GATEWATCHER

CYBER THREATS
SEMESTER REPORT

Juillet – Décembre 2022

SOMMAIRE

01 ENJEUX DU RAPPORT ET NOTES AU LECTEUR

Pour cette seconde 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 juillet et décembre 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 sur chaque thème identifié dans le domaine des cybers menaces ainsi que des focus thématiques rédigés par les analystes de la Purple Team afin de mettre en avant les différentes tendances, établies, émergentes ou originales.

Au sein de Gatewatcher, la Purple Team a pour mission la traque et l'analyse des cybermenaces ciblant nos clients afin de garantir la mise à jour et l'optimisation constante des performances de nos solutions NDR, CTI, d'analyse de menaces ou de détection qualifiée.

La Purple Team se caractérise par la diversité de profils 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.

Le Cyber Threats Semester Report (#CTSR) s'articule autour de 5 sections traitant des thèmes suivants :

- L'utilisation des types de fichiers par les cyberattaquants et leurs évolutions
- Les malwares employés
- Les techniques maveillantes les plus employées sur la période
- Les threat actors les plus actifs
- Les secteurs d'activités ciblés par les cybermenaces

Ce rapport a pour objectif de partager les grandes tendances en matière de cyber menaces constatés sur la période avec par exemple sur ce semestre :

- L'utilisation de fichiers HTML à des fins malveillantes.
- L'importance pour un attaquant d'utiliser des techniques de découvertes du système local et du système d'information dans le cas d'une post-infection.
- La présence du malware Qbot et des threat actors SilverTerrier et Wizard Spider dans le haut de notre top des malwares et threat actors.

Il permet aussi de mettre en avant notre interprétation sur certains faits cyber comme :

- La diminution du nombre de cybermenaces ciblant le secteur des cryptomonnaies
- Le ciblage des gouvernements autoritaires par les hacktivistes
- L'exploitation par les cybercriminels de certains fichiers à des fins d'infection, dans le cadre des modifications d'utilisation de Microsoft Office

La Purple Team a également souhaité décrire des cybermenaces plus anecdotiques mais originales comme l'utilisation de fichier Hangul pour la compromission d'un poste de travail ou l'explication de la survie de Wannacry.

02 VECTEURS D'INFECTIONS :

UN PODIUM STABLE QUI CACHE UNE VARIÉTÉ DE TYPES DE FICHIERS

Dans la continuité du début d'année 2021, nous retrouvons sur le podium les exécutables Linux (ELF) et Windows (PE) avec une large prévalence de ce dernier qui prend la tête du classement sur ce second semestre.

La raison en est que les exécutables se retrouvent invariablement sur une chaîne d'infection et particulièrement dans la phase finale de son mode opératoire. La prévalence des exécutables Windows traduit naturellement l'écrasante domination de l'OS de Microsoft, sur le marché des équipements PC professionnels notamment. Mais aussi le fait que la société ne soit pas parvenue à réduire suffisamment la surface d'attaque sur son système d'exploitation phare, et ceci en dépit de de quelques initiatives concernant la suite bureautique MS Office.

LES MALDOCS, UN ÉCOSYSTÈME EN MUTATION

Après quelques hésitations, l'éditeur de Redmond a finalement pris la décision fin juillet, d'entériner le blocage par défaut des macros sur sa suite Office. La sortie des fichiers Microsoft Office de notre top 3 était, de ce fait, attendu.

Jusqu'à lors, ces fichiers faisaient partie intégrante d'un mode d'infection prédominant débutant par un courriel d'hameçonnage (phishing)[1], à l'allure professionnelle, et contenant, un fichier Word, Excel ou PowerPoint en pièce jointe. Ce type de fichier étant couramment partagé dans le milieu professionnel, la cible était portée à se montrer peu méfiante et à ouvrir la pièce jointe. Cette dernière contenait alors une macro[1], c'est-à-dire du code écrit en Microsoft Visual Basic, exécutant à l'ouverture du fichier [1] une commande PowerShell dans le but de délivrer et d'exécuter une charge malveillante, généralement un fichier exécutable Windows (PE).

Par sa décision, Microsoft éloigne considérablement la victime potentielle de la charge malveillante en augmentant le nombre d'opérations à réaliser avant de pouvoir activer la macro malveillante et, de ce fait, réduit l'attrait des acteurs de la menace vis-à-vis des fichiers de la suite Office.

Par un effet quasi mécanique, nous avons observé, une évolution par les cybercriminels de leurs TTP (techniques, tactiques et procédures) pour se déporter vers d'autres types de fichiers. Parmi les acteurs concernés, nous retrouvons Mummy Spider (Emotet), Mallard Spider (Qbot), Maze Team (IcedID) ou encore Agga (Agent Tesla).

Signe que ces acteurs tâtonnent encore dans leur mise au point d'une chaîne d'infection qui serait amenée à remplacer celles où opéraient alors les fichiers de la suite Office, nous constatons pour chacun d'entre eux un louvoiement entre différentes TTP impliquant, pour chacune d'entre elles, différents types de fichier. Parmi ces derniers citons les LNK, archives et images disque qui restent très présents sur le semestre mais aussi, de façon plus éparse et inattendus, les types de fichiers HTA, CHM, MSI et XLL.

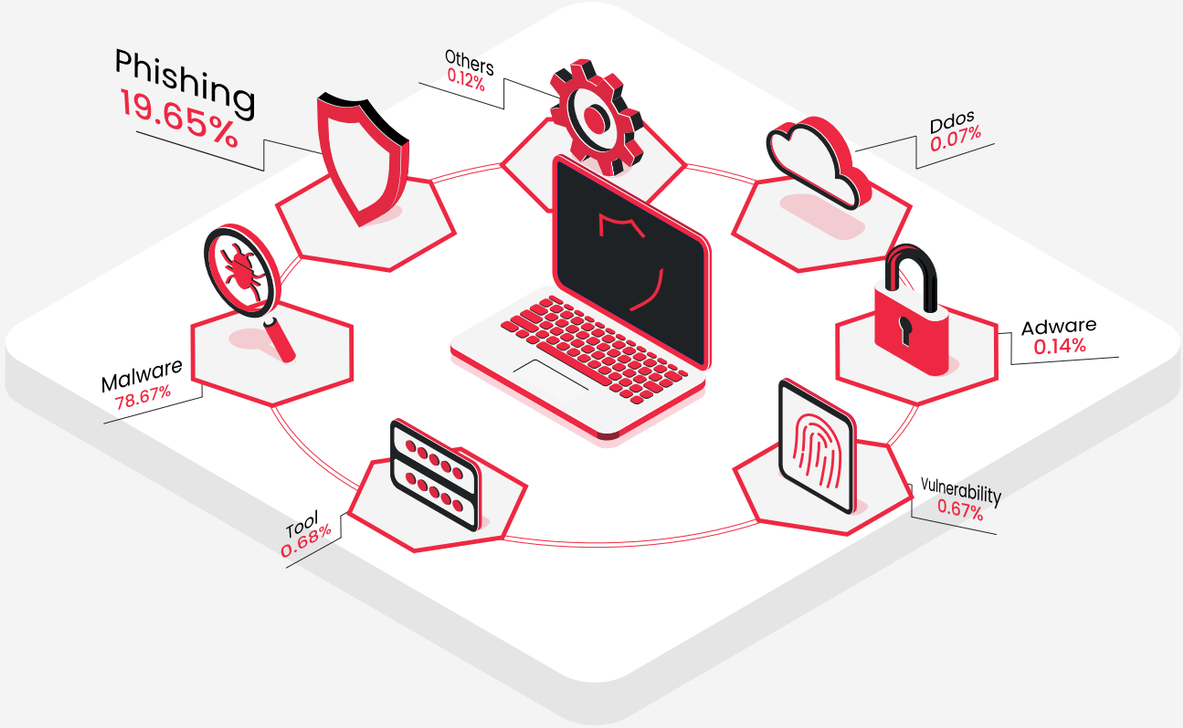
La véritable percée de cette seconde partie d'année concernant les fichiers de type PDF. A l'instar des fichiers MS Office, les PDF sont habituellement perçus comme sûrs et constituent de ce fait un vecteur d'entrée efficace à la suite d'un courriel d'hameçonnage. Ils peuvent notamment être utilisés en vue d'exploiter une vulnérabilité du lecteur Adobe Acrobat pour exécuter du code arbitraire, ou encore pour intégrer du code JavaScript potentiellement malveillant. Les PDF peuvent aussi contenir des liens hypertextes renvoyant vers des sites ou serveurs malveillants pouvant, entre autres choses, initialiser un téléchargement furtif. C'est par exemple le cas sur la campagne IcedID observée en janvier 2023.

TYPES DE FICHIERS MALVEILLANTS :

FICHIERS MALVEILLANTS
LA PÊCHE EST BONNE…

Absents du dernier rapport, les fichiers HTML (HyperText Markup Language) se trouvent, ce semestre, à la deuxième place du podium. Ce type de fichier, qui regroupe de fait les extensions .htm, .hta et, très majoritairement, .html, est si prégnant dans l'écosystème du cybercrime qu'il ne devrait plus quitter le haut du podium dans les semestres à venir.

Évidemment, le rôle classique dans lequel nous retrouvons impliqué ce type de ficher est l'hameçonnage (phishing[1]). Dans ce cas, il s'agit simplement d'imiter une page internet légitime (une banque, un réseau social, un service gouvernemental…) pour inciter la victime à entrer des informations confidentielles (Credentials[1]) ou à télécharger un exécutable malveillant. La tâche est rendue aisée par la prolifération des kits d'hameçonnage (phishing kit) en accès public ou semi-public sur internet. Ces "boites à outils" ont largement contribué à réduire le coût, à la fois technique et opérationnel, ainsi qu'à augmenter la qualité des campagnes d'hameçonnage. Dans ce cadre, il est important de souligner une variante du phishing, le harponnage (Spear phishing[1]) qui ajoute au phishing des techniques d'ingénierie sociale afin de personnaliser l'attaque, la rendant, de ce fait, beaucoup plus efficace.



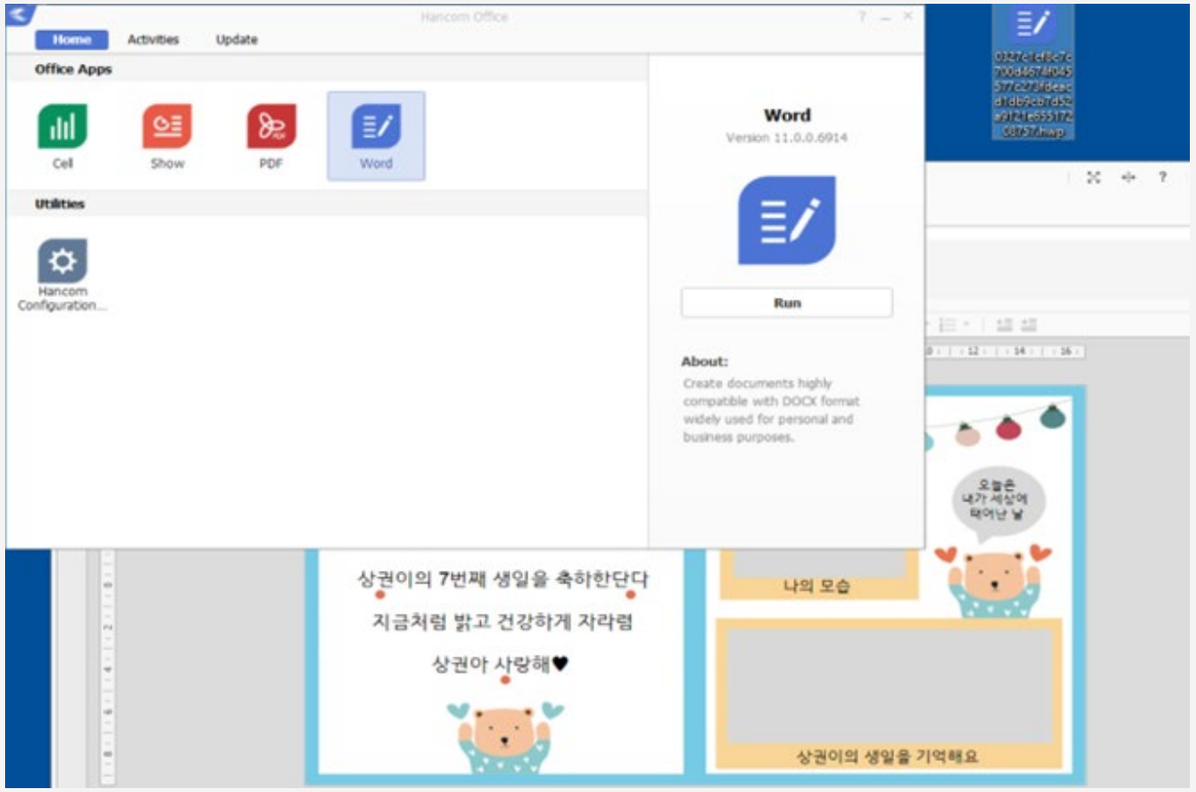
... MAIS AUSSI

Les fichiers HTML peuvent être aussi utilisés dans le but de contourner les passerelles de courrier électronique (email gateways), qui garantissent généralement un certain niveau de sécurité à l'usager en filtrant les courriels potentiellement malveillants ou indésirables de la boîte de réception, en ayant recourt à la technique dite de "HTML smuggling"[1].

Cette technique consiste à cacher une charge malveillante à l'ïntérieur d'un fichier HTML en apparence bénin. La charge sera par la suite reconstruite lors du chargement de la page par le navigateur et téléchargée sur le poste de la victime. C'est notamment la technique d'intrusion utilisée par le logiciel malveillant Qbot[1] évoqué plus loin dans ce rapport.

LES FICHIERS HANGUL, UNE SPÉCIFICITÉ CORÉENNE

Nous retrouvons dans les résultats de notre collecte des fichiers une extension peu commune nommée .hwp. Les fichiers HWP, où Hangul, tirent leur dénomination du logiciel de traitement de texte "Hangul Word Processor", devenu Hancom Office, couramment utilisé en Corée du Sud. Développé par l'entreprise Hancom Inc., ce logiciel a été largement adopté par les organisations nationales et agences gouvernementales dans le cadre d'une politique d'indépendance informatique initiée dans les années 90.



De ce fait, ce sont souvent ces cibles institutionnelles qui se trouvent visées par des campagnes, émanant d'acteurs nord-coréens, reposant sur ce type de fichier.

Si par le passé[1], nous avons observé des campagnes s'appuyant sur des vulnérabilités intrinsèques aux logiciels amenés à traiter les fichiers de type HWP (ex : CVE-2015-1774, CVE-2018-0360) ou encore, abusant de la capacité de ces fichiers à exécuter du code écrit en PostScript, les campagnes sur notre période d'étude reposent principalement sur l'exploitation du protocole OLE (Object Linking and Embedding).

Sur Windows, le protocole OLE permet à des applications utilisant des formats différents de dialoguer entre elles. Il est alors possible d'intégrer, ou de mettre en lien, des objets générés ou gérés par d'autres applications, comme des images, des vidéos ou encore des feuilles de calculs, dans un document texte.

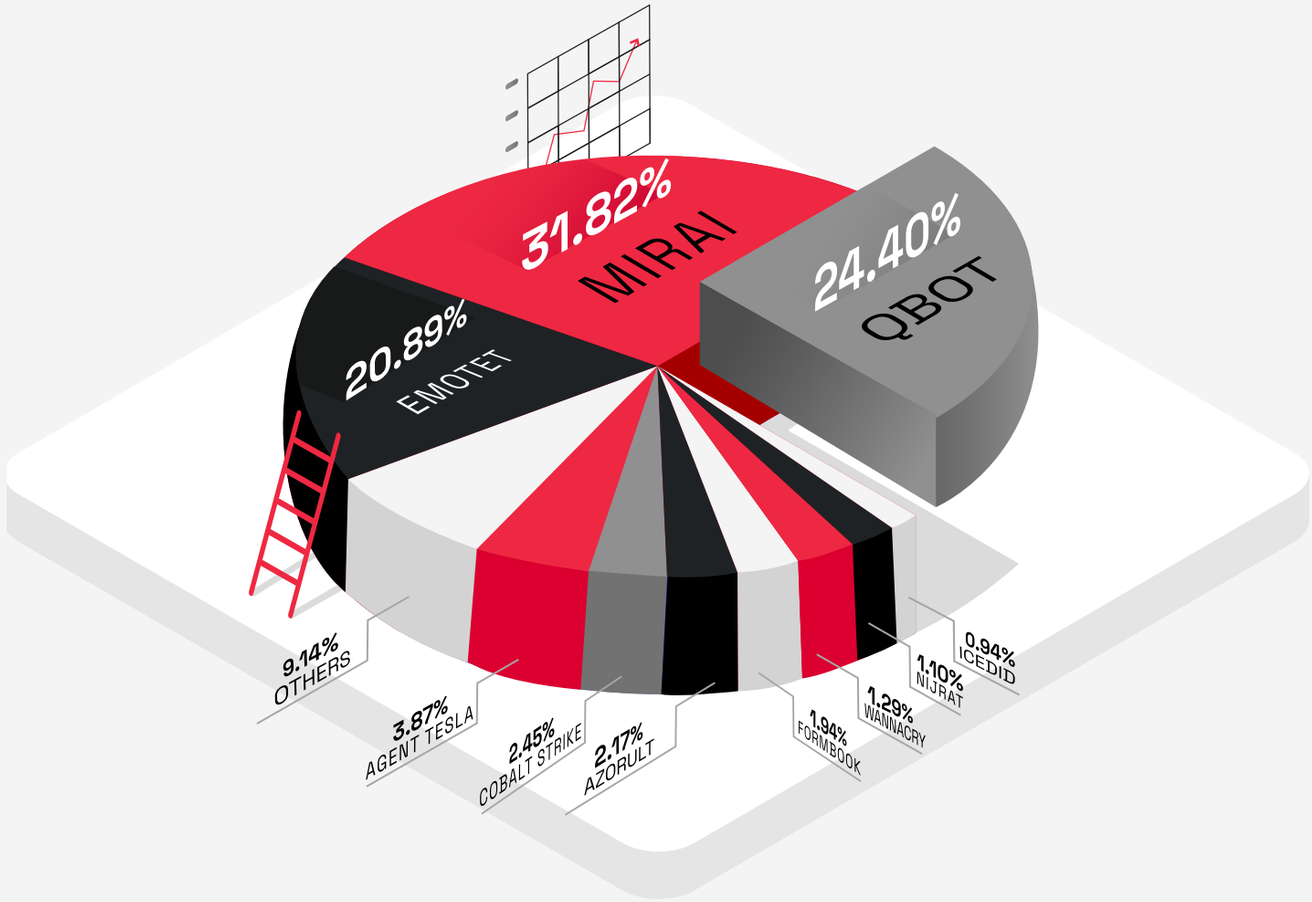
Dans le cas des campagnes actuelles reposant sur les fichiers Hangul, divers scripts (PowerShell et VBS) et exécutables (PE) malveillants sont intégrés au fichier via le protocole OLE et n'attendent qu'un clic de la victime pour délivrer leur charge malveillante. Tout l'objet du document est donc d'amener la victime à cliquer sur le lien OLE en déguisant celui-ci en fenêtre de messagerie, par exemple, ou en tout autre lien d'apparence légitime.

03 MALWARES : DES MENACES **ANCIENNES MAIS PAS OBSOLÈTES**

Dans le rapport portant sur le premier semestre 2022, le haut de notre top des malwares était largement tenu par Emotet que nous avons eu l'occasion d'évoquer dans nos baromètres de mars[2] et de décembre[3] 2022.

Représentant à lui seul plus de la moitié des observations, Emotet a pourtant été détrôné sur le deuxième semestre. Cette brusque descente dans le top est selon nous explicable par l'actualité du groupe Conti., utilisateur intensif d'Emotet qui a cessé ses activités mi-2022 peu de temps après les «Contileaks».

Pour rappel, cet évènement fait suite à la prise de position du groupe Conti dans le conflit entre la Russie et l'Ukraine, où le groupe a affiché son «soutien total» à la Russie.



MIRAI : UN BOTNET EN TÊTE DU CLASSEMENT

Sur le second semestre, la tête du classement est tenue par Mirai et ses variants qui représentent un peu moins d'un tiers des observations. Ces botnets restant toujours très actifs. Un focus lui avait déjà été consacré dans notre baromètre des Cyber Menaces de Juin[4].

La popularité des cibles de Mirai et son comportement lui assure, à l'instar de WannaCry, une place de choix dans notre top, manifestement pour de longues années. Sans grande surprise, le successeur d'Emotet au sein de ce top est le malware Qbot (aussi appellé QuakBot, Pinkslipbot…) présent depuis 2007 dans le paysage des menaces.

L'ANSSI dans son rapport de 2020[5] indiquait déjà que Qbot était distribué par Emotet depuis 2017 et qu'il était devenu la charge malveillante la plus distribuée depuis août 2020. Ce même rapport indique d'ailleurs que le lien entre Emotet et Qbot dépassait probablement la simple relation client / prestataire.

Malgré l'ancienneté de Qbot, ce dernier continue d'évoluer et d'adapter ses méthodes de distribution. Sur la fin d'année 2022, il a été possible de constater par exemple l'utilisation de DLL hijacking dans différents composants de Microsoft Windows ou encore le contournement de la «Mark-of-the-Web» (MotW) qui a fait l'objet d'un focus dans notre baromètre des Cyber Menaces du mois de Janvier 2023[6].

> *« Au vu de ces différents éléments, il est envisageable que la collaboration entre les opérateurs d'Emotet et ceux de Gozi ISFB et de QakBot dépasse la seule interaction client/prestataire.*
>
> **ANSSI | Rapport CERTFR-2020-CTI-010 - p.9**

2017-2021 :
Renforcement des liens avec Emotet

À partir de 2017, Qbot devient un membre incontournable du paysage des malwares avec les premières campagnes fortement médiatisées de 2019/2020.Durant cette période, Qbot acquiert mode opératoire semblable à Emotet : la possibilité de détourner des fils de conversation par e-mail, et ce, de manière localisée.

Durant cette période, la relation entre Emotet et Qbot se renforce : Si Emotet est à ce moment-là le malware le plus distribué, Qbot est la charge malveillante la plus fréquemment délivrée par celui-ci post-infection. C'est également à cette période qu'une campagne d'envergure est lancée avec Egregor, fort des ressources obtenues après l'arrêt des opérations de Maze.

2017 : Observation d'attaque brute-force de compte AD pour se propager

2017 : Distribution par Emotet

2018 : Alerte du FBI sur des clé USB pré-chargées avec Qbot

2019 : Campagne MegaCortex (ransomware)

2019 : Campagne PwndLocker (ransomware)

Mars 2020 : Campagne ProLocker (ransomware)

Août 2020 : Charge la plus distribuée par Emotet

Août 2020 : Apparition du hijacking de fils de discussion localisés

Novembre 2020 : Campagne Egregor

Janvier 2021 : Emotet takedown

Septembre 2021 : Reprise des hostilités, vecteur principal macro VBA Excel

Septembre 2021 : Campagne ProxyShell / Qbot / Cobalt Strike

Octobre 2021 : Campagne Lockean utilisant Emotet / Qbot / Cobalt Strike

Novembre 2021 : Utilisation de la vulnérabilité ZeroLogon

Novembre 2021 : Retour d'Emotet

Février 2022 : Annonce de Microsoft: désactivation des macros

Avril 2022 : Utilisation de MSI

Mai 2022 : Utilisation de LNK

Juin 2022 : Utilisation de Follina (CVE-2022-30190)

Juin 2022 : Observation de QBot dans une campagne de BlackBasta

Juillet 2022 : Utilisation de combinaison HTML smuggling [2]/ ISO / LNK

Juillet 2022 : Utilisation de DLL sideloading dans calc

Septembre 2022 : Utilisation de BruteRatel de fils de discussion localisés

Novembre 2022 : Annonce de MS : propagation de motw aux fichiers des ISO

Novembre 2022 : Utilisation de CVE permettant le bypass de MotW

2021-2022 : Une nouvelle ère

L'arrêt d'Emotet en 2021 redistribua quelque peu les cartes, contribuant naturellement à l'augmentation de l'utilisation de Qbot. On verra également apparaître d'importantes campagnes se basant sur l'exploitation de vulnérabilités comme vecteurs d'infection initiaux.

Enfin, malgré un retour en force d'Emotet sur la fin 2021-début 2022, on notera les adaptations rapides de Qbot, suite aux annonces de Microsoft, dans les méthodes de livraison. Qu'il s'agisse de l'exploitation de vulnérabilités telles que ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021- 31207) ou encore Follina (CVE-2022-30190) ou encore de l'utilisation de types de fichier, à l'époque alternatifs, tels que les fichier LNK ou MSI. Ces adaptations ont permis à Qbot de conserver sa place lors de la mise en retrait d'Emotet sur le deuxième semestre 2022.

WANNACRY EN 2022 : UNE ERREUR DANS LE TOP ?

S'il est encore nécessaire de le présenter, Wannacry (aussi connu sous le nom de WannaCryptor, WannaCrypt ou encore WCry) est un ransomware attribué au groupe Lazarus apparu lors d'une attaque massive ayant eu lieu en 2017 et ayant affecté 150 pays.

Afin de se répliquer, WannaCry a utilisé une vulnérabilité SMB (EternalBlue - CVE-2017-0144) et un outil (Double Pulsar) divulgués quelques temps auparavant lors d'une fuite de données de la NSA publiée par le groupe Shadow Broker ont été utilisés.

Alors que la plupart des malwares présents dans le top ne surprennent pas, la présence de Wannacry en 2022 peut sembler anachronique. Malheureusement, la mise en place d'un simple honeypot SMB durant quelques jours (voire quelques heures) démontre que ce malware est toujours bien présent et toujours actif. Nous pouvons légitimement nous demander comment une menace de 2017 utilisant des vulnérabilités corrigées depuis longtemps peut toujours être active.

Fin 2021, l'éditeur ESET indiquait que 21% de ses détections de ransomwares correspondait à Wannacry. Pour Kaspersky, Wannacry correspondait encore à 12% des détections sur le troisième trimestre 2022[7].

L'explication de cette incongruité est cependant relativement simple. Contrairement à la plupart des menaces actuelles, Wannacry est un ver, qui par définition se réplique dès que l'occasion s'en présente via la vulnérabilité EternalBlue ou en exploitant Double Pulsar. Ainsi, tant que des machines vulnérables seront présentes et accessibles, cette menace ne disparaîtra pas. Une étude de 2021 estime qu'entre 18 et 20 % des clients de Microsoft utilisent des systèmes qui ne sont plus supportés et qu'entre 1.5 et 2 millions de machines exposent encore des vulnérabilités SMB sur internet[8].

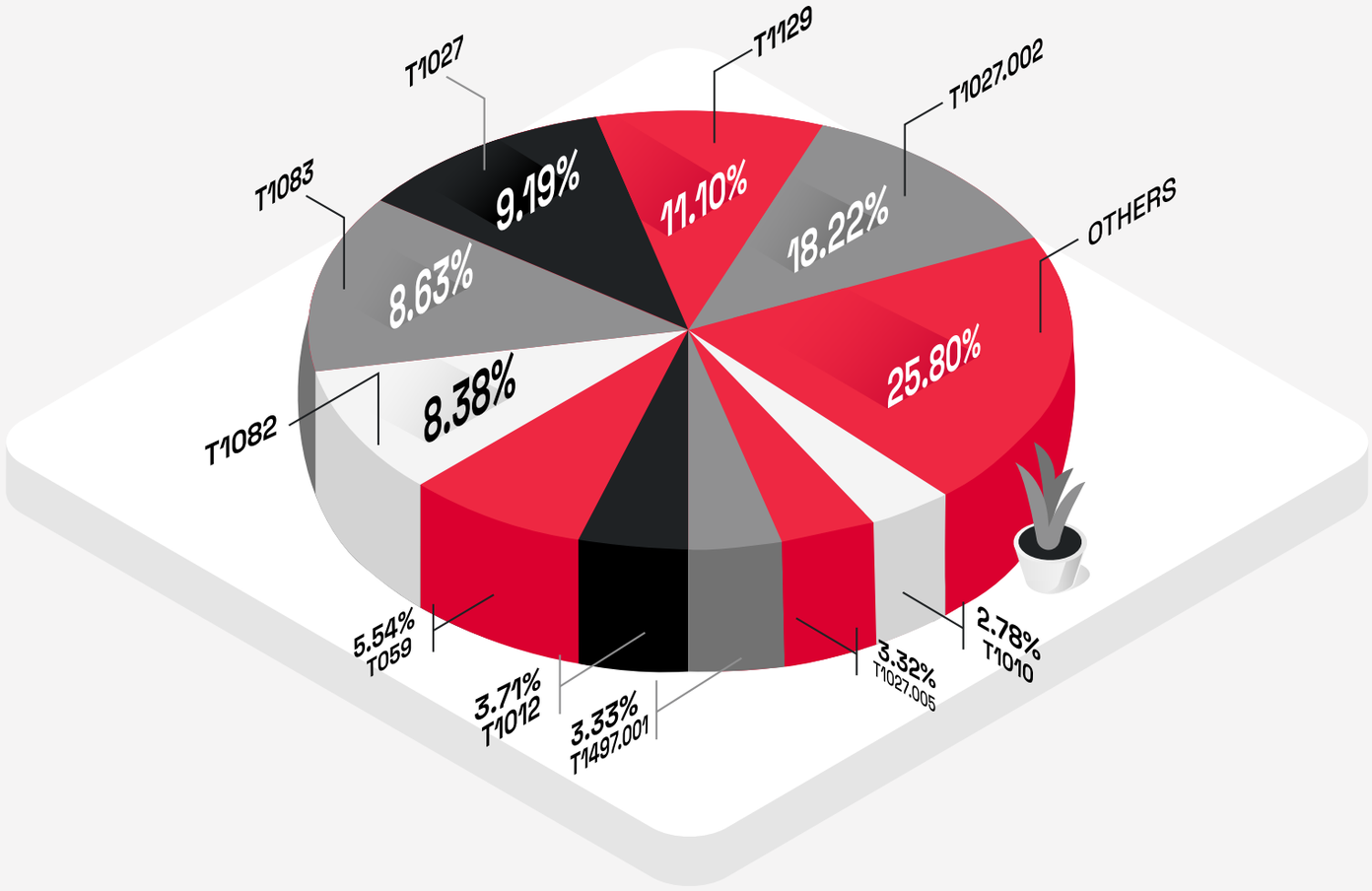
04 TTP : NOUVELLES ATTAQUES, **ANCIENNES TECHNIQUES**

Nos observations sur la seconde partie de l'année 2022 ne nous ont pas fait constater d'évolution notable dans les comportements et techniques utilisés par les acteurs malveillants ce qui entraîne un top10 sensiblement identique à celui du premier semestre.

Les techniques mises en avant ici sont également représentatives des méthodes employées par les malwares que nous retrouvons sur le podium de notre top10 malwares[1]. À noter que cela est rendu possible par le fait que ces méthodes sont suffisamment génériques pour être employées par différents types de logiciels malveillants.

Représentant à lui seul plus de la moitié des observations, Emotet a pourtant été détrôné sur le deuxième semestre. Cette brusque descente dans le top est selon nous explicable par l'actualité du groupe Conti., utilisateur intensif d'Emotet qui a cessé ses activités mi-2022 peu de temps après les «Contileaks».

Pour rappel, cet évènement fait suite à la prise de position du groupe Conti dans le conflit entre la Russie et l'Ukraine, où le groupe a affiché son «soutien total» à la Russie.



FOCUS SUR QBOT

La recrudescence des campagnes Qbot[2] sur ce second semestre 2022 prouve que le malware continue d'être un outil de référence pour de nombreux attaquants. Ce succès est notamment lié à sa modularité qui permet aux différents groupes d'acteurs qui l'utilisent de pouvoir l'adapter facilement à leurs besoins. Mais également à sa modernisation puisque de nouvelles techniques sont régulièrement employées pour ne pas être détectées

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.

Depuis son apparition en 2007 en tant que cheval de Troie bancaire, Qakbot est donc devenu un logiciel malveillant polyvalent qui offre aux attaquants un large éventail de capacités : effectuer des reconnaissances TA0043[1] et des mouvements latéraux, collecter et exfiltrer des données TA0010[1], ou fournir d'autres charges utiles sur les actifs concernés TA0002[1]. Qakbot se propage principalement par l'intermédiaire de pièces jointes et de liens lors d'attaques de type spearphishing (T1566)[1].

D'après les informations collectées par LastInfoSec, notre base de connaissances CTI l'accès initial de Qakbot au cours des troisièmes et quatrièmes trimestres 2022 s'est principalement fait par HTML Smuggling. Cette technique d'évasion qui consiste à s'appuyer sur des fonctionnalités légitimes de HTML5 et Javascript permet aux acteurs de la menace de livrer leurs charges malveillantes via un fichier HTML joint, ou directement via un site internet.

La charge malveillante est directement interprétée par le navigateur de la victime et permet de créer une archive protégée par mot de passe au format zip. En parallèle, une boîte de dialogue s'affiche pour enregistrer le fichier et affiche le mot de passe. Si la victime entre le mot de passe fourni par l'attaquant et ouvre l'archive zip, elle extrait alors un fichier .ISO. Ce fichier permet d'infecter la victime avec le malware Qakbot. Une fois le patient zéro infecté, Qakbot effectue une reconnaissance locale et sur le réseau pour permettre aux acteurs de la menace de se propager et d'atteindre leurs objectifs.

Le vecteur initial de l'attaque étant du phishing, les utilisateurs finaux jouent un rôle majeur dans la lutte contre cette menace. Ils doivent en particulier être sensibilisés au risque de téléchargement d'archives (.zip, .7z…) chiffrées avec un mot de passe sur internet. Cette méthode d'envoi de malware s'est répandue et permet d'outrepasser les éventuels mécanismes de détection présents au niveau du serveur de messagerie ou encore des EDR déployés sur les terminaux. Il peut également être envisagé de désactiver le montage automatique des fichiers d'image disque, tels que les fichiers ISO. Cette action préventive peut être effectué en modifiant les valeurs dans la base de registre Windows.

LA DÉCOUVERTE : UNE ÉTAPE CRUCIALE

Nos recherches ont montré que la découverte d'informations système T1082[1] et la découverte de fichiers et de répertoires T1083[1] font partie des techniques les plus couramment utilisées par les cybercriminels (position 4 et 5 de notre top).

En effet, après l'accès initial à un système infecté, un attaquant tente généralement d'obtenir des informations afin de prendre les bonnes décisions pour la suite de son attaque : élévation de privilèges, mouvement latéral ou encore chiffrement du système d'information. Concrètement, cela se traduit par la tentative d'obtenir des informations détaillées sur le système d'exploitation, les correctifs et les service packs déployés ou encore sur son architecture. Suite à cette collecte l'attaquant aura la capacité de dire s'il souhaite infecter ou non complètement la cible, et par quel biais.

DÉCOUVERTE LOCALE

Qakbot ne déroge pas à la règle puisqu'une fois la machine infectée et la communication avec le serveur Command & Control TA0011[1] établie, sa première tactique est de collecter automatiquement des informations sur le système infecté à l'aide d'une série de commandes exécutées localement. Pour cela, le processus malveillant injecté par Qakbot T1055[1] exécute des commandes utiles à sa reconnaissance en s'appuyant sur des outils en ligne de commandes nativement intégrés à Windows (T1082) / T1083 / T1087 / T1135 /etc.)[1] et donc considérés comme légitimes par les systèmes de protection en place.

Par exemple, la commande «net» peut collecter des informations sur les utilisateurs, les groupes, les hôtes et les fichiers. Le processus malveillant injecté extrait également des informations des navigateurs Web (Internet Explorer et Microsoft Edge) en abusant d'un utilitaire intégré, le binaire Esentutl. Les données du navigateur, y compris les cookies et l'historique du navigateur (T1539), sont collectées à partir du cache web et peuvent permettre d'usurper une session utilisateur pour faciliter la propagation.

DÉCOUVERTE DU SYSTÈME D'INFORMATION

L'interrogation d'Active Directory (AD) est également une autre tactique courante de collecte d'informations. Les attaquants peuvent exploiter les données extraites de l'AD pour obtenir des informations sur le réseau et augmenter leurs privilèges.

Via ce moyen, il est possible de connaître le domaine auquel appartient la machine infectée et d'en apprendre davantage sur les utilisateurs, groupes et assets de ce domaine. Il existe plusieurs outils dédiés à cette reconnaissance : PowerView, ADRecon ou encore Bloodhound.

→ **Ces outils peuvent être utilisés à des fins légitimes, mais ils sont aussi fréquemment utilisés par les groupes de cyberattaquants.**

PAR EXEMPLE...

Des cas récents d'infections par Qakbot ont permis de mettre en évidence le déploiement du framework Brute Ratel[8] comme charge utile. Le support de ce framework permet une intégration facile de l'utilitaire SharpHound qui est le collecteur de données officiel de BloundHound. Le processus malveillant peut donc exécuter cet utilitaire pour cartographier le domaine Active Directory et en apprendre davantage sur la structure du système d'information ciblé : unités organisationnelles Active Directory (T1087.002), les stratégies de groupe (T1615) , les relation de confiance inter/intra-domaines (T1482), les comptes et groupes à privilèges (T1615).Tous les fichiers collectés sont ensuite compressés dans un fichier ZIP en vue d'une exfiltration.

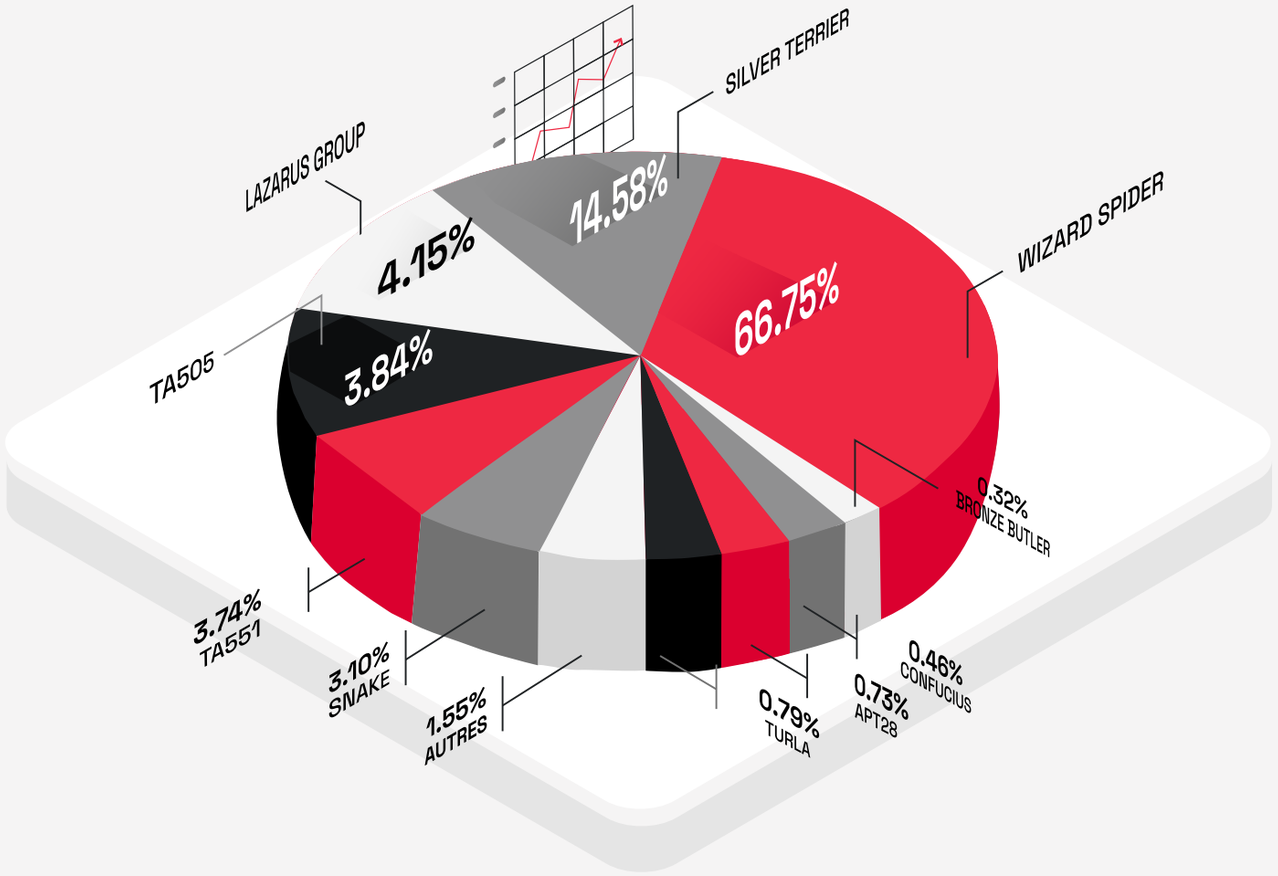
De la même façon, dans les campagnes récentes du malware Emotet[2], il a été constaté l'ajout d'un module de propagation via le protocole SMB[9]. Lorsque ce module est chargé sur la machine infectée, une reconnaissance est lancée énumérant ainsi les ressources réseau (T1135) pour dresser une liste de serveurs. Ensuite, le module parcourt la liste fraîchement établie et tente de se connecter au partage IPC$ en utilisant des listes de noms d'utilisateurs et de mots de passes communs codés en dur (T1110.001).

Si aucune connexion n'est établie avec les informations d'identification disponibles, le module SMB peut également tenter de rechercher des noms d'utilisateurs supplémentaires auprès du serveur ciblé avec la fonction NetUserEnum des API Windows. Chaque nouveau nom d'utilisateur potentiel trouvé fera l'objet d'une attaque en force brute avec avec la liste codée en dur utilisée précédemment. Si une connexion réussit, le module tente enfin de se connecter aux partages ADMIN$ et C$ et copie le loader Emotet sur ledit partage puis l'exécute : un mouvement latéral est alors réalisé.

05 THREAT ACTOR : UN VENT D'EST S'ABAT SUR LE PAYSAGE DES CYBERMENACES

Avec près de 100 acteurs de la menace suivis en cette deuxièmepartie de l'année, nous vous présentons pour la première fois un classement des 10 groupes de cybercriminels les plus observés.

Sans grande surprise, notre classement est principalement composé de groupes russes et chinois. Ces deux régions du monde étant réputées pour avoir un vivier très important de cyber attaquants. Nous remarquons tout d'abord que ces groupes opèrent depuis plus d'une décennie. Deux motifs les animent, le gain financier et le cyber-espionnage.



WIZARD SPIDER

En première place, le groupe Wizard Spider domine ce classement. Cet acteur de la menace affilié selon toute vraisemblance aux réseaux de cybercriminalité russes est aussi identifié sous les noms UNC1878 ou Team9.

Il est principalement connu pour la multitude de malwares que ces membres ont développé depuis 2017 (Emotet, Conti, TrickBot, BazarLoader et Ryuk). Cette organisation a les ressources pour réaliser des campagnes de cyber attaques à très grande échelle, des phases de reconnaissance et d'intrusion, jusqu'au paiement et blanchiment de l'argent extorqué. Wizard Spider est à l'origine de millions de spams, d'attaques par rançongiciel et de vols de données qui leur a, en outre, permis la divulgation frauduleuse d'informations privées.

Le groupe cible les organisations du secteur public (gouvernement, santé, etc.), un large éventail de grandes entreprises privées, le secteur de la défense, et bien d'autres. Malgré une baisse de présence en ce deuxième semestre Emotet reste troisième de notre classement, ce qui explique pourquoi Wizard Spider, le cyber groupe derrière ce trojan, se trouve en première position.

SILVER TERRIER

SilverTerrier, un groupement de plusieurs attaquants nigérians spécialisé dans les escroqueries via BEC (Business Email Compromise). Une fraude par BEC consiste en l'envoie d'un email qui imite la provenance d'une source connue faisant une demande légitime. Ce groupe opère depuis 2014, et cible principalement les entreprises dans la haute technologie, l'enseignement supérieur et le secteur de la production. La position de Silver Terrier dans notre classement fait écho au rapport 2021 du FBI Internet Crime Complaint Center (IC3)[10] où il a occupé la première place pendant 6 années consécutives. Au cours des derniers mois, il a été observé une très forte utilisation des malwares Agent Tesla et Lokibot lors de ses campagnes. Ces derniers occupant respectivement la 4e et 12e place de notre classement des malwares.

LAZARUS GROUP

Lazarus group vient clôturer le podium. Aussi appelé APT38 ce groupe , sponsorisé par l'état nord-coréen, est actif depuis 2009 et est mondialement connu pour mener des attaques à motivation idéologique. Il a pour principaux objectifs l'extorsion d'argent, le vol d'information, le sabotage et l'espionnage. Durant ses nombreuses années d'activités, il a attaqué le secteur bancaire, l'industrie de la défense, des éditeurs de logiciels, des groupes pharmaceutiques, des plateformes de crypto monnaie, des industries dans la production et l'énergie. Il conduit ses attaques en se basant sur l'ingénierie sociale et l'imposture avec des campagnes d'hameçonnage comme premier vecteur d'infection.

Il avait pour objectif de voler les clés privées et d'exploiter des vulnérabilités pour faire des transactions frauduleuses. Ces dernières années, le groupe aurait dérobé approximativement 2 milliards de dollars en crypto-monnaie. Au pied du podium, TA505, un groupe russe principalement connu pour la création du trojan bancaire Dridex et sur lequel nous revenons dans ce rapport.

Ce groupe a attiré notre attention cette année par la diversité des outils utilisés et par sa détermination à améliorer les codes malveillants qu'il a pu éprouver au cours des dernières années. Depuis 2018, TA505 a ajouté Azorult à son arsenal de malware maison. Ce dernier a été observé dans plusieurs campagnes en cette fin d'année et occupe la 6e place de notre top malwares.

Le milieu de ce top est occupé par TA551/Shathak, un groupe distribuant ses malwares par email et ciblant principalement l'Europe et le Japon. Lors de nombreuses campagnes qui lui sont attribués, le malware IcedID (10e du classement malware) a été utilisé, avec une chaine d'attaque qui est devenu courante cette année ; une archive ZIP en pièce jointe contenant un fichier ISO avec un raccourci Windows (.lnk) qui grâce à une commande PowerShell vient charger une librairie Windows (.dll).

Vient après Turla/Snake un groupe russe qui a mené diverses attaques avec l'utilisation de keyloggers comme Agent Tesla et NjRAT. Le reste du classement est composé de groupes menant des actions de cyber-espionnage comme APT 28 (7e), Confucius (8e), Bronze Butler (9e) et Dragonfly (10e). Ces acteurs ciblent principalement des secteurs critiques comme la défense, les gouvernements ou encore l'énergie. La guerre en Ukraine qui a débuté en février 2022, amenant une crise de l'énergie et un contexte géopolitique instable explique la forte représentation de ces cyberattaquants sur la période.

...FOCUS 1 : TA505

TA505 est un groupe cyber criminel russe opérant depuis 2014, connu pour être derrière le cheval de Troie bancaire Dridex et le ransomware Locky. Au début de son existence le groupe se reposait beaucoup sur des services et outils tiers pour mener ses activités frauduleuses puis il a gagné en maturité au fil des années pour arriver à une maitrise indépendante de l'intégralité de la kill chain.

Aussi suivi sous les noms Grateful Spider, Evil Corp, Gold Drake, ATK103, Dudear, Indrik Spider TA505 a pour habitude de lancer des campagnes de phishing massive avec un taux de réussite élevé, exploitant des systèmes vulnérables et incitant les utilisateurs à télécharger leurs logiciels malveillants.

Le gain financier est le motif principal de cet acteur, obtenu grâce au vol de données sensibles et la demande de rançon. Le groupe a aussi extorqué plusieurs millions de dollars à ses victimes. Graceful Spider fait preuve d'un haut niveau de sophistication technique en faisant constamment évoluer ses tactiques pour échapper à la détection. Opérant le botnet Necurs, le groupe a démarré son cœur de métier en vendant des accès aux réseaux compromis à d'autres opérateurs de logiciels malveillants, au travers desquelles il a pu opérer certaines des campagnes de spam les plus notoires.

CHRONOLOGIE :

2014 - 2017 :

Peu d'activité mise à part la distribution de chevaux de Troie et rançongiciels. Opérant le malware Dridex, le groupe de cybercriminel privilégie le rançongiciel Locky en 2016 avant de relancer des campagnes en 2017. TA505 a utilisé le malware TrickBot lors d'attaques en 2017

2018 à aujourd'hui :

Changement de méthode d'intrusion, passage des trojan et ransomwares au backdoor. TA505 proposait un accès aux systèmes d'informations pénétrés mais en garder certains afin de lancer des charges malveillantes sur les machines des victimes. En première phase, le groupe a utilisé différents downloaders (logiciels malveillants permettant de télécharger une charge offensive) comme Quant Loader, Marap, Amadey ou Gelup.

Ces derniers ont permis au groupe d'avoir accès aux machines de leurs victimes via des portes dérobées (backdoor) tel que FlawedAmmyy, tRat, ServHelper, FlawedGrace, FlowerPippi ou SDBot (nous avons pu observer que certains de ces malwares étaient encore utilisés par le groupe en 2022).

D'autres familles de malwares seraient liées à ce groupe comme Flawed Ammyy, le botnet Neutrino et la porte dérobée ServHelper (dont une variable permet de télécharger le remote access trojan[3], FlawedGrace) ou encore le rançongiciel Clop qui aurait infecté de nombreuses entreprises. L'acteur de la menace a pour habitude de déployer des outils d'accès à distance via le protocole RDP (T1572, Protocol Tunneling). Nous avons constaté que les secteurs des banques en ligne et des sites e-commerce ont été victimes de cette backdoor en début de ce deuxième semestre.

Depuis 2019, le cyberattaquant a commencé à utiliser une backdoor nommée ServHelper afin de détourner les comptes des victimes et de déployer des commandes permettant l'enregistrement des frappes au clavier (T1056.001, Input Capture : Keylogging) et le vol de données sensibles.

Depuis août 2022, l'exploitation d'une vulnérabilité (CVE-2022-31199) sur la solution Netwrix Auditor permet de distribuer le malware Truebot. A partir d'octobre 2022, le malware Truebot est distribué via Raspberry Robin. Deux botnets ont été utilisés lors des infections, un premier ciblant le Mexique, le Brésil et le Pakistan et un deuxième plus tard en Novembre visant les USA. Ce deuxième botnet exploitait des machines Windows avec des services ouverts sur internet comme SMB et RDP.

EN FIN D'ANNÉE 2022

Ces attaques pouvaient avoir pour finalité l'utilisation du rançongiciel à double extorsion Clop. En fin d'année 2022 nous avons constaté l'augmentation de la présence du malware Truebot, aussi appelé Silence Downloader, responsable d'importantes attaques sur des organisations financières.

Ce malware a permis de distribuer le malware Grace (également identifié sous les noms FlawedGrace ou GraceWire). Le groupe TA505 a innové en passant d'une méthode de propagation classique grâce à des emails malveillants à une ancienne technique via des clés USB.

...FOCUS 2 : APT41

APT41(G0096) est un acteur sophistiqué du cyber-espionnage, probablement soutenu par le gouvernement chinois, et qui opère depuis au moins 2012. Ce groupe de menaces a ciblé des organisations du monde entier, dans des secteurs verticaux tels que les hautes technologies, les télécommunications, et la santé.

Ce dernier semestre, APT41 a fait la une des journaux aux États-Unis suite à certaines révélations des services secrets Américains[15]. Ces derniers ont fait part publiquement de l'implication du groupe dans ce qu'ils dénoncent comme étant le premier cas de fraude pandémique soutenu par un gouvernement étranger. Grâce à son stratagème, le groupe aurait réussi à voler au moins 20 millions de dollars en avantages liés au COVID 19, notamment en bénéficiant de prêts et de fonds d'assurance-chômage dans plus d'une douzaine d'États.

Par ailleurs, le 22 septembre dernier, le Centre de coordination de la cybersécurité du secteur de la santé (H3C), appartenant au ministère de la Santé et des Services sociaux américain, a publié une note concernant le groupe cybercriminel chinois APT41 et appelle à la vigilance. Bien que cet acteur de la menace ne soit pas présent dans notre top10, les déclarations du gouvernement Américain montre que ce groupe est toujours actif et qu'il mérite encore une attention particulière.

Le groupe se distingue par sa particularité à s'adonner à des opérations à caractère financier ce qui est plutôt inhabituel parmi les groupes de menaces connus qui sont parrainés par l'État chinois. Ce dernier point laisse également supposer auprès des chercheurs en cybersécurité que le groupe fonctionne comme une entreprise avec plusieurs équipes, dont chacune suit des objectifs distincts.

Par le passé, APT41 a abusé à plusieurs reprises des chaines d'approvisionnement logiciels. Le groupe a piraté les environnements de développement de plusieurs fournisseurs de logiciels et a injecté du code malveillant dans des outils signés ce qui lui a permis de distribuer à grande échelle des logiciels malveillants. C'est le cas par exemple de l'attaque menée en 2017 contre CCleaner, qui s'est traduite par la distribution de copies compromises de l'utilitaire[11] à 2,2 millions d'utilisateurs.

Ces dernières années le groupe a également montré une forte capacité à tirer profit des vulnérabilités divulguées publiquement ce qui lui a permis d'accéder à de nombreux réseaux. Par exemple, début 2020, le groupe a été lié à une campagne mondiale d'intrusion qui a exploité des dispositifs et applications de grands éditeurs tels que Cisco, Citrix et Zoho, ce qui lui a permis d'obtenir un accès à des dizaines d'entités, de tous secteurs, dans plus de 20 pays. A noter que contrairement à leurs campagnes historiques dont l'accès initial était plutôt acquis par le phishing ou la diffusion de malwares, dans le cas présent, les attaques menées ciblaient principalement des systèmes et des appareils vulnérables directement exposés sur Internet.

De la même façon, en décembre 2021, à peine quelques heures après la publication du bulletin de sécurité de la Fondation Apache pour la faille Log4j [12], le groupe a exploité la vulnérabilité afin de compromettre deux gouvernements d'État, ainsi que des cibles plus traditionnelles dans le secteur des télécommunications.

Ces opérations incessantes ont conduit le gouvernement américain à délivrer entre 2019 et 2020 deux actes d'accusation contre cinq membres présumés du groupe. A date, ces individus sont toujours en liberté et leurs noms ont été ajoutés à la liste des personnes les plus recherchées par le FBI[13].

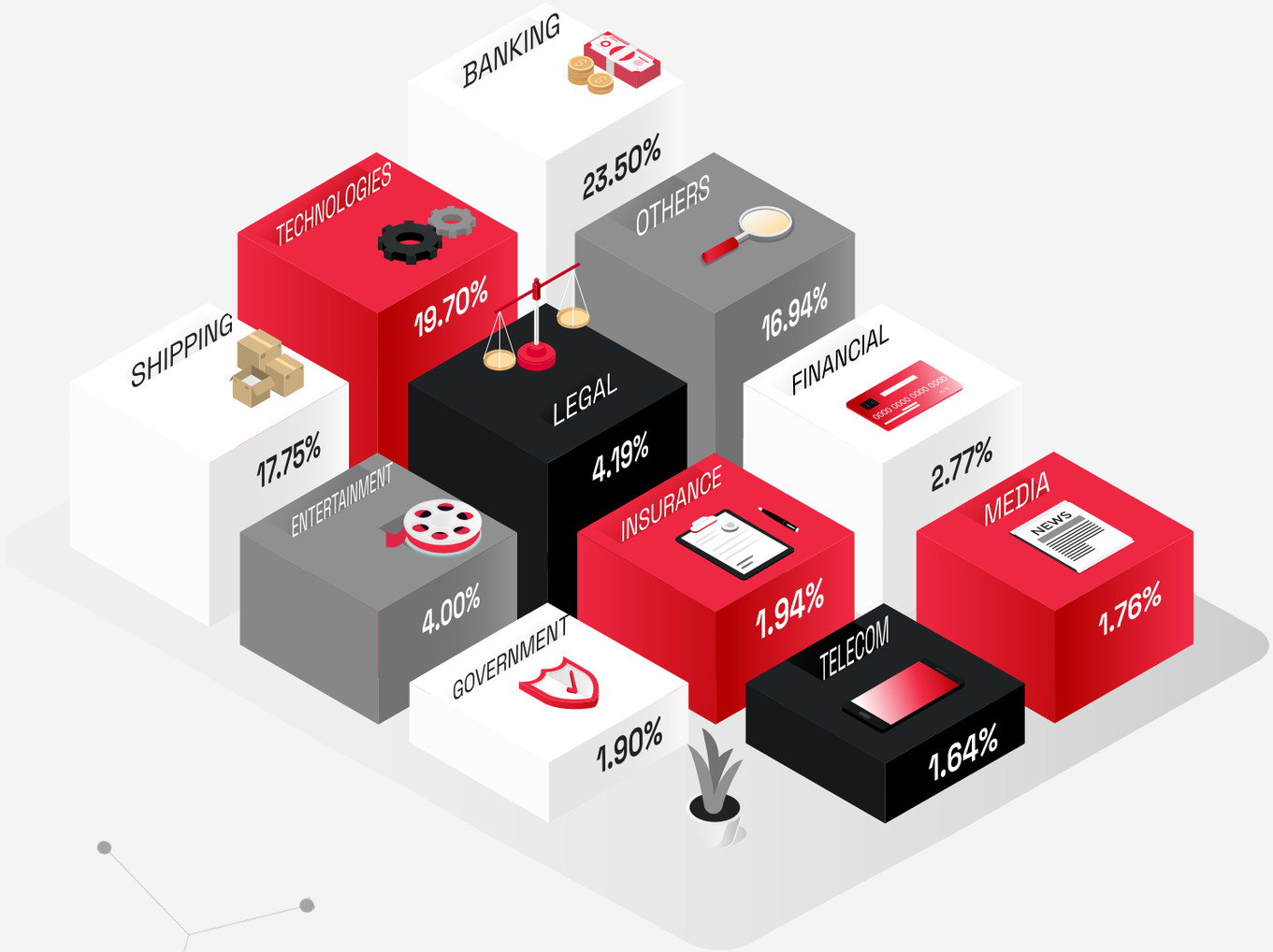
Le groupe se caractérise par ses tactiques de compromission avancées, dont l'exploitation de plusieurs zero-days et la mise en œuvre de plusieurs techniques d'obfuscation pour masquer son activité. En complément, le groupe dispose d'un arsenal d'outils pour accomplir ses missions, y compris des utilitaires grand public, des logiciels malveillants partagés avec d'autres opérations d'espionnage chinoises ou encore des outils qui leur sont propres.

APT41 exploite une variété de techniques courantes pour obtenir un premier accès à ses victimes, nous pouvons citer entre autres l'usage de spear-phishing T1566[1], le déplacement latéral à partir d'un tiers de confiance (1133) [1], l'exploitation d'informations d'identification volées (T1078)[1],etc.

Cependant, une fois introduit au sein d'une organisation victime, cet acteur de la menace peut exploiter des TTP plus sophistiqués et déployer des outils malveillants supplémentaires. Par exemple, au cours d'une campagne de près d'un an, APT41 a compromis des centaines de systèmes et utilisé près de 150 logiciels malveillants uniques, notamment des portes dérobées(T1053.005, T1547.001, T1542.003)[1], des voleurs d'informations d'identification T1112[1] ,et des enregistreurs de frappe T1056[14].

Ce groupe malveillant a prouvé ces dernières années qu'il sait adapter ses techniques d'accès initiales en fonction de sa cible, et qu'il dispose de moyens suffisants pour exploiter rapidement et à grande échelle une vulnérabilité fraîchement rendue publique. Par ailleurs les actes d'accusation contre certains membres du groupe ne semblent pas les avoir découragés dans leurs activités ce qui incite à être vigilant quant aux potentielles futures activités du groupe.

06 SECTEURS PROSPÈRES PLUS MENACÉS ? OUI MAIS PAS SEULEMENT...



À l'image du top secteurs du rapport précédent (1er semestre), nous retrouvons le secteur bancaire en première place de ce classement qui attire les convoitises par les opportunités de gains frauduleux potentiels et la valeur des informations privées monnayables après extorsions.

Le secteur des livraisons, qui se place en troisième position, qui avait déjà fait l'objet d'un focus sur les faux mails et SMS de livraison. Il confirme sa place actuelle de cible privilégiée. D'autres secteurs actuellement dynamiques dessinent également le milieu du classement : le secteur juridique et celui financier, ainsi que le secteur du divertissement qui inclut les jeux d'argent.

Les assurances et les télécommunications composent la fin du classement, accompagnés de secteurs stratégiques comme les médias et les gouvernements, sur lequel nous reviendrons par la suite. Pour conclure, le secteur des cryptomonnaies, qui clôturait le classement précédent, a disparu ce qui peut s'expliquer par la forte correction à la baisse du marché.

CRYPTOMONNAIES : UNE CHUTE EN CASCADE

La chute de la valeur des cryptomonnaies, les NFT qui ne séduisent plus et un métavers qui peine à trouver son public, l'année 2022 a été marquée par un tournant, pour le pire, de l'univers des cryptomonnaies.

Ce sont en particulier les chutes successives des monnaies UST et LUNA, du fond spéculatif Three Arrows Capital et surtout la faillite de la bourse de crypto-monnaies FTX qui ont entraîné une panique extrême des petits investisseurs et un retrait massif des cryptomonnaies sur les plateformes d'exchange.

Les attaques par phishing, menace la plus massivement utilisée sur le secteur, ont en conséquence été délaissées par les attaquants. Une autre menace a pourtant gagné en popularité : l'utilisation malveillante des cryptominers (aussi appelés coinminers). Déjà présents, ces logiciels utilisés pour le minage des cryptomonnaies ont largement été détournés par les attaquants et une évolutimontante du nombre de variants a été observée tout au long de l'année 2022.

L'idée est d'infecter les machines victimes avec un cryptominer pour en utiliser les ressources au profit des attaquants. Une étude produite par Sysdig a mis en avant que chaque dollar « miné » représente un coût de $53 pour les entreprises exploitées[1]. Rentrent notamment en compte les coûts énergétiques et en ressources Cloud qu'un botnet peut engendrer.

La popularité croissante des infections par cryptominers peut être expliquée par différents éléments :

- → L'affranchissement du prix de l'électricité
- → L'absence du besoin d'infrastructures
- → Le peu de connaissances techniques nécessaires
- → La facilité de leur intégration dans une attaque plus large

Même si le déploiement des cryptominers est réalisé principalement au travers du phishing, par le téléchargement de contenus piratés (ou malwares déguisés en ressources légitimes) ou par l'exploitation de vulnérabilités, certains attaquants font preuve de plus d'ingéniosité.

Nous avons pu observer la mauvaise configuration d'API de containers Docker, publiquement exposée et exploitée à grande échelle, ainsi que l'apparition de fausses images Docker de distributions Linux, infectées en amont. Cette dernière méthode a permis aux attaquants de déployer un volume non-négligeable de cryptominers, avec pas moins de 20 millions de téléchargements d'au moins 30 images constatées.

Les voleurs d'information (info stealers) constituent l'autre menace affectant ce secteur. Il s'agit d'une catégorie de trojan modelée pour rassembler les informations présentes sur une machine et les envoyer à l'attaquant. La plupart de ces malwares volent des identifiants présents dans le système ou dans les navigateurs. Ils se sont récemment développés pour récupérer les informations des portefeuilles numérique (digital wallets présents localement). Comme pour les cryptominers, c'est une méthode très peu coûteuse, et il suffit d'un bon ciblage pour obtenir des gains conséquents.

DES ATTAQUES OUBLIÉES, CELLES VISANT LES GOUVERNEMENTS

Les « pendant » et « après » crise du covid ont été rythmés par d'innombrables cas d'infection par ransomwares, particulièrement à l'encontre des services de santé déjà débordés, à l'image de l'attaque contre le CHSF de Corbeil-Essonnes dont nous avons parlé dans un précédent rapport semestriel. La recherche de gains financiers, première motivation des acteurs de la menace, a mis le phishing et les ransomwares sur le devant de la scène.

En parallèle, nous entendons moins régulièrement parler d'attaques étatiques contre les services gouvernementaux et les administrations, qui visent aussi bien à exposer des activités, qu'à perturber des services, ou encore dérober des informations sensibles pour le compte d'autres puissances étatiques.

Nous distinguons généralement trois types d'attaquants :

- Ceux dit «state-sponsored», ils sont supportés par un gouvernement ce qui leur permet de faire des attaques de grande ampleur, quelles que soient les cibles.
- Les organisations criminelles, qui visent principalement les gains financiers que les attaques peuvent générer.
- Les hacktivistes, dont l'objectif est l'évolution sociale et politique.

Cette dernière catégorie s'est beaucoup fait entendre, notamment à travers le groupe «Anonymous» qui a fait parler de lui médiatiquement à de nombreuses reprises pendant ces dernières années. En septembre 2022, ce groupe d'activistes a, par exemple, pris part au conflit iranien en mettant hors-service plusieurs sites web du gouvernement ainsi qu'en obtenant les informations personnelles d'une base de données du parlement.

Différents groupes affiliés aux Anonymous affirment aussi avoir publié des données provenant de services ministériels et gouvernementaux, et ont revendiqué le piratage de la présidence iranienne.Ces différentes attaques apportent un soutien moral au peuple iranien, plongé depuis plusieurs mois dans une interruption quasi-totale de l'Internet.

Le gouvernement iranien n'est pas seulement visé pour ses violations des droits humains, il a aussi été la cible de cyber espionnage par le groupe chinois APT15[2]. Actif depuis 2010 et déjà connu pour ses campagnes d'espionnage contre des gouvernements d'Amérique du nord et sud, d'Afrique et du Moyen-Orient, le groupe s'en est cette fois pris aux institutions iraniennes de juillet à décembre 2022. Pendant cette période, plusieurs infrastructures gouvernementales, dont le ministère des affaires étrangères, ont établi des communications avec serveur C2 connu du groupe APT15.

Ce schéma laisserait plutôt supposer un vol de renseignements plutôt qu'un endommagement des infrastructures. Cette campagne aurait été lancée par le groupe en désaccord avec un programme de coopération signé entre la Chine et l'Iran.

La Chine a également été propulsé au cœur de l'actualité en juillet dernier lorsqu'une base de données de la police de Shanghai a été proposée à la vente. La base de données contenait les informations personnelles de près d'un milliard de citoyens chinois ainsi que plusieurs milliards de rapports de police datant de 1995 à 2019.

Nous y retrouvons notamment les noms, adresses, numéros de téléphone et numéros d'identité de citoyens chinois, pas uniquement d'habitants de Shanghai. Plus incroyable encore, les données étaient accessibles publiquement depuis 14 mois via une interface web reliée à la base de données. La cause serait une mauvaise configuration du service, l'exposant sur internet. Toutes les personnes disposant de l'URL pouvaient y accéder librement, sans authentification.

CONCLUSION

L'analyse par la Purple Team Gatewatcher des renseignements fournis par notre infrastructure CTI entre juillet-décembre 2022 rappelle que les cybermenaces restent globalement stables sur la période. En effet, les motivations des threat actors restent majoritairement l'argent, l'espionnage ou l'hacktivisme.

De plus, les techniques efficaces sur le long terme comme le phishing, le développement de malware ou la recherche d'informations préalables a des mouvements latéraux restent des techniques assidûment utilisées lors des intrusions.

Le rapport détaille comment les threat actors ont eu la capacité de prendre en compte rapidement et efficacement les changements du marché comme le ferait une startup agile et performante. A titre d'exemple, nous notons la forte réduction du phishing ciblant les clients de plateformes d'échanges de cryptomonnaies depuis la chute de FTX et de la baisse du cours des cryptomonnaies

Ensuite, des malwares comme Qbot montrent que l'adaptabilité est le seul moyen de subsister dans cet écosystème en constante évolution technique, ou même l'indétrônable maldocs, en tant que porte d'entrée pour une compromission, a été mis à mal par une décision de Microsoft.

Cette complexification de l'exécution des macros a forcé les cyberattaquants à trouver de nouvelles solutions comme :

→ Utilisation d'images disques (ISO, UDF, ...)

→ Utilisation de raccourci Windows (LNK)

→ Des bypass de systèmes de sécurité comme le Mak-of-the-Web.

De plus, l'analyse des renseignements a mis en avant des situations surprenantes telles que la survie du vers Wannacry qui, même après de nombreuses années d'existence, permet toujours d'infecter de nouvelles machines grâce à son automatisation de la recherche de nouvelles victimes. D'autre part, l'utilisation de types de fichiers quasiment inconnus, tel que Hangul dans notre analyse, a montré l'opiniâtreté de certains threat actors dans l'analyse préalable de la surface d'attaque afin de mettre en place des attaques sur-mesure pour atteindre leurs victimes.

Pour conclure, cette parole de Stephen Hawking «Intelligence is the ability to adapt to change» rappelle que les cybercriminels ont continuellement su s'adapter aux tentatives de défense de leurs proies et évoluer avec brio dans un terrain de chasse numérique à la réalité toujours plus complexe. Les éditeurs et les équipes de cybersécurité auront constamment de nouveaux défis à relever en utilisant le renseignement, l'automatisation, le machine learning et des systèmes d'analyses de menaces de plus en plus performants.

08 GLOSSAIRE ET PRÉCISIONS TECHNIQUES

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

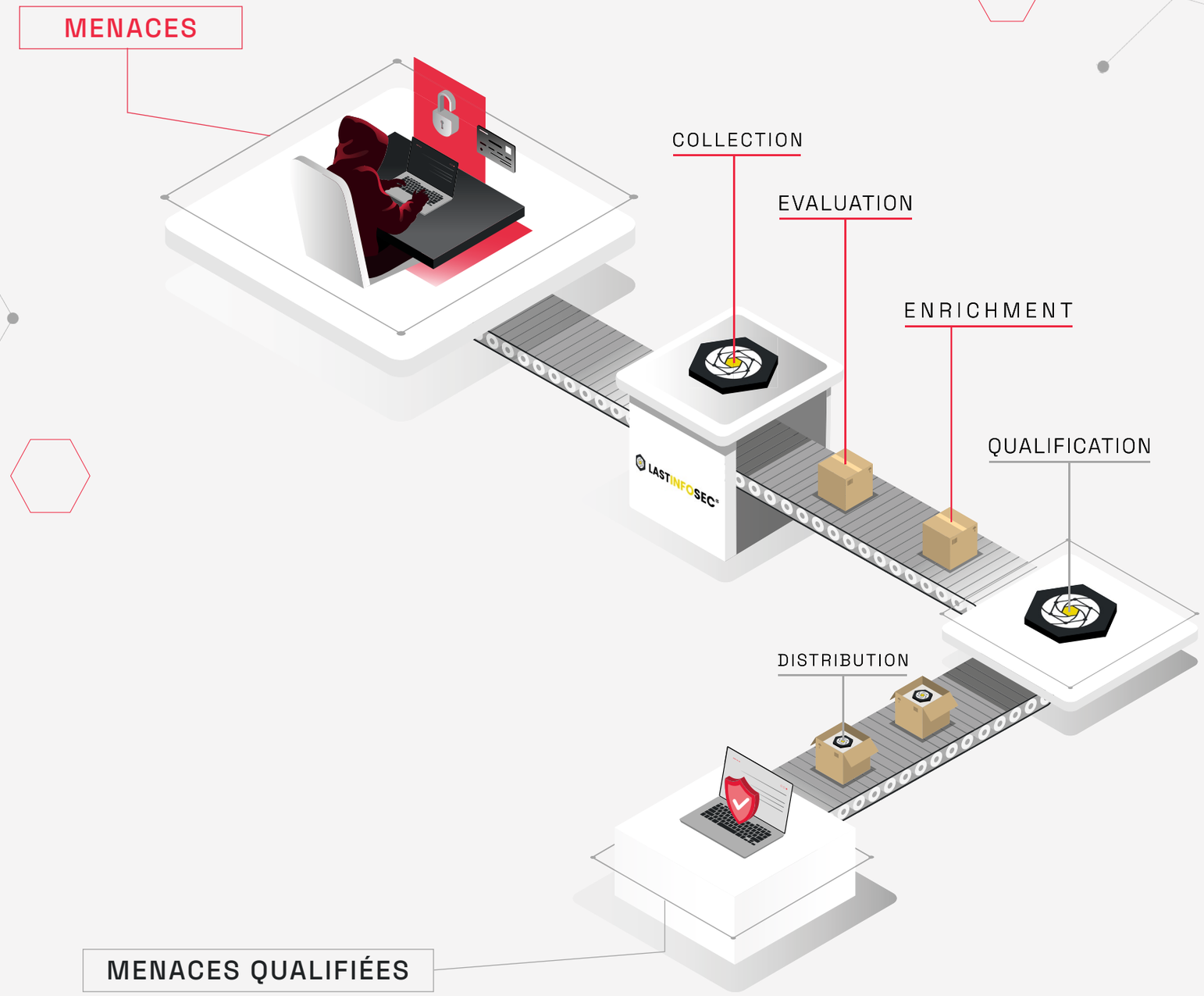
LastInfoSec® est notre plateforme de Cyber Threat Intelligence (CTI) visant à faciliter la détection des menaces internes et externes susceptibles de cibler le système d'information et de suivre les nouvelles techniques, vulnérabilités, outils, utilisés par les attaquants.

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
- → Des rapports sur les vulnérabilités

L'intégration de LastInfoSec® se fait simplement et rapidement grâce à des exports standardisés aux dernières normes CTI (Stix v2, Stix v2.1, TAXII..) et à des connecteurs intégrés disponibles pour les principaux outils d'analyse du marché (TIP, SIEM, SOAR...).



6000

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

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.

Toutes les menaces évoquées dans ce rapport sont en mesure d'être détectées par une solution NDR comme AIONIQ.

AIONIQ®

Grace à une cartographie dynamique de l'intégralité des assets présents sur le SI, AIONIQ peut identifier avec certitude les actions malveillantes et les comportements suspects non couverts par les autres outils de détection. Ses performances inédites d'analyse des flux réseau, même chiffrés, permet une modélisation à 360° du niveau de risque cyber associé à chaque connexion entre assets et utilisateurs, pour un niveau augmenté de détection et de visibilité.
.

SOURCES

[1] Attack Mitre

[2] Édito du CyberThreats Barometer Mars 2022

[3] Édito du CyberThreats Barometer Décembre 2022

[4] Édito du CyberThreats Barometer Juin 2022

[5] Article Malware As a Service Emotet

[6] Édito du CyberThreats Barometer Janvier 2023

[7] Article IT threat evolution in Q3 2022

[8] Article Is WannaCry Still a Threat ?

[9] Article Emotet Returns With New Methods of Evasion

[10] Internet Crime Report 2021

[11] Article Recent findings from CCleaner APT investigation

[12] Bulletin d'alerte du CERT-FR

[13] APT 41 GROUP

[14] APT41 a dual espionage and cyber crime operation

[15] Article Hackers linked to Chinese government