TLP:CLEAR
PAP:CLEAR

FIN12

UN GROUPE CYBERCRIMINEL AUX MULTIPLES RANÇONGICIELS

18 septembre 2023

Sommaire

Synthèse

Le jeudi 9 mars 2023, l'ANSSI a émis un signalement concernant la compromission de l'un des serveurs du centre hospitalier universitaire (CHU) de Brest. Ce signalement a été rendu possible par des investigations menées par l'ANSSI depuis plusieurs années.

La réactivité de l'établissement de santé a permis d'isoler rapidement le système d'information d'Internet et d'entraver la progression du mode opératoire des attaquants (MOA), empêchant ainsi l'exfiltration de données et le chiffrement du système d'information.

La découverte de liens avec un ensemble d'incidents observés sur le périmètre français et rapportés en sources ouvertes a permis à l'ANSSI d'associer cette attaque au MOA cybercriminel FIN12.

Les opérateurs du MOA FIN12 seraient responsables d'un nombre conséquent d'attaques par rançongiciel sur le territoire français. Entre 2020 et 2023, ils auraient employé les rançongiciels **Ryuk** puis **Conti**, avant de prendre part aux programmes de *Ransomware-as-a-Service* (RaaS) des rançongiciels **Hive**, **BlackCat** et **Nokoyawa**. Ils auraient également utilisé les rançongiciels **Play** et **Royal**.

1 Déroulé de l'incident

1.1 Tactiques, techniques et procédures (TTP)

Lors de l'incident, les attaquants n'ont pas exfiltré de données et ne sont pas parvenus à déployer leur charge finale. Néanmoins, un ensemble d'actions malveillantes réalisées par les attaquants a pu être identifié sur plusieurs serveurs de la victime.

Un récapitulatif des TTP et indicateurs de compromission est disponible en annexes 3.1 et 3.2.

1.1.1 Accès initial

L'accès initial au système d'information a été effectué depuis un service de bureau à distance exposé et accessible sur Internet. Les opérateurs du MOA ont utilisé des authentifiants valides d'un professionnel de santé pour se connecter. Il est probable que les authentifiants du compte soient issus de la compromission par un *information stealer* [1] du poste utilisateur, dans le cadre d'une campagne de distribution opportuniste.

Deux acteurs pourraient donc être impliqués dans l'incident, un fournisseur d'accès initial et l'attaquant chargé de la latéralisation et du déploiement du rançongiciel.

1.1.2 Codes malveillants

Les attaquants ont utilisé leur accès de bureau à distance afin d'exécuter deux portes dérobées : **SystemBC** [2] et **Cobalt Strike**.

SystemBC a été exécuté dans un intervalle de 20 minutes après **Cobalt Strike** depuis le même répertoire. Ces deux codes ont donc très probablement été déployés par le même acteur.

Le tableau ci-dessous présente les indicateurs de compromission liés à ces deux codes.

Nom de fichier	Chemin	SHA1	Serveur C2	Commentaire
host.dll	C:\Users\Public\Music\	8a0743f17110dc945007f08f3e63da166a3937dc	149.28.197.120 149.28.213.157	SystemBC
b64.exe	C:\Users\Public\Music\	9e2737994aa8bf0d6900e5369d51978adc4c02f9	youthconscience.com	Cobalt Strike

1.1.3 Persistance

Afin d'assurer leur persistance, les opérateurs du MOA ont tenté, sans succès, de modifier le mot de passe d'un compte local et de créer l'utilisateur « `supp` ».

Nom d'utilisateur	Mot de passe
[expurgé]	Supp@111!
supp	@Supp11@32
supp	Supp@123

1. Un *information stealer* est un type de code malveillant utilisé pour collecter des informations d'identification sur une machine compromise.
2. **SystemBC** est un code malveillant disponible à l'achat sur des forums cybercriminels, il permet d'établir un tunnel SOCKS5 entre la machine compromise et le serveur de l'attaquant.

1.1.4 Élévation de privilèges

Pour élever leurs privilèges, les attaquants ont tenté d'exploiter les vulnérabilités *LocalPotato* [3] (CVE-2023-21746) et la CVE-2022-24521.

Les fichiers suivants ont été observés sur le serveur compromis :

Nom de fichier	Chemin	SHA1	Commentaire
cleanlpe1day.exe	C:\Users\[user]\Downloads\cleanlpe1day\	364a4d9ea6f88eec098b13728fce2c1ead94c48d	Code d'exploitation de la CVE-2022-24521
LocalPotato.exe	C:\Users\[user]\Downloads\	8291929d6f3ede6ec025c21d1559a7fe9d30a9ce	Code d'exploitation de la CVE-2023-21746
lpe.exe	C:\Users\[user]\Downloads\	70ad1a42ce05404c00513989c949c83a94feca92	

L'exécutable d'exploitation de la vulnérabilité *LocalPotato* est disponible sur GitHub [1]. Le fichier « `lpe.exe` » n'a pas pu être récupéré, mais fait probablement référence à « *local privilege escalation* ».

1.1.5 Accès aux données d'authentification

Le MOA a employé trois codes afin de tenter de récupérer des données d'authentification : **AccountRestore**, **SharpRoast** et **Mimikatz**.

AccountRestore est un outil de *bruteforce* de comptes Active Directory qui a été documenté par SECURITY JOES [2]. **Mimikatz** est un outil notamment utilisé pour extraire des authentifiants en environnement Windows. **SharpRoast** permet d'effectuer une attaque par *kerberoasting*. **Mimikatz** et **SharpRoast** sont disponibles en sources ouvertes [3, 4].

Le tableau ci-dessous présente les indicateurs de compromission liés à ces trois codes.

Nom de fichier	Chemin	SHA1	Commentaire
svchost.exe	C:\Users\[user]\Downloads\svchost\	28400c267815762e49c200e8b481a592c67f9cf7	AccountRestore
sharproast.exe	C:\Users\[user]\Downloads\PingCastle_2.11.0.1\	d65969088eb8f6098c33c5427a650e8576cdbfa6	SharpRoast
svchost.exe	C:\Users\[user]\Downloads\svchost1\	-	Mimikatz

1.1.6 Découverte

Les attaquants ont utilisé les outils disponibles en sources ouvertes **Softperfect Network Scanner** pour réaliser de la découverte réseau, ainsi que **PingCastle** et **BloodHound** afin d'identifier de mauvaises configurations de l'Active Directory.

Nom de fichier	Chemin	SHA1	Commentaire
netscan.exe	C:\Users\[user]\Downloads\scan\8.1.5\	eeaf29a71330db50cdd4630f8d9f1c2b6a34578c	Softperfect Network Scanner
PingCastle.exe	C:\Users\[user]\Downloads\8.1.5\Nouveau dossier\	292629c6ab33bddf123d26328025e2d157d9e8fc	PingCastle
PingCastleAutoUpdater.exe	C:\Users\[user]\Downloads\8.1.5\Nouveau dossier\	536734aa6ec0f0b1ba8e43088edc6857eca42667	PingCastle

1.1.7 Latéralisation

Afin de se latéraliser, les opérateurs du MOA ont tenté, sans succès, d'exploiter les vulnérabilités *PrintNightmare* [4] (CVE-2021-34527), *BlueKeep* [5](CVE-2019-0708), puis *ZeroLogon* [6] (CVE-2020-1472) *via* l'outil **Mimikatz**.

3. Vulnérabilité affectant le protocole d'authentification NTLM sur Windows permettant l'élévation de privilèges.
4. Vulnérabilité affectant le service Windows Print Spooler permettant l'exécution de code à distance.
5. Vulnérabilité affectant le protocole RDP Windows permettant l'exécution de code à distance.
6. Vulnérabilité affectant le protocole de contrôle à distance Netlogon permettant l'élévation de privilèges.

Nom de fichier	Chemin	SHA1	Commentaire
LPE-Exploit-RunAsUser.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	e2a68116d52182f207c087f349e04e049982d431	CVE-2021-34527
Step1-RunAsAdmin.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	fae6068d4433b33751bf7de866d7f2900aa15139	CVE-2021-34527
Step2-RunAsUser.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\	d69420a636dacfbafaf01f7153692c197e9b6400	CVE-2021-34527
spn.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\Release\	68a07540fbf58fe743636b7fc8f0370c84134eb3	CVE-2021-34527
spn_nf3.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\Release\	58cb839dbc0232874b6fed9a354d4cc6d355cbac	CVE-2021-34527
spider.dll	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\share\	1e0ec6994400413c7899cd5c59bdbd6397dea7b5	CVE-2021-34527
spider_32.dll	C:\Users\[user]\Downloads\PrintNightmare-Manual\Attacker\share\	35ff55bcf493e1b936dc6e978a981ee2a75543a1	CVE-2021-34527
CreShar.exe	C:\Users\[user]\Downloads\PrintNightmare-Manual\C#-CreateShare\	a00ebf699ea0759e7bf4af65dddd741133c38484	CVE-2021-34527
MakeMeGood.bat	C:\Users\[user]\Downloads\PrintNightmare-Manual\Victim\	df12386df2c0fcf65522282914424d63da962d79	CVE-2021-34527
bks.exe	C:\Users\[user]\Downloads\8.1.5\bluekeep\	-	CVE-2019-0708

La boite à outils d'exploitation de *PrintNightmare* semble être partagée entre plusieurs acteurs, elle a notamment été mise en vente en février 2022 [5] et aurait été utilisé par des affiliés du groupe BLACKCAT [6].

1.2 Infrastructure

Au cours de l'incident, les attaquants ont employé deux portes dérobées : **SystemBC** et **Cobalt Strike**. Leur infrastructure est détaillée ci-dessous.

1.2.1 SystemBC

L'implant **SystemBC** observé dans l'incident communique avec les serveurs de Commande et Contrôle (C2) « `149.28.197.120` » et « `149.28.213.157` » sur le port TCP 4177. Les deux serveurs C2 sont hébergés par VULTR.

L'ANSSI n'a pas connaissance de l'utilisation de l'hébergeur VULTR et du port 4177 par d'autres modes opératoires.

