GATEWATCHER

CYBER THREATS
SEMESTER REPORT

Janvier – Juin 2022

SOMMAIRE

01 ENJEUX DU RAPPORT ET NOTES AU LECTEUR

Pour cette première édition du Semester Threat Report, son rapport semestriel sur les cybermenaces, la Purple Team de Gatewatcher vous présente les tendances des menaces détectées chaque semestre par la plateforme CTI de Gatewatcher et la veille active des cyber analystes de la Purple Team.

Ce rapport a pour objectif d'apporter un éclairage sur les cybermenaces observées entre janvier et juin 2022, l'évolution de ces dernières ainsi qu'une perspective sur les tendances futures afin de faciliter leurs détections et in fine réduire l'impact des futurs incidents de sécurité.

Chaque section comporte un classement explicatif des cyberattaques identifiées ainsi que des focus thématiques rédigés par les analystes de la Purple Team afin de mettre en avant les différentes tendances, établies et émergentes.

Chez Gatewatcher, la Purple Team a pour mission la traque et l'analyse des menaces ciblant nos clients afin de garantir la mise à jour et l'optimisation constante des performances de nos diverses offres NDR, CTI, Sandboxing ou de détection qualifiée. La Purple Team se caractérise par la diversité de profil de ses experts, avec des expériences dans les domaines de la réponse à incident, l'analyse et intégration SoC, le pentesting, l'analyse CTI, et la recherche en cyber sécurité.

Comme dans tout rapport sur les tendances des cybermenaces, il y a des thématiques incontournables comme, par exemple, l'utilisation massive de vulnérabilités pour les applications Office dans le cadre de l'infection d'un poste de travail. Cependant, il ne faut jamais oublier que les cybers attaquants savent évoluer et trouver de nouvelles techniques permettant d'atteindre leurs objectifs avec, par exemple, l'utilisation de sites légitimes pour le stockage de charges malveillantes permettant d'agir avec plus de discrétion sur un système d'information.

Ce document s'articule autour de 5 sections traitant des thèmes suivants[1] :

- → les types de fichiers utilisés par les cybers attaquants
- → les malwares employés
- → les techniques employées par les cybers attaquants
- → les vulnérabilités exploitées
- → les secteurs d'activités ciblés

02 GLOSSAIRE ET PRÉCISIONS TECHNIQUES

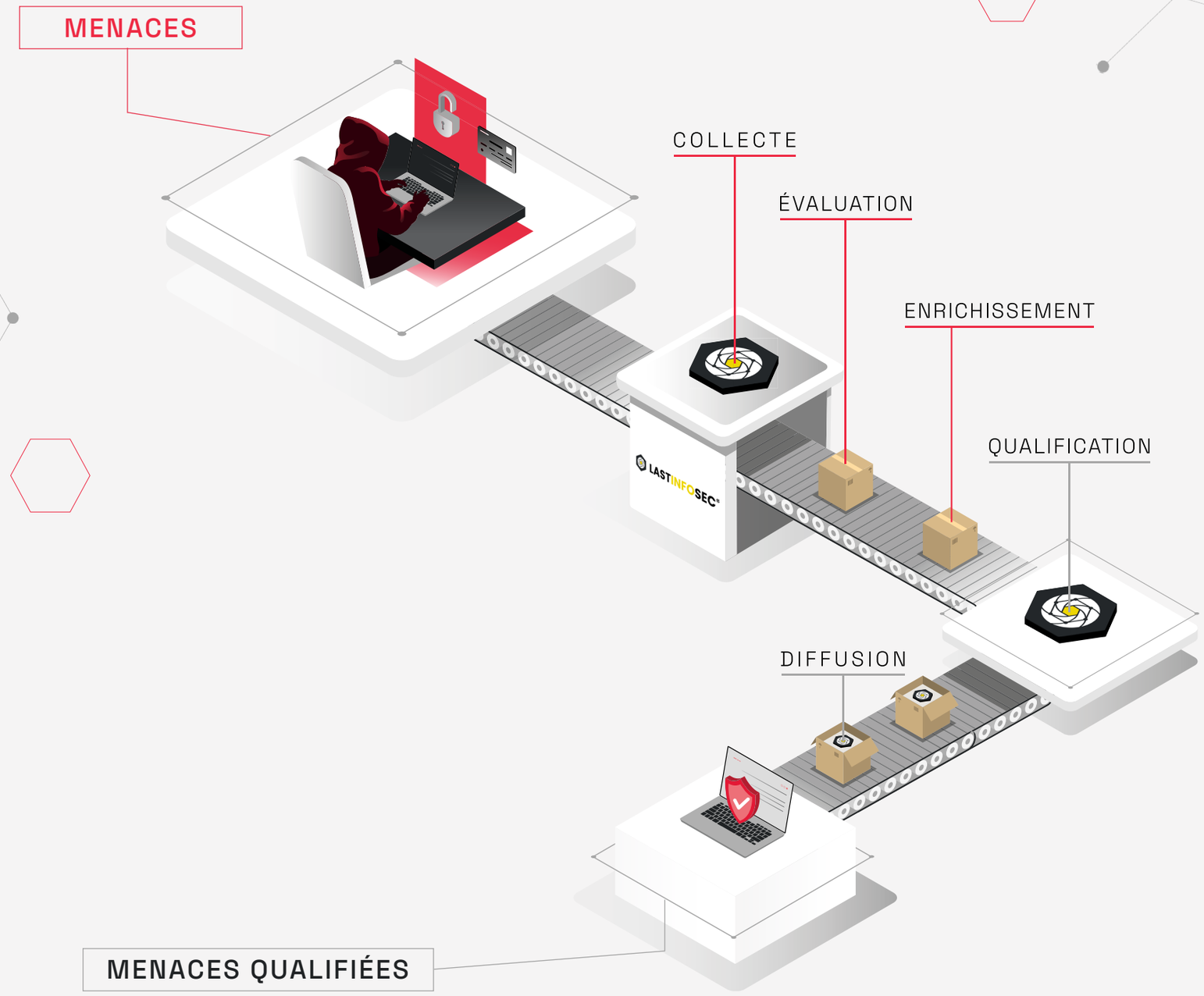
Pour mieux comprendre l'orientation de ces données, il est nécessaire d'expliquer le fonctionnement de notre plateforme LastInfoSec.

LastInfoSec® est notre plateforme de Cyber Threat Intelligence (CTI) visant à faciliter la détection des menaces internes et externes susceptibles de cibler le système d'information et de suivre les nouvelles techniques, vulnérabilités, outils, utilisés par les attaquants.

Ses moteurs automatisés de collecte, d'analyse et de corrélation sont alimentés en permanence par plus de 3000 sources de données provenant de multiples canaux : réseaux sociaux, sites spécialisés, darknet, deep web ainsi que par de la télemetrie provenant de l'infrastructure de détection de Gatewatcher. Cela permet à LastInfoSec de générer plus de 5000 marqueurs qualifiés par jour, quasiment en temps réel et de fournir plusieurs types de renseignements à forte valeur ajoutée sur la menace.

L'infrastructure LastInfoSec® fournit plusieurs types de renseignements sur la menace :

- → Des indicateurs de compromissions enrichis et contextualisés aux secteurs d'activité dans le but de réduire le temps d'analyse d'une menace lors de sa détection
- → Des rapports tactiques sur les nouvelles techniques, failles applicatives, outils, etc. utilisés par les attaquants
- → Rapports sur les vulnérabilités



5500

est le nombre d'IoCs contextualisés en moyenne par jour

+150

est le nombre total de familles de malwares suivies activement

+3000

est le nombre de sources de données alimentant la CTI LastInfoSec

03 FICHIERS MALVEILLANTS

ENTRE ANCIENNETÉ ET NOUVEAUX VECTEURS D'INFECTION

Les plateformes Windows et Linux étant les plus ciblées par les auteurs de menaces cyber, nous retrouvons en haut du classement les fichiers malveillants ELF et PE.

Plusieurs raisons à cela, beaucoup d'entreprises ont fait le choix d'utiliser Windows comme système d'exploitation pour les PC de bureau. Quant à Linux, l'accroissement du Cloud et des objets connectés en fait une cible de choix pour les attaquants. Une question se pose néanmoins : Comment ces fichiers malveillants parviennent-t-ils à s'introduire sur le réseau ?

DES ANCIENNES TECHNIQUES TOUJOURS AUSSI PRÉSENTES

Comme montré dans le classement des CVE, les fichiers Microsoft Office sont très utilisés par les attaquants pour pouvoir exécuter du code arbitraire. Cette suite logicielle bureautique très utilisée en entreprise, avec les fichiers Word, Excel et Powerpoint, est un bon point d'entrée dans l'infrastructure de ces dernières. Souvent envoyés en pièce jointe d'un courriel électronique dans des attaques par hameçonnage (phishing) avec un nom de fichier comme « Facture-XXX.docx, Bilan-2021.xlsx », ils représentent une source d'attaque importante.

Un autre type de fichier couramment utilisé lors d'attaques de phishing est le PDF. Tout comme pour les fichiers Microsoft Office, les fichiers PDF sont « déguisés » en fichiers normaux avec des libellés incitant la victime à l'ouvrir (facture, remboursement, fiche de paie, etc.). Une fois ouvert, une charge malveillante (payload) est exécutée afin de distribuer un autre malware (ex : un keylogger).

TOP FICHIERS MALVEILLANTS

ELF → 45.434%
PE → 34.673%
MS-OFFICE → 9.611%
OTHERS → 6.149%
ARCHIVE → 2.691%
SCRIPT → 0.467%
PDF → 0.309%
RTF → 0.265%
ISO → 0.214%
INK → 0.186%

Les webshells, technique régulièrement utilisée par les cybercriminels, permettent d'avoir un accès permanent sur des serveurs web et de faciliter l'exécution de code arbitraire à distance. Ils sont écrits dans des langages de programmation comme PHP, Python, ASP.NET, JSP, et bien d'autres. Fin juin, une nouvelle vulnérabilité a ciblé la solution Confluence, éditée par la societé Atlassian (CVE-2022-26134) via un webshell.

VERS DE NOUVEAUX VECTEURS D'INFECTION...

Fin mai une nouvelle CVE a été publiée sous le nom de Follina (voir Partie 4). Au travers d'un fichier au format Microsoft Word ou RTF (Rich Text Format), elle permettait à un attaquant d'exécuter du code arbitraire en exploitant le schéma URI ms-msdt. Par sa simplicité d'utilisation et son impact critique sur une machine, elle a été rapidement et massivement exploitée par des malwares comme Emotet ou Qbot ce qui explique son positionnement dans notre classement.

Nous avons pu constater un «nouveau» vecteur d'attaque au cours de ce premier semestre : il consiste en un fichier ISO avec un fichier de raccourci Windows (.lnk) qui va souvent charger une librairie (.dll) ou exécuter une commande PowerShell. Nous avons remarqué que cette méthode avait été utilisée pour distribuer des malwares comme Qbot, Emotet, IcedID, etc. Elle fait suite à des déclarations de Microsoft induisant un changement majeur sur l'exécution des macros dans les fichiers marqués comme provenant d'internet (par défaut ces fichiers auront leurs macros désactivées) ce qui a eu pour conséquence de pousser les attaquants à envisager d'autres moyens d'infections. Le choix du format ISO a pour avantage d'être « monté » directement si la victime double clique sur le fichier, rendant son contenu facilement accessible. Il permet également de contourner Mark-Of-The-Web, un marqueur qui permet d'identifier qu'un fichier provient d'internet ce qui permet à Windows d'adapter ses fonctionnalités de sécurité (exemple bloquer les macros Office).

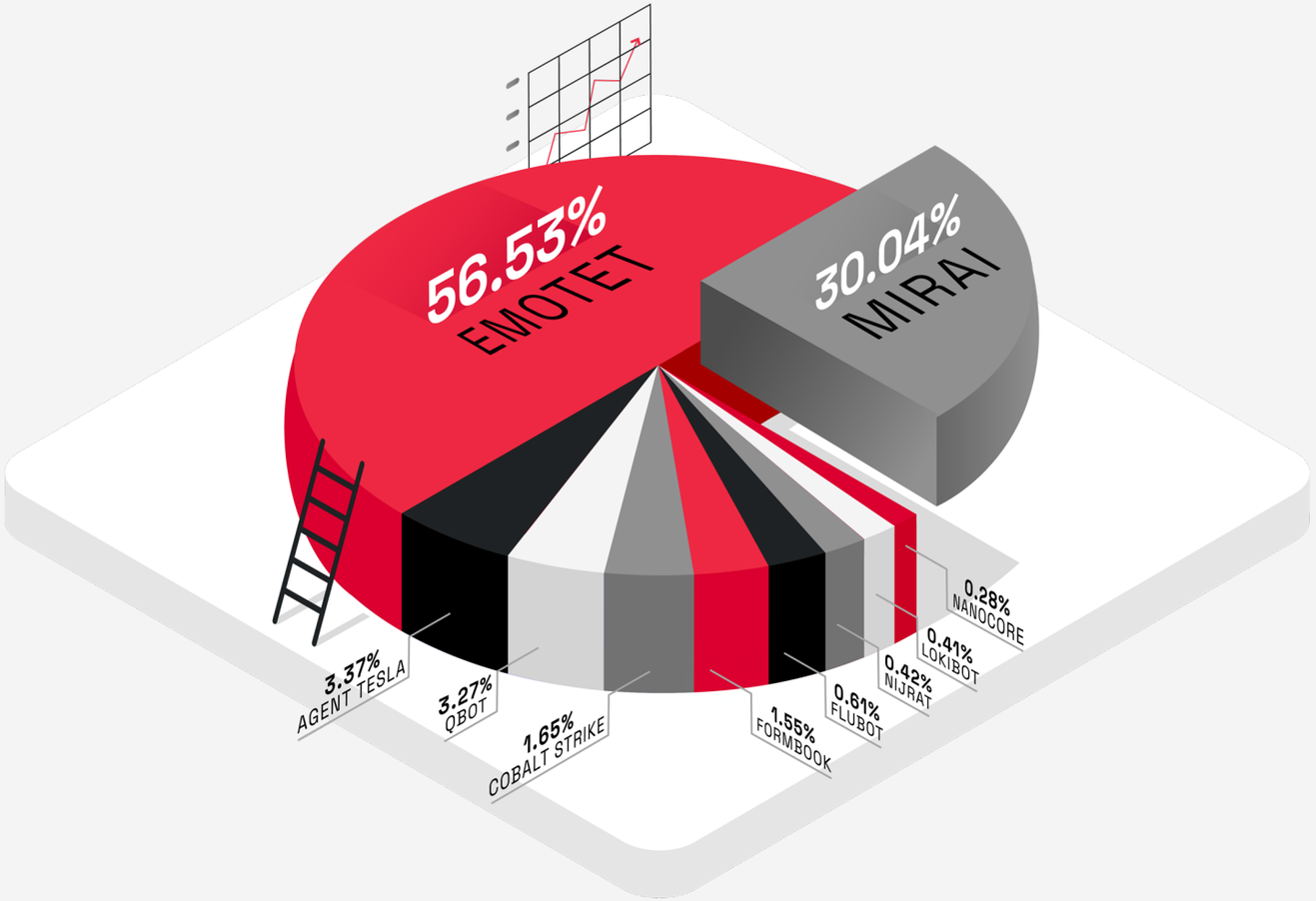
De plus en plus de groupes malveillants ont recours aux archives afin de distribuer leurs malwares. Compresser un fichier et le protéger par mot de passe permet de passer outre certaines sécurités primaires sur un réseau. Si une archive est envoyée en pièce jointe d'un email avec un mot de passe, son contenu ne pourra pas être analysé la plupart du temps. Dans les archives nous retrouvons principalement les fichiers .zip, .rar, .gzip, .7z très connus du grand public, qui sont présents autant sous Linux que Windows.

04 L'EMPLOI ACCRU DE MALWARES ÉVOLUTIFS

Avec plus de 150 familles de malwares suivies au cours de cette première moitié de l'année, nous vous présentons aujourd'hui le top 10 de nos observations.

Ce premier semestre nous avons principalement relevé deux malwares déjà très connus : Emotet et Mirai. En effet, après une interruption de ses activités en janvier 2021 suite à l'arrestation de certains de ses membres et la fermeture de son infrastructure menée par Europol[1], Emotet a fait son retour en novembre 2021.

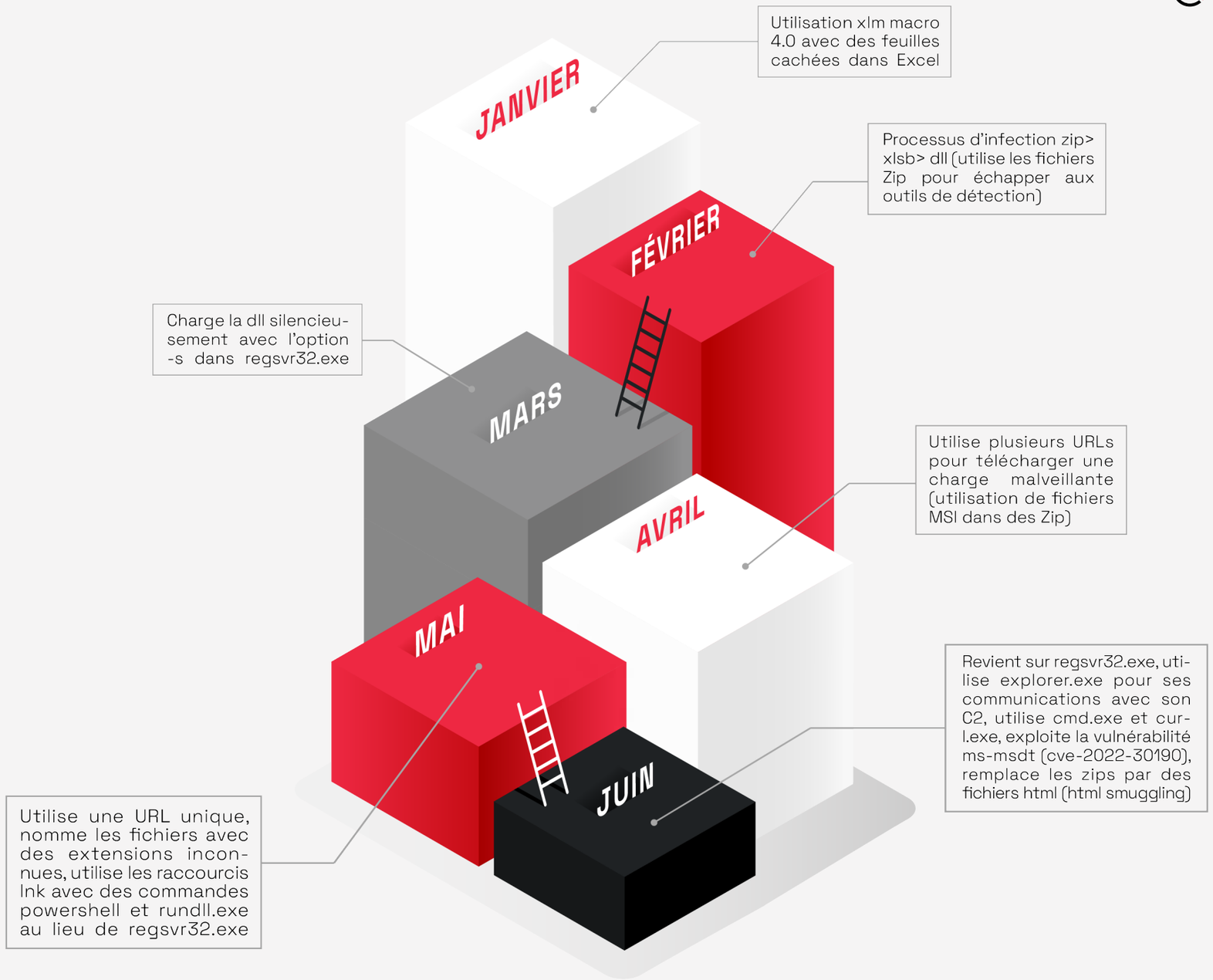
Mirai, quant à lui, est présent depuis 2016. Grâce à la publication de son code source, de nombreux variants ont ainsi pu voir le jour[2].



SUIVI DE MALWARES À FORTE ÉVOLUTION

Certains malwares se distinguent ce semestre par leur évolution particulièrement dynamique sur la période.

Qbot, aussi connu sous le nom de Qakbot est un voleur d'information très modulaire. Il s'est distingué par l'adaptation rapide de ses techniques d'infection en passant de Macros à des fichiers MSI, puis plus récemment à des fichiers LNK et d'URL de phishing provenant de sites légitimes (Onedrive, Google Drive) comme en témoigne la chronologie ci-dessous.



Un deuxième malware a retenu notre attention sur la période : Il s'agit de Flubot, un malware Android ciblant principalement le système bancaire depuis 2 ans en Europe, Asie et Océanie. Ce malware, qui a pour premier objectif de voler les identifiants bancaires de sa victime, s'illustre également par sa capacité accrue à évoluer rapidement. Enfin, en troisième position se trouve l'Agent Tesla, un trojan écrit en .NET que notre équipe a analysé en mars dernier. Ce cheval de Troie privilégie le secteur bancaire, énergétique et les transports. Nous avons constaté qu'il exploite des vulnérabilités présentes dans notre top 10 CVE (p.ex. CVE-2017-11882, CVE-2018-0802).

Voici l'évolution Flubot sur les six derniers mois :

FIN 2021

Possibilité de recevoir des URLs en plus des injections web html et javascript (permettant de sauvegarder les codes d'injection en mémoire).

Ajout de TLD pour générer de nouveaux domaines à l'aide de DGA, propose à l'utilisateur une fausse application Flash Player.

JANVIER 2022

Utilisation du support messages (SMS) pour les attaques par smishing

Ciblage de nouveaux pays (Japon, Hong Kong, Corée du Sud, Singapour, Thaïlande)

Interception des notifications reçues et réponse automatique avec un message configuré par le C2 et utilisation du botnet Flubot pour distribuer Medusa

FEV - AVRIL 2022

Vol de Cookies

MAI 2022

Utilisation du support messages (MMS) pour les attaques par smishing

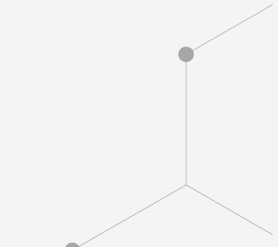
JUIN 2022

Démantèlement de l'infrastructure de Flubot par Europol le 1er juin. Toutefois, la police ne semble pas avoir récupéré les clés RSA privés.

OUTILS ET TECHNIQUES COMMUNS AUX MALWARES

Nous avons pu constater au cours de ces six premiers mois, l'utilisation de Cobalt Strike, cinquième de notre classement, par Qbot et Emotet entre autre. Cet outil de Command & Control (système que nous avions présenté en aout), fait partie des plus utilisé par les attaquants afin de communiquer avec leur malware.

Certains outils sont, par exemple, réutilisés par les attaquants afin de communiquer avec leur malware. Nous avons identifié l'utilisation par les malwares Emotet et Qbot, de Cobalt Strike qui est aujourd'hui un des outils de Command & Control (C2) les plus utilisés par les attaquants (en cinquième place de notre classement).[3]

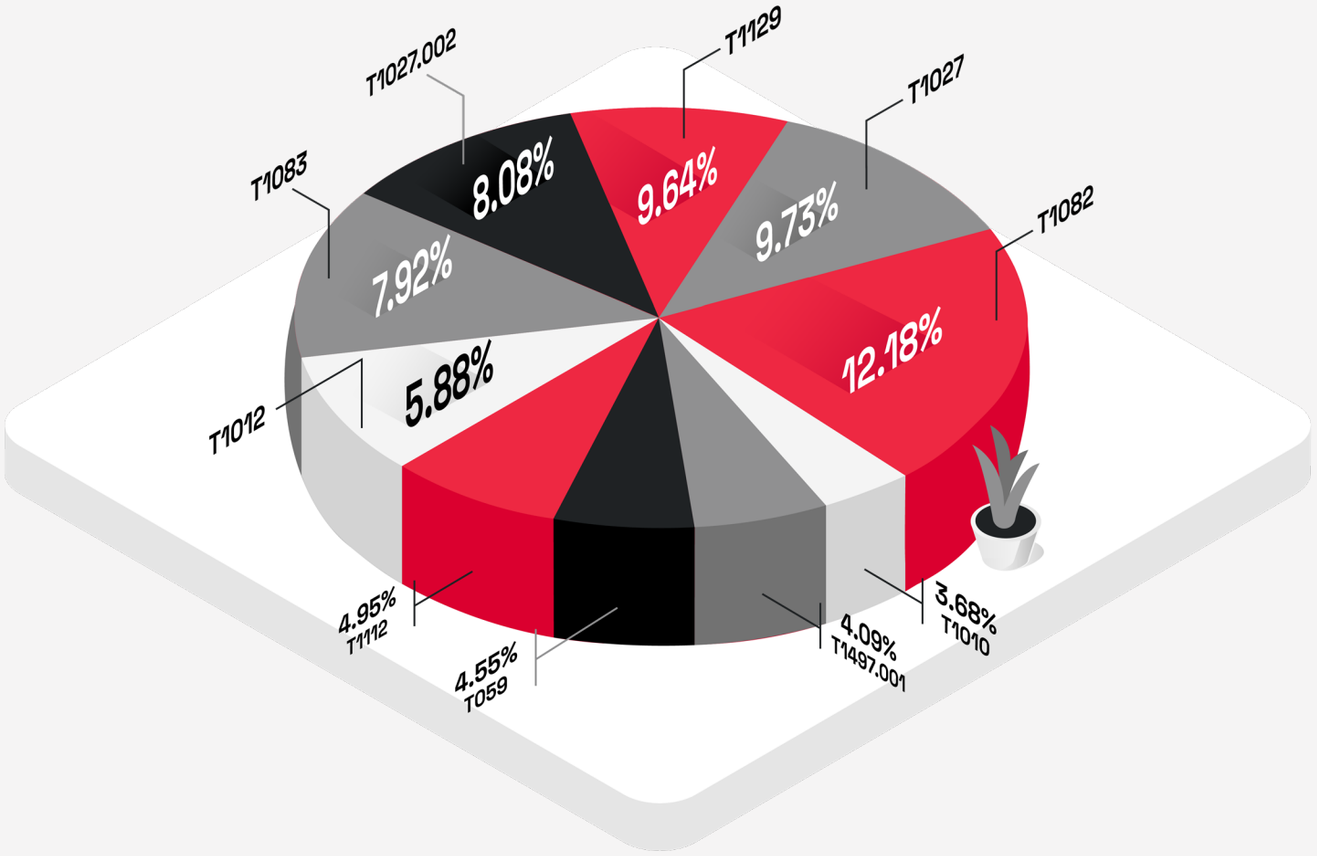


Les attaquants ont également recours aux techniques d'hameçonnage par email pour délivrer leurs logiciels malveillants. L'hameçonnage (phishing en anglais) par email est une technique d'ingénierie sociale visant à provoquer une action chez la victime comme le fait de cliquer sur un lien, ouvrir une pièce-jointe, etc. L'objectif est de récupérer des informations personnelles et/ou exploiter la machine grâce à la pièce-jointe exécutée. C'est le cas pour la plupart des malwares présents dans notre top 10 malware.De plus, les attaques par déni de service distribué (DDoS en anglais) sont encore très présentes. L'augmentation croissante des objets connectés (IoT), les configurations par défaut de diverse machines accessibles au grand public, ainsi que le nombre de CVE avec un score CVSS (Common Vulnerability Scoring System) élevé, permettent à Mirai et ses variants (Satori, Beastmode, RapperBot, etc.) d'être une des menaces les plus présentes et impactantes.

Parmi les malwares les plus diffusés actuellement, nous retrouvons principalement les voleurs d'informations et les rançongiciels. Le voleur d'informations (infostealer), est un type de malware récurrent en ce début d'année. En prenant en compte les trojans et les RATs (Remote Access Trojan) , qui ont des capacités de vols d'informations, les infostealer composent la quasi-totalité de notre classement. Le rançongiciel (ransomware) est une menace en forte progression depuis la crise sanitaire du COVID-19. Il vise à chiffrer les données d'une victime et lui en restituer l'accès contre le paiement d'une rançon. Nous remarquons cependant une baisse de la fréquence d'utilisation de ce type de malware sur les deux premiers trimestre 2022.

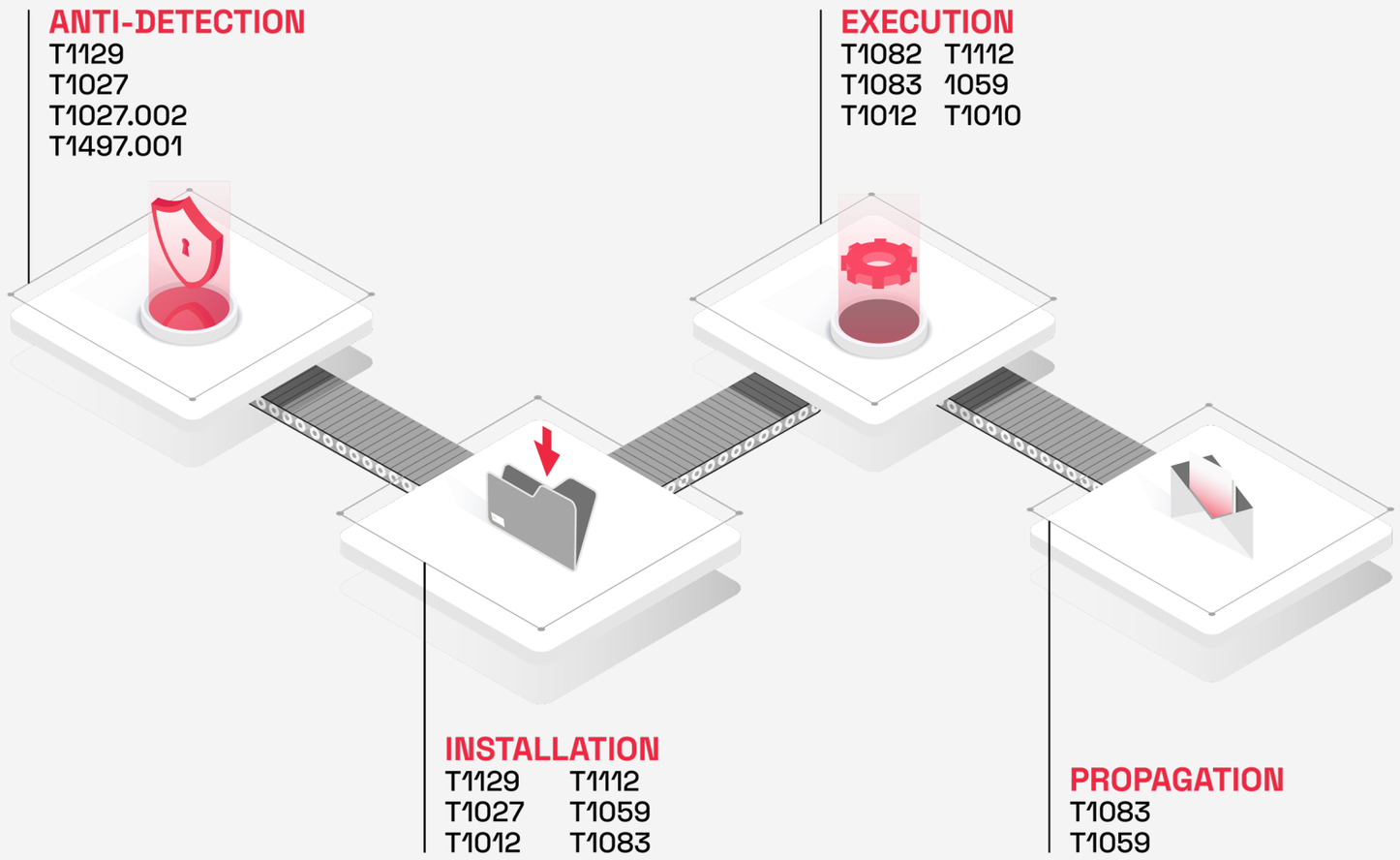
05 LES TENDANCES EN MATIÈRE DE TTP

Les TTP (Tactics, Techniques and Procedures) sont un ensemble de comportements et techniques utilisés par les acteurs malveillants, publié par le MITRE[4]. Il s'agit plus précisément de comportements génériques de malwares, avec de nombreuses manières d'implémenter chacune de ces TTP. Ce top 10 nous permet de constater les comportements malveillants les plus couramment utilisés.



T1129 → Shared Modules
T1027 → Obfuscated Files or Information
T1082 → System Information Discovery
T1027.002 → Obfuscated Files or Information Software Packing
T1083 → File and Directory Discovery
T1012 → Query Registry
T1112 → Modify Registry
T1059 → Command and Scripting Interpreter
T1497.001 → Virtualization/Sandbox Evasion System Checks
T1010 → Application Windows Discover

Ces TTP peuvent être rangées dans différentes étapes de la kill chain d'une infection par un malware [5] :



Un grand nombre de malwares sont distribués en tant que, ou font usage de DLLs (T1129). Il n'est pas rare que certaines étapes de packing fassent également intervenir une DLL, comme c'est le cas pour celui d'Agent Tesla analysé précédemment par nos équipes[6]. L'installation d'un service Windows se fait également avec une DLL.

L'obfuscation d'une charge malveillante est une étape essentielle d'un malware, ce qui lui permet d'éviter la détection et de pouvoir mener à bien ses opérations (T1027). Cette étape est généralement gérée par le packer[7] utilisé (T1027.002). Des packers plus avancés peuvent être utilisés afin de détecter un environnement de Sandboxing par exemple, et limiter les risques de détection automatique (T1497.001). La découverte d'information apparaît comme une étape essentielle (T1082, T1083, T1012, T1010). Il s'agit pour l'attaquant d'obtenir des informations sur le système infecté afin de préparer d'autres attaques, des mouvements latéraux, ou simplement de chiffrer le disque pour un ransomware. Cela peut également aider à la propagation sur d'autres machines (recherche de dossiers partagés notamment).

L'écriture dans le registre Windows (T1112) est souvent utilisée pour assurer une persistance du malware (création d'un service, ajout dans le démarrage automatique, désactivation de protections). L'exécution de commandes shell (T1059) peut également être utilisée pour ces opérations, en plus de permettre une prise de contrôle d'une machine à distance dans le cas d'un Cheval de Troie comme Lyceum[8].

PACKING

Plusieurs TTP précédentes (T1129, T1027, T1027.002, T1112, T1059, T1497.001) sont généralement liées directement ou non à l'utilisation d'un packer. Environ 80% des malwares distribués aujourd'hui sont « packés ». Il existe des packers légitimes qui sont utilisés couramment avec pour objectif de protéger un logiciel propriétaire, ou faciliter sa diffusion. L'installateur de Firefox par exemple est packé avec UPX pour réduire la taille du fichier final. Ces packers légitimes sont toutefois régulièrement utilisés voire détournés par des acteurs malveillants, comme nous avons pu le constater avec NSIS[9]. On trouve par exemple beaucoup de versions modifiées de UPX, ou des malwares packés avec les outils MPRESS, Enigma VMProtect, etc...

Les packers malveillants peuvent se complexifier pour inclure de l'obfuscation de données (dans un fichier JPG par exemple pour Lyceum[10]), et implémenter des protections contre l'analyse de la payload (anti debug, anti-machine virtuelle, anti sandboxing...).

Le développement de nouveaux packers reste toujours d'actualité car il est souvent plus facile pour un acteur malveillant de « repackager » sa charge utile dans un nouveau packer que de la modifier. Des estimations tendent à montrer que 50% des nouveaux échantillons proviennent d'anciens malware « repackagés » dans un autre packer. La détection de packer, et surtout l'unpacking automatique (et l'obtention de la charge utile finale), est donc un objectif essentiel bien qu'il reste un sujet complexe de recherche. Plusieurs pistes sont explorées par Gatewatcher, notamment basées sur de l'émulation.

De nombreux malwares sont aujourd'hui transmis via des documents Offices, et les macros qu'ils contiennent. Il s'agit souvent d'écrire un fichier sur le disque, puis de l'exécuter (soit un PE directement, soit le plus souvent un script shell qui extrait ou télécharge une payload et l'exécute). Plusieurs des TTP précédentes peuvent donc s'appliquer aux macros, qui constituent elles-mêmes la TTP 1137.

Comme indiqué précédemment, les TTP sont des comportements génériques. Ainsi, la détection ou l'évasion de sandbox (T1497.001) peut prendre différentes formes, depuis des techniques simples jusqu'aux plus poussées. Un simple « Sleep » avec une grande durée peut être considéré comme une technique d'évasion de sandbox, le malware ne commençant son exécution qu'après la durée d'analyse maximale de la sandbox. Une sandbox un peu plus évoluée simulera le délai attendu instantanément en « hookant » les appels concernés.

Des techniques de détection de sandbox beaucoup plus avancées existent également, comme l'énumération de matériel pour détecter des périphériques virtuels, la recherche de périphériques USB connectés, la détection d'interaction avec l'utilisateur (est-ce que la souris bouge ?), etc...

STOCKAGE DE MENACES SUR DES SITES LÉGITIMES :

Une TTP non mentionnée précédemment apparaît de plus en plus utilisée. Il s'agit de T1102.003[11].Un nombre croissant de malwares utilisent des services légitimes comme moyens de stocker des données sur internet. En premier lieu Pastebin, Google Drive, Dropbox, dont l'accès est de plus en plus fréquemment bloqué en entreprise, puis Twitter. Plus récemment avec l'utilisation de messageries instantanées comme Telegram ou Discord.

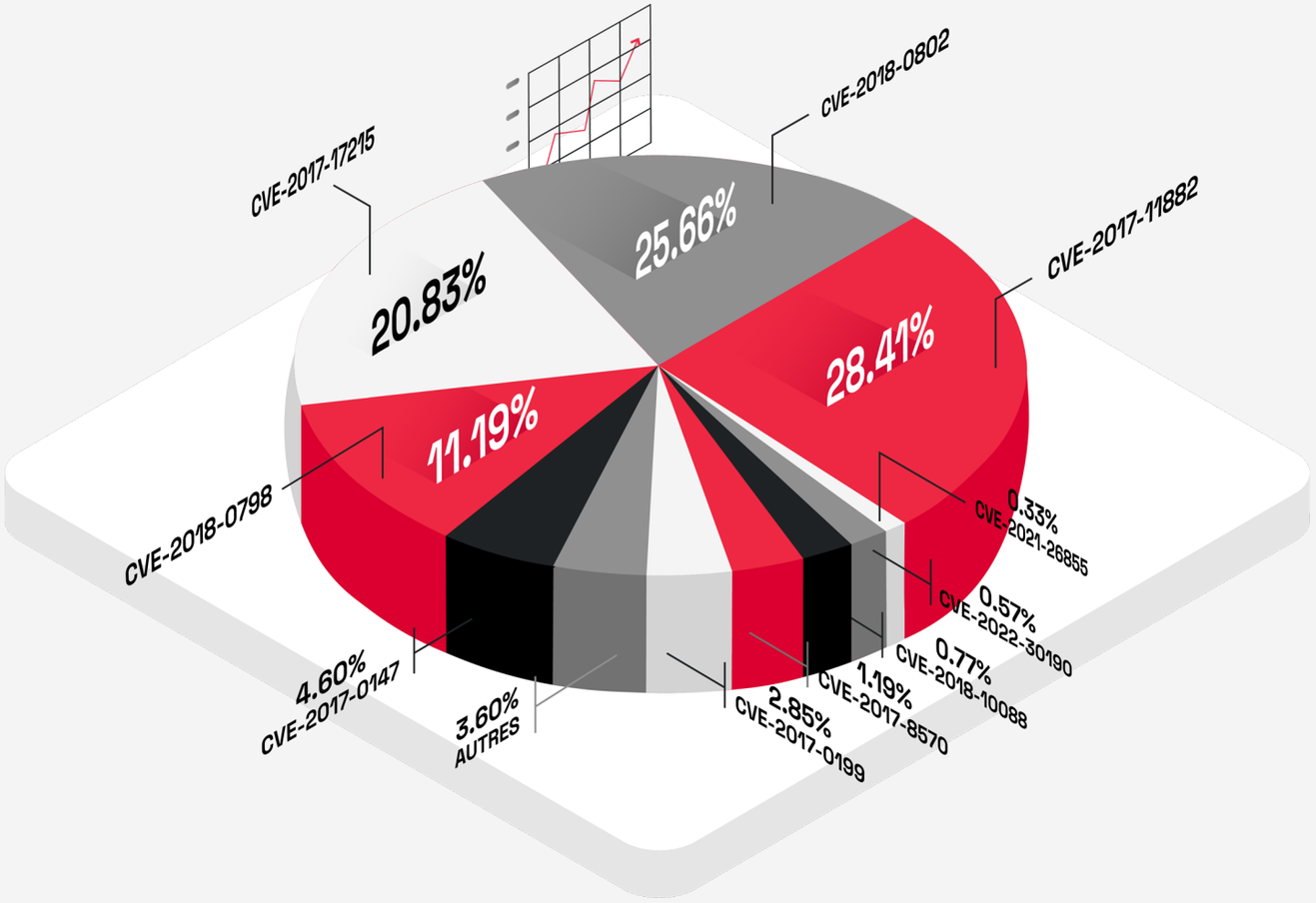
Ainsi lors d'une infection classique, la première payload exécutée ne fait que télécharger une autre plus avancée depuis un de ces services. Certaines familles vont jusqu'à implémenter complètement le C2 dans une de ces messageries, comme Telegram qui a par exemple été utilisé par les malwares ToxicEye et Racoon Stealer.

Cette méthode présente de nombreux avantages pour un attaquant car elle est très facile à mettre en œuvre, ces services étant gratuits et anonymes, et elle reste plus complexe à détecter. S'ils ne sont pas bloqués par la politique interne de l'entreprise, une connexion vers l'un de ces services n'aura rien d'inhabituel ou de malveillant a priori car aucun des indicateurs habituels d'une connexion à un C2 ne sera présent (connexion sur une IP sans DNS, certificat auto signé, IOC connu de malware). Ces services peuvent également être répliqués dans plusieurs zones géographiques, les attaquants tirent ainsi profit du CDN (Content Delivery Network) pour obtenir de meilleures performances, une meilleure résilience, et plusieurs IP virtuellement associées à leur C2.

06 CVE - UNE TENDANCE STABLE **MAIS NON FIGÉE POUR AUTANT**

Il est important de préciser que la nature des vulnérabilités exploitées diffèrera grandement selon qu'il s'agisse d'un environnement industriel ou web. Bien que l'amalgame soit parfois fait, il est important de distinguer les malwares des vulnérabilités. Notre observation portera ici sur les 10 vulnérabilités (CVE) les plus exploitées par les différents malwares.

Ces vulnérabilités sont habituellement utilisées afin de pouvoir obtenir des permissions plus élevées (privilege escalation), s'introduire et se déplacer latéralement au sein du système d'information ou, plus simplement, exécuter du code arbitraire. Il est à noter que d'autres vulnérabilités peuvent être utilisées par les attaquants à différentes étapes de la kill chain. Nous constatons ici que la quasi-totalité du top 10 concerne des vulnérabilités utilisées lors de la première étape d'infection et sont de type RCE (Remote Code Execution).

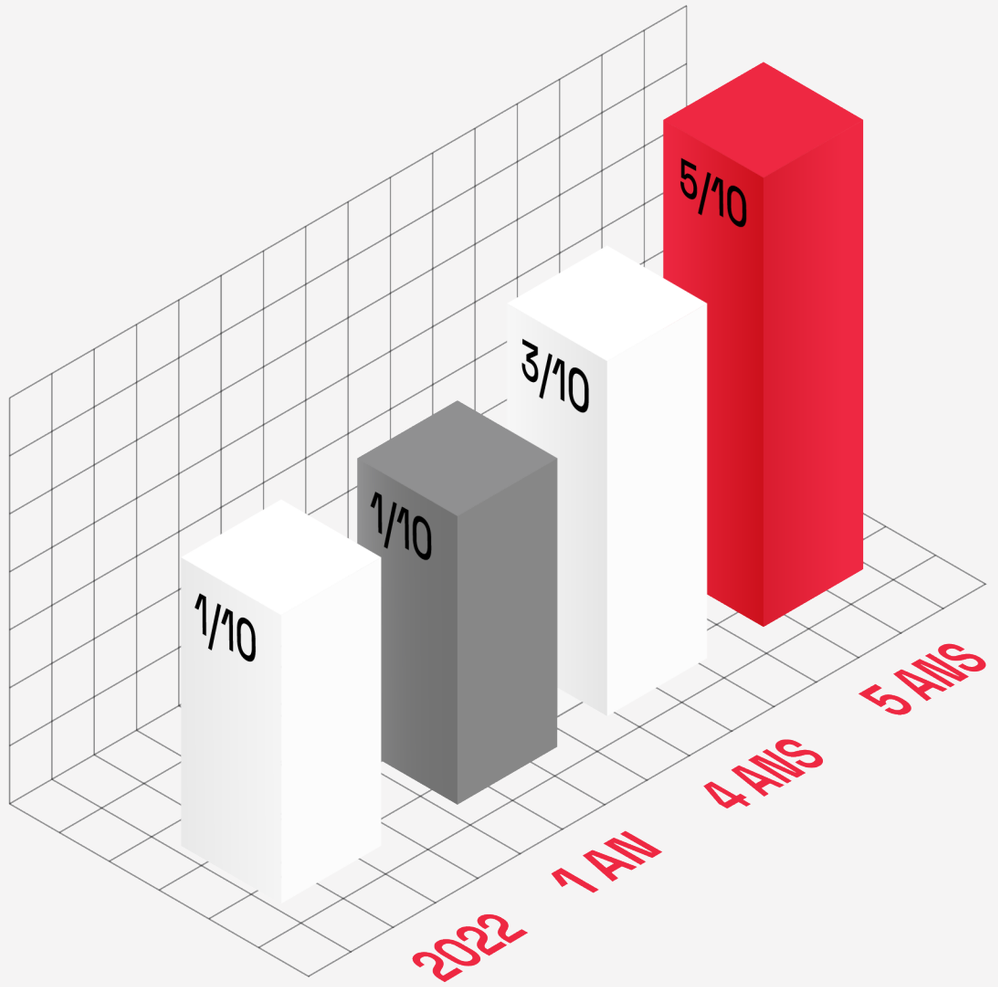


Bien que cela puisse être surprenant, l'écrasante majorité des vulnérabilités utilisées existent depuis plus de trois ans et ciblent, sans surprise, la suite Microsoft Office.

On distinguera cependant les CVE-2017-17215 et CVE-2018-10088 touchant respectivement les routeurs Huawei et le serveur HTTP XiongMai uc-httpd, des équipements représentés ici par leurs utilisations dans le désormais fameux botnet Mirai (et ses variantes telle que Satori) ciblant les appareils IoT et réseaux exposés sur internet.

UNE TENDANCE STABLE DÉMONTRÉE PAR LA VULNÉRABILITÉ OFFICE...

La suite office et les maldocs sont depuis plusieurs années déjà un vecteur d'infection privilégié. Bien qu'une grande majorité des malwares utilisent plus simplement les macros afin d'infecter l'utilisateur peu attentif, certaines utilisent des vulnérabilités afin de pouvoir infecter même un utilisateur méfiant. Ainsi les malwares ont tendance à utiliser les mêmes vulnérabilités et à ne pas en changer tant que ces dernières restent exploitables.



La CVE-2017-11882, une corruption de mémoire permettant l'exécution de code arbitraire dans Microsoft Office, tient le haut du podium depuis déjà plusieurs années.

À peine une semaine après sa correction par Microsoft, cette vulnérabilité a été vue exploitée par APT34. Depuis, sa popularité demeure jusqu'à être mentionnée dans le bulletin d'alerte du CISA de 2020[12] sur les vulnérabilités utilisées les plus régulièrement. Cette CVE reste donc toujours d'actualité, ayant notamment été utilisée encore récemment par des malwares tels que Loki, Formbook, Zbot ou encore Agent Tesla.

Alors que ces vulnérabilités sont aujourd'hui détectées par les solutions de sécurité (une mention spéciale pour la CVE-2017-0199 disposant de pas moins de 12 règles de détection dédiées, en plus de celles incluses au sein des moteurs anti-virus), on peut légitimement se demander pourquoi ces anciennes vulnérabilités sont toujours autant exploitées. La raison tient dans le fait qu'elles représentent toujours un vecteur efficace de propagation pour des cybercriminels qui se professionnalisent et cherchent à rentabiliser leurs actions.

Les équipes en charge des systèmes d'informations sont souvent en manque de main d'œuvre afin de maintenir les parcs à jour. Ce phénomène a une conséquence directe sur le fonctionnement des groupes de ransomwares, qui vont utiliser cet état de fait à leur profit.

... MAIS PAS FIGÉE (VULNÉRABILITÉ FOLLINA)

Cependant, cette faiblesse est connue. De ce fait, de plus en plus d'entités ont amélioré leurs processus afin de réduire le temps de correction de ce type de vulnérabilités. On constate dans le même temps une accélération des différents groupes pour l'exploitation expresse des vulnérabilités lors de la diffusion d'un patch ou de la notification de la vulnérabilité.

Prenons l'exemple d'une des vulnérabilités ayant fait une entrée remarquée dans le top cette année : la CVE-2022-30190 aussi appelée « Follina » et pour laquelle une note dédiée a été rédigée par la purple team de Gatewatcher.

27/05/2022 → Tweet (exploitation détectée)

30/05/2022 → Affectation d'une CVE à cette vulnérabilité / début de couverture presse / Utilisation de la CVE par TA413

31/05/2022 → Mise à disposition des premières règles de détections / mise à disposition d'un workaround par Microsoft

03/06/2022 → Communication auprès de nos clients détaillant la vulnérabilité et fournissant d'autres règles de détections

06/06/2022 → Utilisation dans une campagne de phishing visant les gouvernements locaux américains et les gouvernements européens.

07/06/2022 → Utilisation par TA570 affilié à Qbot

13/06/2022 → Utilisation par le groupe Sandworm dans une campagne visant l'Ukraine

14/06/2022 → Publication d'un correctif par Microsoft

21/06/2022 → Utilisation attribuée à APT28 lors d'une campagne ciblant l'Ukraine

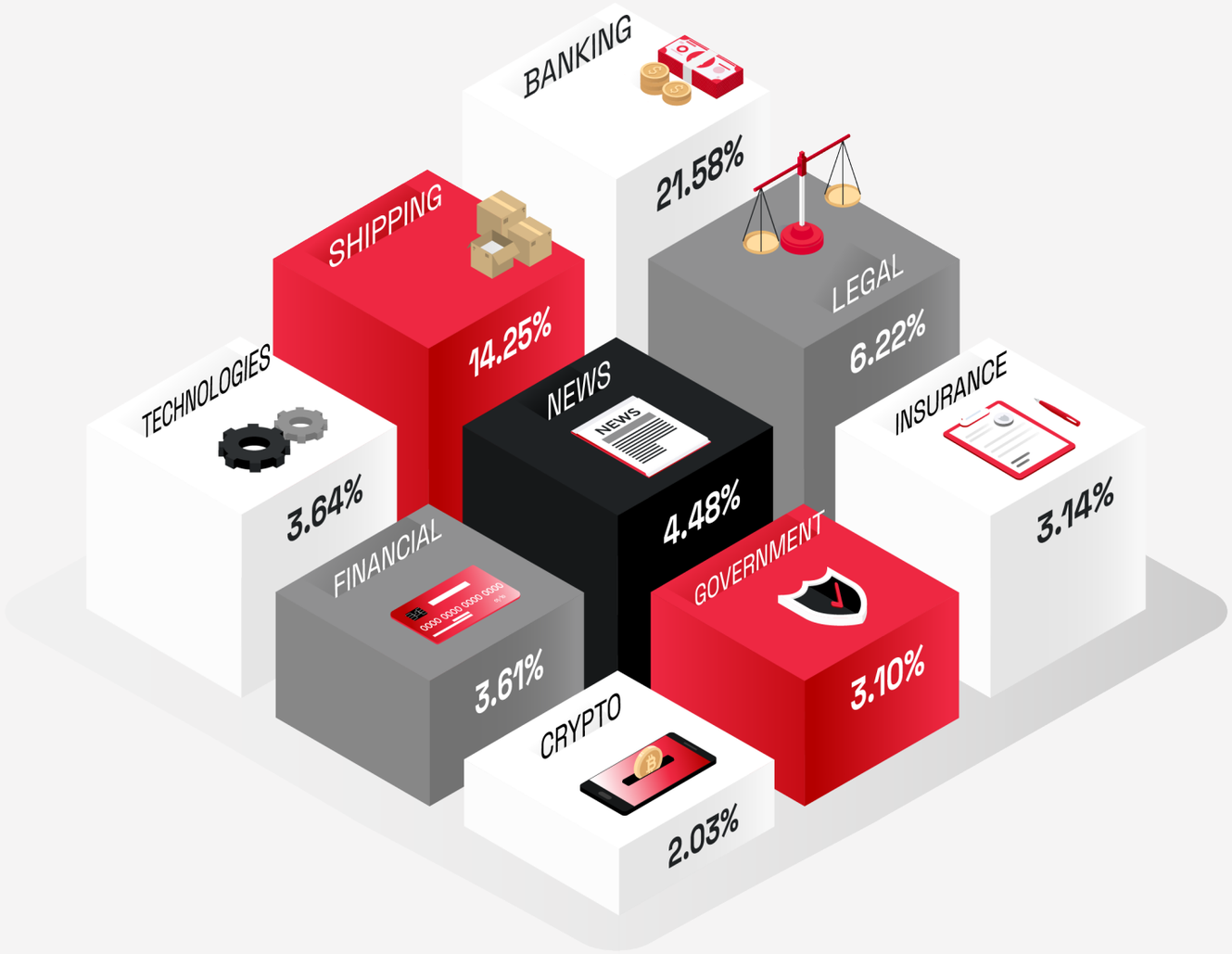
09/07/2022 → Utilisation pour la distribution de Rozena

EOT

Parue à un moment où Microsoft annonçait vouloir bloquer les macros dans les documents Office, cette vulnérabilité a permis de mettre en avant la rapidité de réaction des différents acteurs malveillants pour inclure l'exploitation d'une vulnérabilité dans leurs processus d'infection. Rappelons que cette vulnérabilité permettait sous certaines conditions de déclencher la charge malicieuse lors d'une simple prévisualisation du document. De plus, comme le montre la chronologie des évènements, les moments entre la publication et la correction peuvent être très différents, soulignant ainsi l'importance de la réactivité des systèmes sur la détection de ces évènements.

07 UNE MENACE MULTI-SECTEURS

MARQUÉE PAR L'UTILISATION DU SMISHING



Ce classement n'est pas une surprise quand on sait qu'il s'agit des secteurs parmi les plus dynamiques, cibles privilégiées des attaques par ransomware. C'est le cas évidemment du secteur bancaire, des médias, et des technologies en priorité.

Bien que la motivation financière soit souvent la raison principale des attaques, l'interruption temporaire des médias ou d'un système bancaire, ainsi que l'accès à des données juridiques confidentielles ou gouvernementales sont aussi des objectifs bien présents.

À noter le secteur du fret (logistique expedition) qui, bien que traditionnellement peu impacté, fait une progression remarquée comme nouvelle cible de choix pour les Threat Actors.

FOCUS 1 : LIVRAISON DE CYBERMENACES À TRAVERS LE SMISHING

À l'image des fraudes au compte CPF ou à l'assurance maladie, c'est désormais le phishing à travers de faux mails ou SMS de livraison qui sévit. Cette pratique est de plus en plus répandue et figure actuellement en deuxième position de notre classement sur les secteurs d'activités victimes d'attaques.

Il existe deux types de procédés :

- → Les pirates envoient des SMS en se faisant passer pour des services de livraison légitimes en indiquant au client qu'il doit payer différents frais, comme des frais de douanes par exemple, pour permettre l'acheminement de son colis. Le faible montant demandé n'alerte pas la victime.

- → Les pirates demandent à la victime de renseigner ses identifiants par le biais d'une interface web similaire à celle du service de livraison.

Cette pratique est particulièrement efficace pendant les périodes de fêtes comme Noël, où les particuliers ont davantage tendance à commander des produits sur internet et sont en attente de leurs colis.

Déjà en décembre 2021, la direction générale des douanes françaises avait mis en garde contre cette pratique qui, dans certains cas, imitait les mails de la douane. Le service de livraison allemand DHL a indiqué le 28 juin 2022 être la cible d'une attaque de phishing globale de ce type et travailler activement au blocage de ces attaques et des sites frauduleux associés à travers le monde.

FOCUS 2 : LA SANTÉ DES HÔPITAUX CYBERMENACÉE

Un second secteur qui ne figure pas dans notre top 10 mais dont nous entendons de plus en plus parler ces deux dernières années est celui de la santé. Dès le début de la pandémie, ce secteur de la santé a rapidement été une cible, avec une augmentation de 150% du volume de cyberattaques sur les deux premiers mois de 2020, en particulier contre les hôpitaux. D'autres infrastructures ont été touchées : les organisations de santé nationales, les entreprises de vaccins, les instituts de recherches et également les applications de recherche de contacts.

Bien qu'historiquement ce secteur ait été visé pour obtenir des informations personnelles, les cibles et les objectifs se sont diversifiés. D'un côté, nous avons vu des attaques contre les instituts de recherches ainsi que des campagnes de désinformation, et de l'autre l'apparition de motivations purement financières avec le phénomène des ransomwares.

Focus sur une attaque récente : Le Centre Hospitalier Sud Francilien de Corbeil-Essonnes

Dans la nuit du 20 au 21 août 2021, le CHSF a été victime d'un ransomware qui a chiffré les données de l'établissement ainsi que certaines sauvegardes. L'attaque qui a paralysé son parc informatique, a depuis été stabilisé. Il ne s'agit pas d'un cas isolé. Jean-Noël Barrot, ministre délégué chargé de la transition numérique, a indiqué que les établissements de santé en France étaient victimes d'une cyberattaque toutes les deux semaines en moyenne sur le premier semestre 2022. Dans le cas de cette attaque, la gestion de l'enquête par les services spécialisés de la gendarmerie nationale a mis en évidence l'implication du ransomware Lockbit. Cela est surprenant car le groupe Lockbit indique clairement dans les règles à destination de ses affiliés qu'il est interdit de chiffrer les établissements où l'endommagement des fichiers pourrait entraîner une mise en peril des usagers. Quoi qu'il en soit, le groupe a revendiqué l'attaque début septembre sur leur site vitrine.

Il semblerait que le détournement d'un compte de support d'un prestataire soit à l'origine de l'intrusion initiale, et que les cyberattaquants aient infiltré le réseau de l'établissement hospitalier 10 jours avant de lancer l'attaque.

Aux dernières nouvelles, le groupe de cyberattaquants avait d'abord demandé une rançon de 10 millions de dollars pour le déchiffrement des données, puis a réduit sa demande à 2 millions en échange de la restitution et de la suppression des données volées après que l'hôpital ait refusé la première offre. Le groupe de cyberattaquants a, par ailleurs, diffusé un échantillon des données volées pour faire pression sur le groupe hospitalier, parmi lesquelles on peut voir des certificats médicaux, des contrats avec des partenaires, des relevés de comptes et autres documents administratifs et informations personnelles relatives aux patients.

Pour rappel les consignes de l'ANSSI pour les hôpitaux et établissement de santé sont de ne pas donner suite aux demandes de rançons. Le paiement ne garantissant pas le déchiffrement des données et pouvant inciter les cyberattaquants à reproduire leurs attaques. Ce fût notamment le cas pour le Centre Hospitalier du Grand-Est et celui d'Epinal qui ont vu leurs données confidentielles publiées.

Cette dernière attaque en date a manifestement été celle de trop pour le gouvernement qui a annoncé une enveloppe de 20 millions d'euros au profit de l'ANSSI dans le but de renforcer spécifiquement l'accompagnement des établissements de santé.

Les différentes solutions de détection de menaces comme Lockbit :

- Détection de DGA : l'analyse d'un nom de domaine vu sur le réseau permet d'indiquer le niveau de risque associé, à condition que la connexion ne soit pas chiffrée.
- Solution de sandboxing : l'analyse d'un fichier vu sur le réseau permet d'indiquer le niveau de risque associé.
- Observation de comportements : les virus utilisent souvent des mouvements latéraux pour se propager au sein du réseau d'une entreprise. Dans notre cas, Lockbit se propage notamment à travers le protocole SMB et tente de se connecter à des serveurs en utilisant des identifiants qu'il a réussi à récupérer. Il est possible d'observer ce comportement en étant attentif aux alertes de connexions ayant échouées.
- Detection de Beaconing C2: les virus communiquent généralement avec un serveur de C2 pour recevoir des instructions et envoyer des informations.

POURQUOI LES HÔPITAUX EN PARTICULIER SONT-ILS SI VULNÉRABLES ?

D'abord parce que leur dépendance vis-à-vis d'une connexion a des services numériques (données patients, équipements médicaux connectés) ne pouvant être interrompus les rends plus susceptibles d'accepter de payer les rançons rapidement. De plus, une grande partie se joue au niveau des actifs humains et numériques. Le manque de personnel dans les hôpitaux et le recrutement temporaire de personnels moins qualifiés a accentué les risques cyber.

Il convient de souligner que les systèmes d'informations des hôpitaux, comme souvent parmi les SI industriels, ne sont pas toujours mis à jour car ce serait prendre le risque :

- → d'entraîner le dysfonctionnement de logiciels et applications qui ne fonctionnent correctement que sous une certaine version du système d'exploitation.
- → d'interrompre pendant une durée non négligeable un système d'information dont les soignants ont besoin pour travailler avec une augmentation potentielle du risque vital pour les patients.

CONCLUSION

Lors des 6 premiers mois de l'année 2022, la Purple team a mis en évidence l'utilisation par les cybers attaquants de moyens déjà éprouvés depuis de nombreuses années : exploitation d'anciennes vulnérabilités non patchées (office, routeur…), technique de packing, famille de malwares déjà identifiée comme Mirai, etc.

La principale raison de l'utilisation de ces méthodes, pourtant déjà connues, est qu'elles sont toujours aussi efficaces que ce soit dans leur globalité, ou pour une victime qui n'aurait pas encore la maturité pour mettre en place les protections adéquates.

En outre, les attaquants ne sont pas obligatoirement à la recherche de l'attaque la plus sophistiquée si l'on prend l'exemple des Macro VBA. Ces dernières sont utilisées de façon malveillante depuis de nombreuses années et ce jusqu'à aujourd'hui, même si nous constatons que Microsoft a réduit leur impact en limitant l'exécution par défaut des macros.

Les améliorations dans les domaines de la détection ou de la limitation de l'efficacité d'une attaque montrent aussi que les attaquants cherchent toujours de nouvelles méthodes originales ou innovantes pour atteindre leurs objectifs :

→ Exploitation de nouvelles vulnérabilités (avec l'exemple de la CVE Follina)

→ Utilisation de type de fichiers pour déstabiliser nos habitudes (ISO, LNK…)

→ Utilisation de sites légitimes pour dissimuler une attaque (Discord, Pastebin, google drive…)

A l'instar de la citation de Sun Tzu « *Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.* », une recommandation efficace pour limiter les risques cyber serait de réellement parvenir à comprendre la menace en tant que telle, et d'être en capacité de l'observer sur la durée tout en disposant des outils appropriés pour garantir une détection performante et réactive et ainsi remédier rapidement à leurs impacts.

LASTINFOSEC
CYBER THREAT INTELLIGENCE

LastInfoSec® est une plateforme de Threat Intelligence visant à fournir une amélioration immédiate de votre niveau de protection. Sa technologie exclusive associe machine learning et traitement Big Data pour générer en un temps très court un flux d'information de haute qualité sur les cybermenaces.

- → LastInfoSec® facilite la prise de décision de vos équipes de sécurité opérationnelles et réduit fortement leurs temps d'analyse et de réaction en cas d'incident sans modification de leurs processus internes.
- → Les moteurs automatisés de collecte, d'analyse et de corrélation de LastInfoSec® permettent de rendre accessibles les informations sur les menaces 24 heures en moyenne avant la concurrence.
- → L'intégration de LastInfoSec® se fait simplement et rapidement grâce à des exports standardisés aux dernières normes CTI (Stix v2, Stix v2.1, JSON..) et à des connecteurs disponibles pour les principaux outils d'analyse du marché (Splunk, OpenCTI...)
- → La plateforme de LastInfoSec® inventorie et évalue en permanence les sources de données accessibles sur de multiples canaux : réseaux sociaux, sites spécialisés, dark et deep web...

QUI EST
GATEWATCHER

Leader Européen de la détection d'intrusions et de menaces avancées, GATEWATCHER protège depuis 2015 les réseaux critiques des plus grandes entreprises comme des institutions publiques. Notre vision est d'offrir une approche flexible (cloud, sur site, hybride), innovante et ouverte à l'IA, sans perturber l'architecture en place pour permettre aux équipes cybersécurité une meilleure efficacité dans la priorisation de leurs actions de remédiation.

Les solutions NDR, CTI et Sandboxing de Gatewatcher apportent une amélioration immédiate grâce à une vision à 360° des cybermenaces. Elles combinent l'apprentissage automatique avec différentes méthodes d'analyse poussées du trafic réseau et sont conçues pour être évolutives et immédiatement opérationnelles pour une intégration facilitée dans les SOCs de nos clients et partenaires.

SOURCES

[1] Édito du CyberThreats Barometer Mars 2022

[2] Édito du CyberThreats Barometer Juin 2022

[3] Édito du CyberThreats Barometer Août 2022

[4] Édito du CyberThreats Barometer Mai 2022

[5] Article Malware Analysis Lyceum

[6] Rapport d'Analyse Malware Agent Tesla

[7] Édito du CyberThreats Barometer Juillet 2022

[8] Article Malware Analysis Lyceum

[9] Rapport d'Analyse Malware NSIS Packer

[10] Article Malware Analysis Lyceum

[11] Web Service : One-Way Communication