversifier leurs opérations. Un exemple type est la croissance des sites de fuite (leak sites), où les cybercriminels publient les détails de leurs victimes. Le principe de ce modèle est plutôt simple : si l'organisation paie, ses données ne sont pas publiées. Dans le cas contraire, elles le sont. Mais cette année, on a constaté des développements intéressants dans ce domaine.

En tant que l'un des plus grands groupes de ransomwares, LockBit a été en avance sur le peloton à cet égard. Son nouveau site de fuite, qui va de pair avec la nouvelle version de son ransomware, LockBit 3.0 (également connu sous le nom de LockBit Black, sans doute parce que ses nombreuses caractéristiques et une grande partie de son code semblent être basées sur le ransomware BlackMatter), contient quelques fonctionnalités inédites. Par exemple, l'un des moyens de faire de l'argent imaginé par le groupe consiste à offrir aux visiteurs, ou à la victime, la possibilité de détruire ou d'acheter les données volées, ou de prolonger le compte à rebours jusqu'à la publication.

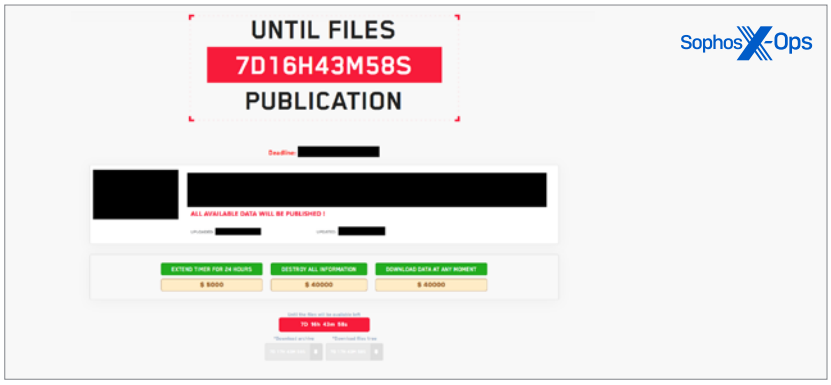


Fig. 23. Des options pour prolonger le compte à rebours du ransomware ou pour télécharger (ou détruire) les données sont présentées à une victime de LockBit.

D'autres groupes de ransomwares, tels que Karakurt et AvosLocker, ont rejoint le mouvement, encourageant les enchères pour les données volées. D'autres encore, comme Snatch, promettent de faire passer leurs fuites en mode abonnement. Certains sites proposent une variante en termes de visibilité après la divulgation. Si la victime paie, non seulement l'information n'est pas rendue publique, mais la fuite elle-même n'est pas rendue publique (ou, si sa situation a été communiquée sur les sites de fuite, cette information est supprimée). La victime peut ainsi se retrouver complice d'une activité de dissimulation qui, dans de nombreux pays, devrait être signalée aux régulateurs.

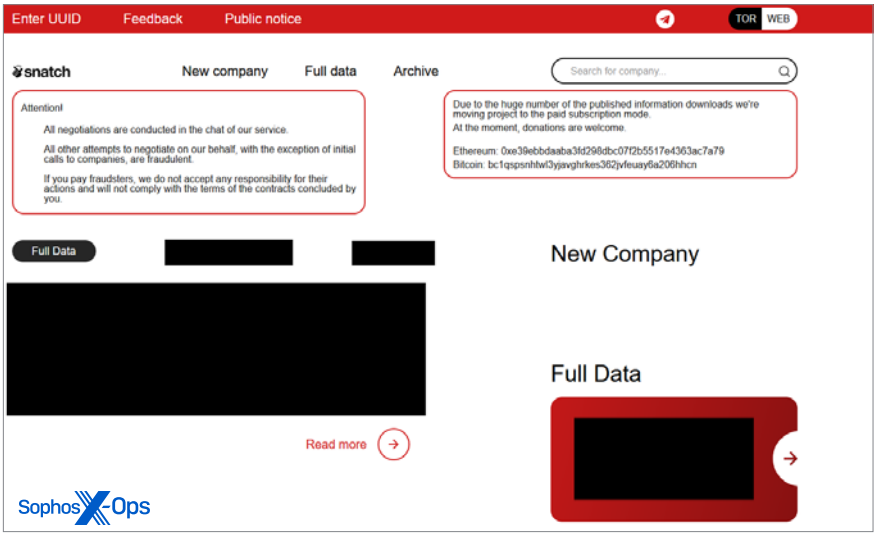


Fig. 24. Le ransomware Snatch passe à un modèle d'abonnement.

Mais LockBit a franchi un palier supplémentaire, en innovant non seulement dans son produit de base, mais aussi dans ses interactions et sa position au sein de la communauté cybercriminelle. Son nouveau site de fuite, par exemple, propose un Bug Bounty, avec une rémunération allant de « 1 000 à 1 million de dollars » offerte pour diverses activités qui, en fin de compte, renforceraient le service :

- La divulgation privée de bugs dans son site Web ou malware
- Un dox réussi sur le chef du propre programme d'affiliation de LockBit, avec des détails sur la façon de procéder, probablement pour que LockBit puisse renforcer son OPSEC. C'est la récompense à un million de dollars.
- Des vulnérabilités dans le messager TOX (un pack de messagerie instantanée fortement utilisé par les cybercriminels)
- Des idées pour améliorer le ransomware LockBit
- Des vulnérabilités en termes de divulgation d'informations dans son domaine de base ou d'autres aspects du réseau TOR

LockBit n'est pas le premier cybercriminel à offrir des Bug Bounty. En novembre 2021, All World Cards, un important gang de carding actif sur plusieurs forums en langue russe, a offert des récompenses allant jusqu'à 10 000 dollars pour les vulnérabilités découvertes dans son store. Et il y en aura sûrement d'autres. Il s'agit d'une méthode efficace de crowdsourcing pour les tests de pénétration et les évaluations de vulnérabilité, tout en garantissant que les résultats restent entre le chercheur et le cybercriminel.

Fig. 25. All World Cards a dévoilé un modeste programme Bug Bounty fin 2021.

Enfin, nous avons relevé quelques groupes de ransomwares ou de fuites moins connus qui, contrairement à certains de leurs homologues plus célèbres, semblent avoir des motivations politiques. Le premier est un site de fuite dédié au partage de ressources provenant d'informations volées de citoyens et d'organisations gouvernementales ukrainiens, bien que l'origine des données et l'implication éventuelle d'un ransomware ne soient pas claires.

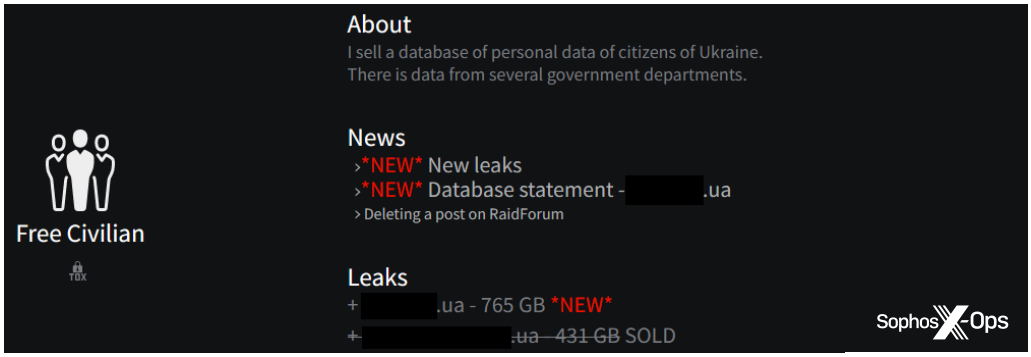


Fig. 26. Civils ukrainiens visés par un attaquant

Nous avons aussi repéré un groupe connu sous le nom de Moses Staff, qui semble cibler les organisations israéliennes avec des tactiques similaires aux ransomwares, mais sans exiger de rançon.

