aDvens

Security for the greater good

Renseignement sur les menaces

Bulletin mensuel juin 2022

CERT ADVENS

04/07/2022 - **TLP WHITE**

Sommaire

1 SYNTHESE

Le mois de juin a été marqué par une activité accrue de la porte dérobée **Emotet**, qui prend ainsi la première place du **TOP 10** des maliciels les plus utilisés, devant FORMBOOK.

L'activité ransomware est dominée par le groupe **Lockbit**, comptabilisant **923** cyberattaques revendiquées. Les trois pays les plus impactés sont les Etats-Unis, l'Allemagne et le Royaume-Unis.

En mai et juin dernier, plusieurs expertises ont évoqué la réorganisation de groupe utilisant le rançongiciel Conti. Selon Advanced Intelligence, ce groupe serait en train de devenir un réseau décentralisé, à l'opposé du modèle économique du traditionnel Ransomware as a Service (RaaS).

Le CERT Ukrainien a mis en lumière des campagnes d'hameçonnage orchestrées par les groupes russes APT 28 et UAC-0098 contre l'Ukraine. Ces campagnes ont utilisé **la faille Follina** pour compromettre les terminaux des victimes.

Une récente analyse réalisée par Secureworks mentionne une possible manœuvre de cyber-espionnage : deux APT chinois, 41 et 10, auraient utilisé des rançongiciels pour dissimuler leurs véritables intentions.

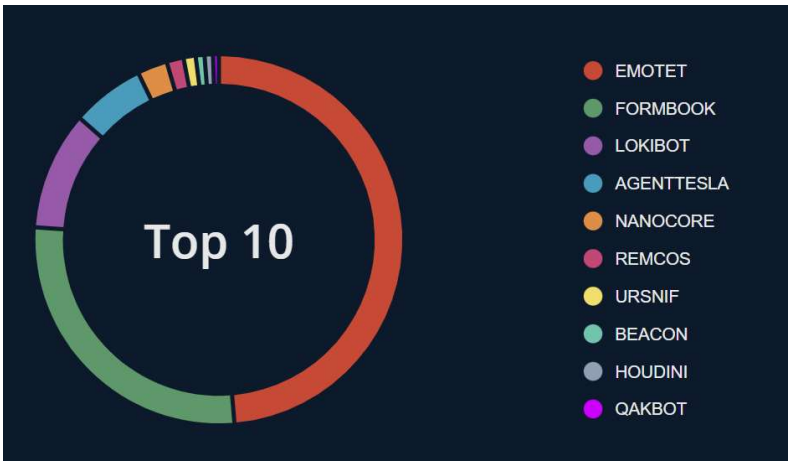
La société de sécurité Kaspersky a mis en exergue l'activité d'un nouvel APT : **Toddycat**. Ce dernier a ciblé principalement depuis décembre 2020, des infrastructures Microsoft exchange d'entités gouvernementales et militaires en Asie et en Europe. Ces infrastructures présentaient une vulnérabilité (*ProxyLogon*) qui a permis de déployer les portes dérobées **Samouraï** et **Ninja**.

2 TOP 10 des logiciels malveillants

2.1 Evolution

Le malware **EMOTET** vient de détrôner **FORMBOOK**, qui était en première position depuis plus de sept mois.

Par ailleurs, le malware **HOUDINI** fait son entrée dans le TOP10.



Le TOP 10 des logiciels malveillants du 1er juin au 1er juillet 2022.

2.1.1 Emotet

Découvert au cours de l'année 2014, Emotet était à l'origine un cheval de Troie dédié au vol des données bancaires. Il est devenu un logiciel malveillant modulaire et polyvalent. Son principal vecteur de distribution est l'hameçonnage.

Emotet propose ses services comme Malware-as-a-Service (MaaS), pour utiliser des logiciels malveillants tiers. En 2017, il a déployé le Remote Administration Tool (RAT) Dridex.

Emotet serait employé par le groupe cybercriminel russophone TA542.

2.1.2 Houdini

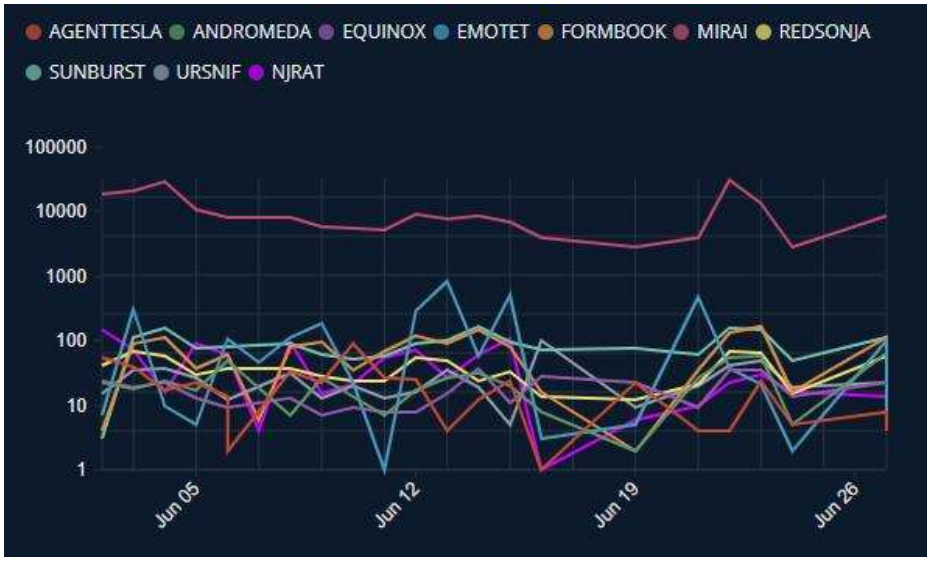
Houdini est une porte dérobée développée en **VBScript**. Elle permet à un attaquant de transférer et d'exécuter des fichiers sur le poste de travail de la victime.

Houdini serait utilisé par les groupes d'attaquants APT40, Molerats, TEMP.Batis et TEMP.Splinter. Le groupe Molerats aurait exploité le maliciel lors d'une cyberattaque à l'encontre du ministère européen des affaires étrangères et des agences de presse du Moyen Orient, en octobre 2019.

Des activités liées à Houdini ont été signalées en Asie du Sud, au cours du mois de mars 2021. Le premier signalement remonte à 2017, lors d'une cyberattaque menée par le groupe **TEMP.Batis** à l'encontre d'Israël et de la Palestine.

2.2 Consultation internet d'activités malveillantes

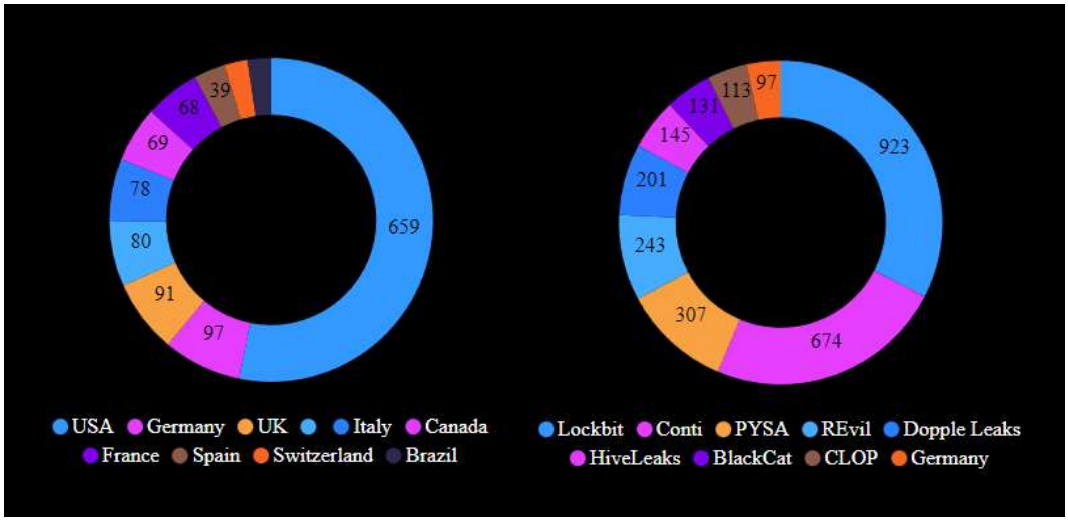
Ci-dessous, une chronologie des activités de logiciels malveillants consultées sur Internet par les internautes et recueillis par la société Mandiant.



Activité des logiciels malveillants du 1er juin au 1er juillet.

2.3 Ransomware

La volumétrie des attaques par rançongiciels montre que les États-Unis sont la principale cible des groupes cybercriminels.



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

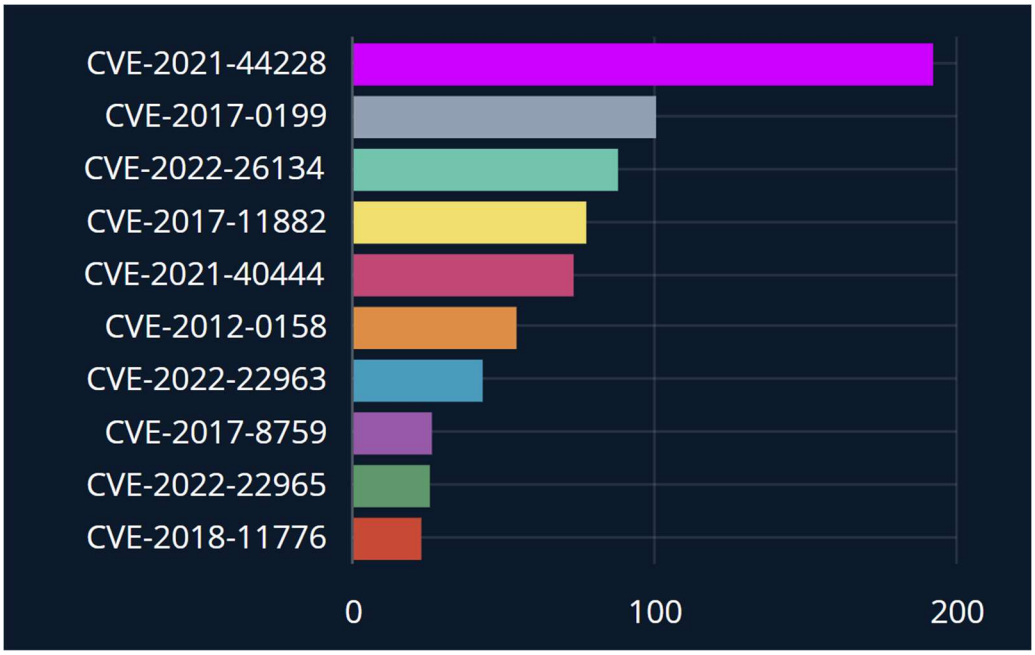
En juin, les trois rançongiciels les plus actifs étaient **Lockbit**, **Conti** et **Pysa**.

3 CVE

3.1 Les 10 vulnérabilités les plus actives

3.1.1 Classement

En juin 2022, la CVE-2021-44228 a été la vulnérabilité la plus employée dans les campagnes d'attaque.



Classement des 10 vulnérabilités les plus actives selon Mandiant. Mise à jour le 29/06/2022.

3.1.2 CVE-2021-4428

CVE-2021-44228 [Score CVSS 3.1 : 10] : Découvert par l'équipe *Cloud Security Team.* Il s'agit d'une vulnérabilité critique au sein de la bibliothèque log4j.

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.

3.2 Campagne d'exploitation de Follina

Une faille zero-day dans Microsoft Windows Support Diagnostic Tool (MSDT) a été découverte en avril dernier, et corrigée par l'éditeur, lors de sa mise à jour de sécurité patch Tuesday du 14 juin.

La **CVE-2022-30190**, connue sous le nom de **Follina**, est une vulnérabilité qui permet l'exécution de code arbitraire sur le système. Elle est exploitée très activement par des groupes de cybercriminels Russes et Chinois pour cibler des institutions gouvernementales aux Etats-Unis, en Europe et en Ukraine.

3.2.1 Description de la vulnérabilité

Le MSDT est un service dans Windows qui permet à l'équipe de support de Microsoft d'analyser les données du système. L'accès à cette application se fait via un code pin. Or, en utilisant une certaine syntaxe, il est possible d'exécuter des commandes *PowerShell* avec MSDT sans procéder à cette identification.

Pour exploiter cette vulnérabilité, un attaquant crée un document office (docx ou rtf) embarquant un *objet OLE* qui appelle une ressource extérieure, comme une page HTML. Cette dernière contient le script malveillant.

A l'ouverture du document, le service MSDT est appelé, et le code s'exécute avec les privilèges de l'utilisateur ; même si le document est en mode protégé ou les macros désactivées.

Le code malveillant peut s'exécuter à la prévisualisation du document office dans un explorateur Windows, augmentant ainsi le risque d'infection pour la victime.

L'attaquant mène des campagnes d'hameçonnage pour inciter la victime à ouvrir le document.

3.2.2 L'exploitation de cette vulnérabilité

La première exploitation de cette vulnérabilité date d'avril 2022, avec l'envoi d'un courriel. Celui-ci embarquait une pièce jointe, invitant la victime (russe) à un entretien pour la chaîne Sputnik radio. Ce document Word joint, exploitait bien sûr cette vulnérabilité.

Microsoft a été informé de ce vecteur d'infection, mais il attendra le 30 mai pour admettre l'existence de cette faille.

Cette vulnérabilité a été utilisée par des groupes cybercriminels, notamment dans le conflit ukrainien, avec l'implication d'**APT 28** (alias Fancy Bear et Sofacy). Selon la société Malwarebytes et le CERT ukrainien, APT 28 aurait mené une campagne d'hameçonnage sur la thématique de la menace nucléaire. Ce courriel contenait une pièce jointe intitulée *Nuclear Terrorism A Very Real Threat.rtf*.

La faille **Follina** permettait à l'attaquant de déployer un maliciel (développé en .NET), pour voler les identifiants et mots de passe des navigateurs Google Chrome, Microsoft Edge et Firefox du poste compromis. Les données étaient ensuite exfiltrées via le protocole IMAP.

APT28 n'est pas le seul groupe de Hackers russes à exploiter cette vulnérabilité. Le CERT ukrainien a ainsi identifié une attaque menée par le groupe **UAC-0098**, qui visait à exploiter la vulnérabilité Follina , via une campagne d'hameçonnage, pour installer un implant Cobalt Strike. Le courriel qui avait pour objet *Notice of non-payment of tax* embarquait un document office intitulé *Imposition of penalties.docx*.

Ces deux groupes utilisent les conditions créées par la guerre en Ukraine pour piéger leurs victimes.

Le groupe chinois **TA413** aurait aussi exploité cette vulnérabilité pour installer la porte dérobée *Qbot*, au sein d'organisations tibétaines.

3.2.3 Remédiation

Windows a publié un correctif pour cette vulnérabilité le 14 juin dernier. La meilleure manière pour s'en prémunir est de mettre à jour son système.

Si cela est impossible, il existe plusieurs solutions de contournement :

- Désactiver le Troubleshooting Wizard en utilisant l'éditeur de politique de groupe ou l'éditeur de Registry.
- Activer l'option « BlockOfficeCreateProcessRule » dans Windows Defender.
- Désactiver le Protocol URL de MSDT.

4 APT

4.1 APT chinois : cyber-espionnage sous couverture de ransomware

4.1.1 Avant-propos

Deux groupes d'attaquants chinois (**APT41** et **APT10**) auraient recours à des cyberattaques de type rançongiciel pour dissimuler des opérations de cyber espionnage. Selon les experts de Secureworks, ces groupes d'attaquants utiliseraient ce stratagème pour dissimuler leurs véritables intentions et pour distraire la cybersécurité. Ainsi, ce qui est présenté comme étant une banale extorsion des données à but lucratif serait en réalité une extorsion de renseignement dont le but est d'alimenter l'intelligence de l'état chinois.

4.1.2 L'intrigue

Les deux APT, 41 et 10, auraient recours au logiciel malveillant **HUI Loader** : il s'agit d'un cheval de Troie signalé pour la première fois au cours de l'année 2015. La particularité de ce logiciel est qu'il semble être très utilisé par divers groupes d'attaquants chinois lors d'opération de cyber espionnage.

Plusieurs campagnes d'hameçonnage auraient permis au logiciel HUI Loader d'infecter des postes de travail pour permettre le déploiement d'autres logiciels malveillants, notamment **PlugX** (permet le contrôle à distance, RAT), **Cobalt Strike** (logiciel légitime détourné, outil post-exploitation) et **QuasarRat** (permet le contrôle à distance, RAT).

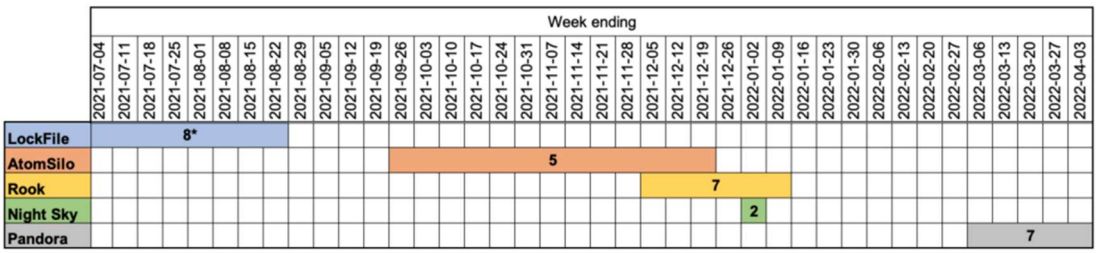
Plus précisément, depuis le mois de mars 2022, les attaquants d'APT 10 auraient utilisé Cobalt Strike et une nouvelle version d'HUI Loader pour déployer des rançongiciels connus sous les pseudonymes suivants : **LockFile**, **AtomSilo**, **Rook**, **Night Sky** et **Pandora**.

Une analyse réalisée par les experts de Secureworks a révélé que les attaquants auraient appliqué une configuration similaire de l'adresse de leurs serveurs C2 lors d'attaques distinctes ayant utilisé **AtomSilo**, **NightSky** et **Pandora**. L'adresse C2 (http post uri), retrouvée lors de l'analyse des attaques, commencerait par : **/rest/2/meetings…**

Par ailleurs, l'analyse montre que les attaques de type rançongiciels réalisées par ces attaquants, jusqu'à avant le 3 mars 2022, sont relativement courtes (seulement cinq opérations), le nombre de victimes serait très faible, et que l'ensemble des opérations a été abandonné brusquement (début le 4 juillet 2021 pour arrêter le 3 mars 2022).

« Also, they were all deserted somewhat prematurely »

Traduction : Les (les attaques rançongiciels) ont été abandonnées prématurément.



Activités des rançongiciels opérés par les attaquants. Selon Secureworks, ces cinq opérations seraient trop courtes, le nombre de victimes serait relativement faible, et l'ensemble des opérations serait brusquement abandonné. Tableau publié sur Bleepingc.

Des similitudes dans les codes malveillants ont été remarquées entre les logiciels Pandora et Hui Loader, cela serait de même pour AvosLocker et AtomSilo. Rook, NightSky et Pandora seraient dérivés d'un ancêtre commun : le rançongiciel **Babuk**.

4.1.3 Une éventuelle stratégie de la diversion

Il est à penser que les APT 41 et 10 auraient mené des opérations de cyber espionnage en utilisant des rançongiciels pour dissimuler leurs véritables intentions. Bien que Secureworks insiste sur le fait que la conclusion de son analyse n'est pas sûre à 100%, il est essentiel de rappeler que ce stratagème est pourtant bien réel :

- En 2018, une cyberattaque à l'encontre du système informatique d'une banque au Chili aurait utilisé un logiciel malveillant de type effaceur de données « disk-wiping malware » pour distraire le personnel pendant que les attaquants auraient exploité le système SWIFT de transfert d'argent.
- En 2022, lors de l'invasion de l'Ukraine par la Russie, le rançongiciel HermeticRansom a été utilisé par des attaquants russes comme moyen pour distraire leurs adversaires. Pendant la distraction, le logiciel malveillant de type effaceur donné HermeticWipper a été utilisé pour impacter plusieurs systèmes informatiques ukrainiens.

4.1.4 APT 41 et 10

4.1.4.1 APT 41

4.1.4.1.1 Le groupe

APT 41 (alias Bronze Riverside, Wicked Spider, Barrium, Wicked Panda, Bronze Atlas) est un groupe d'attaquants doté d'un très haut niveau de compétence de type Advanced Persistent Threat (APT). Ce groupe serait spécialisé dans le cyber espionnage et la cyberguerre, il appartiendrait **au Ministère de la Sécurité de l'État Chinois (MSS)**. Selon l'expertise de FireEye, ce groupe serait sponsorisé par le Parti Communiste Chinois pour mener des cyberattaques lucratives. Ce contraste en l'idéologie et le gain d'argent leur ont aussi valu le surnom de **Double Dragon**. Le principal vecteur d'infection utilisé et l'hameçonnage, ils ciblent les chaines d'approvisionnement et utilisent différents logiciels malveillants pour réaliser leurs opérations.

Actuellement, cinq membres de l'APT 41 ont été identifiés et sont recherchés par le FBI. Les membres identifiés sont : **ZHANG Haoran**, **TAN Dailin**, **QIAN Chuan**, **FU Qiang**, et **JIANG Lizhi**.

Tableau signalétique « FBI Most Wanted » concernant APT41.

4.1.4.1.2 APT 41 : matrice mitre Att&ck

TA0042 : Ressources Development	TA0001 : Initial Access	TA0002 : Execution
T1588.002 : Tools	**T1133 :** External Remote Service	**T1059.001 :** Command interpreter, Powershell
	T1190 : Exploit Public facing application	**T1059.004 :** Command interpreter, Unix Shell
	T1566.001: Spearphishing Attachment	**T1053.005 :** Scheduled Task/job, scheduled task
	T1078 : Valid Accounts	**T1560.002** : System Service, Service Execution
	T1199 : Supply Chain compromise, Software Supply Chain	**T1047 :** Windows Management Intrumentation
		T1203 : Exploitation for Client execuction
		T1059.001 : Command interpreter,Windows Shell

TA0003 : Persistence	TA0004 : Privilege Escalation	TA0005 : Defence Evasion
T1574.002 : Hijack execution flow, DLL side loading	**T1574.002 :** Hijack execution flow, DLL side loading	**T1112 :** Modify Registry
T1574.001 : Hijack execution flow, DLL search order	**T1574.001 :** Hijack execution flow, DLL search order	**T1574.002 :** Hijack execution flow, DLL side loading
T1053.005 : Scheduled Task/job, scheduled task	**T1053.005 :** Scheduled Task/job, scheduled task	**T1574.001 :** Hijack execution flow, DLL search order
T1078 : Valid Accounts	**T1078 :** Valid Accounts	**T1070.003** : Indicator removal host, Clear command history
T1542.003 : Pre OS boot, Bootkit	**T1055 :** Process Injection	**T1070.004** : Indicator removal host, File Deletion
T1574.006 : Hijack execution flow, Dynamic Linker	**T1574.006 :** Hijack execution flow, Dynamic Linker	**T1036 :** Masquerading, Match legitimate name/location
T1133 : External Remote Service	**T1548.006 :** Event Triggered Execution, Accessibility Features	**T1036 :** Masquerading, Rename System Utilities
T1548.006 : Event Triggered Execution, Accessibility Features	**T1543.003 :** Create or modify system process, Windows Service	**T1027 :** Obfuscade code or information
T1543.003 : Create or modify system process, Windows Service	**T1547.001 :** Boot/logon autostart execution, registry/startup	**T1055 :** Process Injection
T1136.001 : Create Account, Local Account		**T1553.002 :** Subvert trust Control, Code signing
T1547.001 : Boot/logon autostart execution, registry/startup		**T1218.001 :** System binary proxy execution, Compiled html
T1197 : Bits job		**T1078 :** Valid Accounts
		T1197 : Bits job
		T1480.001 : Execution Guardrails, environmental keying
		T1574.006 : Hijack execution flow, Dynamic Linker
		T1070.001 : Indicator removal host, Clear Windows logs
		T1218.011 : System binary proxy execution, RunDLL32
		T1014 : Rootkit
		T1542.003 : Pre os boot, Bootkit

TA0006 : Credential Access	TA0007 : Discovery	TA0008 : Lateral Movement
T1056.001 : Input capture, Keyloging	**T1033 :** System Owner / User Discovery	**T1021.001 :** Remote service, Remote Desktop Protocol
T1003.001 : OS Credential dumping, LSASS memory	**T1083 :** File and Directory Discovery	**T1021.002 :** Remote service, SMB Windows Admin shares
T1110.002 : Brute Force, Password Cracking	**T1046 :** Network System Discovery	
	T1135 : Network Share Discovery	
	T1016 : System Network Configuration Discovery	
	T1049 : System Network Connexion Discovery	

T10009 : Collection	TA0011 : Command and Control	TA0040 : Impact
T1560.001 : Archive Collected Data, Archive via Utility	**T1568.001 :** Dynamic resolution, Domain Generation Algorithm	**T1496 :** Ressource Hijacking
T1056.001 : Input capture, Keyloging	**T1102.001 :** Web Service, Dead Drop Resolver	**T1486 :** Data encrypted for impact
T1005 : Data from local System	**T1090 :** Proxy	
	T1071.004 : Application layer Protocol, DNS	
	T1071.002 : Application layer Protocol, File Transfer Protocol	
	T1071.001 : Application layer Protocol, Web protocols	
	T1008 : Fallback Channels	
	T1105 : Ingress Tool Transfer	
	T1104 : Multi Stage Channels	

4.1.4.2 APT 10

4.1.4.2.1 Le groupe

APT 10 (alias Bronze Starlight, Red Apollo, Potassium, MenuPass) est un groupe d'attaquant de type Advanced Persistent Threat (APT). Ce groupe serait spécialisé dans le cyber espionnage et la cyberguerre. C'est entre 2003 et 2006 que le groupe aurait été créé pour œuvrer au service du Tianjin field office du Ministère de la Sécurité de l'État Chinois (MSS). L'APT 10 est connue pour son exploitation de vulnérabilité zero-day, l'utilisation de keylogger et de portes dérobées, de logiciel d'administration à distance (Remote Adminsitration Tool, RAT). Le vecteur utilisé pour l'infection est l'hameçonnage. Les organisations ciblées sont celles dont le secteur d'activité est l'aérospatiale, l'ingénierie, la télécommunication ainsi que les gouvernements que la Chine considèrerait comme un ennemi. En 2016, l'APT 10 aurait volé les données personnelles d'environ 130 000 militaires de l'US Navy.

Actuellement, deux membres de l'APT 10 ont été identifiés et sont recherchés par le FBI. Les membres identifiés sont : **Zhu Hua** et **Zhang Shilong**.

Tableau signalétique « FBI Most Wanted » concernant APT10.

4.1.4.2.2 APT 10 : matrice mitre Att&ck

TA0042 : Ressources Development	TA0001 : Initial Access	TA0002 : Execution
T1583.001 : Domains	**T1204.002 :** Malicious File	**T1059.001 :** Command interpreter, Powershell
T1588.002 : Tools	**T1190 :** Exploit Public facing application	**T1106 :** Native Api
	T1566.001: Spearphishing Attachment	**T1053.005 :** Scheduled Task/job, scheduled task
	T1078 : Valid Accounts	**T1204.002** : User exécution, Malicious File
	T1199 : Trusted relationship	**T1047 :** Windows Management Intrumentation

TA0003 : Persistence	TA0004 : Privilege Escalation	TA0005 : Defence Evasion
T1574.002 : Hijack execution flow, DLL side loading	**T1574.002 :** Hijack execution flow, DLL side loading	**T1140 :** Deobfuscade Code/Decode file
T1574.001 : Hijack execution flow, DLL search order	**T1574.001 :** Hijack execution flow, DLL search order	**T1574.002 :** Hijack execution flow, DLL side loading
T1053.005 : Scheduled Task/job, scheduled task	**T1053.005 :** Scheduled Task/job, scheduled task	**T1574.001 :** Hijack execution flow, DLL search order
T1078 : Valid Accounts	**T1078 :** Valid Accounts	**T1070.003** : Indicator removal host, Clear command history
	T1055.012 : Process Injection, Process Hollowing	**T1070.004** : Indicator removal host, File Deletion
		T1036.003 : : Masquerading, Rename System Utilities
		T1036.005 : Masquerading, Match legitimate name or location
		T1027 : Obfuscade code or information
		T1055.012 : Process Injection, Process Hollowing
		T1553.002 : Subvert trust Control, Code signing
		T1218.004 : System binary execution, installUtil
		T1078 : Valid Accounts

TA0006 : Credential Access	TA0007 : Discovery	TA0008 : Lateral Movement
T1056.001 : Input capture, Keyloging	**T1087.002 :** Account Discovery, Domain Account	**T1210 :** Exploitation of remote service
T1003.004 : OS Credential dumping, LSA secrets	**T1083 :** File and Directory Discovery	**T1021.001 :** Remote service, Remote Desktop Protocol
T1003.003 : OS Credential dumping, NTDS	**T1046 :** Network System Discovery	**T1021.004 :** Remote service, SSH
T1003.002 : OS Credential dumping, Security Account Manager	**T1018 :** Remote System Discovery	
	T1016 : System Network Configuration Discovery	
	T1049 : System Network Connexion Discovery	

T10009 : Collection	TA0011 : Command and Control
T1560.001 : Archive Collected Data, Archive via Utility	**T1568.001 :** Dynamic resolution, Fast Flux DNS
T1119 : Automated Collection	**T1105 :** Ingress Tool Transfer
T1005 : Data from local System	**T1090.002 :** Proxy, External Proxy
T1039 : Data from Network Shared Drive	
T1074.001 : Data staged, Local Data Staging	
T1074.002 : Remote Data Staging	
T1056.001 : Input capture, Keyloging	

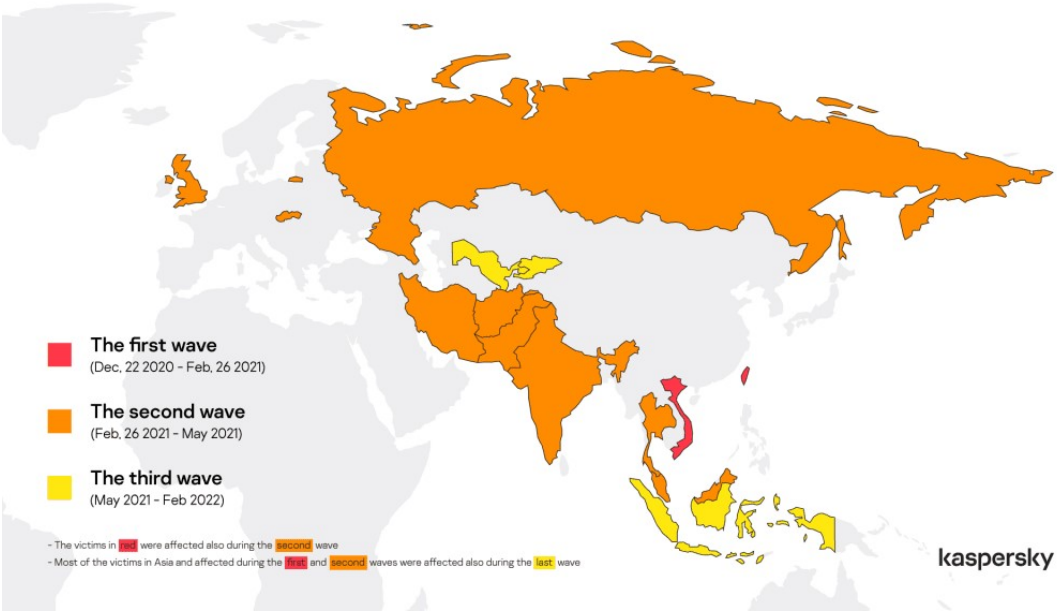
4.2 Toddycat : un nouvel APT méconnu

4.2.1 Contexte

Un nouveau groupe d'attaquants a fait son apparition dans la famille des APT. Baptisé « **Toddycat** » par la société de sécurité Kaspersky, ce groupe a ciblé des entités gouvernementales et militaires en Asie ainsi qu'en Europe.

Leurs premières campagnes ont été détectées en décembre 2020. Ils exploitaient une faille sur certains serveurs Microsoft Exchange d'organisation vietnamienne et taïwanaise. L'absence d'implants n'a pas permis de définir la vulnérabilité utilisée.

Il s'en est suivi deux autres vagues de février 2021 à 2022, durant lesquelles la vulnérabilité *ProxyLogon* a été exploitée sur des infrastructures exchange de divers pays.



Cartographie des victimes lors des différentes campagnes d'attaques.

4.2.2 Le modus operandi

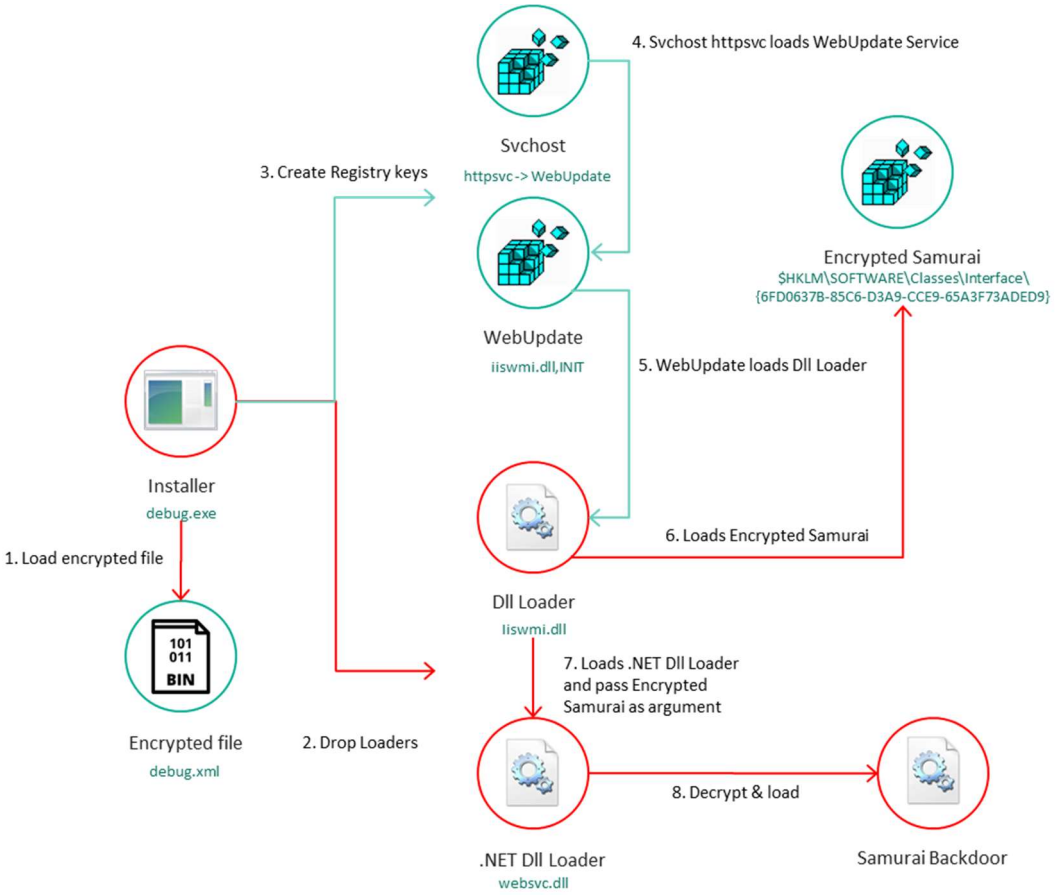
La compromission de ces serveurs a permis aux attaquants de déposer une variante du webshell **China chopper**, afin de conserver l'accès sur les systèmes infectés et ce, dans le but d'installer deux portes dérobées, nommées par Kaspersky « **Samouraï** » et « **Ninja** ».

L'implantation de celles-ci s'est effectuée en plusieurs étapes. La première consistait en l'installation du dropper « ***debug.exe*** », orchestrateur du déploiement des composants et des configurations nécessaires aux prochaines phases. Le dropper vérifiait, entre autres, la version du .NET présent sur le serveur compromis, pour charger des librairies malveillantes appropriées. Il contrôlait également la création de deux clés de registre, pièces maitresses pour la seconde étape.

Cette seconde étape exécutait ensuite la librairie « ***iiswmi.dll*** » pour récupérer le code chiffré de **Samouraï**, présent dans une des clés de registre. Ce code chiffré, était alors transmis en paramètre à un autre implant « ***websvc.dll*** », pour réaliser son déchiffrement, et clôturer la troisième phase. La porte dérobée Samouraï était ainsi exécutée.

```
Registry Key: $HKLM\SOFTWARE\Classes\Interface\{6FD0637B-85C6-D3A9-CCE9-65A3F73ADED9}
Value name:
Value: ILQ3Pz8/Pz87P9IFVEskWKpIeTB0jZx5SVXYXhh1fG...%encoded data%
```

Clé de registre contenant le code chiffré de Samaouraï.



Chaine d'attaque pour l'installation de Samouraï.

4.2.3 La porte dérobée Samouraï

La porte dérobée « **Samouraï** » a été développé en C#. Elle utilise le module .NET *HTTPListener* pour recevoir et interpréter des requêtes Http Post. Ces requêtes contiennent du code chiffré pour que la porte dérobée l'interprète et l'exécute. Kaspersky souligne que l'obfuscation du maliciel et l'emploi de multiples boucles ***while*** et de ***switch cases***, compliquent les analyses en rétroingénierie.

Samouraï propose plusieurs modules pour mener des actions sur les systèmes infectés, comme :

- L'exécution de code à distance,
- L'énumération des fichiers présents sur le disque,
- L'exfiltration des données,
- L'ouverture de connexions proxy vers des IP distantes.

4.2.4 La porte dérobée Ninja

Selon Kaspersky, Samouraï a été utilisée pour déployer la porte dérobée « **Ninja** ». Cette dernière, développée en C++, est plus complexe, et propose une boite à outils post exploitation à l'instar de cobalt strike. Elle permet notamment :

- Lister et interagir avec des processus en cours d'exécution,
- Gérer les systèmes de fichier,
- Exécuter des reverse shell,
- Injecter du code arbitraire dans des processus,
- Fournir un service de serveur mandataire entre le serveur de commande et de contrôle (C2) et un terminal infecté.

Pour échapper aux différents systèmes de détection, **Ninja** camoufle ses communications dans des flux HTTP/HTTPS qui paraissent légitimes, avec l'emploi de noms d'hôtes et d'url courants.

4.2.5 Telegram comme point d'entrée

Les chercheurs de Kaspersky, soulignent que lors de la première vague, les serveurs exchange n'ont pas été les seuls points d'entrées. Des archives au format zip, contenant des charges utiles **Ninja**, ont été envoyées via la messagerie *Telegram*, à des responsables des entités ciblées.

5 CONTI - organisation et réorganisation

5.1 Avant-propos

Conti est considéré comme le rançongiciel le plus virulent de ces deux dernières années.

Il serait opéré par Wizard Spider, un groupe cybercriminel ayant un modèle de fonctionnement similaire à celui d'une entreprise.

De 2016 jusqu'au début de l'année 2022, le groupe cybercriminel aurait œuvré avec une hiérarchie essentiellement verticale et centralisée. Elle aurait appliqué le modèle RaaS (Ransomware as a Service) avec plusieurs groupes cybercriminels affiliés.

Son allégeance envers la Russie lors du conflit ukrainien aurait engendré des tensions internes, provoquant la désertion de plusieurs de ses membres. L'un d'entre eux, pro-Ukrainien, se serait vengé en publiant des informations sensibles sur les activités internes de Conti.

Cette fuite, ajoutée à d'autres problèmes, aurait conduit l'entreprise à une réorganisation structurelle et fonctionnelle.

Actuellement, le nom Conti n'existerait plus, mais l'organisation serait toujours active. Elle serait en cours de réorganisation pour s'orienter vers un modèle décentralisé (plusieurs sous-divisions) et plus horizontal (loyauté parallèle entre les sous-divisions).

5.2 CONTI - son ancienne organisation

5.2.1 L'essentiel

5.2.1.1 Sa découverte

Découvert à la fin de l'année 2019, **Conti est un rançongiciel** qui est devenu rapidement célèbre pour l'étendue de son exploitation et le nombre de ses victimes.

5.2.1.2 Son modèle économique

Depuis ses débuts, Conti a toujours proposé ses services sous forme d'abonnement ou de partenariat, en tant que **Ransomware-as-a-service (RaaS)**.

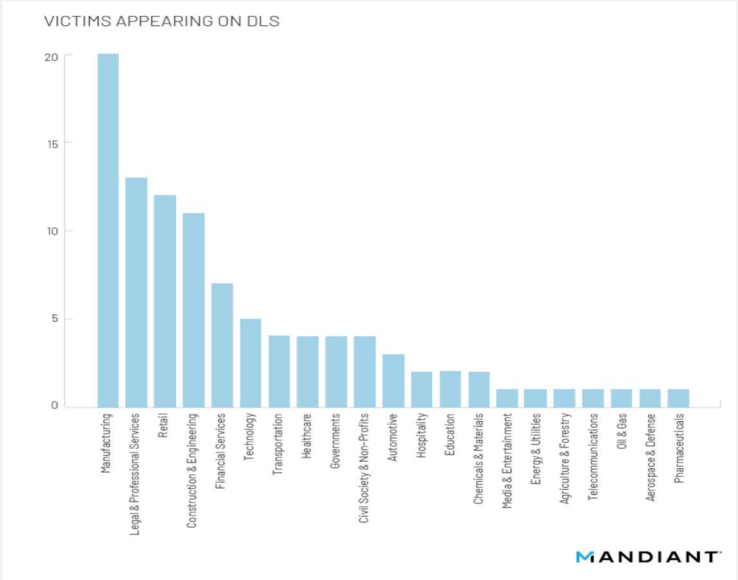
Les cybercriminels dit « affiliés », profitaient d'infrastructure opérationnelle (le rançongiciel, des outils post-exploitations, serveurs C2, site de fuite…) pour mener leurs propres opérations.

5.2.1.3 Ses victimes

Le 1er juin 2022, le journal L'Entrepreneur évoque dans l'un de ses articles, Conti comme le rançongiciel le plus agressif de ces deux dernières années.

Selon Mandiant, en février 2022, les cinq secteurs d'activités les plus impactés ont été les suivants : la manufacture, les services professionnels et légaux, la vente au détail, la construction et l'ingénierie, et les services de la finance.

Les établissements de santé sont en septième position, après le secteur des transports.



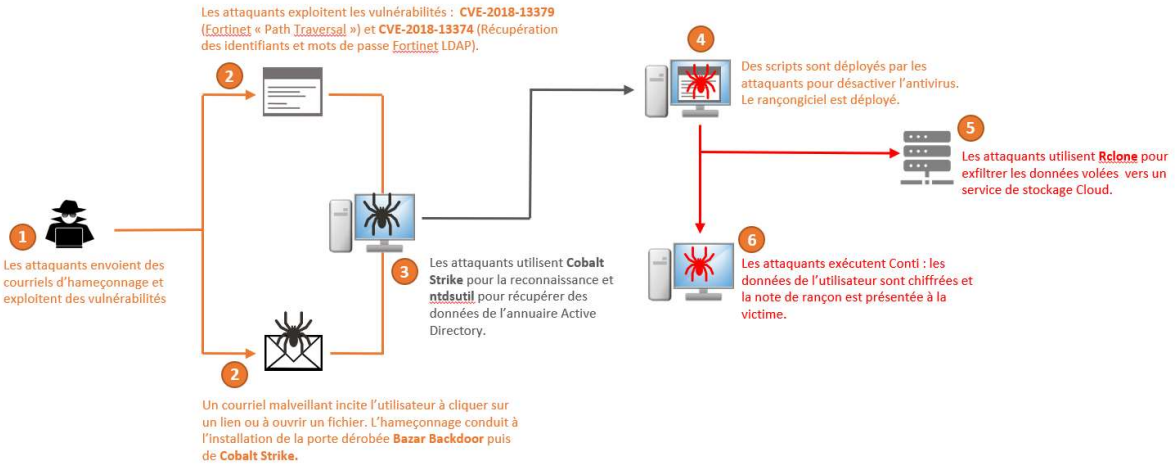
Répartition géographique des victimes selon Mandiant au mois de février 2022.

Toujours selon Mandiant, pour la même période, les victimes sont essentiellement localisées en : Espagne, France, Allemagne, Italie, Grande-Bretagne, aux États-Unis et Canada.

Répartition géographique des victimes selon Mandiant au mois de février 2022.

5.2.1.4 Sa chaine d'attaque

Ci-dessous, une chaine d'attaque utilisée au cours de l'année 2021 par les attaquants de Conti. Les attaquants ont recours à l'hameçonnage pour établir un accès initial dans le réseau de sa victime. Selon Trend Micro, des exploitations de vulnérabilités ont aussi été observées lors de plusieurs cyberattaques. Il s'agit des vulnérabilités Fortinet **CVE-2018-13379** et **CVE-2018-13374**. La présence de la porte dérobée **Bazar Backdoor** (Alias **Bazar Loader**) en tant que **Malware-as-a-service (MaaS)** est utilisée pour aider au déploiement du rançongiciel Conti.



Techniques, tactiques et procédures utilisées par Conti en 2021.

- CVE-2018-13379 : vulnérabilité critique dans Fortinet, l'exploitation permet une traversée de répertoire (« path traversal »). Score CVSS 3.1 : 9.8. Risque : un attaquant non authentifié peut télécharger des fichiers système en utilisant des requêtes http spécifiquement forgées.
- CVE-2018-13374 : vulnérabilité dans Fortinet. Score CVSS 3.1 : 8.8. Risque : un attaquant authentifié peut exploiter cette vulnérabilité pour récupérer des informations sensibles (identifiants et mots de passe) du serveur LDAP configuré dans Fortigate.
- Bazar Backdoor / Bazar Loader : découvert en avril 2020, il s'agit d'un cheval de Troie très sophistiqué utilisé par des attaquants en tant que MaaS pour déployer d'autres logiciels malveillants, notamment le rançongiciel Conti. Bazar Backdoor aurait été développé par les cybercriminels ayant réalisé **Trickbot**. Les détections antivirales peuvent être : **Trojan:Win64/Bazar**, **BackDoor.Bazar** ou **W64/Bazar**.

5.2.1.5 Ses auteurs et l'organisation

Selon Prodaft, de 2021 à 2022, le groupe opérant le rançongiciel Conti serait **Wizard Spider**.

Le groupe serait constitué d'environ 80 membres, ceux-ci seraient localisés à Saint Pétersbourg (Russie), proche d'Erbil (Kurdistan), et en Ukraine.

Dans son œuvre Ransom Mafia: Analysis of the world's first ransomware cartel, Jon DiMaggio révèle que Wizard Spider serait le groupe le plus important du cartel cybercriminel.

Le groupe Wizard Spider serait aussi surnommé **Trickbot**. L'appellation Trickbot (alias **Trickloader**, **Trickster**) est aussi utilisée, depuis 2016, pour le cheval de Troie développé par ce même groupe.

5.2.1.6 Recrutement

Les membres seraient essentiellement recrutés selon leur niveau de compétence et doivent endurer différents tests techniques pour prouver leur ingéniosité. Après avoir réussi ces tests, le nouveau membre se voit attribuer des tâches spécifiques à accomplir au sein d'une équipe. **Vladimir Dunaev** (alias FFX), arrêté en 2021, aurait été un membre de Wizard Spider depuis 2016. Après avoir réussi haut la main les tests techniques lors de son recrutement, il aurait eu pour tâche de développer un module d'injection pour le cheval de Troie Trickbot.

D'autres membres seraient recrutés sans savoir qu'ils œuvrent pour une organisation cybercriminelle. Ce serait le cas, par exemple, d'un membre surnommé **Zulas**. Selon une étude réalisée par Check Point Research, publiée sur ITR News le 17 mars 2022, Zulas aurait été recruté en tant que développeur au sein de Wizard Spider. L'étude des fuites de Conti ont révélé que Zulas ne comprend pas pourquoi son projet « lero » est nommé « trick (Trickbot) » par son responsable.

Ci-dessous, un extrait de l'étude publiée :

(…) un membre du groupe connu sous le surnom de « Zulas », très probablement la personne qui a développé le backend de Trickbot dans le langage de programmation Erlang. Zulas est passionné par Erlang, il s'empresse de montrer des exemples de ses autres travaux et donne même son vrai nom. Lorsque son responsable mentionne que son projet « trick » (Trickbot) a été vu par « la moitié du monde », Zulas ne comprend pas la référence, appelle le système « lero » et révèle qu'il n'a aucune idée de ce que fait son logiciel et pourquoi l'équipe se donne tant de mal pour protéger l'identité des membres. Son interlocuteur lui dit qu'il travaille sur un backend pour un système d'analyse publicitaire.

5.2.1.7 Entreprise

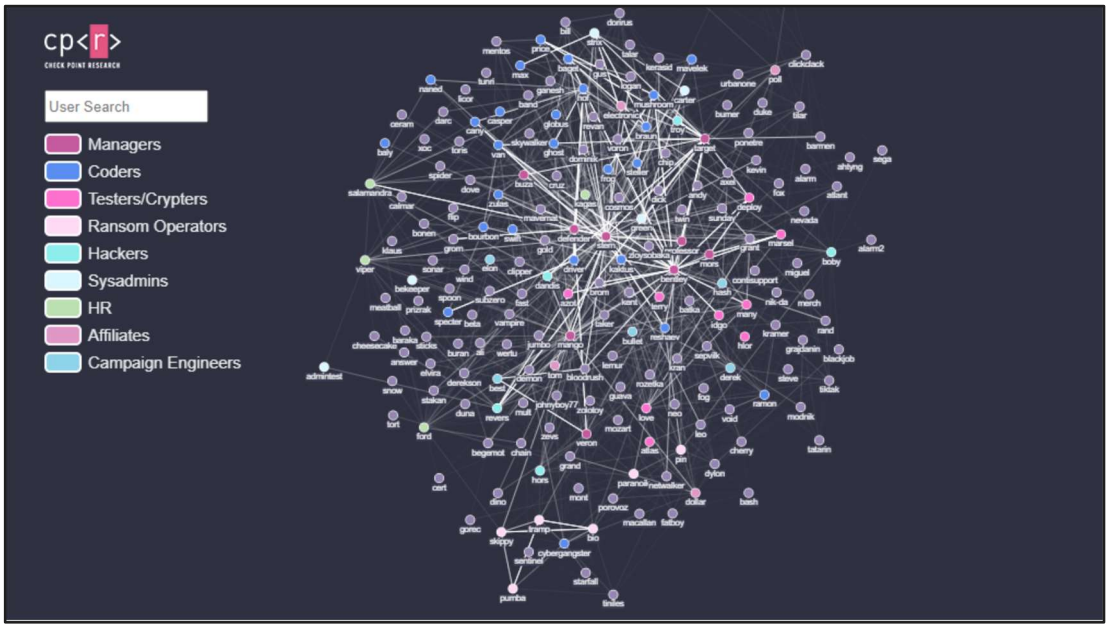
Depuis ses débuts, Wizard Spider a été conceptualisé pour ressembler à une entreprise. Cela se manifeste par sa dimension structurelle (hiérarchie) et fonctionnelle (spécialités).

Un article publié sur BleepingComputer le 28 octobre 2021 révèle que Wizard Spider aurait été organisé comme suit :

- Managers des logiciels malveillants (Malware Manager) : il s'agit des managers qui s'occupent de répondre aux besoins des programmeurs, ils s'occupent aussi de la finance et du déploiement des logiciels malveillants.
- Développeurs de logiciels malveillants (Malware Developer) : les développeurs, ils s'occupent du développement des modules Trickbot.
- Cryptographes (Crypters) : Il s'agit des spécialistes du chiffrement, en charge de chiffrer les modules des logiciels malveillants.

- Les spécialistes de l'hameçonnage (Spammer) : Ils sont les spécialistes des campagnes d'hameçonnage et de la distribution des malwares.

Le 10 mars 2022, Check Point Research publie son étude sur les fuites de Conti. L'étude a permis de mettre en lumière la complexité de l'organisation du groupe. Ci-dessous, le graphique relationnel des principales équipes :



Ce graphique montre les principales équipes, et leurs relations, dans l'entreprise opérant Conti. Check Point Research: Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of. 10 mars 2022.

Au cours de l'année 2021 et 2022, l'entreprise aurait été constituée de plusieurs équipes : Managers, développeurs, testeurs et cryptographes, opérateurs de rançongiciels, hackers, administrateurs système, ressources humaines, affiliées et ingénieurs.

Les membres les plus importants seraient : **Stern** (le grand chef de l'entreprise), **Bentley** (Manager de l'équipe des testeurs et cryptographes), **Mango** (Il assiste Stern dans différentes tâches de gestion de l'entreprise), **Busa** (Manager technique), **Target** (Manager des hackers et il s'occupe aussi des tâches concernant l'ingénierie sociale), **Reshaev** (très important, il serait celui qui conceptualise l'organisation de l'entreprise) et **Veron** (Manager des opérations et de l'infrastructure Emotet).

5.3 CONTI - sa réorganisation

5.3.1 Allégeance prorusse

Le 25 février 2022, lors du conflit en Ukraine, le groupe opérant Conti publie sur son site Conti News son allégeance envers la Russie.

Publication de Conti sur Conti news.

Il s'agit d'un évènement important, puisqu'il provoque une désertion interne d'un membre pro-ukrainien.

5.3.2 La fuite

Le 27 février 2027, un ex-membre de Conti, pro-ukrainnien, publie sur un compte twitter nommé Conti Leaks des informations sensibles de l'entreprise cybercriminelle. Les informations publiées sont des conversations internes entre différents membres importants (managers), des journaux Jabber et Rocket de Conti.

VX underground publie le 1er mars 2022 sur son site des informations internes de Conti : captures d'écrans, conversations, détails techniques et outils de piratage...

Parmi les conversations qui ont fuité, un message particulièrement intéressant est celui d'un membre nommé **Frances**. Le message est daté du 21 février 2022. Frances y explique que la situation est pénible et qu'une réorganisation de l'entreprise est nécessaire. Il ajoute qu'ils ont perdu le contact avec le Stern (le grand chef), et il conseille aux autres membres de faire profil bas.

Extraits du message de Frances :

« As soon as there is any new on payments, reorganization and return to work, I will contact everyone. (…) Those who do not want to move on with us – we naturally understand. For those who will wait – we rest for 2-3 months, take care of your personal lives and enjoy freedom ».

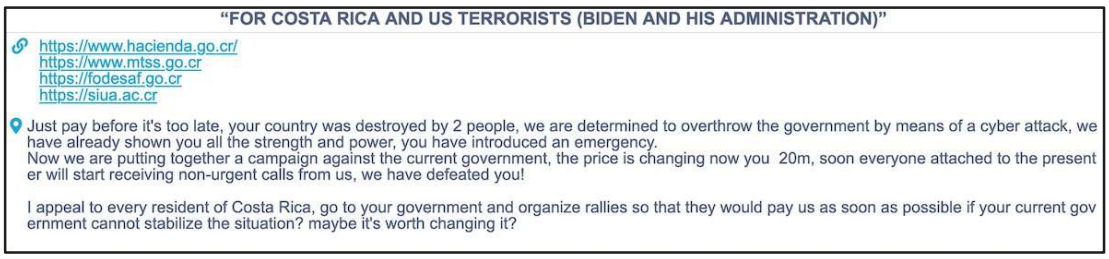
Traduction : dès que nous aurons des informations concernant les paiements, ***la réorganisation et la reprise des activités****, je vous contacterai tous. Ceux qui ne veulent plus nous suivre – nous vous comprenons. Pour ceux qui veulent nous suivre, reposez-vous pendant 2 – 3 mois, prenez soin de vos affaires personnelles et profitez de la liberté.*

« In the near future, we, with those team leaders who remained in the ranks, will think about how to restart all work process, where to find money for salary payments and launch all our work projects with renewed vigor ».

Traduction : Dans un futur proche, nous, les chefs restants, nous allons réfléchir à comment relancer toute l'activité, où trouver de l'argent pour les salaires et relancer tous nos projets avec vigueur.

5.3.3 Cyberattaque COSTA RICA

Le 8 mai 2022, le président du Costa Rica nouvellement élu, Rodrigo Chaves, a déclaré l'état d'urgence du pays à la suite d'une cyberattaque massive qui aurait été menée par l'organisation opérant Conti. La cyberattaque a ciblé 29 institutions publiques (finance, science et technologie, météorologie, électricité, innovation et télécommunication) et impacté environ 860 serveurs du pays.

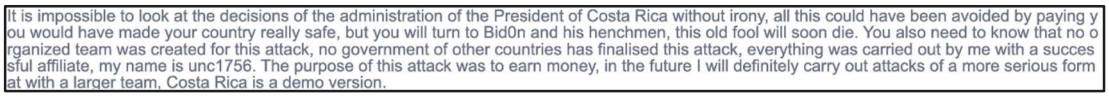


Publication des cybercriminels à l'encontre du Costa Rica, du président Biden et de son administration.

Le Costa Rica n'ayant pas payé la rançon, les opérateurs de Conti ont divulgué environ 670 giga-octets de données extorquées aux agences gouvernementales.

Selon un article publié sur ABC Science, le 3 juin 2022, les attaquants auraient infiltré plusieurs serveurs dès le mois de février.

La cyberattaque aurait été réalisée avec l'aide d'autres attaquants, notamment des opérateurs du rançongiciel **Hive** et d'un nouvel affilié identifié comme **UNC1756**. Depuis la fuite des informations internes de Conti, des managers auraient quitté Spider Wizard pour intégrer le groupe exploitant Hive.



Publication d'un attaquant se revendiquant UNC1756.

La manifestation d'un nouvel affilié de Conti, **UNC1756**, et la migration de certains managers de Conti vers Hive démontrent qu'une réorganisation de l'entreprise cybercriminelle est en cours.

5.3.4 L'art de la déception

Le 19 mai 2022, le site Conti News a cessé son activité. Selon Advanced Intelligence, l'entreprise cybercriminelle aurait planifié la fin de ses activités, sous le nom de Conti, à compter de cette date.

La campagne d'attaques menée contre le Costa Rica avait vraisemblablement pour objectif de mettre sous les feux des projecteurs le groupe cybercriminel.

« The only goal Conti had wanted to meet with this final attack was to use the platform as a tool of publicity, performing their own death and subsequent rebirth in the most plausible way it could have been conceived ».

Traduction : Le seul objectif que Conti désirait atteindre avec cette dernière cyberattaque était d'utiliser sa plateforme comme un outil publicitaire, **de réaliser sa propre mort et sa propre renaissance ultérieure** de la manière la plus plausible que cela puisse être conçu.

Advanced Intelligence aurait investigué la préparation de la cyberattaque depuis le 14 avril 2022. L'investigation met en exergue que la stratégie publicitaire aurait été décidée par les managers de Conti, en interne :

«The agenda to conduct the attack on Costa Rica for the purpose of publicity instead of ransom was declared internally by the Conti leadership ».

Traduction : l'agenda concernant la conduite de la cyberattaque à l'encontre du Costa Rica en vue de faire de la publicité plutôt qu'une extorsion a été déclaré en interne par les chefs de Conti.

«The attack on Costa Rica indeed brought Conti into the spotlight and helped them to maintain the illusion of life for just a bit longer, while the real restructuring was taking place ».

Traduction : l'attaque contre le Costa Rica a mis Conti sous les feux des projecteurs, et a permis de maintenir l'illusion que le celui était toujours en vie, alors qu'en réalité une restructuration / réorganisation de l'entreprise était en cours.

5.3.5 Sa réorganisation

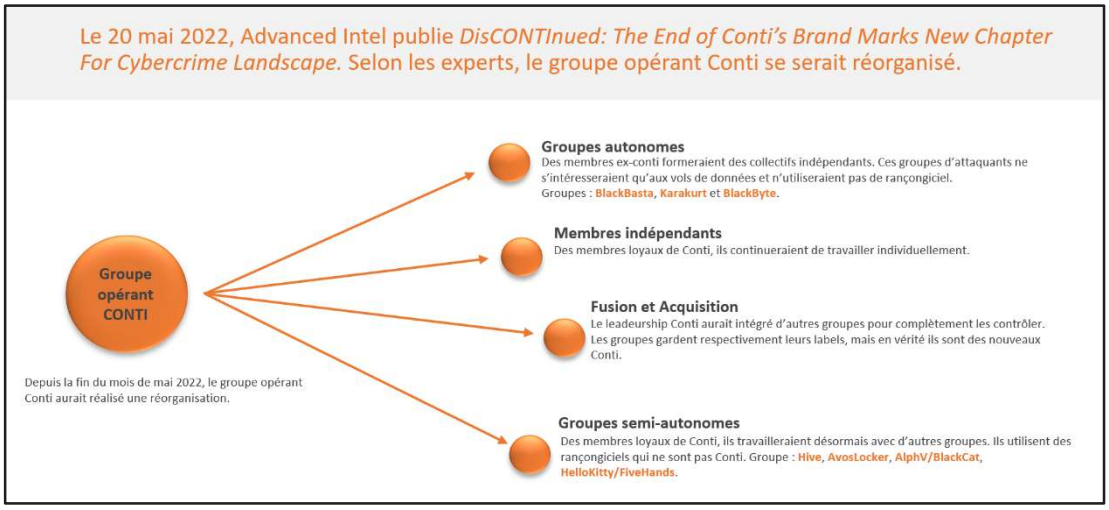
Désormais, l'entreprise cybercriminelle serait en cours de réorganisation en s'appuyant sur deux principes.

La restructuration doit conduire à une organisation décentralisée, avec une coalition de plusieurs sous-divisions. Certaines d'entre elles œuvrerait en toute autonomies, et d'autres appartiendraient à un collectif opérant des rançongiciels. Toutes ces sous-divisions auraient porté allégeance envers un certain un certain « Reshaev ».

«This model is more flexible and adaptive than the previous Conti hierarchy but is more secure and resilient than RaaS ».

Traduction : Ce modèle est plus flexible et plus adaptatif que l'ancienne hiérarchie de Conti, et s'avère plus sécurisé et résilient que le modèle RaaS.

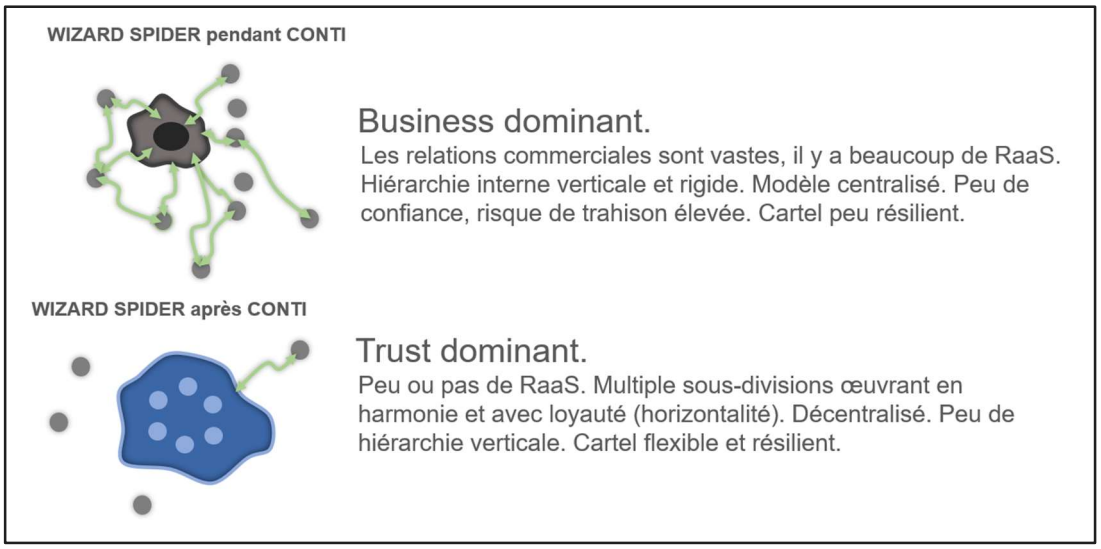
La réorganisation doit permettre la transition « **from data encryption to data exfiltration** », avec pour objectif d'exfiltrer les données sans impacter la victime avec du chiffrement.



Schématique de la réorganisation de l'entreprise ayant opéré Conti.

L'illustration ci-dessous, schématise la différence entre l'ancienne et la nouvelle organisation de l'entreprise cybercriminel ayant opéré Conti.

- Les flèches vertes représentent les connexions avec des affiliés (RaaS),
- Les points gris sont des groupes cybercriminels,
- Le point noir représente l'ancienne organisation de Wizard Spider,
- Les points bleus synthétisent la nouvelle organisation.



Vulgarisation graphique de l'évolution de Wizard Spider.

6 Références

Follina

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware
- https://securelist.com/cve-2022-30190-follina-vulnerability-in-msdt-description-and-counteraction/106703/
- https://blog.qualys.com/product-tech/2022/06/14/detect-the-follina-msdt-vulnerability-cve-2022-30190-with-qualys-multi-vector-edr-context-xdr
- https://www.deepinstinct.com/blog/unfolding-the-follina-zero-day-vulnerability
- https://www.darkreading.com/attacks-breaches/russia-apt28-launches-nuke-themed-follina-exploit-campaign
- https://www.theregister.com/2022/06/09/qbot-malware-microsoft-follina/
- https://securityaffairs.co/wordpress/131843/apt/china-apt-exploits-follina-flaw.html
- Follina — a Microsoft Office code execution vulnerability I by Kevin Beaumont I May, 2022 I DoublePulsar
- Russian govt hackers hit Ukraine with Cobalt Strike, CredoMap malware (bleepingcomputer.com)
- Two Russian threat groups utilised the Follina flaw to target Ukraine (izoologic.com)
- CVE-2022-30190 - Guide des mises à jour de sécurité - Microsoft - Vulnérabilité d'exécution de code à distance dans l'outil de diagnostic du Support Microsoft Windows (MSDT)

APT Chinois

- https://www.bleepingcomputer.com/news/security/chinese-hackers-use-ransomware-as-decoy-for-cyber-espionage/#:~:text=Two%20Chinese%20hacking%20groups%20conducting,cover%20up%20their%20malicious%20activities.
- https://www.fbi.gov/wanted/cyber/apt-10-group
- https://www.fbi.gov/wanted/cyber/apt-41-group
- https://twitter.com/kaspersky/status/1498765385621020680
- https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/

- https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0045%2FG0045-enterprise-layer.json

Toddycat

- https://securelist.com/toddycat/106799/

Conti

- https://www.mandiant.com/resources/conti-ransomware?utm_source=google&utm_medium=cpc&utm_content=paid-search&gclid=CjwKCAjwquWVBhBrEiwAt1Kmwv51SC2Kjnf4cRtTHlstv4npmNAe7pEQ_hiQy2kl_lm_4h0AH2tP6xoC5iUQAvD_BwE&gclsrc=aw.ds
- https://lentrepreneur.co/innovation/cloud/conti-ransomware-explique-ce-que-vous-devez-savoir-sur-ce-groupe-criminel-agressif-01062022
- https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
- https://nvd.nist.gov/vuln/detail/CVE-2018-13374
- https://nvd.nist.gov/vuln/detail/CVE-2018-13379
- https://www.supprimer-trojan.com/trojan-bazar/
- https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60-years-in-prison/
- https://itrnews.com/articles/193953/conti-le-groupe-russe-de-ransomware-mis-a-nu-par-check-point-research.html
- https://www.theregister.com/2022/05/18/wizard-spider-ransomware-conti/
- https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/
- https://www.abc.net.au/news/science/2022-06-04/costa-rica-at-war-with-russian-hackers-cyber-criminals/101116930
- https://ezpublish-france.fr/le-costa-rica-declare-lurgence-nationale-apres-les-attaques-du-rancongiciel-conti/
- https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/
- https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape