aDvens

Security for the greater good

Renseignement sur les menaces

Bulletin mensuel juillet 2022

CERT ADVENS

29/07/2022 - TLP WHITE

Sommaire

1 Synthèse

Le mois de juillet a été marqué par une recrudescence de campagnes de vol de données, avec l'emploi du maliciel **Agent Tesla,** appartenant à la famille des *infostealer*,

L'activité des rançongiciels n'est pas en reste avec l'utilisation des implants **Lockbit**, **Conti** et **Pysa**.

Comme le mois dernier, la vulnérabilité Log4j (**CVE-2021-4428**) est la plus exploitée. Toutefois, des failles datant de 2012 et 2017, sont aussi utilisées dans des campagnes d'attaques récentes.

Fin juin, des chercheurs en sécurité ont révélé l'existence de la porte dérobée **ZuoRAT**. Cette dernière serait une adaptation du maliciel Mirai, et ciblerait des routeurs de constructeurs spécifiques.

Les équipes de sécurité de Microsoft, alertent sur les activités d'un nouveau groupe de menace avancée nord-coréen se faisant appeler **H0lyGh0st**. Il pratique la double extorsion et vise principalement des petites et moyennes entreprises, dans divers pays et secteurs d'activités.

Les cyberattaquants exploitent quotidiennement des failles de logiciels pour compromettre des systèmes d'information. Toutefois, la principale vulnérabilité qu'utilisent les attaquants est le *facteur humain*, via l'ingénierie sociale sous toutes ses formes.

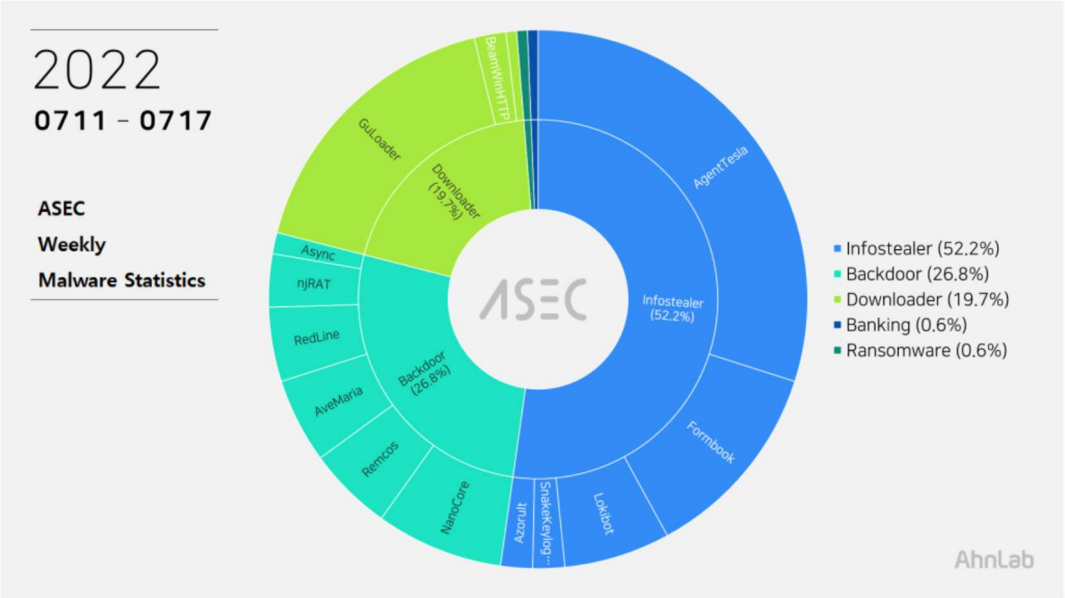
2 Top des logiciels malveillants

2.1 Situation

Pour ce mois-ci, le TOP 3 des logiciels malveillants sont :

- Agent Tesla spécialisé dans le vol de données.
- La porte dérobée Nanocore.
- Le téléchargeur GuLoader.

Les attaques impliquant des chevaux de Troie et des rançongiciels représenteraient moins de deux pourcents des activités malveillantes.



Le TOP des logiciels malveillants utilisés au mois de juillet.

2.1.1 Agent Tesla

Agent Tesla est un logiciel malveillant de type RAT (Remote Adminsitration Tool) découvert en 2004. Ce cheval de Troie est spécialisé dans le vol de données sur le poste du travail de la victime. Il récupère, entre autres, les identifiants et mots de passe stockés par les navigateurs Web et les logiciels de messagerie.

Agent Tesla est aussi définit comme MaaS (Malware-as-a-Service). Il est commercialisé sur le marché noir et peut être utilisé pour déployer d'autres logiciels malveillants.

2.1.2 GuLoader

Connue dans le passé en tant que **CloudEye**, ce logiciel malveillant est désormais appelé **GuLoader**, en raison de l'adresse URL Google Drive qui est souvent utilisé par les attaquants.

GuLoader est considéré comme un MaaS (Malware-as-a-Service). Au cours de l'année 2021, des attaquants l'ont utilisé pour déployer le logiciel légitime de cybersécurité Remcos pour voler des données.

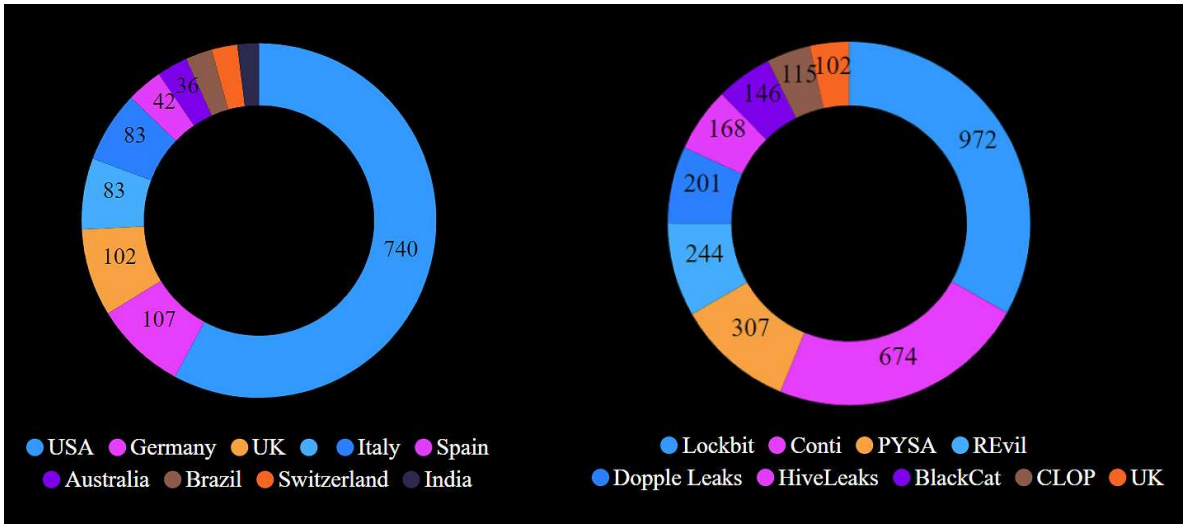
2.1.3 NanoCore

Découvert en 2013, **NanoCore** est un logiciel malveillant de type RAT (Remote Adminsitration Tool) spécialisé dans le vol de données. Ce malware peut permettre aux attaquants d'installer une porte dérobée sur le poste de travail de la victime afin de s'octroyer un accès. Développé en *.Net*, **NanoCore** est commercialisé sur le marché noir et peut être personnalisable via plusieurs plug-ins.

Son auteur, Taylor Huddleson (alias Aeonhacks) a été arrêté par le FBI en début de l'année 2017.

2.2 Ransomware

La volumétrie des attaques par rançongiciels du mois de juillet montre que les États-Unis sont la principale cible des groupes cybercriminels. Les trois rançongiciel les plus virulents sont **Lockbit**, **Conti** et **PYSA**.



À gauche, les pays impactés par les attaques de type rançongiciel. À droite, les groupes d'attaquants les plus actifs.

3 CVE

3.1 Les 10 vulnérabilités les plus actives

3.1.1 Classement

Comme le mois dernier, la CVE-2021-4428 log4j est la vulnérabilité la plus utilisée dans les campagnes d'attaques. A noter que des failles connues et corrigées depuis plusieurs années, sont exploitées massivement. Ce constat démontre l'importance de maintenir à jour la pile logicielle des systèmes d'information.

Classement des 10 vulnérabilités les plus actives selon Mandiant.

3.1.2 CVE-2021-44228

Découverte par l'équipe *Cloud Security Team*. Il s'agit d'une vulnérabilité critique au sein de la bibliothèque log4j, aussi connue sous le nom log4shell.

La faille provient de l'absence de contrôle des commandes reçues par l'interface de programmation (API) JNDI.

Un attaquant infecte le serveur Apache de la victime, via une requête qui contient une adresse d'un serveur LDAP. Cette requête est interprétée par le serveur de la victime qui télécharge l'implant malveillant.

D'après l'entreprise de Cybersécurité *Tenable*, cette vulnérabilité est « la plus importante et la plus critique de tous les temps »

Apache a sorti un correctif. La meilleure manière de se protéger est de mettre à jour Apache Log4j vers la version 2.3.1 (pour Java 6), 2.12.3 (pour Java 7), 2.17.0 (pour Java 8 ou plus) ou une version supérieure. Une autre possibilité est de supprimer la classe JndiLookup. Voir ici pour plus d'informations.

3.1.3 CVE-2017-0199

Il s'agit d'une vulnérabilité critique qui affecte Microsoft Office et WordPad. Cette vulnérabilité est exploitée durant des campagnes d'hameçonnage par différents groupes. Ainsi, lors de la campagne de début d'année, **SnatchCrypto**, l'attaque menée par le groupe APT **BlueNoroff**, un groupe présumé Nord-Coréen, avait pour but de récupérer des comptes de cryptomonnaie.

La faille vient de l'absence de contrôle des liens OLE2 par l'exécutable winword.exe.

Un attaquant créé un document Word exploitant cette faille, qu'il envoie à sa victime. À l'ouverture de ce document, des fichiers HTA malveillants sont téléchargés puis exécutés.

Microsoft a publié un correctif le 11 avril 2017. Pour se protéger, il faut mettre à jour Microsoft Office. Plus d'informations ici.

3.1.4 CVE-2022-26134

Il s'agit d'une zéro-day critique découverte en mai qui affecte des serveurs Atlassian. Plusieurs groupes ont exploité cette vulnérabilité en juin. Le **groupe 8220 Gang**, qui a compromis plus de 30 000 serveurs depuis 2017, a adapté leur Botnet pour utiliser cette vulnérabilité afin d'installer le logiciel de cryptominage, **PwnRig**. Les chercheurs en sécurité de la société Rapid7 ont aussi découvert un site russe qui vendait l'accès à 50 réseaux, aux États-Unis, compromis grâce à cette vulnérabilité.

La faille provient d'une erreur de contrôle des expressions du langage Objet Graph Navigation Language (OGNL) dans Apache Struts. Apache Struts est un framework Java couramment utilisé pour développer des applications web.

Un attaquant infecte le serveur de la victime, via une requête forgée. Cette requête est interprétée par le serveur de la victime, provoque une injection OGNL et permet une exécution de code sur le système.

Atlassian a sorti un correctif le 3 juin. La meilleure manière de se protéger est de mettre à jour ses serveurs. Si une mise à jour n'est pas possible, il existe des méthodes de contournement, décrites ici.

3.1.5 CVE-2012-0158

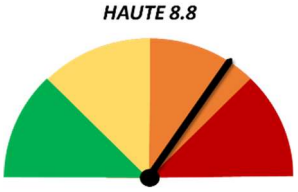
Il s'agit d'une vulnérabilité critique qui affecte plusieurs produits Microsoft. Cette vulnérabilité a maintenant 10 ans, mais reste très exploitée.

La faille est de type Buffer Overflow dans le module MSCOMCTL.OCX de ActiveX Control, qui gère plusieurs commandes Windows.

Un attaquant va mener des campagnes d'hameçonnage afin d'encourager ses victimes à visiter un site malveillant. Ce site web va renvoyer un paramètre exploitant la faille qui corrompra la mémoire du système et permettra une exécution de code sur celui-ci.

Microsoft a sorti un correctif en 2012. Pour se protéger, il faut appliquer les mises à jour Microsoft décrites ici.

3.1.6 CVE-2021-40444



Il s'agit d'une vulnérabilité critique qui affecte Microsoft Windows. Cette vulnérabilité est très similaire à la faille Follina.

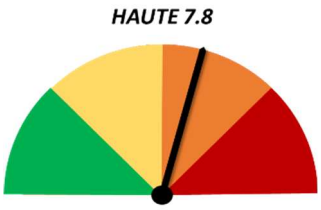
À la fin de l'année dernière, plusieurs entreprises gouvernementales en Asie occidentale et en Europe de l'Est ont été visées par une campagne de vol d'informations. Les entreprises ont reçu des documents sur la thématique de la finance, exploitant cette vulnérabilité afin d'installer le Malware Graphite. Le groupe Trellix soupçonne le **groupe russe APT28**, aussi connu sous le nom **Fancy Bear** ou **Sofacy**, de mener ces attaques.

La faille provient d'un mauvais contrôle de paramètres ActiveX Control par MSHTML.

Un attaquant créé un document Word exploitant cette faille, qu'il envoie à sa victime. Lorsque celle-ci ouvre ce document, même en mode protégé, du code JavaScript est exécuté par Internet Explorer afin de créer un fichier contrôle ActiveX malveillant qui sera utilisé pour infecter le système.

Microsoft a sorti un correctif le 14 septembre 2021. La meilleure manière de se protéger est de mettre à jour ses serveurs. Si une mise à jour n'est pas possible, Microsoft recommande de désactiver ActiveX. Plus d'informations ici.

3.1.7 CVE-2017-11882



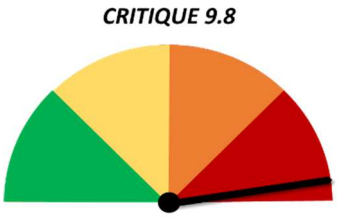
Il s'agit d'une vulnérabilité qui affecte les produits Microsoft Office. Cette vulnérabilité est utilisée dans des campagnes d'hameçonnage et a permis d'installer presque un cinquième des Malwares Emotet.

La faille est de type Buffer Overflow dans le module Microsoft Equation Editor.

Un attaquant créé un document Word exploitant cette faille, qu'il envoie à sa victime. Lorsque celle-ci ouvre ce document, les paramètres du fichier corrompent la mémoire du système et permettent une exécution de code sur celui-ci.

Microsoft a sorti un correctif le 14 novembre 2017. Pour se protéger, il faut mettre à jour Microsoft Office. Plus d'informations ici.

3.1.8 CVE-2022-22963



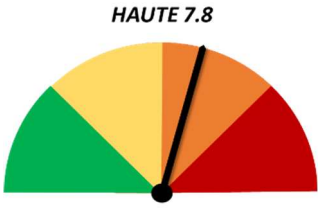
Il s'agit d'une vulnérabilité critique qui affecte Spring Cloud Function, qui est utilisé par certaines applications web Java. Cette vulnérabilité est une zero-day découverte fin mars 2022. Elle est souvent utilisée avec la vulnérabilité CVE-2022-22965 afin d'obtenir un premier accès à un serveur.

La faille provient de l'absence de contrôle des paramètres envoyés par l'utilisateur dans une expression du langage de programmation de Spring (SpEL).

Un attaquant infecte le serveur de la victime, via une requête forgée. Cette requête est interprétée par le serveur de la victime qui télécharge l'implant malveillant.

Des correctifs ont été apportés à cette vulnérabilité. Pour se protéger, il faut mettre à jour Spring Cloud Functions vers la version 3.1.7 ou 3.2.3 ou une version supérieure. Pour plus d'informations, voir ici. Pour des informations sur les produits IBM affectés et le correctif, voir ici. Pour des informations sur les produits Oracle, voir ici.

3.1.9 CVE-2017-8759



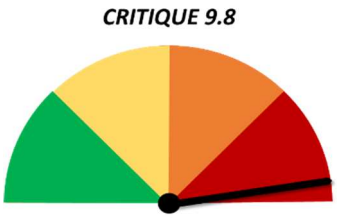
Il s'agit d'une vulnérabilité qui affecte les produits Microsoft utilisant le framework .NET. Cette vulnérabilité est utilisée dans des campagnes d'hameçonnage.

La faille provient d'une erreur dans la vérification d'une URL par le module WSDL. Ceci permet à un attaquant d'injecter du code.

Un attaquant créé un document Word exploitant cette faille, qu'il envoie à sa victime. Lorsque celle-ci ouvre ce document, le code injecté est lancé par l'exécutable osc.exe.

Microsoft a sorti un correctif le 12 septembre 2017. Pour se protéger, il faut mettre à jour ses serveurs. Plus d'informations ici.

3.1.10 CVE-2022-22965



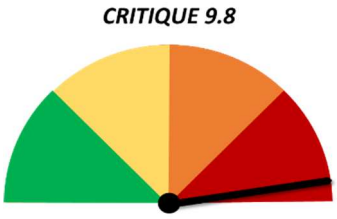
Il s'agit d'une vulnérabilité critique, aussi appelée Spring4Shell ou SpringShell, qui affecte certaines applications Java utilisant Spring Core. Cette vulnérabilité est utilisée pour installer le malware **Mirai** depuis début avril.

La faille provient d'un mauvais contrôle des objets PropertyDescriptor reçus par l'application Spring Java.

Un attaquant infecte le serveur de la victime, via une requête forgée. Cette requête est interprétée par le serveur de la victime qui télécharge l'implant malveillant.

Vmware a publié un correctif. La meilleure manière de se protéger est de mettre à jour le framework Spring vers la version 5.3.18 ou 5.2.20 ou une version supérieure. Une autre possibilité est de mettre à jour le service Tomcat, qui participe à l'attaque, ou de repasser à Java 8. Plus d'informations ici.

3.1.11CVE-2018-11776



Il s'agit d'une vulnérabilité critique qui affecte le framework Apache Struts.

La faille provient d'une mauvaise vérification de champs remplis côté utilisateur qui peut entrainer l'exécution d'une expression OGNL (Object-Graph Navigation Language).

Un attaquant infecte le serveur de la victime, via une requête forgée. Cette requête est interprétée par le serveur, ce qui permet une exécution du code de l'attaquant.

Apache a mis à disposition un correctif. La meilleure manière de se protéger est de mettre à jour Apache Struts vers la version 2.3.35 ou 2.5.17 ou une version supérieure. Voir ici pour plus d'informations et un correctif proposé par Apache.

4 Mirai : la menace Katana et Zuorat

4.1 Avant-propos

Eté 2016, le maliciel Mirai émerge sur la toile, en menant des attaques par déni de service distribué (DDoS). Ces attaques d'envergure s'articulent autour d'un maillage de machines esclaves, appelé botnet. Ce botnet enrôle de nombreux terminaux compromis, des bots, contrôlés à distance par un botmaster.

Le botnet Mirai a été découvert par des hackers éthiques du groupe Malwaremustdie ; un collectif désireux de protéger le bon fonctionnement d'internet contre les logiciels malveillants.

Dès son apparition, Mirai a été le sujet d'une longue enquête menée par le journaliste Brian Krebs, pour connaître l'identité du botmaster. Cette investigation a permis de découvrir qu'un universitaire Jah Paras, réputé pour ses compétences, supervisait cette infrastructure.

Depuis 2016, le maliciel Mirai continue de faire écho dans le cyberespace avec l'apparition de nouveaux variants comme Katana et ZuoRAT. La menace demeure sérieuse et actuelle.

4.2 Mirai – L'essentiel

4.2.1 Lexique

Bot : logiciel qui interagit avec des serveurs sur Internet pour réaliser des tâches automatisées.

Botnet : réseau de machines esclaves, aussi appelé « zombies army ».

Botmaster : superviseur du réseau botnet.

Zombie : terme souvent employé pour décrire Mirai.

4.2.2 Fonctionnement

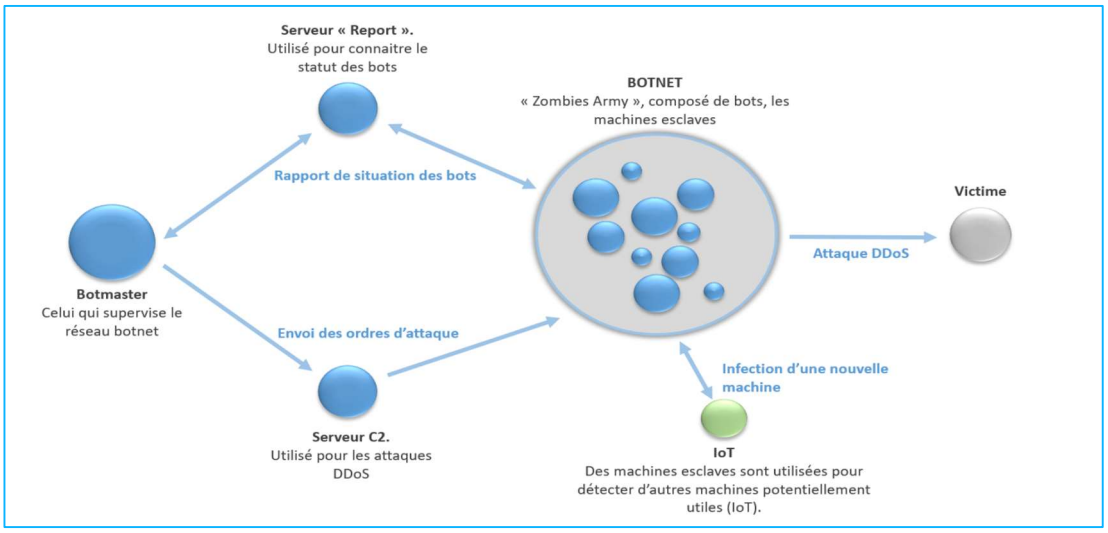
4.2.2.1 Phase par phase

Les attaquants procèdent à une phase de reconnaissance pour lister les cibles de leur campagne. Ces cibles correspondent à des adresses IP publiques affectées à des objets connectés (Internet of Things, IOT). **Les terminaux appartenant à l'United-State Portal Service et au ministère de la défense des États-Unis sont exclus du périmètre de recherche par les attaquants**.

Sur la base de ces listes, les opérateurs de Mirai tentent d'accéder aux IOT en utilisant des dictionnaires qui contiennent des couples d'identifiant et de mots de passe. Si la connexion aboutit, le maliciel est installé. De facto, l'objet connecté est enrôlé comme un bot.

Malgré sa compromission, l'objet connecté fonctionne normalement, tout en présentant une sensible augmentation de sa bande passante et parfois, un ralentissement de ses performances.

Le bot communique, à minima, avec trois serveurs. Le premier, « Report Server », permet au botmaster de connaître le statut des terminaux de son botnet. Le second, « C&C server » est contrôlé par l'attaquant pour mener ses campagnes de DDOS. Le dernier serveur « Loader Server » fait office de dépôt de maliciels.



Fonctionnement du botnet Mirai.

4.2.2.2Infection

Mirai n'a pas de mécanisme de persistance. Dès lors qu'un terminal compromis est redémarré, le processus d'infection doit être réitéré pour l'enrôler dans le botnet. Une procédure réalisable uniquement si le mot de passe n'a pas été modifié.

4.2.2.3Mots de passe

Ci-dessous, la liste des identifiants et mots de passe utilisés par Mirai pour se connecter à une cible. Son contenu révèle la vulnérabilité des objets connectés : la simplicité des mots de passe aisément exploitables par un attaquant. L'utilisation de cette liste a permis l'infection de plusieurs millions d'objets.

[Recommandation] Le changement des mots de passe par défaut et l'emploi de mots de passe complexes participent à la sécurisation de votre environnement numérique.

Identifiant	Mot de passe	Identifiant	Mot de passe	Identifiant	Mot de passe
666666	666666	guest	guest	root	jvbzd
888888	888888	mother	fucker	root	klv123
admin	(vide)	root	(vide)	root	klv1234
admin	1111	root	00000000	root	pass
admin	1111111	root	1111	root	password
admin	1234	root	1234	root	realtek
admin	12345	root	12345	root	root
admin	123456	root	123456	root	system
admin	54321	root	54321	root	user

admin	7ujMko0admin	root	666666	root	vizxv
admin	admin	root	7ujMko0admin	root	xc3511
admin	admin1234	root	7ujMko0vizxv	root	xmhdipc
admin	meinsm	root	888888	root	zlxx.
admin	pass	root	admin	root	Zte521
admin	password	root	anko	service	service
admin	smcadmin	root	default	supervisor	supervisor
admin1	password	root	dreambox	support	support
administrator	1234	root	hi3518	tech	tech
Administrator	admin	root	ikwb	ubnt	ubnt
guest	12345	root	juantech	user	user

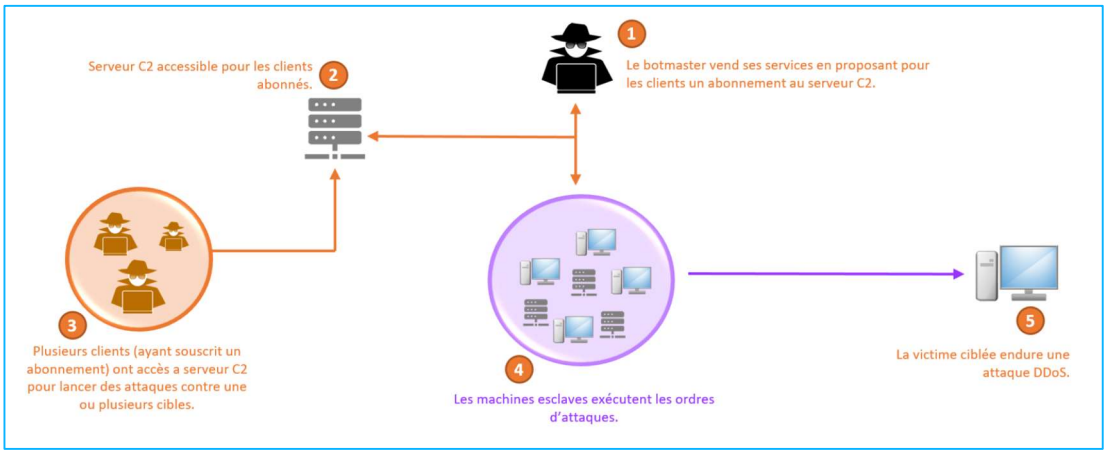
4.2.3 Commercialisation

4.2.3.1 Botnet-as-a-Service

Un article publié le 17 novembre 2016 sur le site Silicon révèle qu'un client mécontent envers Playsation Network aurait loué les services du botnet Mirai pour mener une offensive de type DDoS.

Selon Dale Drew, responsable de la sécurité de Level 3 Communication, l'attaquant aurait simplement « loué un botnet Mirai pour mener à bien son offensive », et aurait réussi à accéder à un réseau de 150 000 objets connectés zombies.

L'illustration suivante décrit le fonctionnement du Botnet-as-a-Service, selon Level 3. Un client peut louer une portion du réseau de machines esclaves. En s'abonnant au service, le client obtient un accès à une interface du serveur C2, sur laquelle il précise la cible ainsi que la durée et l'intensité de l'attaque.



Utilisation de Mirai : pas exclusive à son créateur mais commercialisée.

Depuis la commercialisation du premier botnet Mirai, le principe persiste au travers de nouveaux variants du logiciel malveillant. Par ailleurs, le Botnet-as-a-Service peut mener à des rivalités entre pirates maitrisant les différents variants de Mirai.

C'est le cas du hacker **Scarface#1162**. Pour son propre commerce, ce pirate informatique aurait détourné le botnet **Akiru** (variant de Mirai découvert en 2018, dominé pendant un certain temps par le hacker **Wicked**) afin de l'utiliser avec d'autres variants. Ci-dessous, le Botnet-as-a-Service présenté par Scarface#1162 sur un site Web dissimulé :

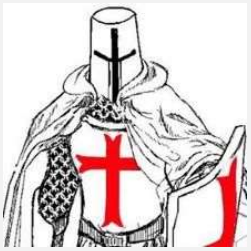
Un cas de Botnet-as-a-Service basé sur des variants de Mirai. Un héritage agressif où les pirates ne semblent nullement hésiter à voler les machines esclaves d'un autre pirate.

4.3 Mirai - Découverte et investigation

4.3.1 Découverte

Mirai a été découvert au mois d'aout 2016, par des hackers éthiques (White Hat) appartenant au groupe **Malwaremustdie (MMD)**. Crée en 2012, Malwaremustdie est une organisation à but non-lucratif, ayant pour objectif principal l'étude et la recherche de logiciels malveillants, afin de protéger Internet. L'organisation est notamment réputée pour son aide significative au démantèlement d'infrastructures cybercriminelles. Le groupe compte moins de 100 membres et possède 4 quartiers généraux localisés en France, Allemagne, aux États-Unis et au Japon.

Le **botnet Mirai** a été découvert par **Malwaremustdie** : un groupe d'Hackers éthiques essentiellement dévoué à la protection d'Internet. Ils sont artistiquement représentés par ce dessin : un chevalier templier.



4.3.2 L'enquête de Brian Krebs

Un mois après la découvre du botnet Mirai par Malwaremustdie, son code source est mis en ligne, le 30 septembre 2016, par un individu ayant pour pseudonyme **Anna-Senpai** (nom d'un personnage d'un dessin animé japonais, Mirai Nikki).

Selon une investigation menée par le journaliste américain spécialiste en cybersécurité, Brian Krebs, trois années ont été nécessaires pour développer le logiciel malveillant. Au cours de son développement, le botnet aurait eu plusieurs noms : **Bashlite**, **Gafgyt**, **Qbot**, **Remaiten** et **Torlus**.

En juin 2014, la société ProxyPipe, chargée de protéger les serveurs du jeu vidéo Minecraft, est victime d'une attaque DDoS de 300 Gbits/S. Le journaliste révèle que le dirigeant de la société, Roberto Coehlo, a fait l'objet de menace par un certain Christopher « CJ » Sculti Jr.

Sculti Jr est propriétaire d'une société de protection contre le DDOS, dont les serveurs sont hébergés chez Protaf Solutions. Lors d'un entretien avec le journaliste, il se serait vanté d'avoir scanné l'internet, et découvert une immensité d'objets connectés vulnérables.

« (…) il se vantait d'avoir scanné le web et avoir découvert de nombreux objets connectés vulnérables. Pour Roberto Coehlo, il ne fait aucun doute que Sculti et ProTraf Solutions étaient les principaux membres de l'organisation Lelddos. » Silicon.fr (2021)

En investiguant sur ProTraf Solution, Brian Krebs découvre qu'un des employés est le développeur des deux botnets IOT Bashlite et Qbot. Il s'agit de Josiah White alias LiteSpeed. Le journaliste apprend du créateur des deux botnets, qu'il a dû fournir les codes sources, suite aux menaces d'un cybercriminel connu sous le pseudonyme « **Vypor** ».

Autre élément intéressant, Brian Kerbs constate que le profil LinkedIn du président de la société, Jha Paras, est étrangement similaire à celui d'Anna-Senpai sur le forum HackForums.

Un autre employé de ProTraf Solution, Ammar Zuberi, confirmera au journaliste que Jha Paras est le développeur du maliciel Mirai.

Profil LinkedIn de Paras Jah.

Jha Paras a été le principal développeur du botnet Mirai.

Deux autres cybercriminels ont contribué au développement et à la commercialisation du botnet : **Josiah White** et **Dalton Norman**.

4.4 Mirai - Variant Katana

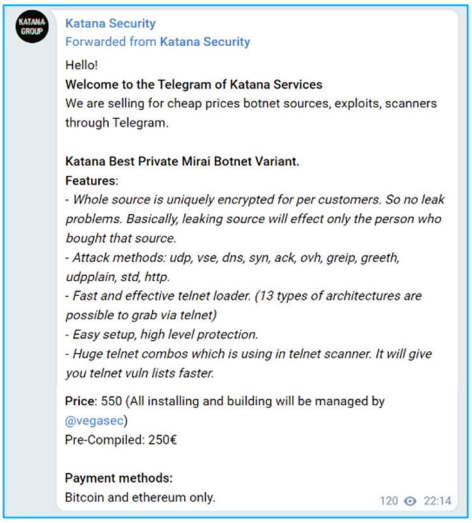
4.4.1 Un sabre virtuel

4.4.1.1 Découverte

Le 27 octobre 2020, Avira Protection Labs publie un article au sujet d'un nouveau botnet baptisé **Katana**. L'analyse de ce maliciel démontre l'emploi du code source de Mirai, avec l'ensemble des fonctionnalités de base agrémenter de nouvelles fonctions. Dont une, **attack_udp_ovhhex**, a été développée spécifiquement pour cibler les serveurs hébergés par l'entreprise française OVH.

« Bien que le botnet Katana soit en cours de développement, il s'appuie déjà sur des modules permettant des attaques DDoS de la couche 7, différentes clés de chiffrement pour chaque source, une autoréplication rapide et un C2 sécurisé. Des indices laissent à penser que Katana pourrait à l'avenir être associé à un botnet de banque en ligne HTTP. » - Avira 2020.

Jusqu'en juin 2022, Katana est commercialisé en tant que Botnet-as-a-Service pour un prix de 550$. Ci-dessous, un exemple d'annonce présentée à plusieurs reprises par le groupe opérant Katana sur leur compte Telegram.



Annonce Botnet-as-a-Service Katana.

Le 5 juillet 2021, le code source de Katana est publié sur Github par un utilisateur allemand surnommé saintly2k.

Capture d'écran du dépôt Github de Katana.

4.4.1.2 Cyberguerre

Deux ans après le développement de Katana, celui-ci a été utilisé massivement lors de l'invasion de l'Ukraine par la Russie à partir du mois de février 2022. Le 15 et 16 février, plusieurs sites internet ukrainiens ont subi des cyberattaques de type DDoS. Des sites gouvernementaux, bancaires, militaires et autres entités critiques ont été impactés.

Sur la base de diverses informations techniques, le conseil national de sécurité américain a accusé le 18 février, la direction générale des renseignements de l'État-Major des Forces armées de la Fédération de Russie (GRU) d'être le commanditaire de cette campagne d'attaque.

Les attaques DDoS à l'encontre de l'Ukraine seraient, selon le Conseil national de sécurité américain, orchestré par la direction générale des renseignements Russes : **le GRU**.

Les investigations menées par le CERT ukrainien, ainsi que 360NetLab et BadPackets confirment l'emploi du botnet Katana dans cette campagne de DDoS. Les analyses ont porté sur deux échantillons **KKveTTgaAAsecNNaaaa.mips** et **a2b1d5g2e5t8vc.elf**. Le 20 février 2022, le site Cadosecurity met à disposition les conclusions de ces investigations.

Ci-dessous, deux extraits des codes sources de Katana. Les noms des deux implants y sont retrouvés dans des variables.

Code source 1

```
exec_bin = "loudscream"
exec_name = "ssh.vegasec"
bin_prefix = "KKveTTgaAAsecNNaaaa."
bin_directory = "z0l1mxjm4mdl4jjfjf7sb2vdmv"
```

Code source 2

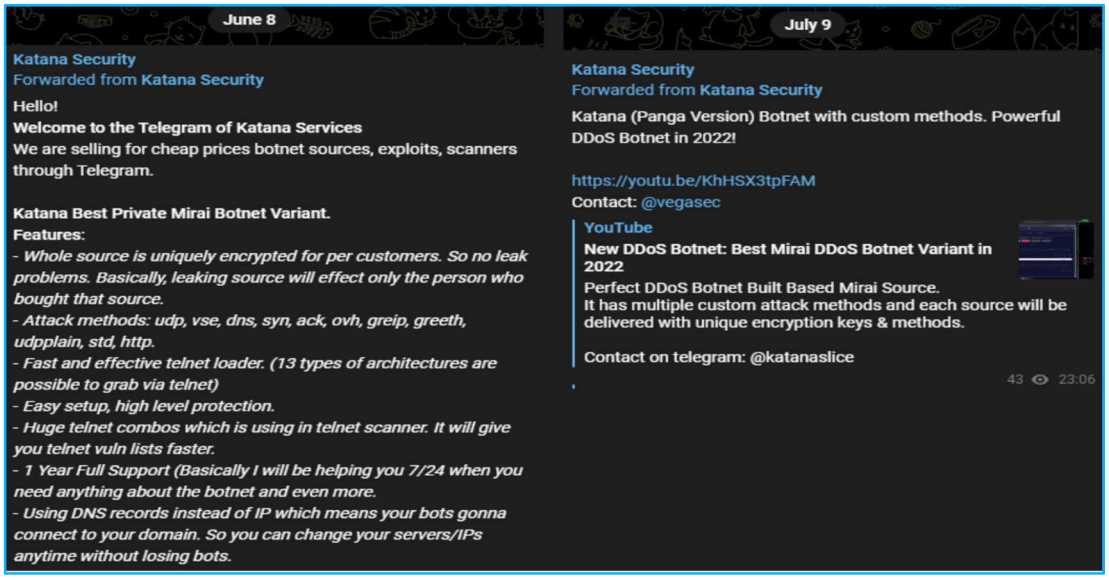
```
#define EXEC_QUERY "/bin/busybox VGA"
#define EXEC_RESPONSE "VGA: applet not found"
#define FN_DROPPER "z916"
#define FN_BINARY ".a2b1d5g2e5t8vc"
```

Suite à la cyberattaque à l'encontre de l'Ukraine, le ministre de la transformation digitale Mykhailo Fedorov a déclaré : *« Cette attaque a été sans précédent, elle fut préparée en avance et son objectif était la déstabilisation, de générer de la panique et le chaos dans le pays »,* Cadosecurity, le 20 février 2022.

4.4.1.3 Menace actuelle

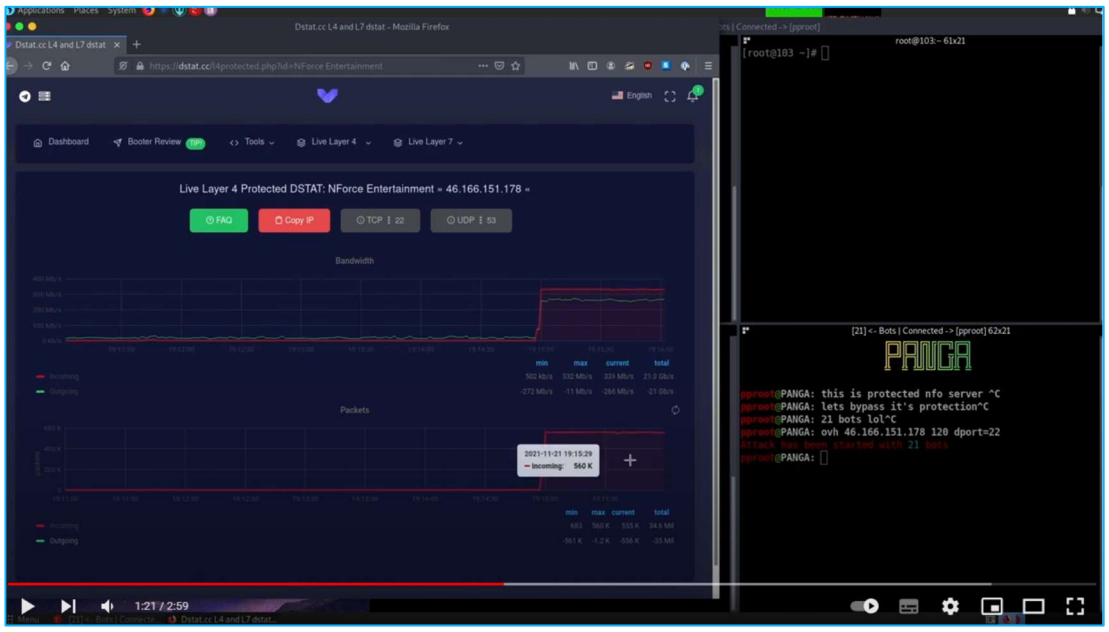
Le botnet Katana présente toujours une menace actuelle. Une investigation réalisée récemment par la CTI d'Advens montre que Katana est toujours commercialisée en tant que Botnet-as-a-Service (la dernière annonce date du 8 juin 2022) et qu'une autre version personnalisable est disponible.

Ci-dessous, à gauche, le 8 juin 2022 le logiciel Katana est toujours commercialisé en tant que Botnet-as-a-service. À droite, le 9 juillet 2022, les mêmes auteurs proposent aussi une version « **Panga Version** » de Katana, celle-ci serait personnalisable pour le client.



Capture d'écran du Telegram des auteurs de Katana.

Ci-dessous, une preuve de concept (POC), datant du 7 juillet : une vidéo révèle l'évolution de Katana (Panga Version).



4.5 Mirai - Variant ZuoRAT

4.5.1 Un cheval de Troie

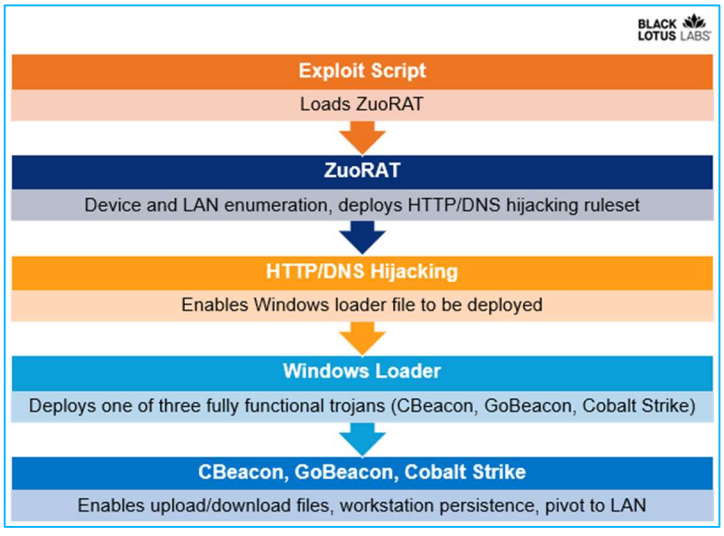
4.5.1.1 Découverte

Le 29 juin 2022, le laboratoire Black Lotus Lab a révélé l'existence d'un logiciel malveillant baptisé ZuoRAT. Selon les experts, ce logiciel serait un cheval de Troie qui permettrait de prendre le contrôle total des postes de travail dotés des systèmes d'exploitation Windows, MacOS et Linux. Les attaquants opérant ZuoRAT cibleraient essentiellement les routeurs développés par les entreprises ASUS, Cisco, DrayTek, er NETGEAR.

ZuoRAT aurait émergé au cours du mois d'octobre 2020 et serait passé inaperçu durant deux années consécutives. Son code serait une version très modifiée de Mirai : « *Le malware est une variante fortement modifiée de Mirai, un implant de type botnet pour les routeurs et autres appareils IOT qui est apparue à l'origine en 2016* » - L'entrepreneur, le 15 juillet 2022.

4.5.1.2 Infection

L'attaque de ZuoRAT peut être divisée en cinq étapes. Ci-dessous, les étapes selon le laboratoire Black Lotus Lab :



Récapitulatif des principales étapes de l'attaque ZuoRAT.

Un fichier exécutable portable Windows compilé en python est d'abord utilisé pour exploiter deux vulnérabilités : la CVE-2020-26878 et la CVE-2020-26879. L'objectif de cette première étape est de permettre l'installation du cheval de Troie. Lorsque l'installation de ZuoRAT est accomplie, celui-ci commence à énumérer les équipements connectés aux routeurs. L'attaquant peut, via la porte dérobée, réaliser à distance un détournement http et/ou DNS dont l'objectif et permettre l'installation d'autres maliciels. Les maliciels déployés sont CBeacon (cible le système Windows), GoBeacon (cible Linux et MacOS) et Cobalt Strike (outil de post-exploitation). In fine, les attaquants

sont en mesure d'établir leur persistance, de télécharger d'autres fichiers malveillants, de récupérer des informations et de pivoter vers le réseau local.

4.5.1.3 Botnet ZuoRAT

Les attaquants ont d'abord utilisé un serveur privé virtuel pour initialiser le premier exploit. L'analyse mené par Black Lotus Lab révèle que ce premier serveur n'a hébergé rien de malveillant pour éviter tout soupçon.

De septembre à décembre 2021, les attaquants ont infecté plusieurs routeurs, situés à Taïwan, pour en faire des serveurs proxys, afin de dissimiler leurs activités malveillantes. Ces routeurs infectés sont utilisés comme intermédiaire entre le serveur C2 des attaquants et les postes de travail ciblés.

De plus, les attaquants ont périodiquement changé de routeurs par discrétion. A partir de décembre 2021 jusqu'à mars 2022, les routeurs compromis se situaient au Canada.

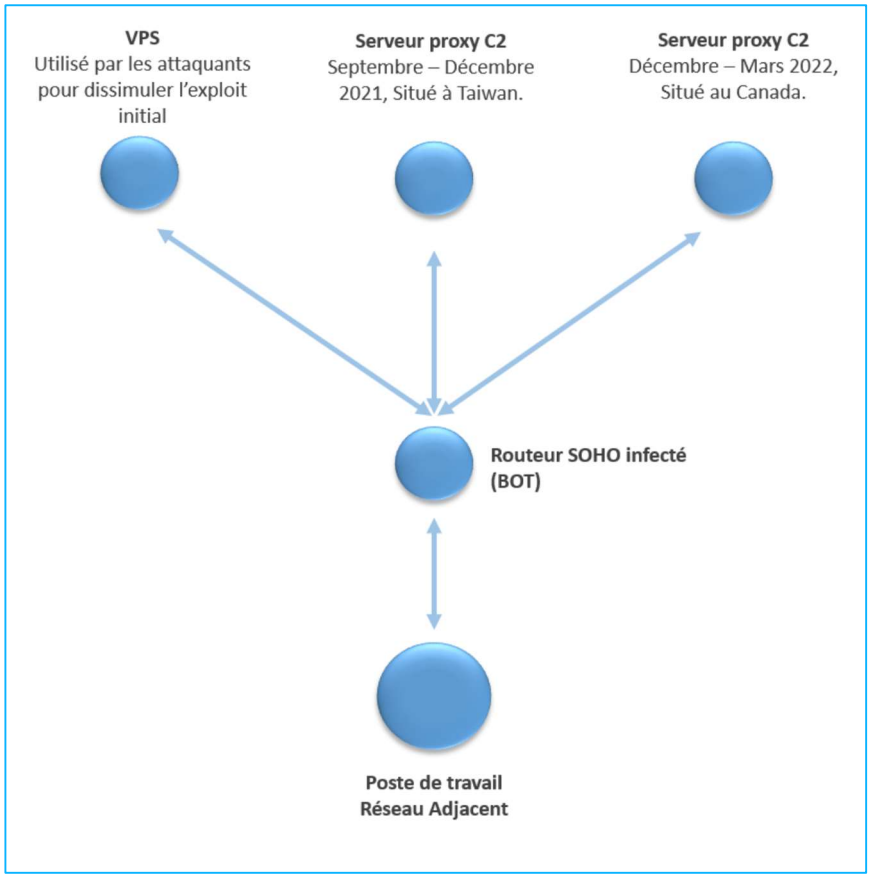


Illustration du botnet ZuoRAT. En plus du routeur infecté qui est transformé en bot, d'autres routeurs sont transformés en serveur proxy C2. Le botnet ZuoRAT est un véritable labyrinthe de routeurs infectés.

La véritable infrastructure C2 des attaquants serait peut-être Chinoise : *« L'identité du collectif adverse derrière la campagne reste inconnue, bien qu'une analyse des artéfacts ait révélé de*

possibles références à la province chinoise de Xiancheng et l'utilisation de Yuque et Tencent d'Alibaba pour le commandement et le contrôle (C2). » Techtribune, le 28 juin 2022.

4.5.1.4 Menace actuelle

La récente étude de Black lotus Lab a montré que la menace Mirai est toujours un sujet d'actualité. Depuis 2016, certains attaquants ont perfectionné leurs arsenaux, notamment en déployant de nouvelles tactiques et techniques pour dissimuler leurs activités malveillantes.

Tandis que les machines esclaves de Mirai ont essentiellement été utilisées pour générer un impact sur la cible, ZuoRAT a manifesté une pratique redoutablement plus efficace : en plus de l'impact, les machines esclaves sont aussi utilisées simultanément pour offusquer et confondre.

5 APT

5.1 H0lyGh0st : une nouvelle menace nord-coréenne

5.1.1 A propos

Dans son article du 14 juillet, l'équipe de sécurité Microsoft Threat Intelligence Center (MSCTIC) alerte sur les activités cybercriminelles d'un groupe d'origine nord-coréenne baptisé **DEV-0530**.

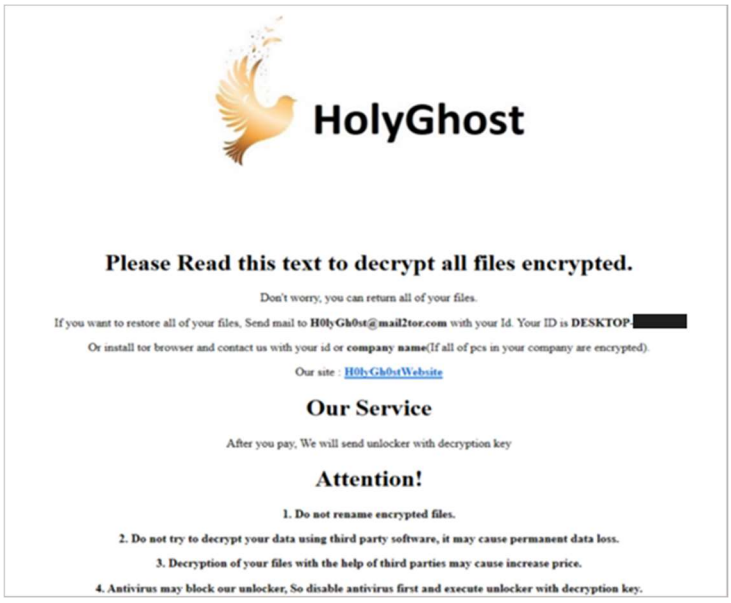
Ce groupe, se faisant appeler **H0lyGh0st**, agirait depuis juin 2021. Il ciblerait principalement des petites et moyennes entreprises, dans divers pays et secteurs d'activité (finance, éducation, industrie…).

5.1.2 Mode opératoire

Le mode opératoire des attaquants consiste à exploiter des vulnérabilités pour implanter leur ransomware du même nom, afin d'exfiltrer et de chiffrer les données de la victime. L'équipe de sécurité Microsoft a découvert l'emploi de la faille **CVE-2022-26352**, impactant le système de gestion de contenu DotCom. Cependant, le groupe cybercriminel n'aurait pas utilisé de zero-day pour mener leurs attaques.

Tout comme ses homologues, HolyGhost pratique la double extorsion en menaçant de divulguer les données en l'absence de paiement de la rançon. Cette dernière varie entre 1,2 et 5 bitcoins. L'attaquant accentue la pression sur la victime, en menaçant d'informer ses clients de la compromission.

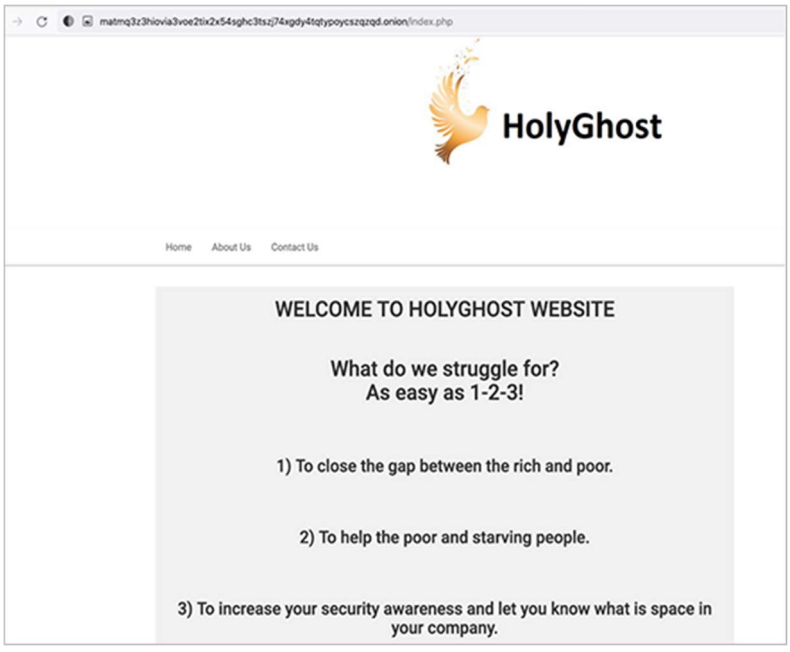
Un fichier intitulé « *FOR_DECRYPT.html*» est présent à la racine du lecteur C :, dans lequel est décrit les modalités d'échange avec l'opérateur du rançongiciel ainsi que le lien de son site hébergé sur le darkweb.



Contenu du fichier FOR_DECRYPT.html

Comme l'illustre l'mage suivante, les attaquants légitiment leurs actions pour des raisons vraisemblablement politiques, et non sans humour, afin de sensibiliser les victimes à la sécurité.

Aujourd'hui, le lien du site n'est plus fonctionnel.



Page principale du site du groupe d'attaquant

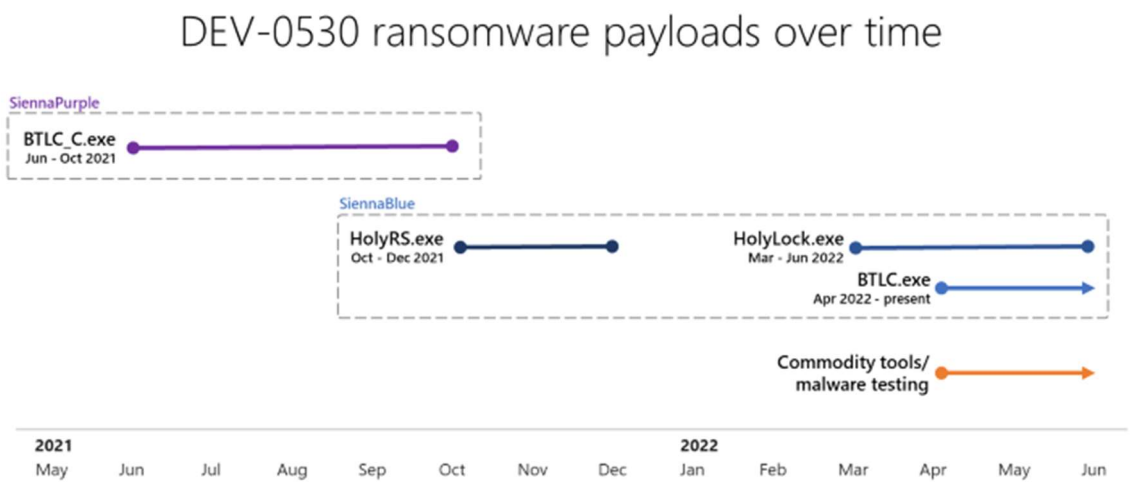
Pour mener ses attaques, H0lyGh0st a développé deux familles de maliciels « **SiennaPurple** » et « **SiennaBlue** ». La première catégorie comprend un seul binaire développé en C++, intitulé

BTLC_C.exe, qui offre des fonctionnalités limitées, nécessitant une exécution depuis un compte administrateur. Ce maliciel a été utilisé dès juin 2021.

Quant à la seconde famille, les trois implants (**H0lyRS.exe**, **HolyLock.exe** et **BTLC.exe**) sont développés en Go, proposant de nouveaux services, comme BTLC.exe, qui garantit la persistance du maliciel en créant (ou supprimant) une tâche planifiée portant le nom lockertask.

```
cmd.exe /Q /c schtasks /create /tn lockertask /tr [File] /sc minute /mo 1 /F /ru system
1> \\127.0.0.1\ADMIN$\__[randomnumber] 2>&1
```

A son exécution, l'implant initie une communication avec le serveur Commande et Contrôle (C2) pour échanger une clé publique afin de procéder au chiffrement des données sur le poste. Les fichiers chiffrés auront comme extension **.h0lyenc**.



Utilisation des implants malveillants depuis 2021

5.1.3 Lien avec d'autres groupes

Microsoft met en évidence l'emploi par H0lyGh0st, d'infrastructure, d'outils et de modes opératoires du groupe de menace avancée nord-coréen **PLUTONIUM**. Toutefois, la temporalité des activités malveillantes ainsi que la victimologie laissent à penser qu'il s'agit de deux groupes distincts.

6 Ingénierie sociale : tendances & évolution

Alors que la menace cyber évolue rapidement et que les outils pour la contrer se complexifient, les attaques par ingénierie sociale sont en hausse et les cybercriminels font preuve de toujours plus de patience et d'ingéniosité pour parvenir à leurs fins.

Selon le rapport 2022 de la compagnie Proofpoint, l'une des raisons de cette hausse semble être une réponse à l'amélioration générale des systèmes de défense cyber. Ces systèmes peuvent en effet être contournés si un seul des personnels travaillant dans l'organisation ciblée tombe dans le piège tendu par les attaquants.

6.1 Leviers & Tactiques

6.1.1 L'erreur humaine : la base

S'il est commun de penser que l'ingénierie sociale ne se limite souvent qu'aux mails de phishing, l'étude de Proofpoint indique que de nombreuses opérations de piratages menées en 2021 impliquaient des conversations étendues avec la mise en place de scénarii élaborés impliquant notamment des appels téléphoniques ou encore l'utilisation de plateformes de téléconférences. Cette analyse est d'ailleurs confirmée par des cas récents d'opérations allant du phishing classique à des opérations ciblées d'envergure :

En juillet 2022, un pirate a publié une archive de 4GB contenant des documents internes à la plateforme de jeux vidéo Roblox grâce à un incident lié à une attaque par phishing, ciblant l'un des employés de Roblox. Comme indiqué précédemment, l'opération peut être plus complexe. Ainsi, un ancien ingénieur de l'entreprise de jeu vidéo Sky Mavis a subi une opération d'hameçonnage élaborée en juin/juillet 2022. Une entreprise fictive l'a effectivement chassé et invité à de faux entretiens d'embauches avant de lui faire une offre alléchante, contenue dans un PDF piégé.

6.1.2 Autres facteurs humains

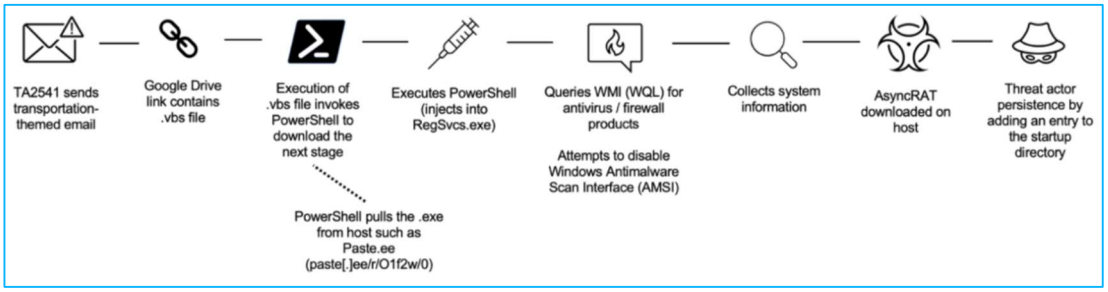
L'erreur humaine n'est pas le seul levier utilisé afin de permettre l'accès à des attaquants. Ce dernier peut également être volontairement donné par une personne en interne, persuadée grâce à un levier de manipulation (argent, peur, désir de vengeance, ego, etc.). Ainsi, quelque temps avant la dernière fuite de données exposée précédemment, Roblox avait déjà été victime d'une fuite de données causée par l'un de ses employés, qui aurait fourni l'accès initial aux attaquants après avoir été soudoyé. Une technique que souhaite utiliser également le groupe cybercriminel **Lapsus$** (pratiquant par ailleurs des opérations d'ingénierie sociale auprès de services d'assistance d'entreprises ciblées) qui publiait, début 2022, une annonce de recrutement pour toute personne travaillant dans de grandes entreprises technologiques désireuses de collaborer avec le groupe.

6.2 Affaires récentes

6.2.1 Marriott

La chaîne d'hôtellerie Marriott s'est fait dérobée en mai 2022, à Baltimore, entre 300 et 400 numéros de cartes de crédit avec leur CVV et dates d'expiration. Les pirates ont ciblé par téléphone un employé de l'hôtel et l'ont persuadé de leur accorder l'accès au réseau de l'établissement. L'intrusion a duré 6 heures et a permis aux attaquants d'exfiltrer 20 Go de données, parmi lesquelles des informations de paiement.

Bien que ces attaques puissent être le fruit d'attaquants d'un niveau technique ne leur permettant pas d'utiliser d'autre méthode, comme l'exploitation de vulnérabilité, un nombre croissant de groupes cybercriminels persistants utilisent également cette technique. Ainsi l'APT **TA2541**, spécialisée dans l'industrie de défense et l'aéronautique, utilise le phishing comme l'un de ses principaux vecteurs de compromission de systèmes.



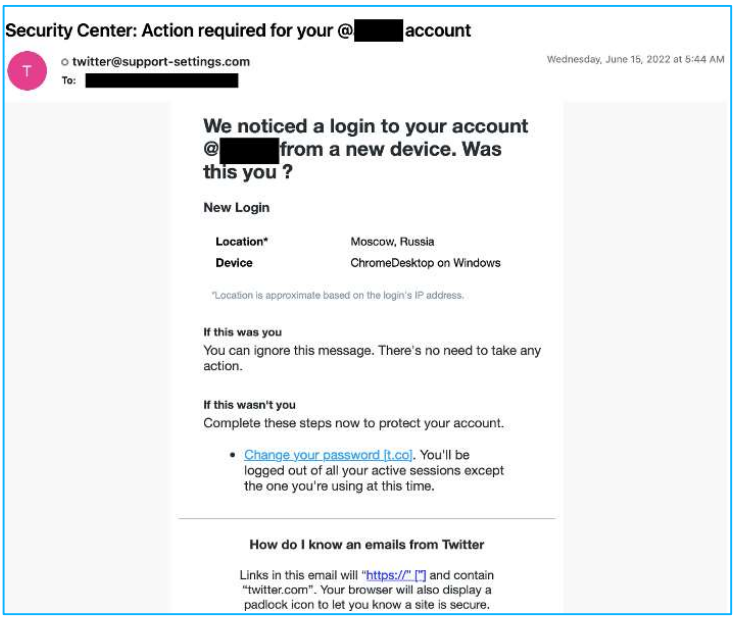
Chaîne d'attaque d'une opération de TA2541 - source : Proofpoint

6.2.2 Journalistes pour cibles

Selon le rapport de Proofpoint, les opérations d'ingénieries sociales ne sont pas seulement l'apanage de groupes privés opérant à des fins lucratives, mais sont également utilisées par des groupes étatiques, principalement à des fins de cyber espionnage.

À titre d'illustration, il a été confirmé que le groupe APT lié à la Chine connu sous le nom de " **Zirconium** " (**TA412**) cible depuis le début de 2021 de nombreux journalistes américains avec des courriels de newsletters contenant des trackers alertant lorsque des messages étaient consultés dans le but de cibler ultérieurement les victimes les plus réceptives.

D'autres groupes ont également été observés, tels que le groupe cybercriminel **TA459**, l'APT nord-coréenne **TA404**, ou encore **TA482**, un groupe turc ciblant les comptes de réseaux sociaux appartenant à des journalistes via de fausses alertes de sécurité.



Fausse alerte de sécurité utilisée par TA482

6.3 Quelle défense ?

Proofpoint, dans son rapport 2022, pose la conclusion suivante : Les entreprises sous-estiment largement l'investissement en temps et en moyens (conversations, utilisation de services légitimes comme OneDrive, etc.) que sont prêts à mettre des cybercriminels pour compromettre une cible. En effet, leurs tactiques évoluent de manière constante afin d'améliorer leur taux de transformation. Les conséquences d'une opération de phishing sont souvent toute aussi désastreuses qu'une compromission via l'exploitation de vulnérabilités, pourtant ces dernières auront souvent droit à bien plus de vigilance de la part des équipes de cybersécurité.

La colonne vertébrale de la politique de défense d'une entreprise en matière de lutte contre les opérations d'ingénierie sociale réside dans la formation de ses collaborateurs vis-à-vis de cette menace. Cette formation, qui se veut essentiellement pratique, doit également être mise à jour régulièrement, grâce notamment à un travail de veille permettant le suivi de l'évolution des différentes techniques dans ce domaine. Cette veille permet également de signaler à temps des campagnes de phishing auprès des collaborateurs d'une même entreprise.

Règles d'analyse des mails :

- Toujours vérifier l'URL de destination avant de cliquer sur un lien contenu dans un mail.
- La prudence est de mise lorsqu'un mail demande des informations personnelles, la plupart des organismes utilisant des sites sécurisés pour recueillir ce type de données à l'heure actuelle.
- Vérification de modification mineure dans les noms de domaine.
- Analyse de contenu du message : accroche générique, changement de registre de langage, fautes d'orthographe, etc.

7 Références

Mirai - Katana - ZuoRAT

- https://www.malwaremustdie.org/
- https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#toc-1
- https://blog.cloudflare.com/content/images/2017/12/mirai-major-events-timeline.png
- https://www.silicon.fr/qui-est-anna-senpai-auteur-du-botnet-iot-mirai-167584.html
- https://librexpression.fr/lukraine-prends-un-coup-de-katana
- https://www.silicon.fr/botnet-mirai-gamer-mecontent-attaque-dyn-162973.html
- https://grahamcluley.com/mirai-botnet-password/
- https://blog.avast.com/fr/7-nouvelles-variantes-de-mirai-et-le-cybercriminel-en-herbe-qui-se-cache-derriere
- https://www.avira.com/fr/blog/katana-une-nouvelle-variante-du-botnet-mirai
- https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/
- https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/
- https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2022/02/17/feature-01
- https://lentrepreneur.co/innovation/cloud/la-campagne-apt-ciblant-les-routeurs-soho-met-en-evidence-les-risques-pour-les-travailleurs-a-distance-07072022
- https://fr.techtribune.net/securite/le-logiciel-malveillant-zuorat-detourne-les-routeurs-du-bureau-a-domicile-pour-espionner-les-reseaux-cibles/351775/
- https://cyware.com/news/zuorat-malware-with-hallmarks-of-a-state-backed-threat-actor-13986ad5

H0lyGh0st

- https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/
- https://www.securityweek.com/microsoft-north-korean-hackers-target-smbs-h0lygh0st-ransomware
- https://threatpost.com/h0lygh0st-ransomware-north-korea/180232/

- https://www.bitdefender.com/blog/hotforsecurity/north-korean-hackers-are-behind-the-h0lygh0st-ransomware-operation-microsoft-says/

INGENIERIE SOCIAL

- https://www.databreaches.net/exclusive-marriott-hacked-again-yes-heres-what-we-know/
- https://www.proofpoint.com/sites/default/files/threat-reports/Proofpoint_Threat_Research_Social_Engineering_Report_2022.pdf
- https://www.globalsecuritymag.fr/Le-rapport-d-analyse-comparative,20220715,127930.html