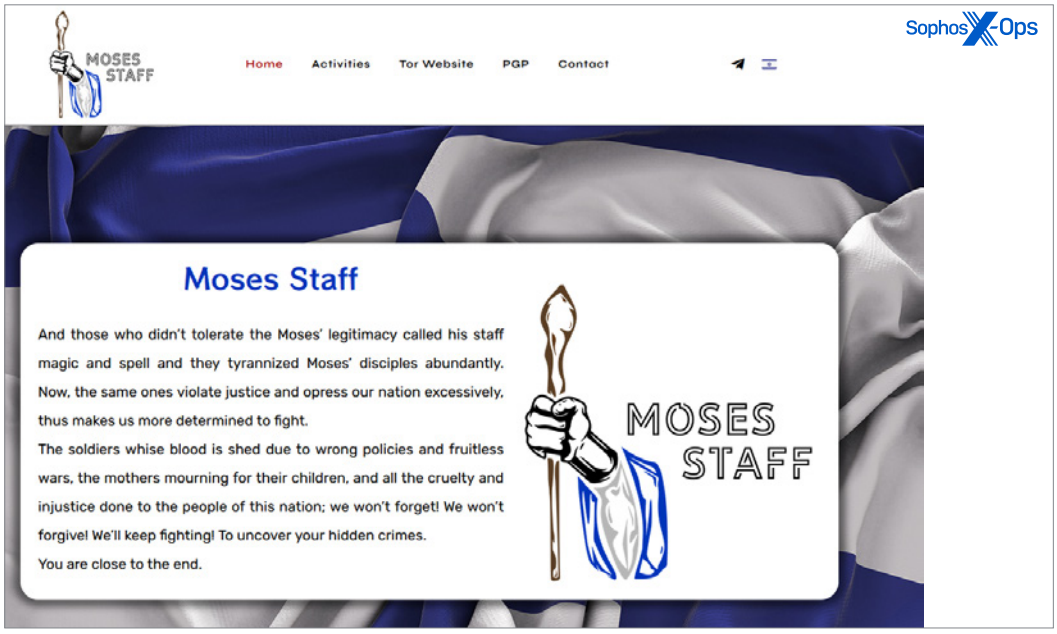


Fig. 27. Groupe anti-Israël qui utilise des tactiques de type ransomware pour harceler

Outils d'attaque

Pour la plupart des acteurs de la sécurité, le « qui » des attaques est moins immédiatement exploitable que le « comment ». Dans cette section, nous verrons comment les attaquants détournent les outils de sécurité offensive à leurs propres fins. Les outils de test d'intrusion sont un cas évident d'exploitation, mais ce ne sont pas les seuls outils de sécurité légitimes compromis. Nous allons brièvement examiner d'autres techniques, y compris l'utilisation d'outils d'accès à distance (RAT) également légitimes. Puis nous parlerons de l'augmentation des « LOLBins », une technique qui exploite des binaires déjà présents sur les systèmes ciblés, et de la recrudescence des attaquants utilisant des pilotes tiers et des DLL par ailleurs légitimes pour introduire du code malveillant à travers les défenses. Nous nous attarderons ensuite sur deux familles de malwares que nous avons trouvées particulièrement intéressantes en 2022 : les ransomwares qui ciblent les mises à niveau de sécurité Endpoint et les logiciels « miners » qui dérobent les ressources des victimes pour créer des cryptomonnaies. Enfin, nous conclurons notre rapport par un aperçu des menaces qui pèsent sur Linux, Mac et les mobiles.

Des outils de sécurité offensive utilisés à mauvais escient

L'utilisation inappropriée des outils de sécurité offensive, c'est-à-dire des logiciels destinés à être utilisés par les équipes de sécurité informatique pour simuler des attaques actives, est monnaie courante dans de nombreuses campagnes de ransomwares. Comme nous l'avons noté l'année dernière, des copies pirates de l'outil de test de pénétration Cobalt Strike sont de plus en plus utilisées par les cybercriminels tels que les affiliés de ransomwares. Les outils open-source développés par les acteurs de la sécurité offensive restent le composant majeur des détections d'outils d'attaque. C'est le cas de l'outil de collecte d'identifiants Mimikatz (dont les versions représentent environ deux cinquièmes des détections d'outils d'attaque dans la télémétrie de Sophos), d'autres outils d'exploitation basés sur PowerShell tels que PowerSploit et les composants « Meterpreter » connectés à la plateforme d'exploitation MetaSploit partiellement open-source.

Mais les copies piratées d'outils de sécurité offensive sont devenues monnaie courante dans les attaques professionnelles plus complexes. Comme nous l'avons vu plus haut, certains groupes passent des annonces pour recruter des individus qui connaissent bien ces outils. Les copies piratées de Cobalt Strike et la version commercialisée de Metasploit sont devenues si courantes que des liens vers des copies gratuites sont fréquemment publiés sur des sites clandestins (même si certaines peuvent en réalité être des malwares).

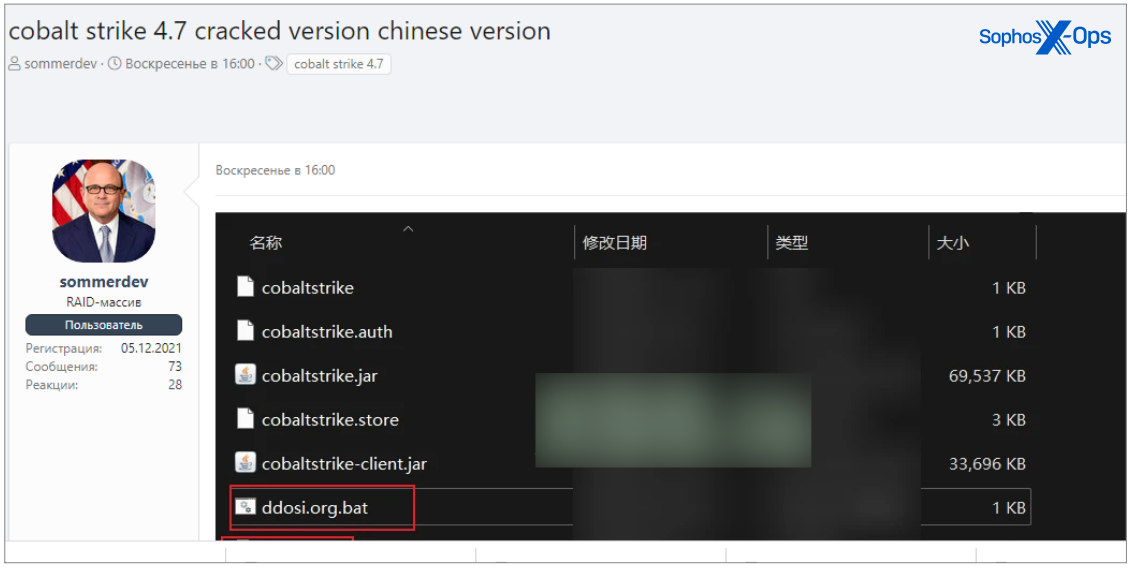


Fig. 28. Version chinoise de Cobalt Strike 4.7 craquée et revendue.

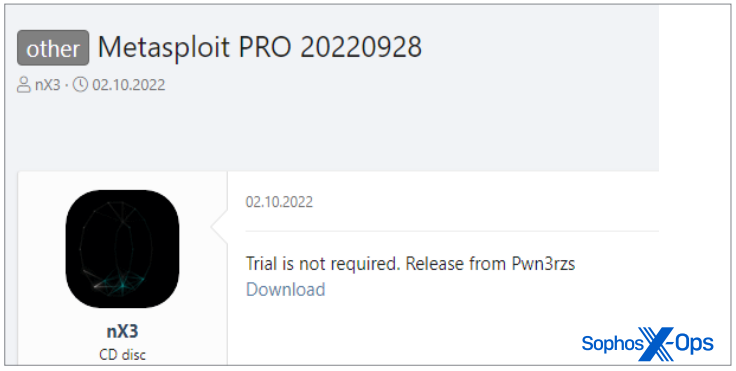


Fig. 29. Version payante de Metasploit craquée et proposée en téléchargement.

Cobalt Strike était en cause dans 47 % des incidents traités par l'équipe Sophos Rapid Response au cours des neuf premiers mois de 2022. Pour la majeure partie, il s'agissait d'opérations ou de préparatifs pour l'opération du ransomware, où des cybercriminels ont été détectés en train d'utiliser des techniques, outils et pratiques typiques des attaques imminentes. Mais Cobalt Strike a également été observé dans le cadre d'attaques contre des états, telles que la campagne SolarWinds en 2020, et d'attaques sur des cibles en Ukraine par des acteurs alignés avec la Russie.

À lui seul, Cobalt Strike représente 8 % de toutes les détections d'outils d'attaque. En plus, son protocole de communication a été intégré à d'autres outils développés par les attaquants. Certaines versions de TurtleLoader, par exemple, se connectent à leur réseau de commande et de contrôle (C2) via le protocole de connexion Metasploit ou Cobalt Strike. Ces acteurs aux multiples outils représentent un défi intéressant pour les experts en cybersécurité, en particulier si ces derniers ont mis en place différentes couches de défense.

Et la surveillance ne s'arrête pas là. À l'heure où nous écrivons ces lignes, par exemple, nous avons constaté une hausse des attaques impliquant Brute Ratel suite à la nouvelle disponibilité de ce toolkit pour les attaquants. Au moment de la publication, les détections de Brute Ratel étaient quasi inexistantes, apparaissant dans moins de 1 % de nos détections en mémoire. Mais ce ne sera certainement plus le cas en 2023, avec la prolifération des cracks pour ce produit.

Détection d'outils d'attaque notables (machines individuelles sur une période de 6 mois)		
Outil d'attaque	**Pourcentage de machines infectées**	**Remarques**
Mimikatz	24,7 %	Outil de post-exploitation de type credential dumping
Apteryx	14,5 %	Version compilée de Mimikatz
Suite PowerSploit	11,7 %	Open source ; plus de support officiel depuis août 2020
SrpSuite	8,3 %	Suite PowerShell open-source de FuzzySecurity
Cobalt Strike	8,0 %	Logiciel propriétaire, souvent piraté/craqué
Meterpreter	7,8 %	Charge utile d'attaque Metasploit open-source ; support commercial disponible
Nishang	6,8 %	Framework et scripts/charges utiles à utiliser avec PowerShell
TheFatRat	6,2 %	Porte dérobée Metasploit open-source/ automatisation des charges utiles
TurtleLoader	5,4 %	Porte dérobée, généralement associée à Metasploit ou Cobalt Strike.
JMeter	5,1 %	Metasploit basé sur Java
Juicy Potato	5,0 %	Exploit BITS open-source (outil d'élévation de privilèges)
winPEAS	4,8 %	Scripts d'élévation de privilèges et de vol d'informations
Swrort	4,6 %	Porte dérobée basée sur Metasploit
Empire	4,5 %	Framework de post-exploitation open-source ; fusion de PowerShell Empire et de Python EmPyre ; plus de support officiel depuis juillet 2019.

Fig. 30 : Pourcentage de machines infectées analysées par Sophos où le nom de l'outil était indiqué, avec des informations complémentaires pour certains outils ; données sur une période de six mois (avril-septembre 2022) et outils détectés sur moins de 4,5 % des machines non détaillés ici par manque de place.

Jusqu'en septembre 2022, le développeur de Brute Ratel a affirmé avoir très peu de contrôle sur l'accès à l'outil via les clauses de licences. Pourtant, des acteurs liés au réseau de ransomware Conti semblent avoir créé de fausses sociétés pour acheter la plateforme, et on a observé au moins un cas de fuite d'une licence par un employé d'un client légitime. Depuis septembre, des copies piratées d'une version récente de Brute Ratel sont largement disponibles sur les marchés clandestins.

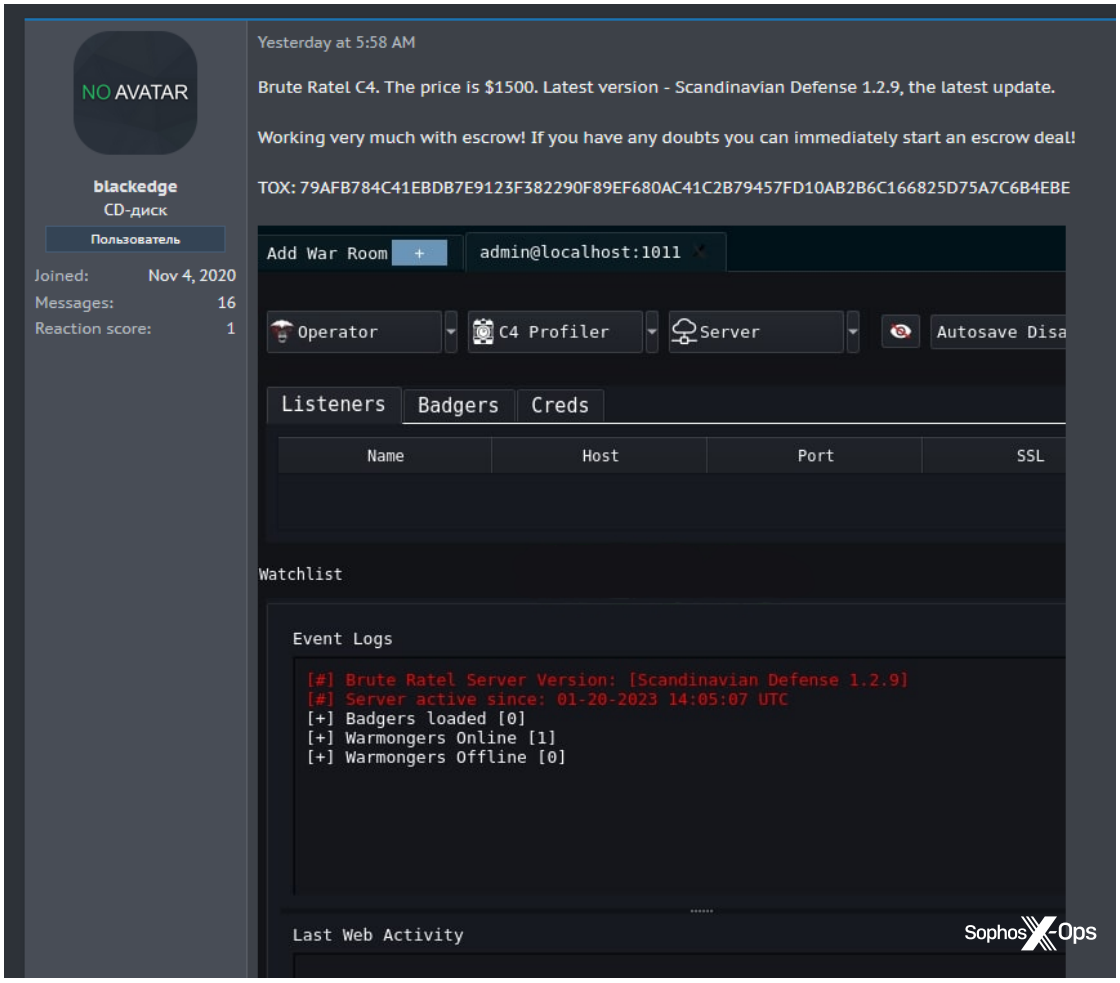


Fig. 31. Une version craquée de Brute Ratel lancée sur le marché clandestin

Jusqu'à présent, nous avons présenté quelques cas d'attaques associées aux composants de Brute Ratel. Lors d'un tri d'incidents par Sophos MDR, nous avons vu des attaquants qui essayaient d'abord d'utiliser Cobalt Strike ; lorsque ce dernier a été détecté et bloqué, ils ont ensuite tenté de déployer Brute Ratel — qui a également été bloqué.

Mais on doit s'attendre à davantage d'incidents de ce type. Peut-être parce que Brute Ratel est plus largement disponible, des recherches récentes ont révélé que ses agents étaient propagés par Qakbot, de la même manière que les balises Cobalt Strike ont été propagées auparavant.

Autres outils de sécurité détournés

Brute Ratel n'est pas le seul toolkit à être utilisé à des fins malveillantes. Les cybercriminels proposent également d'autres outils de sécurité légitimes à la vente sur les marketplaces criminels. On peut citer Core Impact, un framework de test de pénétration, Nexpose, un scanner de vulnérabilités, VirusTotal Enterprise ou encore Carbon Black, une plateforme de protection Endpoint.

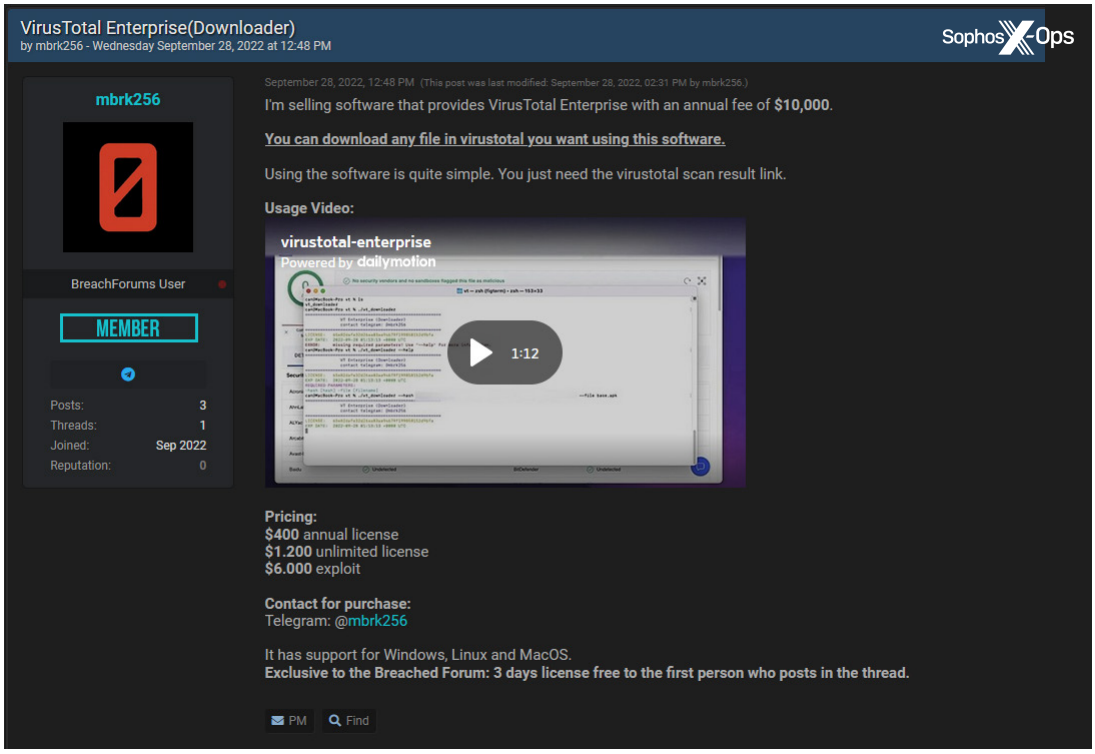


Fig. 32. VirusTotal Enterprise ciblé par des extracteurs de données malveillants.

Les cas d'usage de ces outils parfaitement légitimes par les cybercriminels varient : ils peuvent disséquer les plateformes EDR et de protection Endpoint pour tester les vulnérabilités et les tactiques d'évasion, automatiser l'analyse et l'exploitation des vulnérabilités avec des tests de pénétration et des frameworks d'exploitation, ou encore obtenir des échantillons de malwares et du contre-espionnage avec des outils tels que VirusTotal.

Le double usage des outils d'accès à distance (RAT)

Dans l'éventail de plus en plus large d'outils de sécurité détournés ou simplement exploités, il convient de mentionner tout particulièrement les outils d'accès à distance. Face à la fréquence à laquelle ces outils légitimes sont détournés à des fins illégitimes — servant donc à un « double usage » — les professionnels de la sécurité doivent déployer une surveillance constante des signes d'exploitation et des comportements douteux.

Les outils d'accès à distance sont utilisés pour établir une connexion persistante avec des systèmes compromis à partir desquels ils peuvent lancer des attaques. Parmi les RAT les plus connus, citons :

- NetSupport Manager (NetSupport)
- TeamViewer Remote Access (TeamViewer)
- ConnectWise Control / Screenconnect Remote Access (ConnectWise)
- AnyDesk (AnyDesk Software)
- Atera (Atera Networks)
- Radmin (Famatech)
- Remote Utilities (Remote Utilities)
- Action1 RMM (Action1)

Ces outils peuvent être déployés par les attaquants eux-mêmes ou par des courtiers en accès qui vendent des accès persistants à des réseaux compromis. Certains cybercriminels promeuvent ouvertement un accès via ces outils sur des sites Web clandestins :

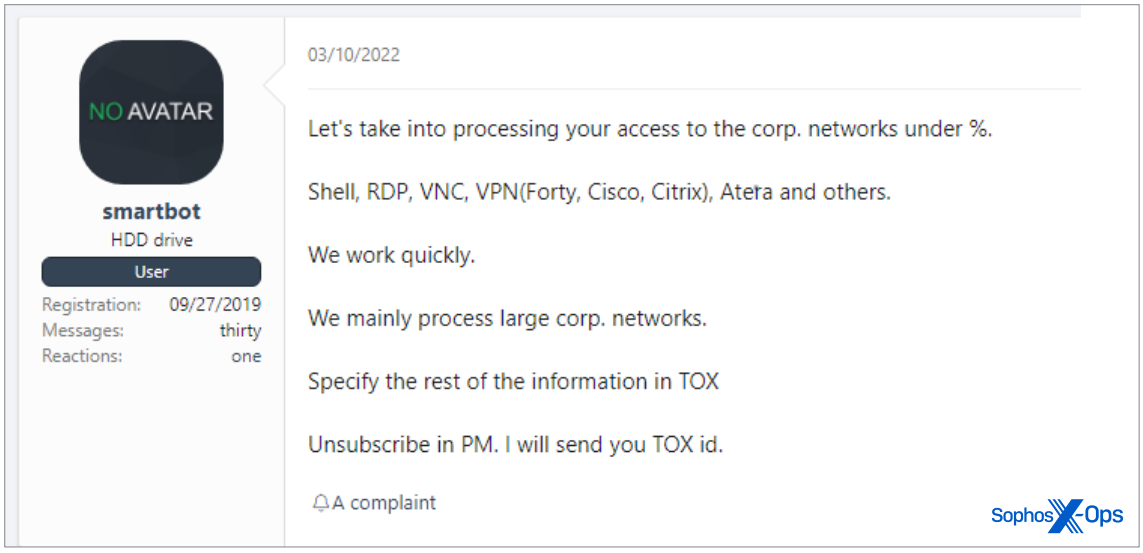


Fig. 33. Offre d'accès à des réseaux compromis via des outils compromis

Atera a été détecté dans le cadre de plusieurs tentatives d'incursions sur lesquelles Sophos a enquêté, notamment dans une série de tentatives de déploiement de malwares exploitant la vulnérabilité Log4J et dans plusieurs cas de ransomware étudiés par l'équipe Sophos Rapid Response. Dans les tentatives d'exploitation de Log4J, qui visaient les serveurs VMWare Horizon, les attaquants ont tenté d'exécuter un script PowerShell à distance pour télécharger et installer l'agent Atera subrepticement avec une licence d'essai (ainsi qu'un autre outil d'accès à distance légitime détourné, Splashtop Streamer). Dans les incidents traités par Sophos Rapid Response, les installations d'Atera ont été réalisées en exploitant des serveurs Microsoft Exchange vulnérables. TeamViewer et AnyDesk ont récemment été détournés par les opérateurs du ransomware BlackCat.

Dans un grand nombre de cas, l'utilisation abusive de ces outils légitimes peut être détectée et bloquée sur la base d'un contexte anormal, comme des événements d'installation étranges (par exemple, une version de NetSupport installée par PowerShell dans un répertoire anormal). Dans certains cas, il est aussi possible de détecter l'abus de ces outils par l'utilisation d'une licence d'essai pour le déploiement. Sophos a déployé des règles de comportement qui détectent l'abus de la licence d'essai d'Atera et continue à développer des techniques de détection comportementale pour le détournement de ce logiciel, mais aussi d'autres solutions d'accès à distance.

LOLBins et exécutables légitimes

L'une des principales caractéristiques des attaques actives, ainsi que de certaines attaques plus automatisées, est l'utilisation des LOLBins ou « Living Off The Land Binaries ». Ces composants natifs de Windows sont exploités par les attaquants pour exécuter des commandes système, contourner les fonctions de sécurité prédéfinies, télécharger et exécuter des fichiers malveillants à distance, et se déplacer latéralement sur les réseaux.

Le principal LOLBin, le shell de commande Windows (cmd.exe), est utilisé par la plupart des portes dérobées et des shells pour exécuter des commandes système et lancer des programmes malveillants, de sorte qu'il est présent dans pratiquement toutes les attaques de malwares sous une forme ou une autre. Chacune des plateformes de script Windows (PowerShell, l'hôte d'application Microsoft HTML [mshta.exe] et l'hôte de script Windows [wscript.exe]) est utilisée comme outil pour exécuter des appels API Windows, télécharger et exécuter d'autres contenus malveillants, exécuter des commandes système et collecter des données. En outre, PowerShell est utilisé par de nombreux outils d'attaque mis au point par les cybercriminels.

Les opérateurs de ransomware prennent aussi souvent le contrôle d'un autre composant de Windows, rundll32.exe, pour charger des malwares propagés au format DLL (Dynamic-Link Library). Mais il existe d'autres exécutables légitimes et signés qui peuvent être exploités de la même manière dans le but d'exécuter une porte dérobée ou un ransomware.

Pour d'autres LOLBins, leur utilisation n'est pas si évidente. L'utilitaire de certificat Windows (certutil.exe), qui peut récupérer le contenu de serveurs Web distants, est fréquemment utilisé par les opérateurs de ransomware et autres cybercriminels pour télécharger et décoder des fichiers malveillants. Bitsadmin.exe, l'utilitaire de ligne de commande du service de transfert intelligent en arrière-plan (ou Background Intelligent Transfer Service en anglais) est utilisé pour déplacer des fichiers vers, depuis et au sein d'un réseau ciblé sans que le processus qui a lancé le transfert doive rester actif, ce qui en fait un outil idéal pour le déplacement latéral de malware ou l'exfiltration de données.

Ce type de comportement peut être détecté et bloqué de plusieurs façons. Les comportements malveillants utilisant PowerShell et d'autres moteurs de script peuvent être détectés par la surveillance de l'interface AMSI (Antimalware Scan Interface) de Microsoft. L'analyse comportementale de l'exécution de LOLBins par des appels système ou à partir d'une ligne de commande permet également de détecter cet abus.

Les dix principaux LOLBins par pourcentage d'ordinateurs affectés		
LOLBin	**Pourcentage de détections brutes**	**Remarques**
cmd	92,26 %	Interpréteur de commande par défaut
powershell	1,79 %	Ligne de commande et script shell plus avancés
certutil	1,09 %	Programme de ligne de commande installé avec les services de certificat
mshta	1,01 %	Microsoft HTML Application Host, permet l'exécution de .HTA (application HTML)
bitsadmit	0,95 %	Service de transfert intelligent en arrière-plan, utilisé avec Windows Update pour le transfert de fichiers
wscript	0,93 %	Windows Scripting Host prenant en charge l'exécution JScript et VBScript
bcdedit	0,83 %	Outil de ligne de commande pour la gestion de Boot Configuration Data
rundll32	0,52 %	Utilisé pour charger et exécuter des DDL 32 bits
nltest	0,39 %	Outil permettant d'obtenir des informations de diagnostic
procdump	0,21 %	Application en ligne de commande qui fournit des informations sur les processus système

Fig. 34. Le fichier omniprésent cmd.exe est de loin la cible la plus fréquente pour les abus LOLBin généralisé sur les systèmes Windows (d'avril à septembre 2022).

La technique du BYOVD — Bring Your Own Vulnerabilities

Outre les LOLBins, d'autres exécutables légitimes sont souvent utilisés dans les attaques de ransomware et autres cybercrimes. Dans ce scénario, les applications exploitées sont fournies par l'attaquant. Dans certains cas, ce sont des exécutables vulnérables qui peuvent être utilisés pour charger latéralement un code malveillant. Ce fut le cas avec un composant archaïque signé par McAfee utilisé dans une attaque de ransomware AtomSilo l'année dernière pour déployer une porte dérobée Cobalt Strike.

Une autre version de cette méthode est la technique du BYOVD ou « Bring Your Own Vulnerable Driver », qui exploite un pilote légitime et signé présentant une vulnérabilité exploitable pour obtenir un accès de bas niveau au système d'exploitation. Par exemple, les chercheurs de Sophos ont découvert que les opérateurs déployant des ransomwares BlackByte abusaient de RTCore64.sys et RTCore32.sys, des pilotes utilisés par l'utilitaire d'overclocking de la carte graphique Micro-Star MSI AfterBurner 4.6.2.15658, largement répandu. En effet, une vulnérabilité dans ces pilotes (CVE-2019-16098) permettait à un utilisateur authentifié de lire et d'écrire dans une mémoire arbitraire, ce qui, dans ce cas, a été exploité pour contourner et désactiver certains logiciels de sécurité.

Parmi les autres incidents récents utilisant la technique BYOVD, on a recensé deux autres cas : en juillet, un attaquant inconnu qui a abusé d'un pilote anti-triche vulnérable pour le jeu Genshin Impact et, en mai, une variante du ransomware AvosLocker qui a exploité un pilote anti-rootkit vulnérable d'Avast. Dans les deux cas, les pilotes ont été exploités pour contourner ou désactiver des logiciels de sécurité.

Au total, l'équipe Sophos Rapid Response a observé une activité suffisante pour déduire un certain nombre de signaux d'alerte utiles indiquant qu'une attaque par ransomware est en cours. Dans une enquête sur les incidents traités au cours des neuf premiers mois de 2022, au moins 83 % des ransomwares ont été précédés de signaux d'alerte. Voici les plus courants, avec leur classification MITRE ATT&CK :

- T1003 — Accès aux informations d'identification — Vidage des informations d'identification du système d'exploitation
  - Dumping des identifiants, en texte clair ou chiffré, pour obtenir des informations de connexion et d'identification du système d'exploitation et du logiciel ciblés.
- T1562 — Évasion des défenses — Altération des défenses
  - Modification ou désactivation des composants de l'environnement de la victime afin de contourner ou de ralentir les dispositifs de défense déjà en place, notamment les mesures préventives et les fonctionnalités d'audit/journalisation.
- T1055 — Elévation des privilèges — Injection dans les processus
  - Injection de code dans l'espace d'adressage des processus de confiance, ce qui permet au code de l'attaquant d'échapper aux défenses ou d'élever ses privilèges. Le préchargement et le chargement latéral de DLL entrent dans cette catégorie.
- T1021 — Mouvement latéral — Services à distance
  - Utilisation de services à distance via des comptes valides/non protégés pour se connecter à un système et effectuer des actions en tant qu'utilisateur connecté, en utilisant peut-être un RAT ou un RAT à double usage comme décrit ci-dessus.
- T1059 — Exécution — Interpréteur de commandes et de scripts
  - Utilisation abusive d'interpréteurs de commandes et de scripts pour exécuter des commandes, des scripts ou des binaires. Peut s'effectuer aussi via des terminaux ou des interpréteurs de commandes interactifs, ou via des services à distance comme mentionné ci-dessus.

Nous avons également repéré d'autres caractéristiques qui, même si elles n'entrent pas dans une catégorie précise, présentent un intérêt pour les cybercriminels :

- 64 % des attaques de ransomware (plus précisément, le déploiement du ransomware) ont commencé entre 22 heures et 6 heures du matin, heure locale.
- La période la plus courante pour le début des attaques est la nuit du lundi au mardi matin.
- L'exfiltration précède d'environ deux jours la phase de demande de la rançon.
- Le temps de séjour moyen de l'attaquant est de 11 jours.

Ransomware ciblant les mises à niveau de la sécurité Endpoint

Dans la liste ci-dessus des signes avant-coureurs d'une attaque de ransomware, la catégorie « T1562 — Évasion des défenses — Altération des défenses » mérite un examen plus approfondi. L'une des évolutions dominantes constatées dans les interventions de Sophos Rapid Response en 2022 témoigne à la fois de la réussite de Sophos à empêcher les ransomwares de causer des dommages et de la reconnaissance de cette réussite par les principaux groupes de ransomwares et leurs affiliés : Désormais, les attaques de ransomware impliquent systématiquement, préalablement au déploiement du malware de chiffrement, des tentatives d'accès aux contrôles qui gèrent la sécurité de la cible.

Comme nous l'avons décrit dans un précédent chapitre, les « adversaires actifs » des ransomwares, c'est-à-dire ceux qui opèrent sur leur clavier pendant l'attaque, utilisent régulièrement des outils de reniflage ou d'extraction de mots de passe dans le but d'obtenir des identifiants admin. Ils exploitent des utilitaires comme Mimikatz, outil créé à l'origine pour renforcer la sécurité, pour renifler et extraire les mots de passe des utilisateurs des réseaux ciblés.

Auparavant, ces mots de passe étaient ensuite utilisés pour prendre le contrôle d'outils de gestion (comme les contrôleurs de domaine Windows) que les attaquants pouvaient exploiter pour déployer le ransomware. Mais dans les attaques plus récentes, les hackers utilisent de plus en plus ces données d'identification pour accéder aux contrôles centralisés qui permettent de gérer la protection de la sécurité Endpoint. Dans certains cas, ils ont immédiatement utilisé ces identifiants volés pour se connecter aux outils de gestion centralisés et désactiver les fonctions antialtération de ces outils de sécurité Endpoint, voire dans certains cas pour désactiver complètement la sécurité Endpoint.

Pour contrecarrer ce type d'attaques, Sophos et d'autres sociétés ont ajouté des fonctions d'authentification multifactorielle (MFA) aux pages de connexion de la console d'administration centralisée, ainsi qu'aux appareils physiques tels que les pare-feux, qui exigent des identifiants de connexion. Mais les utilisateurs de ces produits, à savoir les administrateurs des systèmes IT et de la sécurité, doivent s'assurer d'activer ces fonctions et de s'enregistrer pour qu'elles soient effectives. Sophos encourage donc tous ses clients à activer ces protections dès que possible.

Malwares crypto-mineurs

Les malwares crypto-mineurs utilisent la puissance de calcul pour effectuer des tâches cryptographiques dans l'espoir de gagner de nouveaux « coins » (jetons), en participant généralement à un pool de processeurs ou de machines en réseau. Pour de nombreuses crypto-monnaies, l'extraction nécessite du matériel spécialisé avec des unités de traitement graphique dédiées à ce travail gourmand en traitement. Mais il existe d'autres options pour exploiter du matériel à usage plus général et extraire la crypto-monnaie, ainsi que de vastes réseaux de robots crypto-mineurs qui s'auto-propagent et tentent d'exploiter les systèmes vulnérables et de voler la puissance de traitement à des fins lucratives.

Si ces malwares n'ont pas d'impact sur les données des organisations, ils sapent les ressources informatiques et augmentent les coûts énergétiques et de refroidissement. Et souvent, ils sont un signe précurseur d'autres malwares, car ils sont généralement déployés via des vulnérabilités logicielles et réseaux facilement exploitables.

La plupart des crypto-mineurs visent le Monero (sigle boursier XMR), et ce pour un certain nombre de raisons. Le type de travail requis pour produire le XMR ne nécessite pas de cartes graphiques spécialisées, ce qui signifie qu'il peut être miné avec des serveurs pas forcément sophistiqués dans ce domaine. Enfin, le XMR est moins traçable que de nombreuses autres crypto-monnaies, le rendant plus attrayant pour les opérations cybercriminelles.

Les robots crypto-mineurs sont souvent les premiers malwares à exploiter les vulnérabilités les plus récentes. La vulnérabilité Java Log4J et les exploits ProxyLogon/ProxyShell de Microsoft Exchange Server ont été rapidement exploités par ces botnets. Dans de nombreux cas de ransomwares ayant fait l'objet d'une intervention, l'équipe Sophos Rapid Response a trouvé des preuves de malwares crypto-mineurs qui utilisaient le même point de compromission initial que le ransomware — dans certains cas, plusieurs mois avant l'attaque.

Les crypto-mineurs sont également un problème multi-plateforme. Même si un grand nombre des robots crypto-mineurs détectés par Sophos sont basés sur Windows (et exploitent PowerShell et d'autres moteurs de script Windows pour s'installer et se maintenir), on a également identifié des versions Linux de ces botnets, ciblant souvent des appliances réseau ou des serveurs Web non corrigés.

Certes les crypto-mineurs de XMR sont toujours prisés et répandus, mais les fluctuations (principalement dans le mauvais sens) de la valeur de certaines crypto-monnaies ont eu un effet sur les opérateurs. En effet, la chute de la valeur du XMR a entraîné une baisse de la rentabilité des botnets, ce qui semble avoir eu un impact sur les efforts déployés par les opérateurs pour développer leurs pools de minage. Certaines fluctuations dans le taux de détection des déploiements de crypto-mineurs ont suivi les fluctuations de la valeur de XMR, comme indiqué ci-dessous. En particulier, nous pouvons noter à la mi-juin, la chute concomitante de la valeur de XMR et du taux de détection des crypto-mineurs.

Détection de crypto-mineurs de Monero et fluctuations des prix, d'avril à septembre 2022

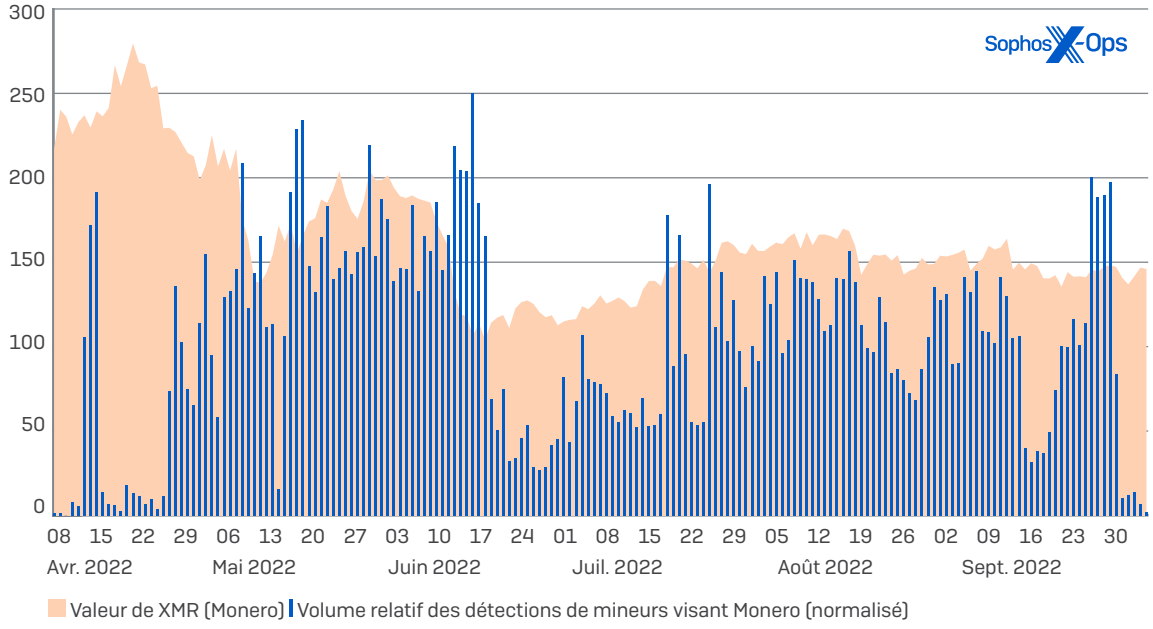


Fig.35. Le taux de détection de Monero sur les douze derniers mois (en bleu, totaux normalisés pour l'échelle) montrant une certaine cohérence avec sa valeur au cours de la période (en orange).

Mais la rentabilité des crypto-mineurs se voit affectée non seulement par la valeur de la monnaie visée, mais aussi par la longévité du mineur. En effet, de nombreux mineurs traquent des mineurs similaires et les éliminent des serveurs qu'ils exploitent. Dans certains cas, les mineurs déploient même des correctifs pour corriger les vulnérabilités qu'ils ont installées afin d'empêcher d'autres mineurs de les déraciner — ce qui leur permet de persister lorsque les organisations effectuent des analyses à la recherche de systèmes vulnérables.

Au-delà de Windows : les menaces pesant sur Linux, Mac et les mobiles

Jusqu'à présent, nous avons principalement évoqué les malwares et les outils d'attaque qui affectent Windows. Ce n'est pas surprenant compte tenu de la place prépondérante de ce système dans les listes de ciblage de la plupart des attaquants. Mais Windows n'est pas la seule cible viable dans l'entreprise, et nous entendons de plus en plus parler de campagnes d'attaque dont les charges utiles « prennent en charge » plusieurs plateformes. Ces charges utiles sont conçues soit en utilisant des langages supportant plusieurs plateformes tels que Go ou Python (souvent regroupées dans pyinstaller) ou des frameworks comme Electron, soit en préparant des binaires pour tous les principaux frameworks. Dans cette dernière section, nous examinerons brièvement le contexte des menaces pour Linux, Mac et les plateformes mobiles, tout en sachant que bon nombre de ces mineurs sont présents sur ces plateformes et bien d'autres encore.

Menaces ciblant Linux

Les systèmes Linux sont visés depuis longtemps pour les services les plus fréquemment déployés sur ce système d'exploitation, notamment les sites Web d'entreprises, les serveurs de machines virtuelles, les appliances réseau, les serveurs de stockage et l'infrastructure applicative. De plus en plus, les criminels développent des ransomwares multi-plateformes et d'autres malwares pour mieux cibler ces ressources à des fins lucratives. Dans les six premiers mois qui ont suivi la sortie de ses solutions Linux, Sophos a détecté 14 serveurs Linux ciblés par des ransomwares.

Bon nombre des malwares affectant les systèmes Linux (ainsi que d'autres plateformes de serveurs) sont conçus pour miner des cryptomonnaies. Plus de 40 % de toutes nos détections et 72 % des systèmes Linux détectés avec des malwares résultent de mineurs.

Menaces Linux par pourcentage de détections Linux		
Menace	**Pourcentage des détections**	**Remarques**
Mineur	43,0 %	Détection de mineurs génériques
DDoS	27,1 %	Détection liée à Mirai
Tsunami	12,3 %	Client DDoS basé sur IRC
Gognt	11,5 %	Détection générique pour les malwares écrits dans Go
Rst	1,3 %	Infecteur de fichiers vieux de 20 ans
Loit	1,1 %	Exploit local
Swrort	0,9 %	Mettle (implémentation de Meterpreter) pour Linux
SSHDoor	0,7 %	Porte dérobée SSH
XpMmap	0,6 %	Exploits visant la mémoire
DrtyCoW	0,6 %	Exploit Dirty COW (CVE-2016-5195)
ProcHid	0,4 %	Trojan dissimulant des processus
Ngioweb	0,2 %	Botnet Proxy
Psdon	0,1 %	Agent Poseidon pour le framework Mythic Red Teaming
GoScan	0,1 %	Scanner Go cherchant des machines vulnérables

Fig. 36. Malgré l'incertitude qui règne sur les cryptomonnaies en 2022, les mineurs sont une infection qui demeure malheureusement fiable sur Linux.

Les mineurs ont dominé les constats d'infection sur Linux cette année — et davantage que ne le suggère ce graphique. Le terme « mineur » désigne la détection générique d'un mineur par Sophos. Mais ils peuvent également être détectés sous d'autres noms. Par exemple, la menace « Gognt » correspond à la détection Sophos de familles de malwares sans rapport entre eux et écrits dans Go. Cela signifie qu'il existe probablement des mineurs qui n'ont pas fait l'objet d'une détection en tant que « mineur », et donc qu'il en existe plus que ce qui est rapporté ici.

Menaces Linux par pourcentage de détections uniques Linux		
Menace	**Pourcentage de machines individuelles**	**Remarques**
Mineur	74,3 %	Détection de mineurs génériques
Gognt	5,1 %	Détection générique pour les familles de malwares écrits dans Go
DDoS	4,3 %	Détection liées au Mirai
Swrort	3,2 %	Mettle (implémentation de Meterpreter) pour Linux
DrtyCoW	3,1 %	Exploit Dirty COW (CVE-2016-5195)
Ngioweb	2,8 %	Botnet Proxy
Tsunami	2,7 %	Client DDoS basé sur IRC
Roopre	0,9 %	Porte dérobée ciblant les serveurs Web
SSHBrut	0,9 %	Décodeur de mots de passe SSH par force brute
Loit	0,8 %	Exploit local
Shell	0,8 %	Malware donnant un accès Shell à l'attaquant
Bckdr	0,6 %	Détection de portes dérobées génériques
Ransm	0,6 %	Ransomware

Fig. 37. L'impact des mineurs dans l'environnement Linux est encore plus évident lorsqu'il est réparti par machine affectée.

Les autres catégories les plus importantes de détections sur les systèmes Linux affectés sont liées à Gognt et à des toolkits de déni de service distribué (DDoS). Si la quasi-totalité des vulnérabilités visées par ces malwares ont été corrigées dans les versions plus récentes de Linux, elles restent toujours sans correctifs sur un nombre considérable d'appareils et d'appliances.

Plusieurs botnets et portes dérobées figurent toujours parmi les menaces majeures pesant sur Linux, mais l'une des plus intéressantes, du point de vue de l'entreprise, est sans doute Tsunami, une porte dérobée Linux de longue date qui a récemment évolué pour cibler les serveurs d'applications Jenkins et WebLogic.

Menaces ciblant Mac

En 2022, nous avons constaté qu'un nombre croissant d'outils d'attaque open-source et de frameworks post-exploit/C2 prenant en charge macOS pouvaient être identifiés sur des services tels que GitHub. La présence de code sur le répertoire ne correspond pas exactement à une explosion surprise des attaques sur Mac, mais elle indique sans doute au moins un intérêt croissant — et le souhait de le partager.

Sur la plateforme macOS, la principale menace reste les applications potentiellement indésirables, notamment les applications qui installent des plug-ins pour le navigateur Safari d'Apple (ainsi que d'autres navigateurs). Ces applications injectent du contenu dans les pages web afin de rediriger les utilisateurs vers des contenus frauduleux ou malveillants.

Applications potentiellement indésirables (PUA) sur macOS, d'avril à septembre 2022		
Détection	**Pourcentage de machines individuelles**	**Remarques**
Adloadr	16,2 %	Détection d'adwares génériques
Genieo	8,9 %	Hijacking de navigateur (recherche)
Bundlore	8,4 %	Adware
Dynji	4,6 %	Hijacking de navigateur (barre d'outils)
Pirrit	3,7 %	Adware
AdvMac	3,2 %	Adware
HistColl	3,0 %	Collecte de données du navigateur
Keygen	2,3 %	Outil de piratage de logiciels

Fig. 38. Adloadr, largement en tête de la liste des PUA Mac en 2022.

L'application Adloadr, l'une des nombreuses PUA qualifiée d'adware, arrive en tête de nos statistiques télémétriques pour Mac en 2022, avec près de deux fois plus d'infections de machines individuelles que le hijacking de navigateur Genieo, en deuxième position.

Du côté des malwares, nous avons observé un nombre élevé de NukeSped, VSearch et Dwnldr — un Trojan d'accès à distance, un adware et un Trojan téléchargeur, respectivement. Chropex et ProxAgnt, deux applications d'assistance associées à la famille Adloadr, figurent également dans notre liste des détections courantes.

Détection de malwares sur macOS, d'avril à septembre 2022		
Détection	**Pourcentage de machines individuelles**	**Remarques**
NukeSped	22,2 %	Trojan d'accès à distance
VSearch	15,6 %	Adware/hijacking de navigateurs
Dwnldr	10,8 %	Détection de Trojans génériques
Agent	10,8 %	Détection de malwares génériques
Keygen	6,4 %	Générateur de clés pour contourner la protection contre la copie
FkCodec	6,2 %	Adware se faisant passer pour un programme d'installation de codecs vidéo
Chropex	5,0 %	Adware présentant également un comportement de hijacking de navigateurs
ProxAgnt	1,9 %	Trojan
Swrort	1,5 %	Trojan d'accès à distance

Fig. 39. NukeSped, VSearch et Dwnldr en tête du classement des détections de malwares sur macOS.

Jusqu'au mois d'octobre, nous avons pu repérer 5 nouvelles menaces macOS pour 2022. Aucune d'entre elles n'est arrivée en tête de notre classement des malwares macOS, mais nous les observons avec intérêt au fur et à mesure de chaque nouvelle détection.

Nouvelles menaces macOS observées en 2022			
Mois	**Nom**	**Détection**	**Remarques**
Janvier	SysJoker	OSX/SysJoker	Porte dérobée multi-plateforme prenant en charge macOS
Janvier	DazzleSpy	OSX/DazzleSpy	Technique d'infection liée à MACMA, une porte dérobée qui visait des militants pro-démocratie à Hong Kong.
Mars	Gimmick	OSX/Gimmick	Communique via les API de Google Drive pour dissimuler le trafic réseau aux systèmes de surveillance.
Mai	pymafka/CrateDepression	Troj/Pymaf, OSX/Cobalt	Attaque de la supply chain sur un package hébergé sur pypi ; dépose balise Cobalt Strike.
Octobre	Alchimist	Exp/20214034-D	Framework d'attaque multiplateforme écrit dans Go

Fig. 40. Cinq nouvelles menaces macOS sont apparues au cours des dix premiers mois de 2022.

Menaces ciblant les plateformes mobiles

Les applications mobiles étant devenues le principal mode d'interaction avec Internet, les portables sont au cœur d'un nouveau type de cybercriminalité. Alors que la plateforme Android est toujours en proie à un flux constant de malwares, diffusés sous la forme de fausses applications et d'infostealers, Android et iOS sont de plus en plus ciblés par des applications frauduleuses, et même les remparts si bien protégés des appareils Apple se retrouvent victimes de cybercriminalité via l'ingénierie sociale notamment.

Les injecteurs de logiciels malveillants, les spywares et les malwares ciblant le secteur financier sont toujours en tête des packages APK Android malveillants que nous détectons, tout comme les applications qui génèrent de faux clics publicitaires. Mais les applications potentiellement indésirables, notamment celles dont le seul but est d'agir comme moyen de collecter des « achats In-App » dissimulés auprès des victimes, continuent d'être une menace croissante pour les utilisateurs mobiles. Et l'an dernier, on a vu émerger une toile sophistiquée de réseaux dédiés à la fraude financière, utilisant de fausses applications, qui est devenue une véritable industrie en Asie du Sud-Est.

En 2021, Sophos a commencé à suivre une campagne de cybercrime organisé que nous avons baptisée CryptoRom. La campagne repose sur une forme de cyberfraude, connue sous le nom de sha zhu pan [杀猪盘] — qui signifie littéralement « plateau d'abattage de porcs » en chinois. Elle est soutenue par un syndicat bien organisé de développeurs d'applications et de sites web frauduleux, de créateurs de faux profils sociaux et d'individus qui se sont engagés dans des efforts d'ingénierie sociale scénarisés via les médias sociaux et les sites de rencontre afin de piéger les victimes et de les arnaquer.

En octobre 2021, nous avons décrit la progression mondiale de la campagne. La formule a changé et muté, passant d'un faux programme d'investissement dans les crypto-monnaies à de faux investissements en dérivés de crypto-monnaies, puis à d'autres marchés financiers tout aussi factices. Pour que ces stratagèmes semblent légitimes, les réseaux créent de fausses applications et de faux sites Web mobiles qui se font passer pour des organismes financiers légitimes. Nombre de ces applications se sont glissées sans être détectées dans les app stores comme les applications de « minage de liquidités » qui ont été retrouvées dans l'App Store d'Apple et Google Play Store.

Parallèlement, les escrocs ont également trouvé des moyens d'exploiter iOS, en utilisant des Web Clips et des programmes de déploiement de test des développeurs d'applications pour introduire leurs applications sur les systèmes iOS. On peut citer par exemple le schéma de distribution ad-hoc « Super Signature » d'Apple, les tests bêta « Test Flight » et les schémas des applications d'entreprise pour éviter le contrôle de sécurité de l'App Store d'Apple. La même approche peut être utilisée pour d'autres malwares ciblant iOS, mais nécessite une certaine activité d'ingénierie sociale de la part de la cible pour permettre l'installation initiale.

Ces applications, qui ont entraîné des centaines de millions de dollars de pertes pour les victimes, font partie d'un écosystème de cybercriminalité en croissance constante qui s'est propagé à travers des promesses de mariage ou d'autres escroqueries d'ingénierie sociale sur des plateformes comme Facebook, Twitter et LinkedIn. Ces arnaques continuent d'évoluer et sont reprises par d'autres réseaux criminels, chacun apportant sa propre touche finale.

Android et iOS sont également la cible de campagnes publicitaires malveillantes, notamment de fausses alertes qui imitent les alertes du système et qui dirigent souvent les utilisateurs vers un App Store pour acheter une application qui comporte des frais d'abonnement cachés, installe d'autres malwares, ou les deux à la fois.

Sophos continue ses recherches pour trouver des moyens de bloquer ces menaces et avertit les développeurs de systèmes d'exploitation mobiles dès qu'un nouvel usage abusif est repéré sur leur App Store.

Conclusion

Sur l'ensemble du spectre des menaces, deux tendances se dégagent clairement : tout d'abord, un terrain de jeu de plus en plus accessible pour les cybercriminels en herbe qui souhaitent se lancer, deuxièmement, la marchandisation de ce qui, autrefois, était considéré comme des outils et des tactiques ATP (Advanced Persistent Threat). Même s'il existe depuis longtemps un marché florissant pour les outils de piratage, les malwares et l'accès aux réseaux vulnérables, les connaissances issues de l'histoire récente sur les ransomwares et les opérateurs malveillants et bien financés deviennent plus rapidement accessibles à la communauté cybercriminelle au sens large — tout comme les outils de sécurité commercialisés conçus pour déjouer certaines défenses.

De leur côté, les conditions géopolitiques n'ont certainement pas aidé à faciliter la lutte contre la cybercriminalité. Suite à la tension accrue des relations sino-américaines, la Chine a mis fin, cette année, à sa coopération avec les forces de l'ordre américaines dans la lutte contre la cybercriminalité. Parallèlement, alors que le pays a renforcé sa répression contre les arnaques aux crypto-monnaies et autres cybercrimes au niveau national, les opérateurs de langue chinoise se sont rapidement tournés vers l'exportation de leurs activités criminelles. Et alors que la guerre en Ukraine a brièvement perturbé certains réseaux criminels de langue russe, ces derniers se sont rapidement reconstitués.

Contre toutes ces menaces, il n'existe aucune défense infaillible. Mettre en place une sécurité proactive est le seul remède pour empêcher les incursions de causer des dégâts. Mais, pour de nombreuses organisations, ce travail est trop complexe à assumer toutes seules. C'est pourquoi Sophos travaille sans relâche à améliorer les fonctionnalités de ses solutions, afin d'aider les entreprises de toutes tailles à faire face à l'évolution constante des menaces, en offrant une sécurité réseau et endpoint, ainsi que des services d'opérations de sécurité managés à la pointe de la technologie.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

22-11-17 FR (NP)

SOPHOS