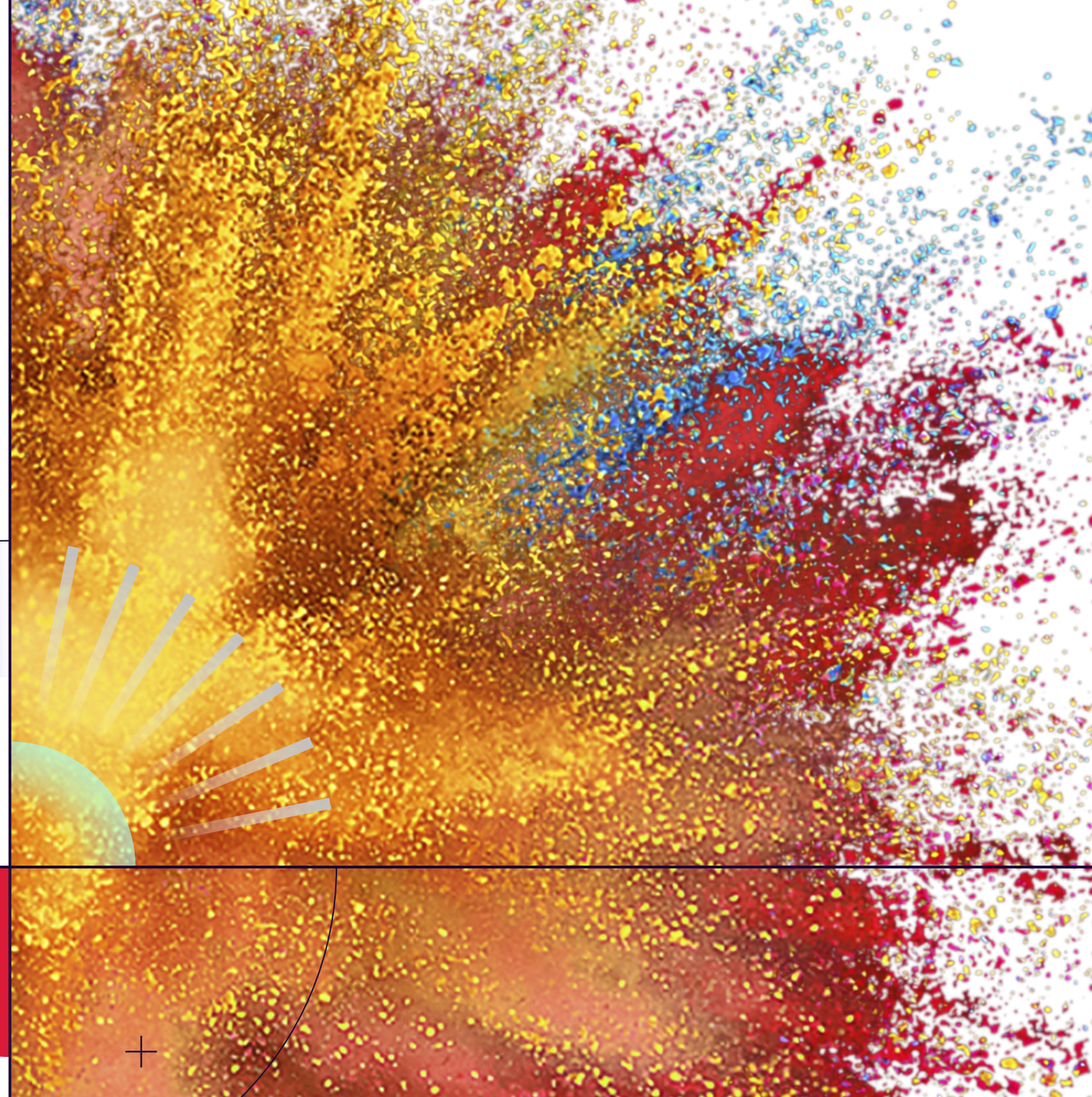
GATEWATCHER

Cyber Threats Semester Report_

Janvier - Juin 2023



*Sommaire_*

*Introduction_*

La Purple team de Gatewatcher a le plaisir de vous présenter son troisième Cyber Threat Semester Report (#CTSR) portant sur la période janvier-juin 2023.

L'objectif de ce rapport est de fournir éclairage, analyse et mise en perspective des cybermenaces observées chaque semestre par Gatewatcher CTI, notre plateforme de Threat Intelligence et par la veille active des analystes de la Purple Team.

Au sein de Gatewatcher, la Purple Team a pour mission de traquer et d'analyser des cybermenaces afin de garantir la mise à jour et l'optimisation constante des performances de nos technologies de cyberdétection (NDR, CTI, sondes qualifiées ANSSI,..). La Purple Team se caractérise par la diversité des profils de ses experts dans des domaines tels que la réponse à incident, l'analyse et intégration SoC, le pentesting, l'analyse CTI, et la recherche en cyber sécurité.

Ce nouveau rapport s'articule autour de cinq sections principales axées sur :

- Les malwares les plus fréquemment employés par les cyberattaquants
- Les types de fichiers utilisés à des fins malveillantes et leurs évolutions
- Les threat actors les plus actifs
- Les principaux secteurs d'activité ciblés par les cybermenaces
- Les régions et secteurs les plus impactés par des fuites d'identifiants (adresse courriel/mot de passe)

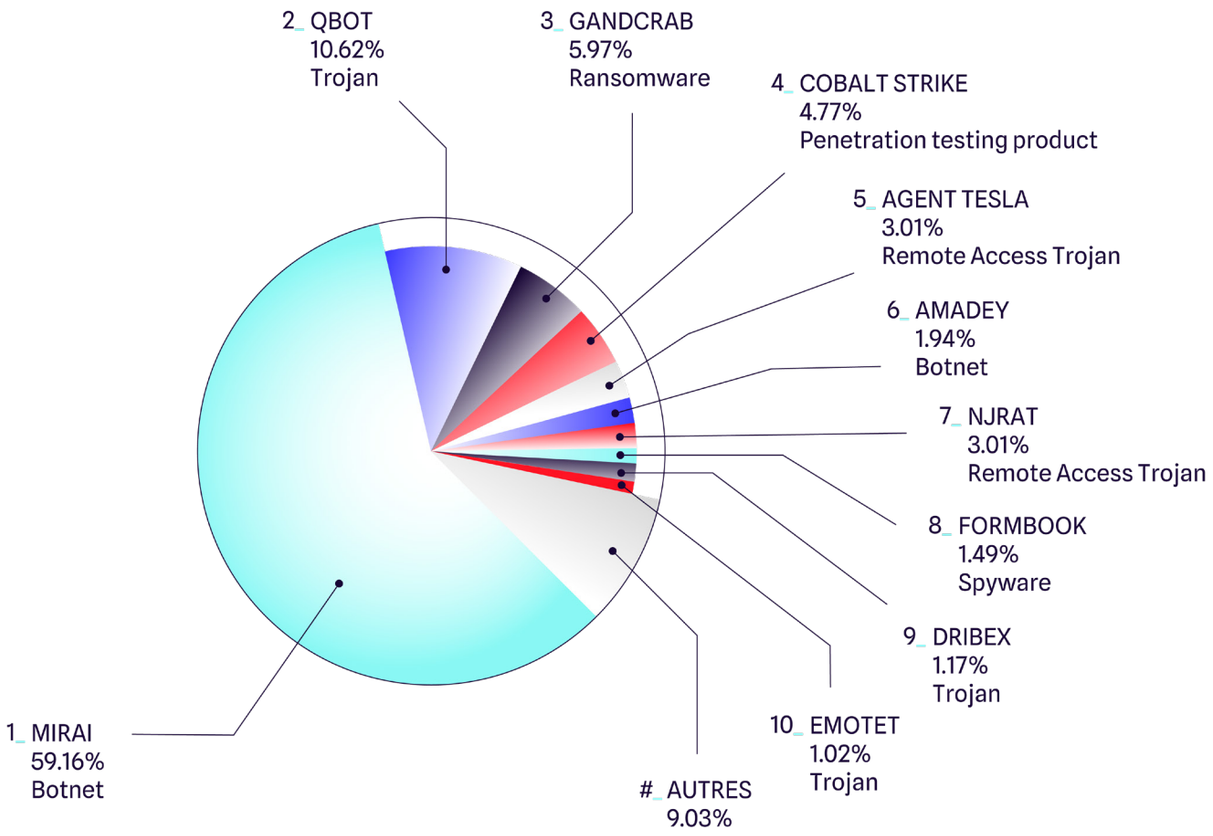
Chaque section comporte un classement explicatif sur chaque thème que les auteurs ont identifié dans le domaine des cybermenaces ainsi que des focus thématiques qu'ils ont rédigé afin de mettre en avant les différentes tendances qu'elles soient établies, originales ou émergentes afin de faciliter leur détection et in fine réduire l'impact des futurs incidents de sécurité.

Dans ce CTSR, une nouvelle section a été ajoutée sur le thème de la fuite d'identifiants (emails/mots de passe) afin de sensibiliser les lecteurs à ce risque. Cette section est partie des fuites détectées par la plateforme Gatewatcher CTI afin de mettre en évidence les noms de domaines de premier niveau (TLD) qui sont les plus impactés.

Comme pour les éditions précédentes, la Purple Team dresse un panorama des principales tendances observées et analysées sur la période en matière de cybermenaces avec en particulier :

- L'utilisation de fichiers des bibliothèques de liens dynamiques (DLL) à des fins malveillantes
- La stratégie de ciblage opérée par les threat actors avec l'exemple significatif de la situation du secteur de l'éducation
- La popularisation du détournement d'outils légitimes par les cybercriminels a travers l'exemple de CobaltStrike
- L'intérêt grandissant pour les attaques par la chaine d'approvisionnement ;
- La vulnérabilité des secteurs publics dans le monde face aux fuites d'identifiants
- L'augmentation de l'utilisation de PowerShell par les cybercriminels dans le cadre des intrusions.

La Purple Team aborde également d'autres tendances encore émergentes et plus discrètes de cybermenaces, comme le début de la diversification des plateformes ciblées par le développement de malware à l'origine pour Windows ciblant maintenant Linux ou MacOs. Une autre attention est également portée aux fuites de données dans les universités et écoles secondaires américaines.



1 Malware : La fin d'un *règne*_

Pendant plus de trois ans, deux malwares largement reconnus dominaient le monde des logiciels malveillants : Mirai et Emotet. Nous observons sur ce premier semestre 2023 une continuité de la tendance à la baisse d'Emotet que nous évoquions déjà fin 2022. Le choix de Microsoft de désactiver le vecteur d'attaque principal de ce malware, à savoir les macros, et l'apparente difficulté des opérateurs d'Emotet à trouver un nouveau vecteur tout aussi efficace peuvent expliquer la sortie d'Emotet du trio de tête des logiciels malveillants.

Emotet n'appartient toutefois pas encore au passé et quelques campagnes ont encore été détectées début 2023 bien que sans commune mesure avec celles ayant eu lieu durant son âge d'or. Ces campagnes s'apparentant plus à des tests afin d'observer l'efficacité de différentes méthodes comme faire grossir artificiellement la taille des payloads afin d'échapper aux analyses (technique connue sous le nom de *binary padding (T1027.001)* ou encore l'utilisation de fichiers OneNote.

Sans surprise, Qbot remplace Emotet dans la categorie des Ransomware-as-a-Service (Raas) en occupant une confortable seconde place. L'activité de Qbot reste particulièrement présente tout comme sa capacité à varier les méthodes d'infection parmi lesquelles on pourra noter sur ce début d'année : l'utilisation de fichier OneNote, l'enchainement PDF/WSF (Windows Script File) ou encore le détournement de DLL de Wordpad en utilisant une archive contenant Wordpad et une DLL malicieuse.

Le malware Mirai s'assure une présence pérenne dans le top qui s'explique par ses capacités d'auto-réplication, la popularité de ses cibles auprès du grand public et du manque de mise à jour de ces dernières.

Le reste du top des observations de malware reste globalement stable, avec Cobalt Strike toujours fréquemment rencontré lors des secondes étapes d'infection, malgré les efforts de Fortra pour limiter les utilisations de son outil à des fins illégales, et la mise à disposition par Google Cloud d'indicateurs de détection pour cette menace.

Cobalt Strike est toujours au coude à coude avec Agent Tesla qui, malgré son ancienneté - certes relative comparée à Qbot mais néanmoins présente - reste très utilisé.

On remarquera l'arrivée d'Amadey directement à la sixième place du classement. Bien que déjà présent durant le deuxième semestre 2022, un pic d'utilisation a été constaté sur la toute fin d'année 2022.

Mirai : une famille *envahissante*_

Le malware Mirai premier du nom, est apparu à l'été 2016. Il s'agit d'un réseau d'équipement infecté (botnet) *utilisé* pour mener des attaques par *déni de services distribués (DDoS).* Il a rapidement gagné en notoriété après avoir attaqué le site KrebsOnSecurity, blog du journaliste Brian Krebs, ainsi que les infrastructures de la société Dyn. La même année, au mois de septembre 2016, le code source a été publié sur HackForums et a permis l'analyse du mode opératoire du malware qui s'est avéré extrêmement simple mais efficace. L'objectif : infecter les équipements IoT en utilisant des mots de passe par défaut, couper les accès et tenter d'infecter d'autres équipements en attendant un ordre d'attaque. Une des particularités de Mirai réside dans des capacités d'infection multi architecture affectant tous types d'IOT ayant pour base un système d'exploitation linux indépendamment de son architecture (par exemple ARM ou MIPS). Cette technique spécifique le rend remarquable car elle est assez rare dans le monde des malwares.

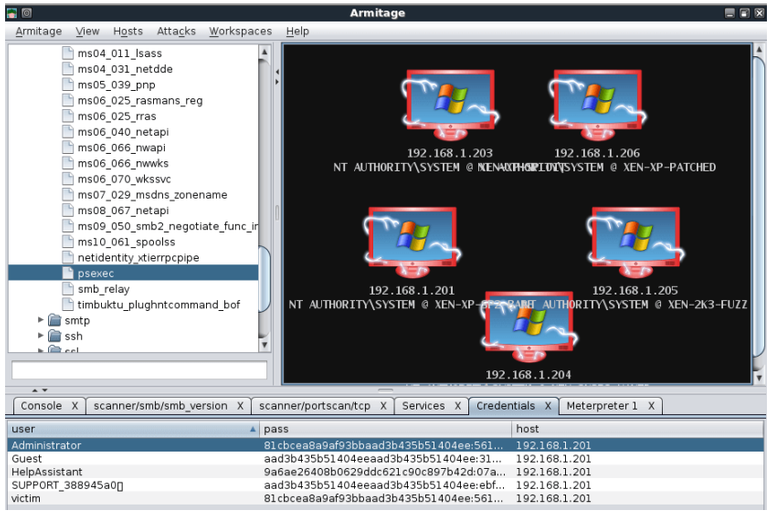
Comme cela s'est produit avec la publication du malware Zeus en 2011, la publication du code source de Mirai a engendré l'émergence de différents variants qui se sont enrichis au fil du temps de nouvelles méthodes d'infection, notamment en intégrant l'exploitation de vulnérabilités comme les variants Satori, Okiru ou encore OMG, qui permettent d'utiliser les équipements infectés comme proxy.

Malgré plusieurs actions des autorités ayant conduit à l'arrestation de ses auteurs d'origine, mais également des opérateurs d'autres variants, Mirai est toujours bel et bien actif. On peut par exemple citer l'attaque à l'encontre d'un opérateur de télécommunication sud-américain en début d'année, avec un volume de 1.3Tbps (Tera-bit par seconde).

“Cobalt Strike : le bon outil dans de mauvaises mains”

Souvent déployé comme charge secondaire afin de permettre à un attaquant de se propager dans un réseau, Cobalt Strike est désormais bien identifié dans le paysage des malwares. À l’instar d’autres logiciels comme Sliver, il fait partie de la famille des outils de test d’intrusion (pentest frameworks).

Initialement, Cobalt Strike était destiné à succéder à Armitage, une surcouche graphique de l’outil Metasploit. Et c’est en tant que tel qu’il a vu le jour en 2012.

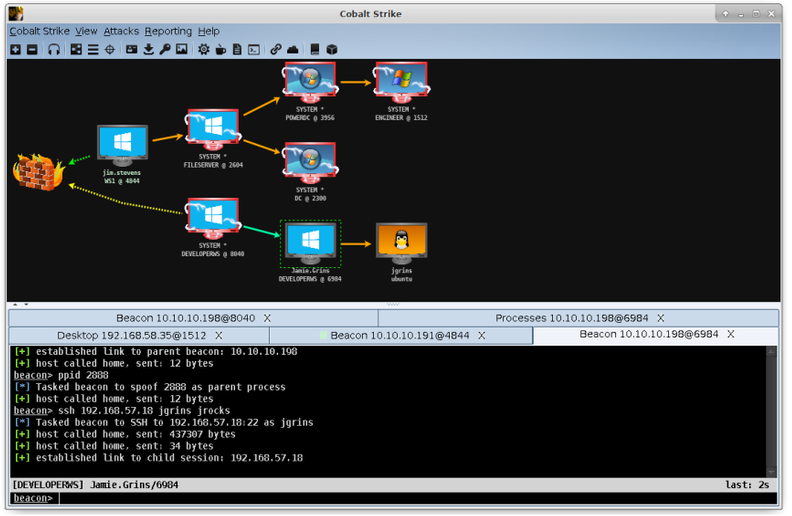


Armitage Screenshot CC-BY-SA

Très rapidement, un grand nombre de fonctionnalités ont été intégrées, comme la communication via DNS, l’intégration des Beacons, etc. Il est ainsi devenu un outil de choix pour les professionnels de la cybersécurité réalisant des tests d’intrusions. Ces derniers étaient, et sont toujours, au cœur du marché de la société Fortra qui commercialise aujourd’hui Cobalt Strike.

Cependant, en 2019, l’outil commence à apparaître dans le cadre d’actions malveillantes. L’une de ces premières apparitions fut lors de campagnes de malware visant l’Allemagne durant laquelle la chaîne, alors classique, de malspam contenait un document Word avec une macro.

Durant cette campagne Cobalt Strike était alors associé au ransomware Maze. Les capacités de mouvement latéral apportées Cobalt Strike en ont fait un outil de choix pour les ransomgroups car cela leur permet d’augmenter le périmètre de l’attaque finale. Dès lors, la chaîne d’infection conçue autour d’un loader, puis de Cobalt Strike pour finir par un ransomware va se généraliser.



Cobalt strike screenshot

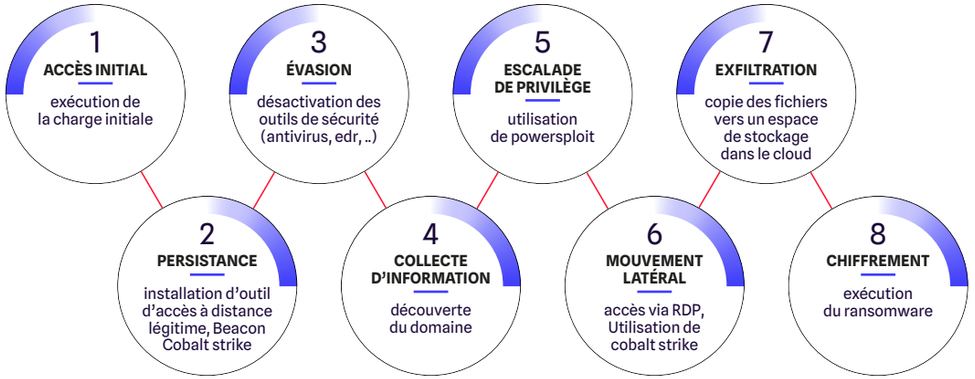
En 2020, le code source de la version 4.0 du logiciel fuite et est publié sur GitHub. Le dépôt d'origine a alors été dupliqué plus de 170 fois en douze jours, sans compter les téléchargements de ces sources. Le code publié semble être issu d'une décompilation avec une légère modification mais qui aura son importance : la suppression de la vérification de la licence. Bien que des versions crackées étaient déjà utilisées par les acteurs de la menace, la mise à disposition de code source d'outils offensifs, y compris s'il ne s'agit pas du code source original, entraîne une augmentation des occurrences des outils dans la période qui suit, comme cela avait pu être observé avec le malware Zeus.

Des observations indiquent, lors de certaines campagnes impliquant Emotet, l'abandon de la chaîne d'infection classique basée sur la combinaison Emotet-Trickbot-Ryuk, pour se passer des malwares intermédiaires en les remplaçant par Cobalt Strike en deuxième étape d'infection et délivrer ainsi sa charge finale plus rapidement en limitant la détection.

L'une des fonctionnalités les plus prisées de Cobalt Strike réside dans le Beaconing et les "Malleable Profiles" qui permet de modifier le comportement du beacon, complexifiant ainsi la détection en se basant sur le mode de communication ou certaines données spécifiques.

> **"Cette fonctionnalité combinée à une livraison au plus tôt dans la chaîne d'infection font de Cobalt Strike un outil redoutable pour les attaquants et un risque qui l'est tout autant pour les systèmes d'informations."**

Pour illustrer cela, citons l'exemple d'une campagne ayant eu lieu durant ce premier semestre de l'année 2023 menée par le groupe "Royal". Reprenant un mode opératoire qui se popularise, le vecteur d'infection initial est le malvertising (technique consistant à utiliser les régies publicitaires pour inciter les utilisateurs à télécharger un logiciel en se faisant passer pour le logiciel d'origine). La séquence d'infection était la suivante :



Afin de permettre une détection rapide des comportements comme celui de Cobalt Strike, les équipes de Gatewatcher ont développé Beacon Detect, une nouvelle fonctionnalité, qui permet de détecter au plus tôt la communication avec des serveurs de commandes et contrôle (C2).

Visualisation d'une detection C&C sur la plateforme NDR de Gatewatcher

L'éditeur, Fortra, tente, avec un succès mitigé, de limiter l'utilisation de ses produits à des fins illégales en renforçant les vérifications effectuées sur la légitimité de leurs clients mais également en faisant front commun avec Microsoft. Dans une décision du 31 mars 2023, la cour du district de New-York a autorisé Fortra, Microsoft et Health-ISAC (une communauté de personnes gérant des infrastructures liées à la santé) à demander l'arrêt d'infrastructure hébergeant des versions du logiciel piratées aux fournisseurs d'accès.

Malware : de l'autre côté de la fenêtre

Lorsqu'il est question de malware, la majorité des sujets tournent autour de l'écosystème de Microsoft qui représente près de 70 % des ordinateurs personnels que ce soit dans le monde de l'entreprise où ActiveDirectory et ses GPO (Group Policy Object) règnent quasi sans partage, ou dans la sphère personnelle ce dernier équipant par défaut l'écrasante majorité des équipements.

Cela peut parfois faire oublier qu'il existe d'autres systèmes d'exploitation qui, contrairement à une croyance populaire, ne sont pas épargnés par les menaces. Du côté des alternatives, nous pouvons notamment citer Apple et son système d'exploitation MacOs dont l'usage privé et professionnel est en progression ces dernières années.

Côté serveurs, et de façon assez marginale côté utilisateurs, on trouve les systèmes GNU/Linux, ou encore la famille des BSD (FreeBSD, OpenBSD, ...).

Regardons plus en détail l'état de la menace ciblant ces environnements alternatifs, en commençant par Apple.

L'actualité récente la plus notable réside probablement dans les initiatives menées par le groupe Lockbit qui, en avril 2023, travaillait au portage de son logiciel malveillant vers MacOS. Bien que les échantillons observés puissent être considérés comme une première ébauche, probablement issues de la version Linux, il s'agirait, si cette transition aboutit, d'un mouvement significatif d'un groupe reconnu afin de cibler ce système.

Parmi les découvertes de ce début d'année se trouvait également le portage d'un beacon Cobalt Strike pour MacOS nommé Geacon implémenté en Go. Très vite d'autres versions sont également apparues comme Geacon Plus qui fut observée dans des échantillons présents sur VirusTotal, ce qui laisse à penser que des campagnes ont déjà été lancées.

À l'instar de l'écosystème Microsoft, les infostealers ont également le vent en poupe sur MacOS avec des cibles similaires : les navigateurs, les portefeuilles de crypto-monnaie, les fichiers sensibles, et le trousseau iCloud spécifique à MacOS. Parmi les nouveautés de ce début d'année, on peut citer les infostealers MacStealer, Atomic (AMOS), Noknok ou encore Realst. Ce dernier ayant été observé lors d'une campagne multi-OS, ciblant Windows avec Redline Stealer et MacOS avec Realst, selon le système d'exploitation de la victime. Il se pourrait que cette approche reflète le futur des campagnes de malware, visant à couvrir un large éventail de scénarios.

Moins visibles que les systèmes grand public, les environnements Linux ne sont pas non plus épargnés par les acteurs de la menace mais cette fois-ci pour d'autres raisons. En effet, bien que les ordinateurs personnels sous linux restent relativement rares, il en va tout autrement pour les serveurs qui, pour une grande partie, utilise ce système d'exploitation. Nous mettrons ici de côté le botnet Mirai et ses variants qui constituent un cas particulier pour nous intéresser aux autres malwares observés depuis le début d'année.

À l'image de LockBit pour MacOS, le groupe APT27 (aussi connu sous le nom Iron Tiger), a commencé à déployer lors de campagne d'attaque son malware Sys-Update porté sous linux. Ce malware présente la particularité d'utiliser une technique de DNS-Tunneling afin de communiquer avec son serveur de contrôle.

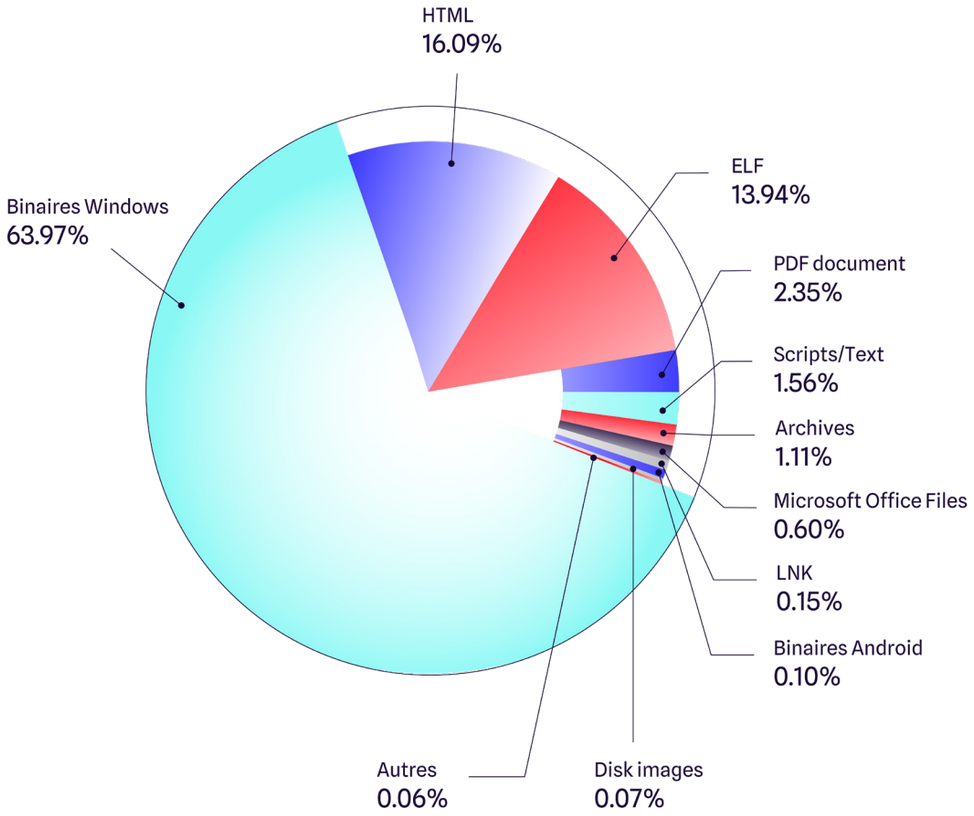
Certaines vulnérabilités logicielles sont également l'occasion pour les acteurs de la menace de mener de nouvelles attaques. Récemment, un nouveau malware surnommé Akira, apparu initialement en tant que ransomware ciblant les systèmes Windows en mars, a su s'adapter en exploitant la vulnérabilité CVE-2021-21974 des serveurs VMWare Esxi. Ce malware rejoint ainsi la longue liste d'acteurs ayant tiré parti de cette vulnérabilité, comme EsxiArgs et Royal en février, ou encore Black Basta, LockBit, ou Revil, et bien d'autres, avant eux. Bien que n'étant pas basé sur un noyau Linux, les serveurs Esxi utilisent également le format de binaire ELF.

S'agissant du vecteur d'infection principal, les vulnérabilités critiques sont toujours accompagnées par une série de campagnes aux objectifs variables (espionnage, ransomware, ...) suivant les attaquants. Cela est également l'occasion pour de nouveaux botnets d'apparaître en reprenant le modèle de Mirai et ses variants utilisant des vulnérabilités et du brute-force afin de se propager. C'est le cas du botnet Chaos, qui cible à la fois Windows et Linux, mais également différentes architectures.

Plus étonnant, nous assistons dernièrement à une recrudescence de campagnes ciblées vers certaines catégories de personnes comme l'opération DreamJob (aussi appelée Nukesped) menée par le groupe Lazarus. Cette opération cible des développeurs par de fausses offres d'emploi via LinkedIn et d'autres réseaux sociaux, ou encore des experts de la sécurité informatique ciblés par de fausses preuves de concept d'exploitation de vulnérabilités.

Bien que l'activité malveillante sur ces systèmes soit d'une intensité moindre que celle concernant les systèmes Microsoft, on constate qu'aucun système n'est à l'abri de ces menaces et que cette tranquillité apparente tend à disparaître au fil du temps, rappelant qu'au final la meilleure solution reste d'adopter les bonnes pratiques de sécurité.

2 Type de *fichier_*



Par rapport au précèdent semestre, le haut du palmarès des types de fichiers n'évolue pas. En effet, dans le rapport du deuxième semestre de 2022 [0], les binaires Windows, HTML et ELF occupaient déjà le podium des fichiers malveillants les plus présents. Cependant, en analysant la représentation de chaque type de fichiers, nous constatons une régression notable concernant les fichiers HTML qui perdent 12 % d'occurrence par rapport aux semestres précédents. Si certains perdent du terrain, d'autres comme les fichiers ELF et les binaires Windows semble échapper à cette tendance.

Les fichiers ELF sont l'équivalent des binaires Windows pour les systèmes Linux. Ce sont des fichiers exécutables utilisés pour tous types d'action, y compris malveillantes. Même si cette progression d'environ 1,5 % semble mineure, elle est notable.

Un élément peut expliquer ce changement. Il est relatif à la versatilité des attaquants. En effet, de plus en plus de développeurs de ransomware et d'infostealers se diversifient en proposant des malwares Cross-Platform ciblant aussi bien les systèmes Linux que Windows. Par exemple, le cas très récent d'utilisation de fichiers ELF dans le cadre d'une campagne ransomware menée par le groupe Abyss [1] qui visait les systèmes Esxi de l'entreprise VMWare.

Les ransomwares représentant une part importante des attaques sur les systèmes, il est par conséquent logique que cette diversification mène à une évolution des statistiques dans notre top.

Malgré cette augmentation de fréquence d'utilisation des binaires Linux, l'évolution la plus notable est attribuée aux fichiers portables exécutables. En effet, ces derniers représentent environ 64 % des types de fichiers malveillants contre 42 % le semestre précédent. C'est en disséquant ces derniers et leurs utilisations que nous avons pu nous pencher sur des techniques encore peu courantes relatives à l'utilisation des DLL.

Bibliothèques de Liens Dynamiques (DLL) : Les Coulisses d'Attaques Sournoises

En analysant les statistiques liées aux types de fichiers exploités par les attaquants, il n'est guère surprenant de constater que les fichiers exécutables portables malveillants spécifiques à *Windows* dominent largement. Au cours du premier semestre de 2023, ces fichiers ne représentaient pas moins de 64 % des contenus malveillants identifiés par notre plateforme de renseignement sur les menaces. Lorsque nous avons croisé ces données avec celles concernant les malwares les plus couramment observés, nous avons identifié la présence, peu commune, d'outils offensifs utilisant les DLL pour réaliser leurs exactions. En effet, *Qbot*, qui figure à la deuxième position de notre top malware, dispose d'une capacité particulière, à savoir le DLL *sideloading*.

Avant d'approfondir ce cas spécifique, il convient de rappeler la raison d'être et le rôle des DLL.

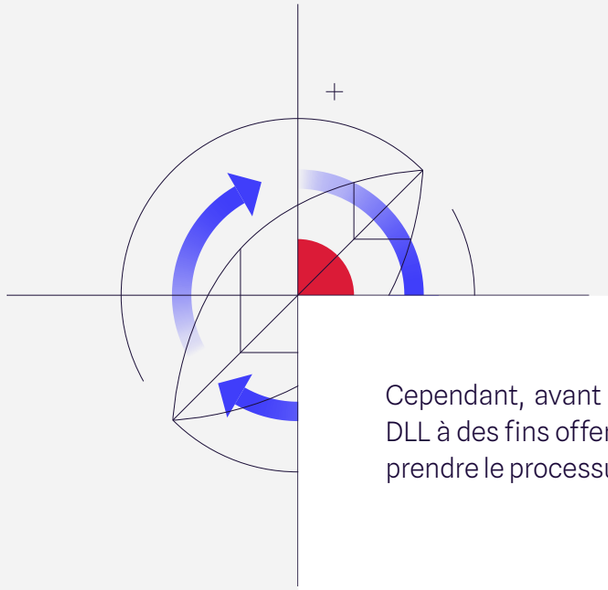
Les DLL (ou Dynamic Link Library, soit Bibliothèque de Liens Dynamiques en français) sont une bibliothèque contenant du code et des données pouvant être utilisés simultanément dans plusieurs programmes.

L'utilisation des DLL permet une optimisation significative du système afin de :

- Modulariser les tâches : Le découpage des tâches conséquentes en plusieurs plus petites.
- Réutiliser du code : Pour une opération similaire, plusieurs applications utiliseront la même DLL. Il est même possible qu'une DLL soit utilisée par plusieurs applications simultanément.

Lorsqu'un programme s'exécute sous un environnement *Windows*, la plupart des opérations réalisées font appel aux DLL. Par exemple, dans le cas où un programme ouvre une boîte de dialogue pour interagir avec l'utilisateur, il est probable qu'il fasse appel à la DLL native de *Windows*, Comdlg32. Afin de visualiser plus clairement ce concept, imaginez que deux programmes différents ouvrent chacun une boîte de dialogue. Dans ce cas, ils feront tous deux appels à cette même DLL, bien qu'ils soient distincts l'un de l'autre.

Les DLL représentent par conséquent une composante essentielle du bon fonctionnement du système d'exploitation Windows et des programmes s'exécutant dessus. C'est pourquoi elles sont régulièrement la cible d'attaques sophistiquées.



Cependant, avant d'expliquer l'utilisation des DLL à des fins offensives, il est crucial de comprendre le processus de recherche des DLL.

Les emplacements indiqués en bleu foncé correspondent aux emplacements potentiellement accessibles et modifiables par un attaquant ayant des privilèges utilisateurs. Il est important de noter que si un attaquant manipule ces emplacements, il peut alors exploiter ce processus de recherche afin de charger une DLL malveillante.

PROCESSUS DE RECHERCHE DES DLL

Mémoire	Recherche dans la mémoire pour savoir si la DLL y est déjà chargée
Répertoire de l'application	Recherche dans le répertoire de l'application afin de vérifier que la DLL soit dans le même répertoire que l'exécutable
Répertoire système	Recherche dans le répertoire *system*, dans "C:\Windows\System32" pour les DLL 64 bits et "C:\Windows\SysWOW64" pour les DLL 32 bits sur les systèmes 64 bits.
Répertoire système du programme	Recherche dans le répertoire système du programme C:\Program Files" ou "C:\Program Files (x86)"
Répertoire définis dan les variables d'environnement	Recherche dans les répertoires spécifiques définis dans les variables d'environnement système

Dans un premier temps, nous avons plongé au cœur du fonctionnement des DLL et découvert les différentes caractéristiques qui y sont attachées. Dès lors, il convient de préciser la manière dont les DLL sont exploitables dans le cadre d'attaques dans les systèmes *Windows*.

Tout d'abord, les attaques sur les DLL font partie de la grande famille des actions offensives de type *Living Off The Land* (T1218) qui consistent à tirer profit des fonctions natives d'un système dans le cadre d'actions malveillantes perpétrées sur ce dernier. En mai dernier la Purple Team a eu l'occasion de décrire ce genre d'attaque dans le cadre de la campagne VoltTyphoon.

Voici les types d'attaques réalisables en utilisant les DLL :

1. **DLL Side-Loading (Chargement Latéral de DLL)** *(T1574.002)* : Les attaquants forcent la victime à télécharger un répertoire contenant une DLL malveillante ainsi qu'une application légitime ou non. Cette dernière chargera alors la DLL malveillante au lieu de la DLL légitime, permettant alors à l'attaquant d'exécuter du code non autorisé.

2. **DLL Injection (Injection de DLL)** *(1055.001)* : Les attaquants vont, dans cette méthode, injecter une DLL malveillante dans le processus d'une application en cours d'exécution. Cela peut se faire en exploitant les vulnérabilités de l'application ou en manipulant le processus de chargement de DLL.

3. **Reflective DLL injection (Injection de DLL réflexive)** *(1055.001)* : Il s'agit d'une technique avancée d'injection de DLL par laquelle les attaquants chargent cette dernière mémoire sans avoir besoin d'écrire sur le disque.

4. **Search Order Hijacking (Détournement de l'Ordre de Recherche)** *(T1574.001)* : Les attaquants modifient l'ordre de recherche des DLL pour inciter l'application à charger une DLL malveillante avant la DLL légitime, permettant ainsi l'exécution de code non autorisé.

5. **Phantom DLL Attacks (Attaques de DLL Fantôme)** *(T1574.001)* : Les attaquants créent de fausses DLL avec des noms similaires à ceux attendus par une application. L'application charge alors la DLL malveillante au lieu de la DLL légitime.

6. **Remote injection DLL (injection DLL à distance)** *(1055.001)* : Les attaquants font appel à une DLL malveillante hébergée sur un serveur distant et chargée par une application vulnérable. Cela peut permettre à un attaquant de contrôler le code exécuté sur le système cible.

Après avoir identifié les moyens potentiels qu'un attaquant possède afin d'arriver à ses fins, nous allons maintenant analyser un exemple dans lequel la technique d'injection latérale de DLL est mise en œuvre.

Pour ce faire, nous prendrons l'exemple de *Qbot* (aka *Qakbot*).

Qbot est un cheval de Troie utilisé pour le vol d'information bancaire. Ce logiciel malveillant possède plusieurs moyens de propagation et d'exécution. Dans le cas nous nous concentrerons sur l'utilisation du chargement latéral de DLL via la calculatrice *Windows*.

Dans notre exemple, la propagation du cheval de Troie se fait par email. La victime reçoit un courrier électronique contenant un lien permettant de télécharger une archive zip. Dans cette dernière, un fichier image de type iso est compressé et 4 fichiers y sont contenus :

- Le fichier légitime calc.exe
- Un raccourci de fichier permettant d'exécuter calc.exe
- *WindowsCodecs.dll* : DLL malicieuse permettant le lancement de la DLL suivante
- *7533.dll* : contenant le malware *Qbot*

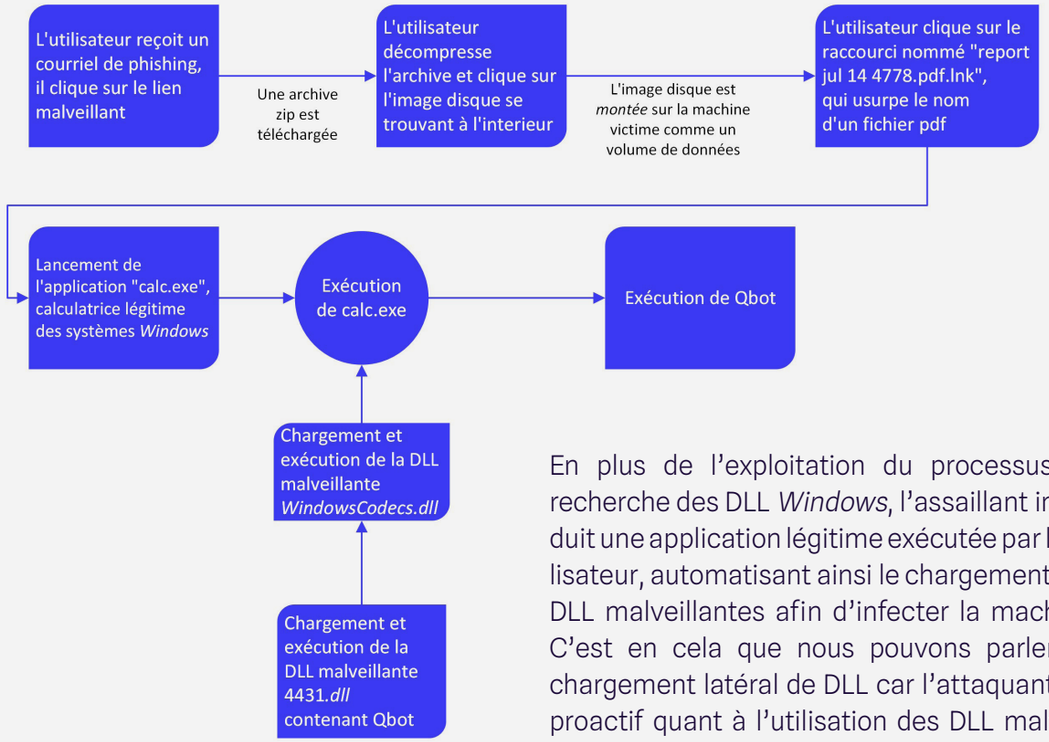
Une fois que l'utilisateur ouvre l'archive téléchargée et clique sur l'image disque qu'elle contient, cette dernière sera *montée* dans le système, ce qui aura pour conséquence l'apparition d'un nouveau volume de données dans l'explorateur de fichiers.

Dans un deuxième temps, un raccourci (un lien .lnk) sera créé dans ce volume de données sous le nom *"Report Jul 14 4778.pdf.lnk"*. Afin de tromper la vigilance de l'utilisateur, ce raccourci usurpera l'icône fichier pdf. Il est important de noter que, dans l'explorateur de fichiers, les extensions des raccourcis (.lnk) ne sont pas affichées par défaut. Sans recherches complémentaires dans les propriétés du fichier, la supercherie est indécelable.

Dans un troisième temps, si l'utilisateur, pensant ouvrir un pdf, clique sur le raccourci, il lancera alors la calculatrice *Windows (calc.exe)* présente dans le volume de données nouvellement créé. Les DLL malveillantes situées dans le même répertoire seront chargées à la place des librairies dynamiques légitimes utilisées par *calc.exe*. De ce fait, les DLL *WindowsCodecs.dll puis 4431.dll*, créées par l'attaquant, seront chargées et installeront le code malveillant de *Qbot* sur la machine.

À noter que le nom de la DLL malveillante peut changer mais se trouve toujours sous la forme suivante : [nombre].dll.

SCHÉMA RÉSUMANT L'INFECTION DE LA MACHINE PAR QBOT



En plus de l'exploitation du processus de recherche des DLL *Windows*, l'assaillant introduit une application légitime exécutée par l'utilisateur, automatisant ainsi le chargement des DLL malveillantes afin d'infecter la machine. C'est en cela que nous pouvons parler de chargement latéral de DLL car l'attaquant est proactif quant à l'utilisation des DLL malveillantes et ne se contente pas d'implanter une DLL hostile en attendant qu'une application légitime l'exécute.

> **Les attaques utilisant les DLL sont sophistiquées et requièrent de bonnes connaissances des systèmes *Windows*. Elles permettent de mettre en place des opérations offensives contournant certains systèmes de détection.**

Découvrons maintenant quels sont les avantages procurés par ces techniques sur des systèmes de détection :

- **Une détection sur les noms de fichiers impossible.** Même si une convention de nommage existe chez *Microsoft* [1], rien n'oblige les développeurs à respecter ces règles. De plus, réaliser une détection sur les noms de fichiers n'est pas très utile dans notre cas. En effet, il est nécessaire d'usurper au moins un nom de DLL légitime pour que l'attaque réussisse.

- **L'utilisation de fonctionnalités du système *Microsoft* détourné.** Aucune opération anormale vis-à-vis du fonctionnement nominal du système n'est réalisée. En effet, une application légitime, ici la calculatrice, utilise des DLL situées dans son répertoire. En outre, le fait que l'application en question utilise des librairies dynamiques de liens avec un nom légitime pour s'exécuter, il devient donc difficile de séparer les DLL légitimes des DLL malveillantes.

- **Un fonctionnement possible sans laisser de trace sur le disque.** Dans le cas de *Qbot*, les DLL sont téléchargées sur le système puis exécutées, mais il existe une variante à ce genre d'attaques. Si l'attaquant ne veut pas laisser de traces sur le disque, il peut tout à fait faire en sorte que la DLL qu'il aura fabriquée ne comporte pas de code malveillant. Ce dernier peut être chargé et exécuté depuis un serveur distant. Ainsi il n'y aura aucune trace de fichiers malveillants en local, mais uniquement celui d'un fichier exécutant, en mémoire, du code à distance.

Pour conclure, la plupart de ces techniques permettent de contourner les systèmes de protection simples. Néanmoins, seuls, elles ne suffisent pas face à des technologies de détections sophistiquées. En effet, ces dernieres, comme les EDRs (Endpoint Detection and Response), sont très intéressants du point de vue de la détection sur des systèmes d'entreprises génériques. Si nous considérons que cette solution est suffisante, cela revient à mettre de côté tous les systèmes industriels, bancaires et autres qui ne peuvent pas bénéficier de ces technologies pour diverses raisons.

Ainsi, il est légitime de réfléchir aux moyens nécessaires pour protéger efficacement ces systèmes cruciaux. Pour répondre à cette problématique, l'une des approches envisageables repose sur la détection à partir des flux réseaux. La première solution serait de restreindre les flux de manière à ce que le téléchargement de DLL soit exclusivement autorisé via *Windows Update*. Cependant, il est important de souligner que cette solution, bien que simple à mettre en œuvre, n'est pas toujours réalisable. En effet, certaines applications industrielles peuvent parfois nécessiter le téléchargement direct de ressources depuis le site du fabricant.

Une autre solution consiste à exploiter la reconstruction des fichiers en transit sur le réseau. Une fois cette reconstruction achevée, grâce à un processus d'analyse de menace en profondeur, Il est possible de déterminer si le fichier téléchargé (la DLL dans ce cas) est malveillant.

Nous pouvons également renforcer les capacités de détection en utilisant le flux de renseignement sur les menaces (ou flux CTI pour Cyber Threat Intelligence). À ce jour, les analystes de l'équipe Purple de Gatewatcher ont repéré plus de 18 000 liens renvoyant à des DLL malveillantes au cours des six derniers mois. Cette compilation d'indicateurs de compromission permet ainsi d'enrichir les mécanismes de détection en proposant des règles fondées sur ces données mises à jour quotidiennement.

ID	Technique
T1574.001	DLL Search Order Hijacking
T1574.002	DLL Sideloading
T1055.001	DLL Injection
T1218	System Binary Proxy Execution

TTP en lien avec les techniques d'attaques décrites dans cet article

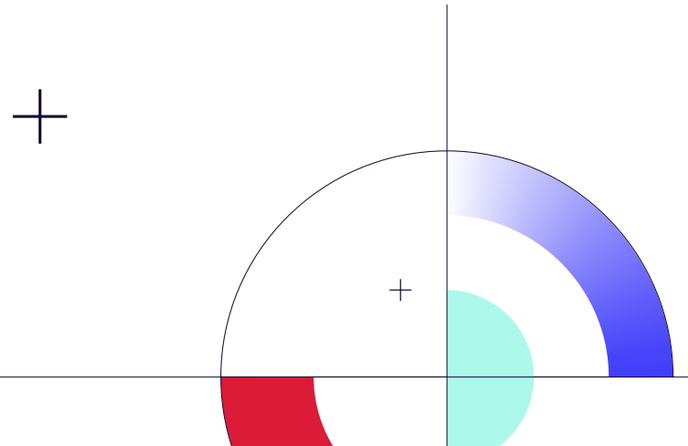
PowerDrop et PowerStar : la montée en puissance de PowerShell dans le monde des Malwares

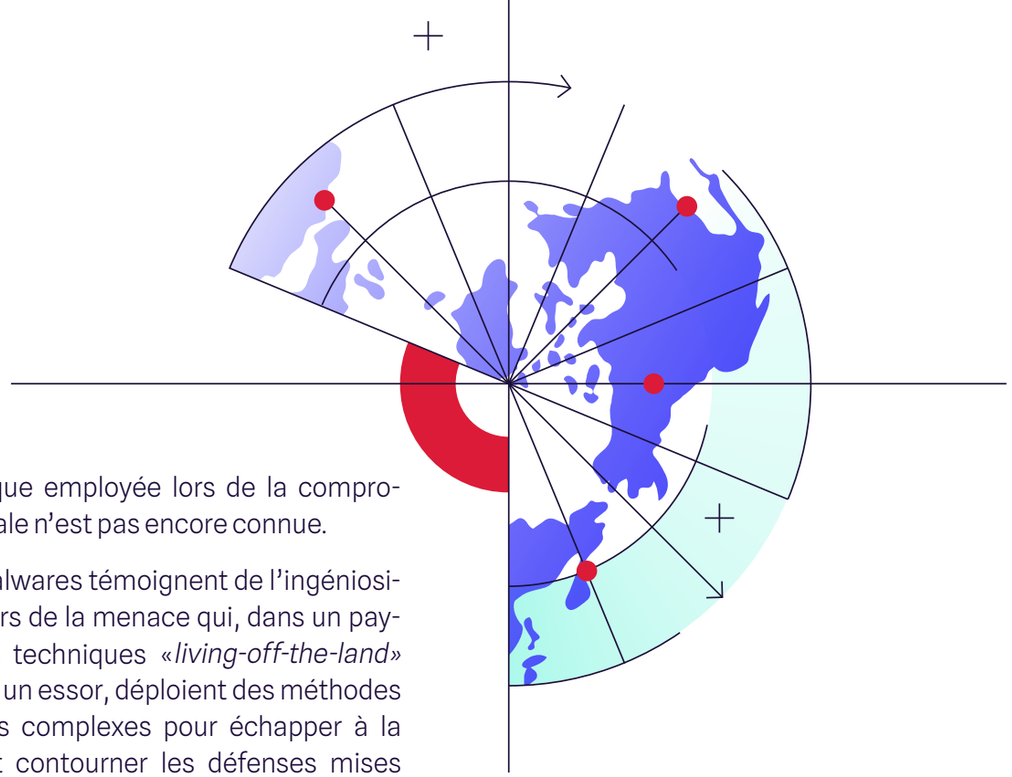
PowerShell, cet outil puissant et polyvalent développé par Microsoft, est devenu un atout de choix pour les cybercriminels cherchant à élaborer des malwares sophistiqués. À ce titre les malwares PowerDrop et PowerStar, basés sur PowerShell et qui ont récemment attiré l'attention, illustrent la montée en puissance de cette technologie dans le monde des cyberattaques.

Les cybercriminels tirent parti des avantages offerts par PowerShell pour exploiter les outils déjà présents sur les ordinateurs ciblés, une pratique connue sous le nom de *«living off the land»*. Cette approche permet aux attaquants de se fondre parmi les activités normales de l'environnement informatique, minimisant ainsi les traces laissées derrière eux et rendant la détection plus difficile.

Les scripts malveillants PowerShell sont souvent utilisés comme «loaders» lors de la phase initiale d'une attaque, notamment via des macros-office. Ensuite, ils sont mis à profit pour effectuer des mouvements latéraux, permettant ainsi aux menaces de se propager à l'intérieur du réseau et d'exécuter des commandes à distance directement en mémoire. Cette capacité d'exécution rend l'investigation post-incident plus difficile, car le malware n'a pas besoin d'écrire sur le disque dur et laisse donc peu de trace.

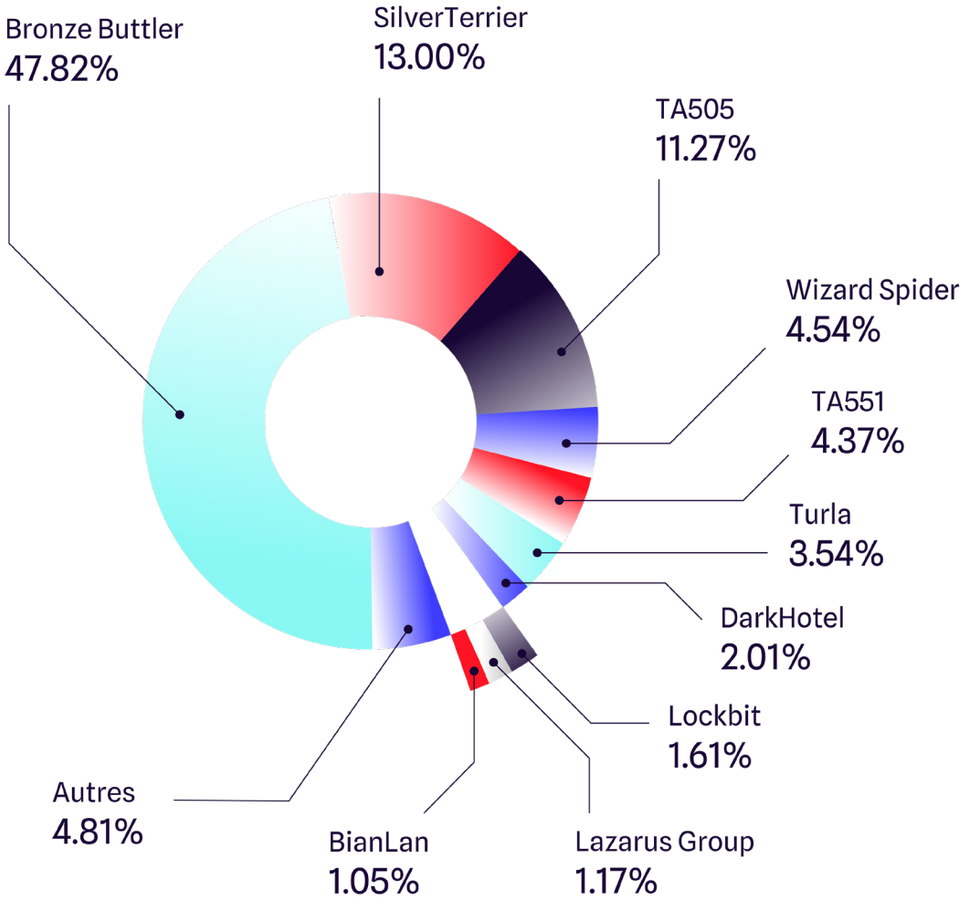
Parmi ces malwares, PowerStar, également connu sous le nom de CharmPower (*S0674*)[1], a été lié au groupe de cyberattaquants Charming Kitten (*G0059*)[2], originaire d'Iran. Initialement découvert en janvier 2022 lors d'attaques exploitant les vulnérabilités Log4Shell[3] dans des applications Java accessibles au public, ce malware a depuis été impliqué dans plusieurs campagnes, démontrant une volonté d'améliorer ses tactiques et de renforcer sa sécurité opérationnelle. Des mesures innovantes, telles que la livraison séparée de la méthode de déchiffrement du code initial et l'utilisation d'une infrastructure d'hébergement privée comme Backblaze et IPFS ont été intégrées pour distribuer le malware et compliquer toute analyse éventuelle. Il a été observé que Charming Kitten tentait de distribuer POWERSTAR via des messages de spear-phishing contenant un fichier LNK à l'intérieur d'un fichier RAR protégé par mot de passe.





De son côté, PowerDrop s'est récemment manifesté en ciblant l'industrie aérospatiale aux États-Unis. Ce malware utilise des tactiques sophistiquées pour se soustraire à la détection, telles que l'utilisation de leurres, l'encodage et le chiffrement. Découvert chez un sous-traitant américain de la défense aérospatiale en mai dernier, PowerDrop utilise PowerShell et Windows Management Instrumentation (WMI) pour installer un Remote Access Trojan (RAT) persistant sur les réseaux des victimes. Son fonctionnement repose sur l'envoi de messages de requête de protocole de contrôle Internet (ICMP), servant de déclencheur pour son système de commande et de contrôle, tandis que des techniques de ping ICMP similaires sont utilisées pour exfiltrer des données. Pour le moment, la méthode d'infection spécifique employée lors de la compromission initiale n'est pas encore connue.

Ces deux malwares témoignent de l'ingéniosité des acteurs de la menace qui, dans un paysage où les techniques «*living-off-the-land*» connaissent un essor, déploient des méthodes toujours plus complexes pour échapper à la détection et contourner les défenses mises en place sur les terminaux. La montée en puissance de PowerShell dans le monde des malwares semble inéluctable, car les acteurs de la menace découvrent constamment de nouvelles façons de l'exploiter pour exécuter des attaques sophistiquées. Les organisations doivent donc rester en alerte et renforcer leurs mesures de sécurité pour contrer cette tendance croissante.



3 Threat *Actors_*

Dans cet éclairage, émerge ce classement qui met en lumière certains de ces acteurs éminents. Des noms tels que Bronze Butler, TA505 Wizard Spider, ou encore Turla surgissent, chacun avec ses compétences uniques et des objectifs bien définis, dessinant ainsi les contours d'un paysage numérique complexe.

Les tactiques employées par ces cybercriminels deviennent de plus en plus sophistiquées, que ce soit dans les méthodes d'évasion qu'ils emploient ou dans la manière dont ils ciblent leurs victimes. L'innovation et l'adaptabilité sont devenues leurs atouts clés, leur permettant de naviguer dans un environnement numérique en constante évolution.

Attaques par la chaîne d'approvisionnement : le défi de la résilience dans un monde interconnecté

Les attaques par chaîne d'approvisionnement *(T1195)* sont devenues un sujet préoccupant ces derniers mois, en raison de leur augmentation significative. Les cybercriminels exploitent les vulnérabilités présentes dans la chaîne d'approvisionnement logicielle des organisations pour compromettre leurs systèmes et accéder à des données sensibles. Selon les estimations de Gartner, pas moins de 45 % des organisations seront victimes d'une attaque par chaîne d'approvisionnement logicielle, d'ici à 2025. Le succès de ces attaques est principalement dû à leur rentabilité pour les acteurs malveillants. En effet, le retour sur investissement obtenu à partir d'une seule attaque par chaîne d'approvisionnement dépasse de loin tout autre type d'attaque dans l'industrie de la cybercriminalité puisqu'une seule compromission peut aboutir à des centaines, voire des milliers de victimes.

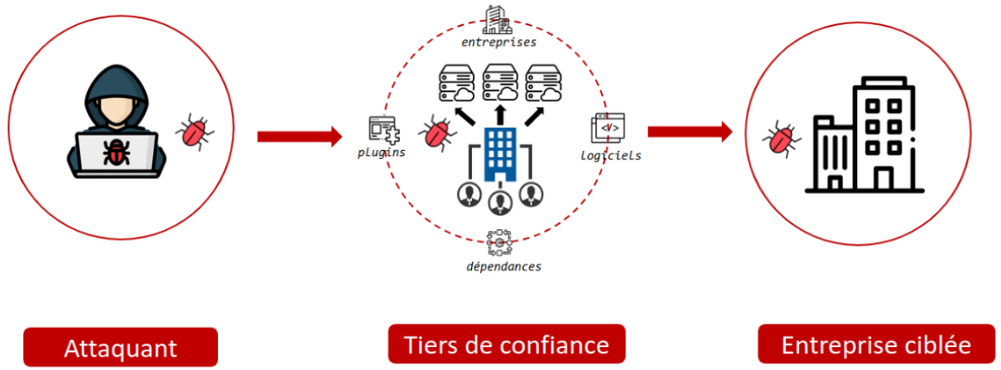


SCHÉMA ILLUSTRANT UNE ATTAQUE PAR CHAÎNE D'APPROVISIONNEMENT

Les précurseurs des attaques par chaîne d'approvisionnement

Attaque CCleaner_

Ces attaques sont à l'origine de piratages dévastateurs à l'image de l'attaque ayant visé le logiciel CCleaner en 2017. Les cybercriminels ont réussi à compromettre le logiciel populaire de nettoyage et d'optimisation système, CCleaner, en insérant un code malveillant dans l'une de ses mises à jour officielles. Cette version corrompue a été téléchargée par des millions d'utilisateurs, exposant ainsi leur système à un risque sérieux de compromission.

Attaque NotPetya_

Un autre exemple majeur est l'attaque NotPetya *(S0368)* également en 2017, qui a été menée par le groupe Sandworm *(G0034)*. Initialement masquée en tant que ransomware, NotPetya était en réalité un wiper *(S0041)* conçu pour se propager rapidement à travers les réseaux. L'attaque a commencé par infecter la chaîne d'approvisionnement de la société de comptabilité MeDoc en Ukraine. À partir de là, le malware s'est propagé via les mises à jour logicielles légitimes de MeDoc à de nombreuses organisations dans le monde entier, entraînant des pertes financières massives et des dommages considérables pour des entreprises de renom.

Attaque SolarWind_

De même, l'attaque SolarWinds *(C0024)* en 2020, qui a secoué le monde de la cybersécurité, a été attribuée au groupe APT29 (aussi connu sous le nom de Cozy Bear) *(G0016)*, présent dans le top 10. Dans cette attaque d'une ampleur sans précédent, les cybercriminels ont réussi à compromettre le réseau de SolarWinds, un fournisseur de logiciels de gestion des réseaux largement utilisé par de nombreuses grandes entreprises et agences gouvernementales. En introduisant discrètement un code malveillant dans une mise à jour logicielle, les attaquants ont pu accéder aux systèmes de centaines d'organisations clientes de SolarWinds. Cette attaque sophistiquée a été une véritable prise de contrôle à grande échelle, mettant en lumière les vulnérabilités critiques présentes dans les chaînes d'approvisionnement logicielles.

Les attaques récentes sur PyPI et NPM mettent en évidence les vulnérabilités des gestionnaires de packages

Le 20 mai dernier, PyPI, le gestionnaire officiel de packages Python, a pris une mesure sans précédent en annonçant la suspension temporaire de l'enregistrement de nouveaux utilisateurs et de nouveau projet à la suite d'une découverte inquiétante faite le même jour sur l'Index des Packages Python (PyPI). Des acteurs malveillants ont introduit un cheval de Troie d'accès à distance (RAT) et un voleur d'informations entièrement équipé dans PyPI. Cette attaque, baptisée *«Colour-Blind»*, illustre comment les pirates informatiques intègrent aisément les fonctions courantes de logiciels malveillants dans des langages modernes tels que Python. De plus, les chercheurs à l'origine de cette découverte ont également remarqué que *Colour-Blind* partage de nombreuses similitudes avec le malware W4SP, découvert en novembre 2022, indiquant ainsi une possible relation entre les deux. Ces attaques soulèvent l'importance pour les organisations de procéder à une surveillance attentive de l'utilisation des packages l'utilisation de packages open-source et de mettre en place des mécanismes de sécurité pour détecter les dépendances tierces malveillantes.

Brainleeches est une opération malveillante qui a également suscité de vives inquiétudes. Cette campagne qui a débuté en mai dernier a visé le référentiel open source npm et s'est avérée être une campagne «double usage» sans précédent. En exploitant la plateforme npm, ses auteurs ont publié plus d'une douzaine de paquets malveillants qui ciblaient à la fois les utilisateurs finaux d'application et les utilisateurs de Microsoft 365. Les packages malveillants ont été conçus pour faciliter des attaques d'hameçonnage et compromettre la chaîne d'approvisionnement logicielle. Pour mener à bien cette opération, les cybercriminels ont imité des paquets npm légitimes et largement utilisés, tels que jquery, afin de tromper les utilisateurs et d'éviter la détection. Heureusement, grâce à une intervention rapide, les paquets malveillants ont été retirés de npm avant de causer des dommages généralisés.

Attaque par la chaîne d'approvisionnement chez 3CX : une chaîne de réaction inédite

La société 3CX a récemment fait face à une attaque de la chaîne d'approvisionnement qui a soulevé des inquiétudes quant à la sécurité et à la résilience des réseaux interconnectés. L'attaque, liée à des pirates informatiques présumément soutenus par la Corée du Nord, a eu des répercussions importantes sur l'entreprise et ses clients. Selon les experts de la société de cybersécurité Mandiant, cette attaque a été rendue possible par une chaîne d'approvisionnement compromise qui a débuté avec l'insertion d'un code malveillant dans l'application X_Trader édité par la société Trading Technologies, X_Trader a ensuite été téléchargé et utilisé ultérieurement par un employé de 3CX. Ce code malveillant a ensuite permis aux attaquants d'accéder au réseau de 3CX, d'infecter son logiciel et de compromettre une large partie de sa base de clients. Cette attaque par chaîne d'approvisionnement, qui a fait l'objet d'une note en mai dernier sur notre site (gatewatcher.com/threat-barometer/mai-2023/), est particulièrement préoccupante, car elle a montré comment un seul groupe de pirates peut utiliser une attaque pour en mener une autre, entraînant une réaction en chaîne de la chaîne d'approvisionnement.

La vulnérabilité zéro-day de MOVEit révèle les risques des solutions éditeurs

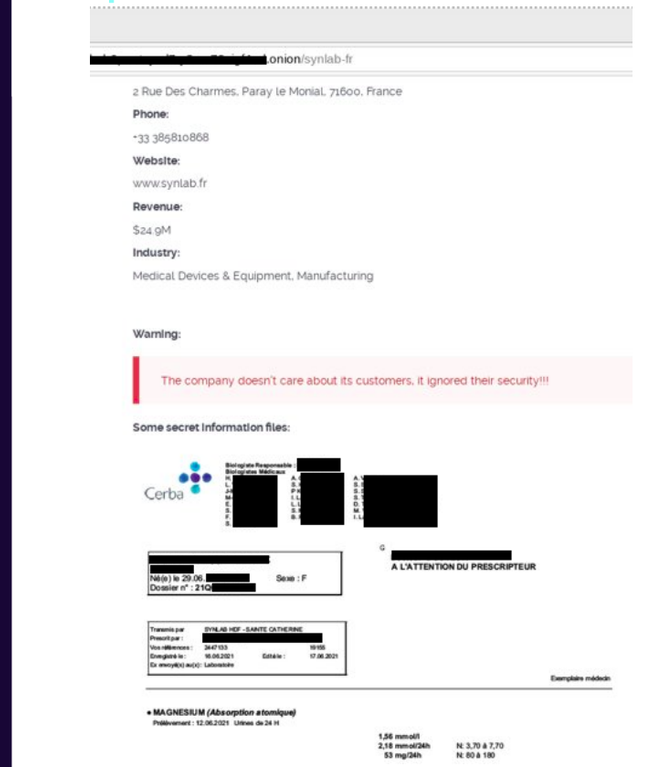
Le logiciel de transfert sécurisé MOVEit, développé par la société Progress Software, a été la cible d'une série d'attaques par chaîne d'approvisionnement, avec pour origine l'exploitation d'une 0day.

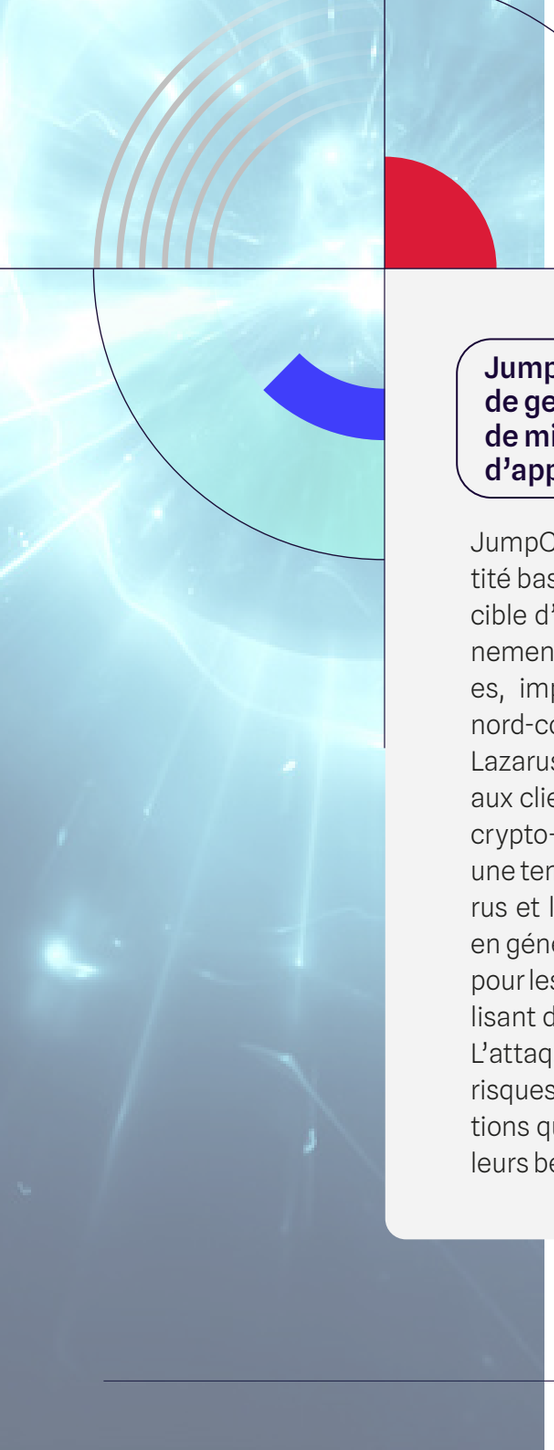
Cette vulnérabilité critique, communiquée le 31 mai, était une faille d'injection SQL présente dans l'application web MOVEit Transfer. Les attaquants ont exploité cette vulnérabilité pour extraire des informations des bases de données des victimes, exécuter des requêtes SQL malveillantes et manipuler voire supprimer des données sensibles. Officiellement identifiée sous le nom de CVE-2023-34362 avec un score CVSS de 9,8 (critique), cette vulnérabilité a été largement exploitée dans la nature avant son signalement et sa correction par le Progress Software. D'autres vulnérabilités liées à l'injection SQL ont été découvertes, notamment la CVE-2023-35036 et la CVE-2023-35708, offrant aux attaquants un accès privilégié et la possibilité d'exfiltrer des fichiers ou de déployer des logiciels malveillants tels que des rançongiciels.

L'entreprise Zellis, qui assure des services de paie pour diverses entités au Royaume-Uni telles que British Airways (BA), BBC, Boots et DHL, a également été touchée par cette série d'attaques. Comme de nombreuses autres organisations, Zellis utilise le logiciel MoveIT pour gérer ses transferts de fichiers, et c'est par le biais de cette plateforme que les attaquants ont réussi à accéder aux données personnelles des employés.

La gravité de ces attaques est encore accentuée par le fait que le groupe de ransomware Cl0p a revendiqué son exploitation depuis 2021, suggérant que les pirates étaient conscients de ces vulnérabilités bien avant leur divulgation publique. Cette longue période d'exploitation a permis aux attaquants de compromettre avec succès de nombreuses organisations, dont certaines grandes entreprises et des entités gouvernementales. Les événements récents ont mis en évidence l'ampleur du problème, avec plus de 500 organisations impactées, notamment des entreprises bien connues telles que Shell, Deloitte ou encore en France les laboratoires Synlab comme en atteste la capture figurant à droite de cette page

CAPTURE D'ÉCRAN PROVENANT DU SITE DE CL0P ET MONTRANT UNE FUITE DE DONNÉES LIÉE À LA SOCIÉTÉ SYNLAB





JumpCloud : un fournisseur de gestion d'identité dans la ligne de mire des attaques par chaîne d'approvisionnement

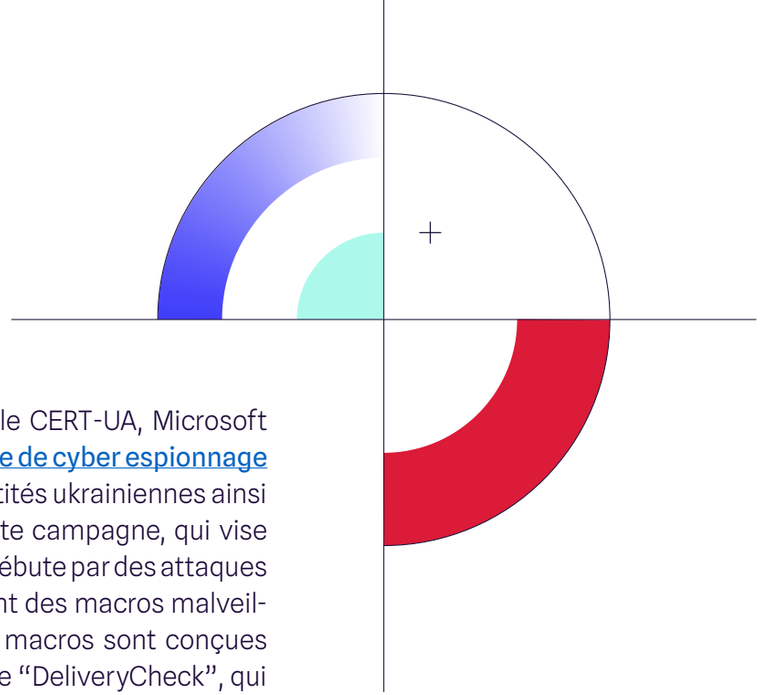
JumpCloud, un fournisseur de gestion d'identité basé sur le cloud, est également devenu la cible d'une attaque par chaîne d'approvisionnement. L'incident, révélé début juillet 2023 es, impliquait un acteur parrainé par l'État nord-coréen connu sous le nom de groupe Lazarus, qui a piraté des comptes associés aux clients de JumpCloud dans le secteur des crypto-monnaies. Cette attaque s'inscrit dans une tendance bien établie pour le groupe Lazarus et les groupes d'attaquants nord-coréens en général, qui ont montré un intérêt croissant pour les crypto-monnaies et les entreprises utilisant des infrastructures liées à la blockchain. L'attaque sur JumpCloud met en évidence les risques auxquels sont confrontés les organisations qui dépendent de fournisseurs tiers pour leurs besoins en gestion d'identité et d'accès.

En conclusion, les attaques par chaîne d'approvisionnement représentent un défi de taille dans notre monde interconnecté. Ces derniers mois, leur augmentation significative a mis en évidence la nécessité pour les organisations de renforcer leur résilience et leur sécurité face à cette menace croissante. La RSA Conference, qui s'est tenue le 8 juin dernier, est l'une des principales conférences mondiales en matière de cybersécurité, et elle a souligné l'importance de sécuriser toute chaîne d'approvisionnement dans un contexte de cybercriminalité en constante évolution. L'ENISA a également publié un dossier intitulé «Good Practices for Supply Chain Cybersecurity», qui offre un aperçu des pratiques actuelles de cybersécurité de la chaîne d'approvisionnement appliquées par les entités essentielles et importantes de l'UE.

Pour protéger efficacement leurs systèmes et données sensibles, il est essentiel que les organisations mettent en œuvre des pratiques de sécurité robustes tout au long de leur chaîne d'approvisionnement logicielle. Cela inclut une surveillance continue des dépendances tierces, la mise en place de contrôles de sécurité rigoureux sur les gestionnaires de packages, ainsi qu'une sensibilisation accrue des employés aux risques liés aux attaques par chaîne d'approvisionnement.

> **“Alors que nous avançons vers un avenir où l'intelligence Artificielle sera de plus en plus nativement intégrée aux systèmes d'informations, les enjeux de la supply chain prendront une nouvelle dimension. Les chercheurs et développeurs en IA devront eux aussi relever le défi de garantir la provenance des données utilisées pour former les modèles d'IA. Il faudra donc développer de nouvelles recherches, de nouvelles meilleures pratiques et de nouvelles technologies pour assurer la sécurité de cette nouvelle forme d'approvisionnement en données.”**

Turla : L’espionnage Russe qui défie le temps

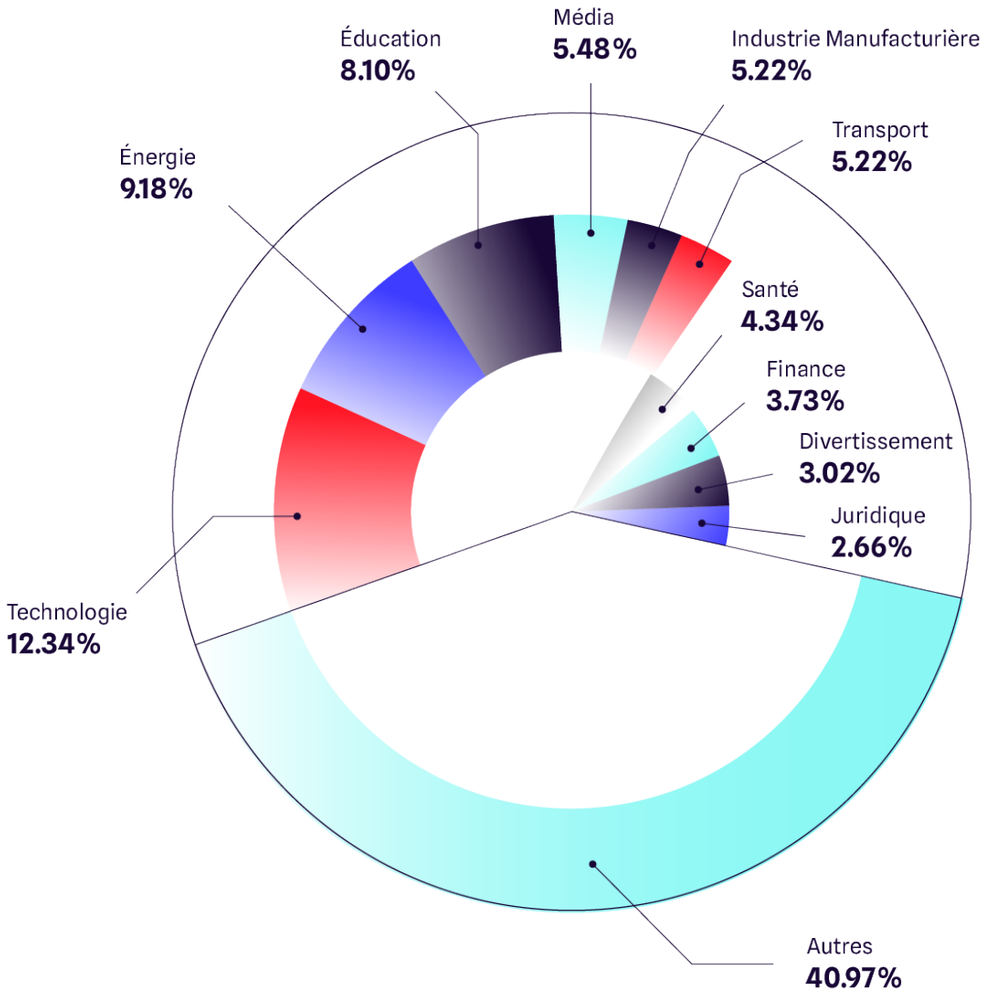


Le groupe de cyberespionnage Turla *(G0010)*, étroitement lié au FSB, le service de renseignement intérieur russe, s’est distingué par sa ténacité et la sophistication de ses opérations. Actif depuis le début des années 2000, ce protagoniste a principalement ciblé les gouvernements membres de l’OTAN ainsi que d’autres entités avec une importance stratégique.

Au cœur de leur arsenal se trouve Snake, un malware emblématique pour le groupe Turla, qui l’a exploité sur près de deux décennies dans plus de 50 pays pour dérober des informations sensibles dans plus de 50 pays. L’opération MEDUSA lancée en mai dernier a néanmoins sérieusement compromis cette pérennité. Menée en collaboration avec le Département de la Justice des États-Unis et d’autres agences partenaires, MEDUSA a en effet permis de neutraliser le malware Snake. Le Cybersecurity and Infrastructure Security Agency (CISA) a publié un article très complet sur le sujet, fournissant des informations détaillées sur le fonctionnement du malware.

Plus récemment, en collaboration avec le CERT-UA, Microsoft a mis en évidence une nouvelle campagne de cyber espionnage menée par le groupe Turla, ciblant des entités ukrainiennes ainsi que d’autres pays d’Europe de l’Est. Cette campagne, qui vise principalement le secteur de la défense, débute par des attaques de phishing, où des documents contenant des macros malveillantes sont utilisés comme appâts. Ces macros sont conçues pour installer une porte dérobée nommée “DeliveryCheck”, qui assure sa persistance en se lançant en mémoire via une tâche planifiée.

Ces événements récents illustrent la vigueur persistante du groupe Turla dont l’ingéniosité continue de représenter une menace sérieuse malgré les efforts déployés pour le neutraliser.



4 Secteurs_

Dans notre classement des secteurs d'activité les plus ciblés par les cyberattaques au cours du premier semestre 2023, on retrouve sans surprise le secteur des technologies, le secteur de l'énergie ou encore ceux de la manufacture et financier : des secteurs dynamiques et prospères qui attirent les convoitises. Cependant, deux secteurs se démarquent en raison de leurs enjeux stratégiques : celui de la santé, déjà évoqué dans notre premier rapport avec l'incident du Centre Hospitalier Sud Francilien attaqué par LockBit début 2022, et celui de l'éducation, qui s'est soudainement hissé en troisième place.

Rançongiciels 101 : le secteur scolaire tire des leçons

La présence du secteur de l'éducation en tête de notre classement ne constitue pas une surprise compte tenu de son actualité en matière de cyberattaques. Les infrastructures informatique des établissements de l'enseignement secondaire et supérieur ont été particulièrement visées par des attaques de rançongiciels sur le premier semestre de 2023. Bien que victime de quelques attaques par rançongiciel notables en 2022, avec en particulier celles ayant touché l'INP de Toulouse mi-septembre et l'IUT Paris – Rives de Seine début décembre, la France demeure relativement épargnée par rapport à l'ampleur du phénomène aux États-Unis et dans les pays anglophones.

Pourquoi le secteur de l'éducation est-il particulièrement ciblé ?

À l'image des hôpitaux, et plus généralement, des systèmes industriels, les écoles et universités souffrent d'un manque important et récurrent de ressources et présentent les facteurs de risque suivants :

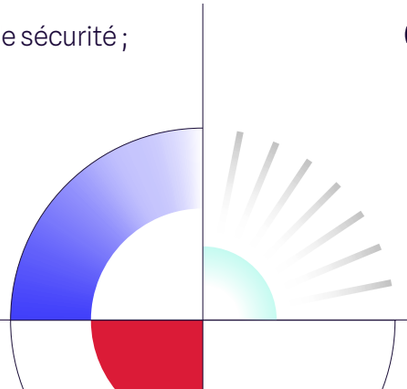
- Un manque de maturité comparé à d'autres secteurs prolifiques comme les banques ou les entreprises privées, déjà préparés à ces menaces depuis longtemps ;
- Un manque d'investissement récurrent dans des outils de cyberdéfense et des retards concernant le déploiement des mises-à-jour et correctifs de sécurité ;
- Un manque de personnel formé pour faire face aux risques cyber.

En ajoutant la présence de données confidentielles sur le personnel enseignant et les étudiants, ces deux éléments font du système éducatif une cible privilégiée pour les attaquants, qui ne font pas de la sécurité informatique une priorité.

En France, François Gilles, directeur des systèmes d'Information de la région académique d'île-de-France (DRASI) indique que «le numérique est désormais omniprésent dans le fonctionnement des établissements et irrigue tous les services», ce qui n'est pas spécifique à l'éducation, mais «donne aux hackers une surface d'attaque très significative». Il ajoute aussi que «les acteurs de la cyber malveillance peuvent parfois être des élèves eux-mêmes».

Au de-là d'attaques par rançongiciel, les attaquants qui ciblent l'éducation en France visent :

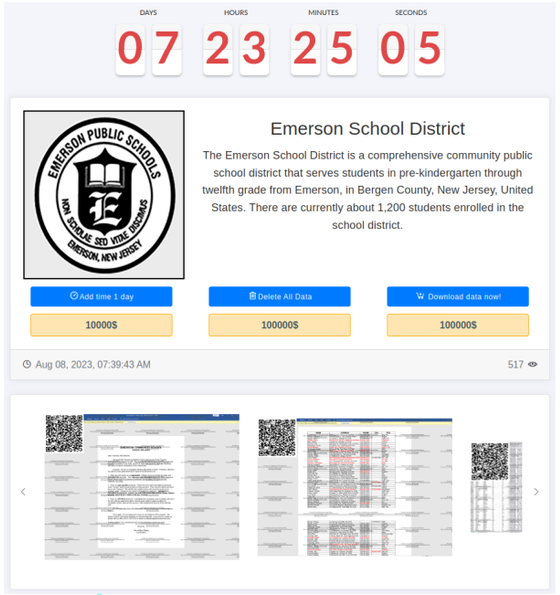
- Les bases de données évidemment, mais aussi les comptes d'accès des élèves et des enseignants, ainsi que toutes informations confidentielles qui peuvent se revendre ;
- Le sabotage d'organisations d'épreuves nationales ou de campagnes d'affectation via Parcoursup ;
- L'obtention de renseignements technologiques et techniques au travers des établissements de recherche.



Qui attaque ?

Les purs et durs sans états d'âme_

Les auteurs de ces attaques massives sont essentiellement les opérateurs de rançongiciels, qui chiffrent les données présentes sur le système d'informations et exigent en contrepartie une rançon pour le déchiffrement. Désormais, il est même monnaie courante d'exfiltrer les données des victimes et de menacer de les divulguer si la rançon n'est pas payée dans le temps imparti, procédé connu sous le nom de double extorsion. Ces groupes disposent souvent d'un site vitrine sur le dark web sur lequel ils publient les attaques effectuées par eux ou par leurs affiliés, ainsi qu'un échantillon des données piratées tant que le compte à rebours pour la rançon est en cours, et les données complètes quand le temps est écoulé.



DEMANDE DE RANÇON VISANT UNE ÉCOLE PUBLIQUE AMÉRICAINE VUE SUR LE SITE VITRINE DE MEDUSA, ACCOMPAGNÉE D'UN ÉCHANTILLON DE DOCUMENTS

Les documents publiés sur ces plateformes ne sont généralement pas triés, ni organisés, nécessitant une exploration minutieuse. L'analyse a mis en évidence des documents financiers et administratifs liés aux institutions éducatives, notamment des extraits bancaires, des fiches de paie, des audits internes, ainsi que des informations personnelles comme des passeports, des documents de santé, des données bancaires et globalement toutes informations concernant les étudiants et les membres du personnel comme leur adresse, date de naissance, numéros de téléphone et photos.

Parmi ces attaquants, les plus actifs sont Vice Society, BianLian, Medusa ou encore AvosLocker, auteur de attaque de l'INP de Toulouse, qui divulguent de nombreuses données en moyenne plusieurs fois par semaine en les publiant sur leur site vitrine. Déjà bien connus, ces groupes malveillants sans scrupules ne considèrent pas le secteur de l'éducation comme une exception : aux États-Unis des établissements de l'école primaire aux études supérieures, publics ou privés sont indifféremment pris pour cible. Tout opportunité est considérée si potentiellement lucrative.

Le 11 mai 2023, le CISA publiait un rapport concernant l'exploitation de la CVE-2023-27350 qui permet une exécution de code à distance sans authentification sur certaines versions des logiciels PaperCut NG et PaperCut MF. Ces solutions de gestion d'impression papier sont utilisées par plus de 100 millions d'utilisateurs selon l'éditeur, y compris par les établissements d'éducation. Le groupe Bl00dy Ransomware Gang a rapidement tenté d'exploiter cette vulnérabilité pour mener des attaques, bien que le CISA n'ait pas fourni de détails spécifiques sur les cibles visées.

Les voyous au grand cœur_

Il existe au contraire des groupes qui présentent une certaine éthique. L'opérateur du rançongiciel LockBit, dont le modèle économique est le Ransomware-as-a-Service, impose une liste de règles pour les groupes affiliés qui utilisent le rançongiciel. Cette liste, disponible sur le site vitrine de LockBit, stipule clairement les cibles que l'opérateur permet d'attaquer. Dans le cas des établissements d'enseignement, LockBit autorise les attaques à condition que les établissements soient privés et qu'ils génèrent des revenus. La liste des cibles peut également mentionner des «public universities», car ces établissements aux États-Unis pratiquent des frais de scolarités, parfois élevés qui les rendent attractifs.

Les indécis_

On trouve enfin une troisième catégorie de groupes auteurs d'attaques par rançongiciel : ceux pour qui le positionnement n'est pas très clair. Le groupe responsable du rançongiciel Royal a communiqué mi-juillet qu'il refusait de partager les données qu'il avait récupéré de Braintree Public Schools, en précisant «respecter le caractère sacré des services d'éducation et de soins de santé». Très louable mais tout aussi étonnant quand on peut lire un mois plus tôt sur leur blog que le groupe menaçait de divulguer les informations personnelles des étudiants et employés d'une autre école. Peut-être un changement de cap de leur part.

De façon similaire, l'opérateur ALPHV (aussi connu sous le nom de BlackCat) a supprimé de son site des données volées par un groupe affilié, qui étaient liées à un centre de soins mentaux en précisant que l'affilié avait enfreint les règles. Nous n'avons pas trouvé les règles encadrant les attaques de cet opérateur, il est d'ailleurs souvent rare de mettre la main dessus.

De l'éducation à la maturité

En matière de protection du secteur de l'éducation, le CISA prend son rôle à cœur et s'engage dans la sécurisation du système public allant de la maternelle au lycée, ce que l'on nomme communément outre atlantique les «K-12 schools». L'agence américaine met à disposition sur son site de nombreuses ressources, outils et programmes pour aider les écoles à anticiper, se protéger et atténuer les risques et menaces. Bien qu'il n'existe pas d'équivalent français, et qu'aucune mesure ne semble avoir été mise place par l'ANSSI (peut-être parce que la France est moins impactée), l'agence nationale intervient tout de même en réponse à des incidents liés aux attaques par rançongiciel qui ont lieu à l'encontre des établissements d'éducation, et plus généralement pour toutes attaques par chiffrement, peu importe le secteur.

Le niveau de maturité du secteur face aux menaces cyber est bien en développement, l'éducation se rend compte qu'elle est très vulnérable face aux attaques informatiques. Les équipes de Gatewatcher constatent régulièrement la réalité de cette prise de conscience lors de leurs échanges avec des acteurs de ce secteur, en demande active d'un renforcement de leur cyber protection.

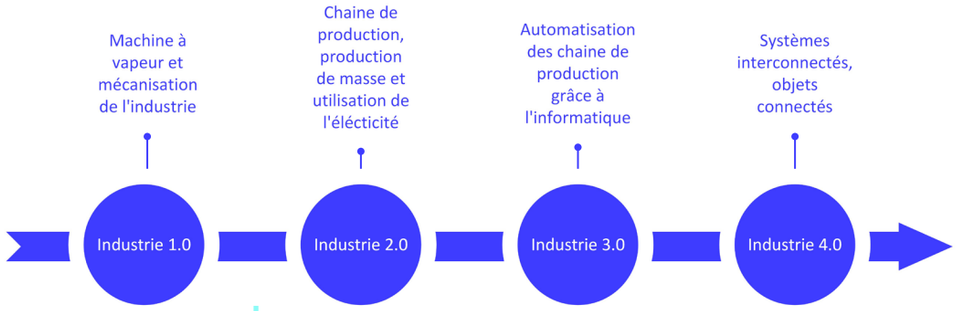
L'industrie : une cible invariée pour les cyberattaquants

Lorsqu'on s'intéresse aux différents secteurs présents dans notre top des domaines les plus ciblés, certains caracolent fréquemment dans les 10 premières places. Ces derniers comme l'énergie, l'industrie de la manufacture, la santé ou encore celle de la haute technologie ont un dénominateur commun. Ils font tous partie du domaine Industriel.

Les cyberattaques visant des systèmes Industriels restent assez peu documentées. Cela tient en partie de leur caractère stratégique, souvent essentiel au fonctionnement d'un pays ainsi qu'à la diversité des domaines concernés.

Dans le passé, l'industrie était considérée comme un système informatique à part, fonctionnant avec ses propres protocoles et rarement connectée directement aux systèmes informatiques de l'entreprise. Cependant depuis quelques années, de plus en plus de systèmes industriels s'ouvrent dans le cadre d'interconnexion globale des réseaux pour maintenir fiabilité et productivité et sont de facto exposés aux cybermenaces. Cette tendance s'est accélérée avec l'arrivée de la pandémie du COVID-19 [0]. En effet, beaucoup d'entreprises de toutes tailles ont dû ouvrir à la hâte leur système de gestion industrielle afin de permettre un accès à distance à leurs employés. Depuis, ce mode de fonctionnement s'est démocratisé et il n'est pas rare de voir des équipements industriels vulnérables exposés sur le web.

L'augmentation de la surface d'attaque n'est pas seulement due à la pandémie et à l'exposition d'équipements industriels en ligne. La volonté d'aller vers une industrie 4.0, de plus en plus automatisée, pose aussi la question de la sécurisation des communications. L'objectif de l'industrie 4.0 est de permettre aux lignes de production, aux systèmes de gestion des stocks et à tous les autres systèmes de l'entreprise de communiquer entre eux afin d'optimiser les coûts tout en réduisant les écarts entre la demande client et le produit final. Cette évolution vise à apporter une flexibilité sans pareille permettant la gestion optimale des automates tout en évitant les risques humains, grâce à un pilotage décentralisé. Cette unification des systèmes visant à créer des réseaux globaux intégrant l'informatique de l'entreprise et les systèmes industriels apporte néanmoins des risques importants. En effet, l'isolement physique des systèmes n'étant plus de mise, sans une segmentation stricte du réseau, une personne ayant la main sur le système de l'entreprise aura également la main sur le système Industriel de cette dernière.



LES DIFFÉRENTES GÉNÉRATIONS DE L'INDUSTRIE

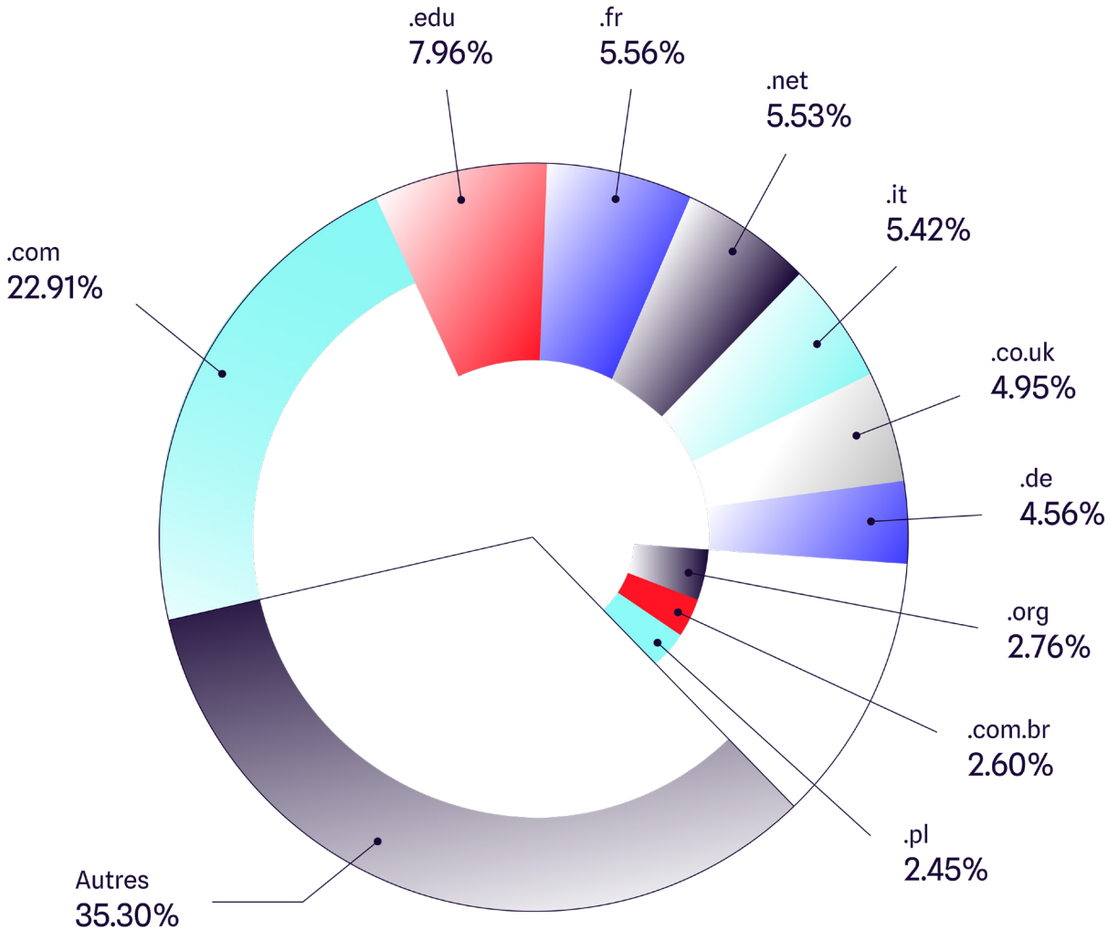
Il est important d'appréhender en quoi l'industrie diffère de l'informatique traditionnelle. Dans un premier temps, les priorités ne sont pas les mêmes : la continuité opérationnelle est primordiale. C'est sur cet axe que les opérateurs de rançongiciels vont jouer, car s'ils bloquent une ligne complète de production, le coût de la rançon peut être inférieur au coût de l'indisponibilité durant la désinfection et/ou la création d'un réseau sain. Dans un deuxième temps, dans ce milieu, les humains et les machines se côtoient continuellement et une prise de contrôle qui pourrait entrainer des dysfonctionnements dans des installations telles qu'un centre de stockage pétrolier ou une centrale nucléaire pourrait avoir des conséquences humaines tragiques au-delà de l'importance stratégique.

Pour expliquer la complexité de la protection des équipements industriels, il est essentiel de prendre en considération plusieurs aspects. Tout d'abord, maintenir le fonctionnement ininterrompu d'une usine revêt une importance capitale, étant donné les conséquences économiques significatives qui découleraient de tout arrêt imprévu. Ensuite, il convient également de reconnaître le rôle crucial de l'historique dans cette problématique. Tant que les équipements fonctionnent correctement, il n'y a aucune raison de les changer, et certains automates peuvent demeurer en place jusqu'à 20 ans, s'ils sont bien entretenus, selon cette infographie de l'entreprise *Euautomation*. Ce chiffre laisse à penser que certains automates sont en service sur les chaînes de production depuis plusieurs décennies. On peut donc légitimement penser que des protocoles historiques, comme Modbus, sont encore en usage, ce qui nécessite des ponts entre ces systèmes plus anciens et les systèmes actuels afin de créer une synergie permettant un travail efficace. Lorsque l'on parle de sécurisation de systèmes industriels, on doit mettre de côté l'installation de tous types de systèmes de détection sur les postes de travail industriels car ces machines, qui assurent la gestion continue des systèmes industriels, ne peuvent être redémarrées sans un potentiel impact sur la production.

Le moyen de protection le plus efficace reste donc les sondes de détection déployées au niveau du réseau. De nombreux attaquants utilisent des techniques de compromission spécifiques aux systèmes informatiques des entreprises, et d'autres spécifiques aux systèmes industriels. Pour couvrir ces deux axes, il est essentiel d'utiliser des systèmes de détection prenant en compte ces deux dimensions.

Nous avons pu constater que la convergence des systèmes informatiques industriels et d'entreprise représente un défi technique en matière de cybersécurité.

> **“Malgré tous les bénéfices en termes de gestion et de production offert par l'industrie 4.0, la complexité croissante de la protection de ces réseaux nous emmène vers une période où l'Industrie restera l'un des secteurs les plus ciblés.”**



5 Fuites *d'identifiants_* (Top Level Domains)

Une nouvelle catégorie fait son entrée dans ce rapport. Elle concerne les TLD (Top Level Domain, ou nom de domaine de premier niveau en français) des identifiants (adresses mail + mots de passe) ayant le plus fuités sur ce dernier semestre. Ces données proviennent de tentatives de phishing, de vols de données par malwares ou simplement de fuites de bases de données collectées par la plateforme de CTI de Gatewatcher.

La première place du top est occupée par le TLD .com qui correspond historiquement aux domaines enregistrés par des entreprises. Les TLD .net et .org correspondent également à des domaines associés respectivement aux entreprises technologiques et aux ONG, projets open-source ou communautés. On observe également une proportion importante de TLD qui correspondent à ceux de pays, comme on peut le voir avec le .fr de la France en troisième position, ou le .it de l'Italie et le .uk du Royaume-Uni en cinq et sixième position.

Finalement, le dernier TLD qui détonne et qui se positionne en deuxième position est celui réservé au système éducatif américain .edu.

Le secteur scolaire américain livre ses secrets

Le secteur de l'éducation est décidément au cœur des problématiques de sécurité informatique.

Le TLD .edu correspond au système éducatif américain, implémenté pour mettre en place une hiérarchie pour les entreprises liées à l'éducation et créer une communauté. Pour pouvoir enregistrer un domaine en .edu aux États-Unis, il faut respecter des critères définis par EDUCAUSE comme être un établissement scolaire secondaire basé sur le territoire américain et être accrédité par une institution du département de l'éducation américain. Dans le reste du monde, d'autres pays respectent cette nomenclature en y ajoutant le TLD respectif de leur pays, comme .edu.au pour l'Australie. Cette tendance n'est cependant pas spécifique aux pays anglophones, on la retrouve sur tous les continents, beaucoup en Amérique du Sud et en Asie, mais aussi en Europe et en Afrique avec la Pologne et le Nigéria pour ne citer qu'eux. Ces pays ne sont cependant pas pris en compte pour la suite de ce thème qui se concentre uniquement sur le TLD .edu qui correspond au système américain.

La carte des états américains les plus ciblés par des fuites de données dans le secteur de l'éducation met en avant une certaine homogénéité des attaques. Certains états se démarquent tout de même : l'état de l'Indiana qui ouvre ce classement a fait face début juillet à une fuite de données de l'Université de l'Indiana qui s'est retrouvée sur le darknet. Cette fuite présentait les noms complets et les adresses mail de quasiment deux cent cinquante mille étudiants et personnels. Un peu plus tôt, le département de l'enseignement supérieur du Colorado indiquait le 19 juin être informé d'une fuite de données qui s'est déroulée du 11 au 19 juin, concernant les informations d'étudiants ayant occupé différents établissements de l'état entre 2007 et 2020.

La fuite de données n'est pas la seule raison qui place l'éducation si haut dans le classement des TLD dont les identifiants ont le plus fuité, le phishing ne rougit pas. Même si le vol d'identifiants reste la menace principale, ce n'est pas la seule contre laquelle les universités américaines mettent leurs étudiants en garde. Bien que les fausses pages de phishing soient monnaie courante, les attaquants font aussi preuve d'originalité en ciblant les étudiants avec des fausses offres d'emploi et une demande de commission pour être considéré. Des fraudes aux frais de scolarité, où les arnaqueurs demandent aux étudiants de leur payer leurs frais de scolarité en échange d'une réduction ou de taux de conversion monétaire intéressants sont aussi observés. Les universités américaines sont de plus en plus vigilantes et sensibilisent leurs étudiants en expliquant les méthodes employées par les attaquants, comment les repérer (faux sentiment d'urgence de la part d'une figure d'autorité, intimidation ainsi que les actions à prendre en cas de méfait (changer ses identifiants, contacter les autorités compétentes.

Les étudiants constituent la partie de la population la plus connectée à Internet et à ses services, donc très enclin à utiliser leur adresse courriel sur de nombreuses plateformes. Cela augmente non seulement la probabilité que leur adresse de courriel soit associée à une fuite de données, mais augmente également la surface d'attaque pour les acteurs de la menace. Si l'on ajoute ce fait aux fuites de données sur les établissements scolaires, souvent par rançongiciels dont nous avons parlé plus tôt dans la partie secteurs ciblés, nous comprenons mieux la place de ce TLD en deuxième position de ce classement. Le double risque associé à la fuite d'identifiants est la facilité pour un attaquant de pivoter d'une plateforme à une autre dans le cas où l'utilisateur utilise le même mot de passe pour plusieurs comptes.

Si les identifiants sont si prisés par les attaquants, c'est parce qu'ils constituent un vecteur d'attaque initial (T1078) facilement exploitable pour pénétrer le réseau des établissements scolaires en se connectant à des services légitimes et ensuite entreprendre une attaque plus large comme le vol des publications issues de la recherche académique, de données personnelles, ou encore, comme vu plus haut dans ce rapport, le chiffrement de systèmes d'information pour demander une rançon, mais aussi pour pouvoir évoluer facilement au sein d'un réseau infecté.

Dans une volonté de prévenir au mieux les attaques par rançongiciels, le CISA a répertorié les méthodes d'attaques, IoCs (IP, domains, outils, scripts), et tactiques et méthodes MITRE relatifs aux principaux opérateurs de rançongiciels. Vice Society ou encore BianLian, utilisent comme vecteur d'entrée initial les identifiants d'employés récupérés à travers du phishing ou via des courtiers d'accès initiaux (IAB, Initial Access Brokers) qui sont des cybercriminels spécialisés dans la revente des données.

Fuites de données : le cas Mercer

Le 9 mai, l'Université Mercer en Géorgie, États-Unis, expliquait via un court communiqué sur leur blog qu'un accès non-autorisé au réseau informatique de l'université avait eu lieu. L'établissement indiquait que, malgré les mesures de sécurité qui avaient été prises pour la protection des données confidentielles des étudiants et enseignants, les numéros de sécurité sociale et les permis de conduire ont été retirés du système informatique par les attaquants, ce qui implique que ces derniers étaient alors en possession de ces informations. L'université précise tenir informés les étudiants et enseignants concernés par la fuite de leurs données personnelles et qu'une enquête a été lancé par les autorités.

La réalité des faits est alarmante : l'attaque aurait affecté près de cent mille personnes, dont le nom, le numéro de sécurité sociale et le permis de conduire ont fuité. L'université n'a contacté les victimes qu'un mois après avoir découvert l'incident, ce qui aurait suscité beaucoup de réactions de la part de ces dernières. Ces données personnelles peuvent par exemple être utilisées par les attaquants comme pour faire de fausses demandes d'emprunt au nom de la victime, ce qui a d'ailleurs été le cas pour une victime qui a indiqué avoir subi des prélèvements bancaires frauduleux.

Les plaignants mettent aussi en cause les normes de sécurité informatique et accusent l'université de ne pas avoir mis en place la segmentation du réseau, ni d'avoir chiffré les informations confidentielles circulant sur le système d'informations, deux éléments qui permettent d'augmenter la sécurité des informations, et plus généralement de l'établissement. Un professeur de Yale qui avait enseigné à Mercer plusieurs années avant l'incident reproche aussi à l'université d'avoir manqué de réactivité dans son enquête et de n'avoir découvert l'exposition des données personnelles que trop tard. L'attaque qui a eu lieu du 12 au 24 avril, n'ayant été découverte que le 30 avril.

Toutes les données des étudiants et enseignants ont depuis fuité et sont disponibles publiquement sur le darknet depuis le 9 mai, soit à la date du communiqué de l'Université Mercer, sur le site vitrine de l'opérateur de rançongiciel Akira, ce qui laisse entendre que Mercer n'a pas souhaité payer la rançon demandée par les attaquants.

ANNONCE DE LA FUITE DE DONNÉES DE L'UNIVERSITÉ MERCER PAR L'OPÉRATEUR DE RANÇONGICIEL AKIRA

Le manque de maturité de ces établissements en fait des cibles faciles pour les attaquants, et la taille non-négligeable de la communauté étudiante et des anciens étudiants engendre des fuites de données massives qui placent le secteur de l'éducation parmi les secteurs dont les identifiants fuitent le plus.

Fuite d’identifiants du secteur Public à l’échelle mondiale

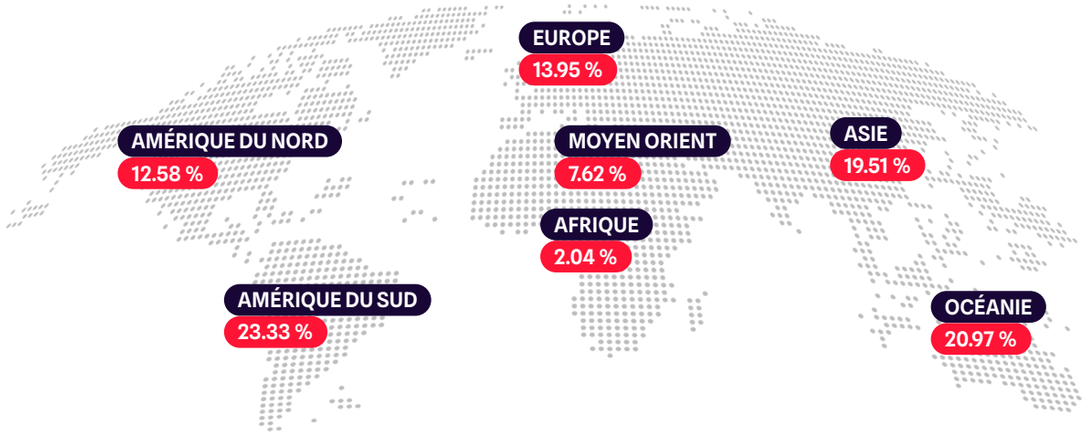
Une technique simple et efficace pour réaliser un vol de données confidentielles ou une intrusion consiste à commencer par accéder à un des utilisateurs de l’entreprise. Les fuites de données et le phishing sont des moyens triviaux et efficaces permettant d’obtenir des accès dans le cas d’une attaque ciblée par simple opportunité.

Actuellement, les fuites d’adresses emails accompagnées des mots de passe sont fréquentes en raison de l’usage répandu de ce système d’authentification. Même si les sociétés et organisations sensibilisent de plus en plus leurs collaborateurs aux risques liés au phishing. Cependant, comme nos analyses CTI nous le confirment, même les entités les plus sensibilisées sur la confidentialité de leurs données comme les ministères, les entités gouvernementales et les services publiques peuvent avoir leurs identifiants exposés sur Internet.

Le pourcentage par rapport à la totalité des données investiguées reste actuellement faible car seul 0.78 % des fuites détectées sont en liens avec ces entités.

L’analyse de la Purple Team concernant ces 0.78 % de fuites d’identifiants a mis en évidence 146 domaines de premier niveau (TLD : top-level domain) différents qui, dans ce cas, impactent plus de la moitié des états sur la période d’analyse de ce rapport.

La répartition des identifiants fuités concernant les services publics d’après les renseignements analysés par la plateforme de CTI de Gatewatcher est la suivante :



Près de la moitié des identifiants sont situés en Océanie et en Amérique du Sud, à cause des nombreuses fuites de données liées aux services publics en Australie, Nouvelle Zélande et Brésil, résultant d’attaques par ransomware et différentes fuites de données.

SECTEURS PUBLICS LES PLUS TOUCHÉS DANS LES RENSEIGNEMENTS CYBER DE GATEWATCHER

Le trio de tête pour les secteurs publics ayant le plus de fuites d'identifiants dans le monde.

1. **Les préfectures et mairies_**
2. **L'éducation_**
3. **La santé_**
4. **La culture_**
5. **Les transports_**
6. **La justice et l'intérieur_**
7. **Les affaires étrangères_**
8. **L'économie et la finance_**
9. **L'énergie_**
10. **La défense_**

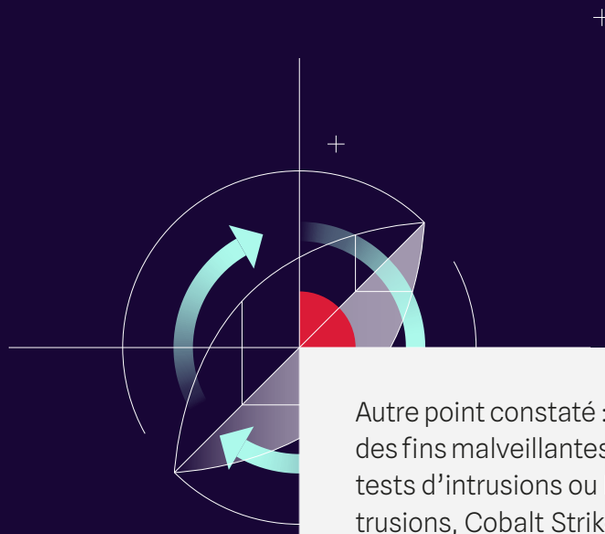
> Dans tous les secteurs, privés comme publics, l'utilisation des fuites de données reste, un moyen extrêmement simple et efficace pour réaliser une intrusion. Il est donc nécessaire de continuer de sensibiliser les utilisateurs à l'importance des risques liés au stockage de données confidentielles et en parallèle d'utiliser l'"Identity Intelligence" pour prévenir le risque d'utilisation de cette surface d'attaque.

*Conclusion_*

Notre observation de l'actualité Cyber du premier semestre 2023 nous permet de dresser quelques premières constatations :

Tout d'abord la persistance de certaines tendances lourdes comme le phishing, le développement de malware pour l'environnement de la firme de Redmond ou encore l'utilisation d'identifiants ayant fuités dans le cadre d'une tentative d'intrusion.

Nous avons porté une attention particulière sur les attaques par la chaine d'approvisionnement (« Supply Chain Attacks ») qui se banalisent et deviennent de plus en plus prisées des groupes de cybercriminels comme en témoigne l'incident lié à 3CX. L'efficacité de ce type d'attaque n'est plus à démontrer dès lors qu'une faiblesse est trouvée chez un éditeur (qu'il soit privé ou une fondation) comme a pu rappeler l'attaque sur le gestionnaire de paquet Pypi. Les éditeurs sont de plus en plus sensibilisés aux risques pour leurs clients et mettent en place des systèmes de détection et de contrôle pour ce type d'attaques. De plus, les instances gouvernementales suivent de près le sujet comme le montre le dossier de l'ENISA «Good Practices for Supply Chain Cybersecurity».



Autre point constaté : l'utilisation de plus en plus courante à des fins malveillantes d'outils légitimes comme les outils de tests d'intrusions ou PowerShell. Pour le cas des outils d'intrusions, Cobalt Strike fait partie des outils les plus utilisés par les acteurs malveillants. La fuite de son code source a permis aux cybercriminels de prendre la main sur cet outil efficace. Même si la société Fortra (propriétaire de Cobalt Strike) tente de réduire son utilisation malveillante, l'outil occupe toujours une place importante dans notre top d'outils malveillants (3eme place). L'utilisation d'outils légitimes complexifie fortement la détection d'incidents de sécurité et oblige les équipes de sécurité à mettre en place une détection spécifique des comportements malveillants en analysant les scripts PowerShell, en traquant les infrastructures Cobalt Strike ou en détectant de communication entre la victime et le serveur C2.

La présence inhabituelle de l'éducation dans le peloton de tête des secteurs le plus ciblés et ainsi la présence significative du TLD ".edu" dans le classement des identifiants fuités a suscité l'intérêt de l'équipe d'investiguer plus en profondeur. L'analyse a révélé que l'éducation est un secteur intéressant pour les cybercriminels au niveau mondial du point de vue financier (propriété intellectuelle, informations personnelles et financières) et par une maturité encore faible de ce secteur face aux risques cyber comme ont pu le montrer les attaques par ransomware ou les importantes fuites de données d'étudiants et des professionnels de l'éducation. Le secteur de l'éducation prend progressivement conscience des risques liés aux cybermenaces comme témoignent les campagnes de sensibilisations dans les universités américaines et le programme "K-12 schools" lancé par le CISA.

Comme il a été mentionné en début de cette conclusion, Windows demeure le système d'exploitation le plus ciblé par les logiciels malveillants et les binaires exécutables représentent toujours une constante majeure dans l'arsenal de cybercriminels constamment à la recherche de nouveaux relais de croissances comme en témoigne cette tendance encore discrète mais émergente de portage de malwares Windows sous Linux ou MacOS.

> **Le suivi des tendances des nouvelles menaces et leur visibilité sont les méthodes les plus efficaces pour réduire les risques cyber et atténuer l'impact des incidents de sécurité.**

À PROPOS DE *Gatewatcher_*

Reconnaître toutes les cyber-attaques, signaler immédiatement la menace et réagir aussi vite que l'éclair. C'est ce que nous appelons la protection instantanée des réseaux. Chez Gatewatcher, nous fournissons une plateforme complète réduisant le temps moyen de détection et réponse au minimum. Notre modèle de protection associe l'IA aux dernières techniques d'analyse du trafic réseau pour offrir une détection en amont du déclenchement de l'attaque ainsi qu'une visibilité à 360° adaptée aux nouveaux besoins des organisations. Disponibles en version On-Premise ou Cloud, nos solutions sont conçues pour être interopérables et immédiatement opérationnelles pour une intégration facilitée dans votre SOC. Chez Gatewatcher, nous vous donnons le pouvoir de protéger votre réseau et la tranquillité d'esprit dont vous avez besoin pour vous concentrer sur votre activité.

NDR_

Gatewatcher NDR est une plateforme ouverte de détection et de réponse réseau offrant une cartographie à 360° des assets présents sur le SI et l'analyse contextuelle des cybermenaces pour une détection instantanée et une visibilité augmentée.

CTI_

Gatewatcher CTI est un service de Threat Intelligence accessible par Feed, TIP ou plugin navigateur qui permet en un temps très court la détection des menaces internes et externes en fournissant des indices de compromissions enrichis et contextualisés à votre activité.

SENSORS_

Gatewatcher Sensor est une solution, certifiée par l'ANSSI, qui garantit une détection de tous les types d'attaque et intrusions sur les infrastructures critiques des organisations les plus critiques et les plus exposées (banque, industrie, énergie, transport...).

TAP_

Gatewatcher TAP est une gamme complète de TAP optiques et cuivre actuellement en cours de qualification par l'ANSSI. Passifs, non alimentés et avec plusieurs ratios de répartition disponibles, ils couvrent tous les besoins de surveillance et de détection réseau.

Sources_

P 7

Schéma *Armitage Screenshot CC-BY-SA*
> Source : wikimedia

Schéma *Cobalt strike screenshot*
> Source : cobaltstrike.com

P 30

Copie écran *Demande de rançon*
> Source : http://medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion

Notes_

P 19

[1] https://attack.mitre.org/software/S0674/

[2] https://attack.mitre.org/groups/G0059/

[3] https://www.ssi.gouv.fr/uploads/2021/12/anssi-communique_presse-log4shell.pdf