1.2.2 Cobalt Strike

Les attaquants ont employé le nom de domaine « `youthconscience.com` » comme serveur C2 **Cobalt Strike**. Il utilisait le *Content Delivery Network* CLOUDFLARE.

D'après la configuration de l'implant **Cobalt Strike** disponible en annexe 3.3, le profil *Malleable C2*[7] a été généré par l'outil **Random C2 Profile Generator** [7].

Les investigations de l'ANSSI ont permis d'identifier 11 serveurs C2 **Cobalt Strike** supplémentaires liés au mode opératoire.

Nom de domaine	Date d'enregistrement
tumbleproperty.com	2022-11-24
texasflooddesign.com	2022-11-24
performernews.com	2022-11-24
getinteriorartstudio.com	2022-11-24
youthconscience.com	2023-01-09
tributepower.com	2023-01-09
realversedesign.com	2023-01-09
purpleinfluenceonline.com	2023-01-09
herbswallow.com	2023-03-13
psychologymax.com	2023-03-16
jacketsupport.com	2023-03-16
mirrordirectory.com	2023-03-29

7. Un profil *Malleable C2* est un fichier de configuration qui permet de personnaliser les communications de l'implant **Cobalt Strike** avec son serveur C2.

2 Un mode opératoire cybercriminel historique

2.1 Liens techniques avec un ensemble d'incidents

Les analyses de l'ANSSI ont permis d'établir des liens entre l'incident du CHU de Brest et le chiffrement d'une trentaine d'entités entre 2020 et 2023.

2.1.1 Liens d'infrastructure

Le 11 mars 2022, le compte Twitter @Cryptolaemus1 a identifié la distribution d'un implant **SystemBC** par le *botnet* Epoch 5 lié au *Malware-as-a-Service* (MaaS) **Emotet**. L'infrastructure de commande et de contrôle **SystemBC** était similaire à celle employée par les attaquants impliqués dans l'incident du CHU de Brest. Les serveurs C2 étaient hébergés par VULTR et utilisaient le port 4177 : « `96.30.196.207` » et « `45.32.132.182` » [8].

Concernant l'infrastructure **Cobalt Strike**, le nom de domaine « `tumbleproperty.com` » identifié dans la partie 1.2.2, a été observé par la CISA en décembre 2022 dans un incident impliquant le rançongiciel **Royal** [9].

De plus, grâce à des liens d'infrastructure, l'ANSSI a pu rattacher au même MOA plusieurs exploitations de la vulnérabilité *ProxyNotShell* (CVE-2022-41080 et CVE-2022-41082) ayant mené au déploiement de **Play**.

*Commentaire : les opérateurs du mode opératoire impliqué dans l'incident du CHU de Brest utiliseraient donc les rançongiciels **Play** et **Royal**. Ils auraient également eu recours aux services du code malveillant **Emotet** en 2022.*

2.1.2 Tactiques, techniques et procédures (TTP)

L'ANSSI est parvenue à lier le MOA impliqué dans l'incident du CHU de Brest avec un ensemble d'attaques par rançongiciels notamment observées sur le périmètre français.

Ces incidents présentent des caractéristiques techniques dont la plupart sont similaires à celles observées au CHU :

- accès initial au système d'information par l'utilisation d'authentifiants valides ;
- utilisation conjointe des codes malveillants **SystemBC** et **Cobalt Strike** ;
- le stockage de charges dans le répertoire « `C:\Users\Public\Music\` » ;
- nom du chiffreur similaire : « `xxx.exe` », bien que celui-ci n'ait pas pu être observé dans l'incident du CHU.

Dates	Source *	Rançongiciel	Authentifiants valides	SystemBC	Cobalt Strike	Répertoire « Music »	Chiffreur « xxx.exe »
2019 / 2021	Mandiant	Ryuk Conti	■	■	■	■	■
2020 / 2022	Microsoft MSTIC	Ryuk Conti Hive BlackCat Nokoyawa	?	■	■	?	■
2020-10 / 2021-02	2 incidents FR	Ryuk	BazarLoader	■	■	■	■
2021-01 / 2021-05	9 incidents FR	Ryuk	■	■	■	■	■
2022-01 / 2022-05	4 incidents FR	Hive	■	■	■	■	■
2022-05	1 incident FR	Nokoyawa	■	■	■	■	■
2022	Trend Micro	Hive	?	■	■	■	■
2022	Trend Micro	Nokoyawa	?	■	■	■	■
2022-07	Trend Micro	Play	■	■	■	■	■
2022-07 / 2022-12	4 incidents FR	Play	■	■	■	■	■
2023-03	CHU de Brest		■	■	■	■	

** Les incidents français correspondent à ceux rapportés ou suivis par l'ANSSI.*

*Commentaire : les attaquants impliqués dans l'incident du CHU de Brest seraient donc actifs depuis au moins 2019 et auraient utilisé successivement les rançongiciels **Ryuk**, **Conti**, **Hive**, **Nokoyawa** et **Play**. Ils auraient également eu recours aux services du code malveillant **BazarLoader** entre 2020 et 2021.*

2.2 PISTACHE TEMPEST : l'héritier de FIN12

D'après les analyses de l'ANSSI, les attaquants responsables de l'incident du CHU de Brest pourraient donc être affiliés à différentes attaques par rançongiciel. Ils auraient utilisé les rançongiciels **Ryuk**, puis **Conti**, avant de distribuer **Hive**, **Nokoyawa**, **Play** et **Royal**. Une analyse historique de leur mode opératoire les lie à FIN12 ainsi qu'à d'autres opérations de rançongiciels ayant succédé à la fin des opérations du groupe CONTI (WIZARD SPIDER). Microsoft suit ce mode opératoire sous la dénomination PISTACHE TEMPEST ou DEV-0237 [10].

2.2.1 Liens avec FIN12

Des analyses de l'ANSSI ont mis en évidence des liens de TTP et d'infrastructure avec le mode opératoire FIN12 suivi par Mandiant (ex-UNC1878 [8]).

En effet, d'octobre 2020 à mai 2021, plusieurs serveurs C2 **Cobalt Strike** observés dans des incidents **Ryuk** de la partie 2.1.2 étaient associés au MOA UNC1878.

De plus, la configuration des serveurs **Cobalt Strike** de l'incident du CHU de Brest est similaire avec de précédentes campagnes associées à FIN12 [11] : utilisation du service CloudFlare et d'outil de génération de profil *Malleable C2* aléatoire.

Les opérateurs de FIN12 seraient responsables d'une partie importante, mais non exclusive, des campagnes d'attaques des rançongiciels Ryuk et Conti entre 2020 et 2021. Le mode opératoire FIN12 serait caractérisé par un intérêt pour les entreprises susceptibles de payer des rançons élevées (*Big Game Hunting*) ainsi que par un ciblage important du secteur de la santé (au moins 20% des victimes du groupe) [12]. Les opérateurs de FIN12 seraient notamment responsables de plusieurs attaques majeures contre ce secteur, dont la campagne du rançongiciel Ryuk en 2020 contre des établissements publics de santé aux États-Unis attribuée à UNC1878 [13]. Le ciblage des opérateurs de FIN12 se concentrait sur l'Amérique du Nord et l'Europe [12].

2.2.2 Le MOA PISTACHE TEMPEST

L'éditeur Microsoft suit ce mode opératoire sous la dénomination PISTACHE TEMPEST (ou DEV-0237) et met en évidence la participation de ses opérateurs à divers programmes de rançongiciel [10, 14]. En plus des rançongiciels **Ryuk**, **Conti**, **Hive** et **Nokoyawa** dont l'utilisation a été observée par l'ANSSI, Microsoft ajoute l'utilisation des rançongiciels **BlackCat**, **Agenda** et **Mindware**. L'ANSSI n'a pas été en mesure de confirmer l'utilisation de ces rançongiciels, mais les TTP décrites par l'éditeur correspondent aux observations de l'ANSSI.

L'une des particularités de ce MOA est de ne recourir que rarement à des méthodes de double extorsion. Les opérateurs de PISTACHE TEMPEST (FIN12) semblent privilégier le chiffrement rapide des réseaux compromis au détriment de l'exfiltration des données de la victime. Ce constat correspond au *Time-To-Ransom* [9] des opérateurs de FIN12, qui est d'environ 4 jours [11]. Enfin, le mode opératoire PISTACHE TEMPEST est utilisé pour cibler le secteur de la santé, comme lorsque ses opérateurs agissaient au sein du groupe cybercriminel CONTI.

En dépit de l'utilisation récurrente de certaines TTP entre 2020 et 2023, l'ANSSI constate une diversification des méthodes d'accès initial de ce MOA [11]. Les opérateurs de FIN12 auraient notamment réduit leur utilisation du code malveillant **Bazarloader** à partir de 2021 [10]. Le vecteur d'infection privilégié semble être le recours à des authentifiants valides. Néanmoins, la distribution par le code malveillant **Emotet** d'un implant de **SystemBC** lié à PISTACHE TEMPEST confirme le recours ponctuel à des services de distribution. Selon Microsoft, les opérateurs de PISTACHE TEMPEST auraient également utilisé le code malveillant **TrickBot** et le MaaS **GoziAT** [14].

2.2.3 De multiples affiliations après la fragmentation du groupe CONTI

À la suite de la déclaration d'allégeance de CONTI à la Russie et des « Conti *Leaks* », les opérateurs de CONTI, dont l'acteur « Reshaev » meneur et développeur du code source de Ryuk et Conti, auraient décidé d'arrêter progressi-

8. L'éditeur Mandiant suivait d'abord ce MOA sous l'appellation UNC1878 avant de choisir FIN12.
9. Terme utilisé pour désigner le délai entre l'intrusion initiale de l'attaquant et le chiffrement du système d'information.
10. **BazarLoader** est un code malveillant identifié pour la première fois en avril 2020 et opéré par le groupe CONTI (WIZARD SPIDER). Sa disparition progressive coïncide avec deux évènements : la divulgation en août 2021 d'un manuel technique distribué par le groupe CONTI à ses membres [15] et les révélations sur les CONTI *Leaks* de février 2022 [16].

vement leurs opérations en répartissant leurs activités au sein de multiples opérations de rançongiciel [17].

Dans la continuité de cette fragmentation, un ou plusieurs ex-membres de FIN12 pourraient s'être détachés du groupe CONTI en souscrivant à différents programmes de *Ransomware-as-a-Service* (*RaaS*), tout en utilisant des TTP similaires. Cette réorientation est observable dans l'utilisation par PISTACHE TEMPEST de **Hive** dès octobre 2021 [14]. Alors que le groupe CONTI avait déjà commencé à créer des filiales, dont KARAKURT, BLACKBYTE et BLACKBASTA, plusieurs *pentesters* du groupe auraient entrepris de migrer vers d'autres programmes d'affiliés tout en conservant leur loyauté à CONTI. Le programme du *RaaS* HIVE compte parmi ceux avec lesquels auraient commencé à travailler ces ex-membres de CONTI [17].

D'après des informations recueillies dans les « Conti *Leaks* », l'acteur « Troy » pourrait être l'un des individus responsables des opérations associées au mode opératoire FIN12. Il serait issu d'une des anciennes équipes du groupe cybercriminel CONTI et pourrait encore être en activité en tant qu'opérateur de PISTACHE TEMPEST [18].

À partir de juillet 2022, PISTACHE TEMPEST aurait commencé à utiliser le rançongiciel **Play** alors que ses opérateurs affirment ne pas fonctionner comme un *RaaS*, cela témoigne des relations étroites des opérateurs de PISTACHE TEMPEST avec d'autres opérateurs de rançongiciels.

Au début de l'année 2023, l'utilisation par les opérateurs de PISTACHE TEMPEST du rançongiciel **Royal** indique l'existence continue de relations entre des ex-membres de CONTI. ROYAL constitue notoirement un groupe de rançongiciel né de l'interruption des activités de CONTI [19, 20, 21].

Commentaire : les opérateurs de PISTACHE TEMPEST entretiendraient donc des relations étroites avec le reste de l'écosystème cybercriminel et pourraient collaborer au sein de cercles restreints d'opérateurs de rançongiciels, facilitant les multiples affiliations des opérateurs du MOA.

2.2.4 Synthèse chronologique

Le recoupement des analyses de l'ANSSI avec les publications d'éditeurs permet d'effectuer la synthèse chronologique suivante :

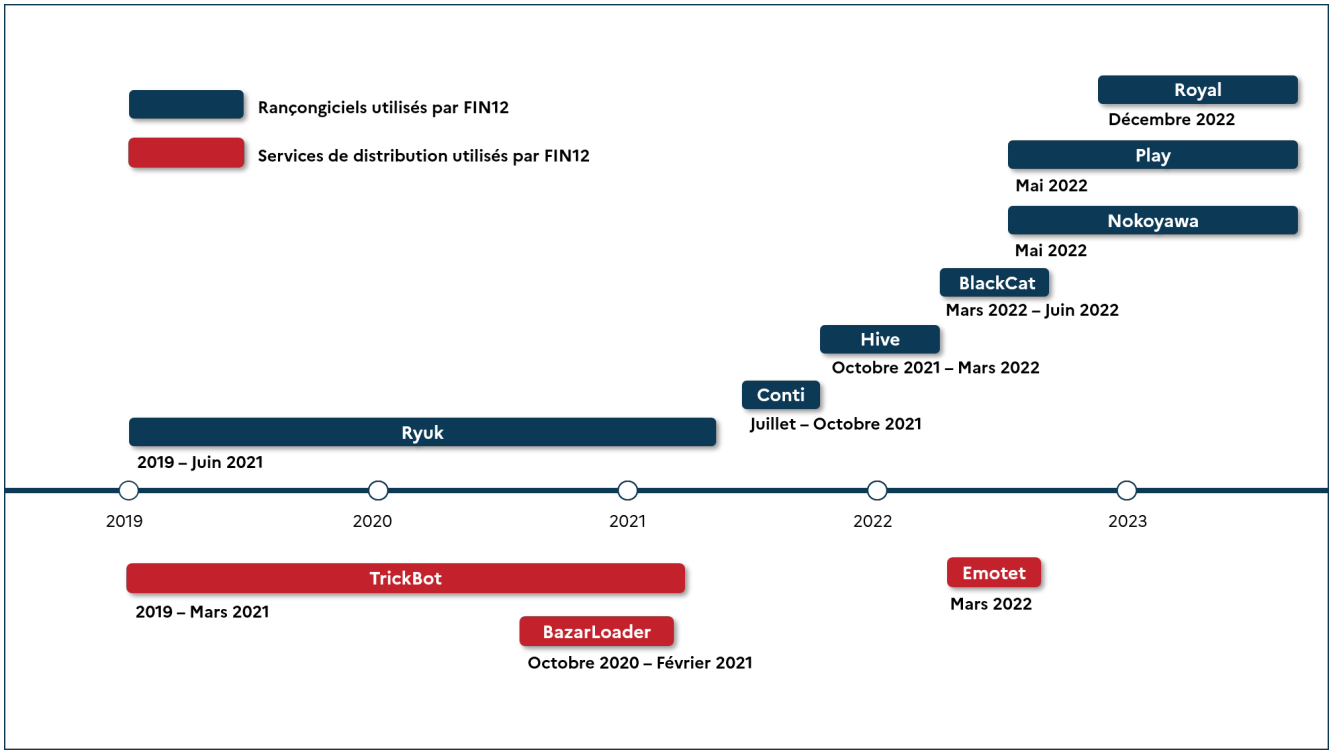

FIG. 2.1 – Synthèse chronologique des activités connues du MOA FIN12 (PISTACHE TEMPEST) depuis 2019 [11, 14, 22, 23].

3 Annexes

3.1 Tableau de TTP

Phase	Technique	Nom	Commentaire
Resource Development	T1588.002	Obtain Capabilities: Tool	Utilisation de l'outil **Random C2 Profile Generator** pour générer le profil *Malleable C2* **Cobalt Strike**.
Resource Development	T1583.004	Acquire Infrastructure: Server	Utilisation de VPS hébergés chez Vultr comme serveurs C2 **SystemBC**, et utilisation du port 4177.
Initial Access	T1133	External Remote Services	Connexion à un service de bureau à distance.
Initial Access	T1078.002	Valid Accounts: Domain Accounts	Utilisation d'authentifiants valides pour se connecter à un service de bureau à distance.
Persistence	T1136.001	Create Account: Local Account	Tentative de création du compte « supp ».
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Tentative d'exploitation des vulnérabilités *LocalPotato* (CVE-2023-21746) et CVE-2022-24521.
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Utilisation des répertoires « `C:\Users\Public\Music\` » et « `C:\Users\[user]\Downloads\` ».
Credential Access	T1110.003	Brute Force: Password Spraying	Utilisation de l'outil **AccountRestore** avec le dictionnaire « `Passwordar.txt` ».
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Utilisation de l'outil **Mimikatz**.
Credential Access	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	Utilisation de l'outil **SharpRoast**.
Discovery	T1046	Network Service Discovery	Utilisation de l'outil de découverte réseau **Softperfect Network Scanner**.
Discovery	T1018	Remote System Discovery	Utilisation des outils de découverte **PingCastle** et **BloodHound**.
Lateral Movement	T1210	Exploitation of Remote Services	Tentative d'exploitation des vulnérabilités *PrintNightmare* (CVE-2021-34527), *BlueKeep* (CVE-2019-0708) et *ZeroLogon* (CVE-2020-1472).
Command and Control	T1090.004	Proxy: Domain Fronting	Utilisation du CND CloudFlare afin de dissimuler le serveur C2 **Cobalt Strike** final.
Command and Control	T1572	Protocol Tunneling	Utilisation d'un tunnel SOCKS5 via l'implant **SystemBC**.

3.2 Indicateurs de compromission

Nom de fichier	Commentaire	SHA1
host.dll	SystemBC	8a0743f17110dc945007f08f3e63da166a3937dc
b64.exe	Cobalt Strike	9e2737994aa8bf0d6900e5369d51978adc4c02f9
cleanlpe1day.exe	Code d'exploitation de la CVE-2022-24521	364a4d9ea6f88eec098b13728fce2c1ead94c48d
LocalPotato.exe	Code d'exploitation de la CVE-2023-21746	8291929d6f3ede6ec025c21d1559a7fe9d30a9ce
lpe.exe	-	70ad1a42ce05404c00513989c949c83a94feca92
svchost.exe	AccountRestore	28400c267815762e49c200e8b481a592c67f9cf7
sharproast.exe	SharpRoast	d65969088eb8f6098c33c5427a650e8576cdbfa6
netscan.exe	Softperfect Network Scanner	eeaf29a71330db50cdd4630f8d9f1c2b6a34578c
PingCastle.exe	PingCastle	292629c6ab33bddf123d26328025e2d157d9e8fc
PingCastleAutoUpdater.exe	PingCastle	536734aa6ec0f0b1ba8e43088edc6857eca42667
LPE-Exploit-RunAsUser.bat	Code d'exploitation de la CVE-2021-34527	e2a68116d52182f207c087f349e04e049982d431
Step1-RunAsAdmin.bat	Code d'exploitation de la CVE-2021-34527	fae6068d4433b33751bf7de866d7f2900aa15139
Step2-RunAsUser.bat	Code d'exploitation de la CVE-2021-34527	d69420a636dacfbafaf01f7153692c197e9b6400
spn.exe	Code d'exploitation de la CVE-2021-34527	68a07540fbf58fe743636b7fc8f0370c84134eb3
spn_nf3.exe	Code d'exploitation de la CVE-2021-34527	58cb839dbc0232874b6fed9a354d4cc6d355cbac
spider.dll	Code d'exploitation de la CVE-2021-34527	1e0ec6994400413c7899cd5c59bdbd6397dea7b5
spider_32.dll	Code d'exploitation de la CVE-2021-34527	35ff55bcf493e1b936dc6e978a981ee2a75543a1
CreShar.exe	Code d'exploitation de la CVE-2021-34527	a00ebf699ea0759e7bf4af65dddd741133c38484
MakeMeGood.bat	Code d'exploitation de la CVE-2021-34527	df12386df2c0fcf65522282914424d63da962d79

Marqueur réseau	Commentaire	Première observation	Dernière observation
getinteriorartstudio.com	Cobalt Strike	2022-11-24	-
performernews.com	Cobalt Strike	2022-11-24	-
texasflooddesign.com	Cobalt Strike	2022-11-24	-
tumbleproperty.com	Cobalt Strike	2022-11-24	-
purpleinfluenceonline.com	Cobalt Strike	2023-01-09	-
realversedesign.com	Cobalt Strike	2023-01-09	-
tributepower.com	Cobalt Strike	2023-01-09	-
youthconscience.com	Cobalt Strike	2023-01-09	-
149.28.197.120	SystemBC	2023-02-06	2023-04-30
149.28.213.157	SystemBC	2023-02-06	2023-04-30
herbswallow.com	Cobalt Strike	2023-03-13	-
jacketsupport.com	Cobalt Strike	2023-03-16	-
psychologymax.com	Cobalt Strike	2023-03-16	-
mirrordirectory.com	Cobalt Strike	2023-03-29	-

3.3 Configuration Cobalt Strike

```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 114564
MaxGetSize                      - 1403031
Jitter                          - 47
MaxDNS                          - Not Found
PublicKey_MD5                   - 32f7e0b84b76a8f8ec0069e2188475e5
C2Server                        - youthconscience.com,/Remove/x/996NV95ZCC
UserAgent                       - Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
     Chrome/56.0.2924.87 Safari/537.36
HttpPostUri                     - /activate/v3.45/JAIUN0X5L
Malleable_C2_Instructions       - Remove 2080 bytes from the end
                                  Remove 2844 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - ConstHeaders
                                       Accept: text/html, image/*, application/json
                                       Accept-Language: no
                                       Accept-Encoding: identity, br
                                  Metadata
                                       mask
                                       netbiosu
                                       prepend "secure_id_LKY1IRT3DSN9L7CA703JDZGX0F4Z="
                                       header "Cookie"
HttpPost_Metadata               - ConstHeaders
                                       Accept: application/json, image/*, text/html
                                       Accept-Language: fa
                                       Accept-Encoding: br, compress
                                  SessionId
                                       mask
                                       netbios
                                       parameter "_PAKDYYEK"
                                  Output
                                       mask
                                       netbiosu
                                       print
PipeName                        - Not Found
DNS_Idle                        - Not Found
DNS_Sleep                       - Not Found
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
SSH_Banner                      - Host: youthconscience.com

HttpGet_Verb                    - GET
HttpPost_Verb                   - POST
HttpPostChunk                   - 0
Spawnto_x86                     - %windir%\syswow64\Locator.exe
Spawnto_x64                     - %windir%\sysnative\w32tm.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
```

```
Proxy_Behavior                  - Use IE settings
Watermark_Hash                  - bfnETSwzb1Xsa2g6gr+auA==
Watermark                       - 674054486
bStageCleanup                   - True
bCFGCaution                     - False
KillDate                        - 0
bProcInject_StartRWX            - False
bProcInject_UseRWX              - False
bProcInject_MinAllocSize        - 5782
ProcInject_PrependAppend_x86    - b'\x0f\x1f\x84\x00\x00\x00\x00\x00\x90\x0f\x1f\x00\x0f\x1fD\x00\x00f\x90\x0f\x1f@\
    x00\x90\x0f\x1fD\x00\x00\x0f\x1f\x00\x0f\x1f\x80\x00\x00\x00\x00f\x0f\x1fD\x00\x00\x0f\x1fD\x00\x00'
                                  b'f\x0f\x1fD\x00\x00PX\x0f\x1f\x00\x0f\x1fD\x00\x00PX\x0f\x1f\x84\x00\x00\x00\x00\
                                      x00\x0f\x1f\x00\x0f\x1fD\x00\x00\x0f\x1fD\x00\x00'
ProcInject_PrependAppend_x64    - b'f\x0f\x1f\x84\x00\x00\x00\x00\x00\x0f\x1f\x84\x00\x00\x00\x00\x00PX\x90f\x0f\x1f\
    x84\x00\x00\x00\x00\x00\x0f\x1f@\x00f\x0f\x1f\x84\x00\x00\x00\x00\x00\x90PXf\x90\x0f\x1fD\x00\x00\x0f\x1f\x84\x00
    \x00\x00\x00\x00\x0f\x1fD\x00\x00\x0f\x1f@\x00f\x90\x0f\x1f@\x00PX'
                                  b'\x0f\x1fD\x00\x00\x90PX\x0f\x1f\x00f\x0f\x1fD\x00\x00f\x0f\x1f\x84\x00\x00\x00\
                                      x00\x00PXf\x0f\x1f\x84\x00\x00\x00\x00\x00\x0f\x1f\x00PX\x0f\x1f\x84\x00\x00\
                                      x00\x00\x00f\x0f\x1f\x84\x00\x00\x00\x00\x00f\x0f\x1fD\x00\x00f\x0f\x1f\x84\
                                      x00\x00\x00\x00\x00\x0f\x1f\x80\x00\x00\x00\x00f\x90\x0f\x1f\x84\x00\x00\x00\
                                      x00\x00\x0f\x1f\x00PX'
ProcInject_Execute              - ntdll:RtlUserThreadStart
                                  CreateThread
                                  NtQueueApcThread-s
                                  CreateRemoteThread
                                  RtlCreateUserThread
ProcInject_AllocationMethod     - NtMapViewOfSection
bUsesCookies                    - True
HostHeader                      - Host: youthconscience.com

headersToRemove                 - Not Found
DNS_Beaconing                   - Not Found
DNS_get_TypeA                   - Not Found
DNS_get_TypeAAAA                - Not Found
DNS_get_TypeTXT                 - Not Found
DNS_put_metadata                - Not Found
DNS_put_output                  - Not Found
DNS_resolver                    - Not Found
DNS_strategy                    - round-robin
DNS_strategy_rotate_seconds     - -1
DNS_strategy_fail_x             - -1
DNS_strategy_fail_seconds       - -1
Retry_Max_Attempts              - 0
Retry_Increase_Attempts         - 0
Retry_Duration                  - 0
```

4 Bibliographie

[1] DECODER-IT. *Decoder-It/LocalPotato*. 2 mai 2023.
URL : https://github.com/decoder-it/LocalPotato.

[2] Ido SECURITYJOES. « Sockbot in GoLand – Linking APT Groups with Ransomware Gangs ». 9 mars 2022.
URL : https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf.

[3] *Gentilkiwi/Mimikatz: A Little Tool to Play with Windows Security*.
URL : https://github.com/gentilkiwi/mimikatz.

[4] *GhostPack/SharpRoast: DEPRECATED SharpRoast Is a C# Port of Various PowerView's Kerberoasting Functionality.*
URL : https://github.com/GhostPack/SharpRoast.

[5] SPLOITUS. *Exploit for Improper Privilege Management in Microsoft CVE-2021-34527 CVE-2021-1675*.
URL : https://sploitus.com/exploit?id=86F04665-0984-596F-945A-3CA176A53057.

[6] CISA. *BlackCat/ALPHV Ransomware Indicators of Compromise*. 19 avril 2022.
URL : https://www.ic3.gov/Media/News/2022/220420.pdf.

[7] GITHUB. *Threatexpress/Random_c2_profile: Cobalt Strike Random C2 Profile Generator*.
URL : https://github.com/threatexpress/random_c2_profile.

[8] @CRYPTOLAEMUS1. *Cryptolaemus on Twitter*. 11 mars 2022.
URL : https://twitter.com/Cryptolaemus1/status/1502069552246575105.

[9] CISA. *#StopRansomware: Royal Ransomware |*. 2 mars 2023.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a.

[10] MICROSOFT. *Comment Microsoft nomme les acteurs de menace*. 20 avril 2023.
URL : https://learn.microsoft.com/fr-fr/microsoft-365/security/intelligence/microsoft-threat-actor-naming.

[11] MANDIANT. *FIN12 GROUP PROFILE: FIN12 PRIORITIZES SPEED TO DEPLOY RANSOMWARE AGAINST HIGH-VALUE TARGETS*. Octobre 2021.
URL : https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf.

[12] MANDIANT. *FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets*. 10 août 2021.
URL : https://www.mandiant.com/resources/blog/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets.

[13] REUTERS. « Building Wave of Ransomware Attacks Strike U.S. Hospitals ». 29 octobre 2020.
URL : https://www.reuters.com/article/us-usa-healthcare-cyber-idUSKBN27D35U.

[14] Microsoft Defender Threat Intelligence CENTER (MSTIC) Microsoft Threat Intelligence. *Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself*. 9 mai 2022.
URL : https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/.

[15] THE RECORD MEDIA. *Disgruntled ransomware affiliate leaks the Conti gang's technical manuals*. 21 août 2021.
URL : https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals.

[16] TRELLIX. *Conti Leaks: Examining the Panama Papers of Ransomware | Trellix*. 31 mars 2022.
URL : https://www.trellix.com/en-gb/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html.

[17] ADVINTEL. *DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape*. 20 mai 2022.
URL : http://web.archive.org/web/20230208190313/https://www.advintel.io/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike.

[18] GitHub. *TheParmak/Conti-Leaks-Englished: Google and Deepl Translated Conti Leaks, Which Is Shared by a Member of the Conti Ransomware Group.*
URL : https://github.com/TheParmak/conti-leaks-englished.

[19] BushidoToken. *The Continuity of Conti*. 4 avril 2023.
URL : https://blog.bushidotoken.net/2022/11/the-continuity-of-conti.html.

[20] Trend Micro. *Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks*. 21 décembre 2022.
URL : https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html.

[21] AdvIntel. *Vitali Kremez*. 4 avril 2023.
URL : https://twitter.com/VK_Intel/status/1557003350541242369.

[22] Trend Micro. *New Nokoyawa Ransomware Possibly Related to Hive*. 9 mars 2022.
URL : https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html.

[23] Trend Micro. *Play Ransomware Attack Playbook Similar to That of Hive, Nokoyawa*. 6 septembre 2022.
URL : https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html.

18 septembre 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité