TLP:WHITE

LE RANÇONGICIEL RYUK

27/11/2020

TLP:WHITE

Sommaire

1 Contexte

1.1 Origines

Le rançongiciel Ryuk a été observé pour la première fois en août 2018 [1]. C'est une variante du rançongiciel Hermes 2.1, vendu sur le forum souterrain exploit.in à partir de février 2017 par le groupe cybercriminel CryptoTech pour environ 400 dollars [2].

En juin 2018, alors qu'un membre du forum émet des doutes quant au fait que le groupe soit le développeur d'Hermes 2.1, CryptoTech réaffirme être à l'origine du rançongiciel et annonce la diffusion prochaine d'une nouvelle version d'Hermes. Or, aucune nouvelle version d'Hermes, autre que Ryuk, n'est apparue à la suite de cette annonce [3].

A la différence d'Hermes, Ryuk n'a pas été mis en vente sur exploit.in et CryptoTech a cessé ses activités sur le forum après cette annonce [4]. Ainsi, un doute subsiste quant à l'origine de Ryuk.

Commentaire : La disparition de CryptoTech pourrait s'expliquer par un changement de modèle économique, induisant un cercle plus restreint d'utilisateurs de son nouveau rançongiciel Ryuk. L'apparition de Ryuk pourrait également s'expliquer par l'acquisition du code source d'Hermes 2.1 par un autre groupe d'attaquants, qui aurait développé Ryuk sur cette base.

D'après des chercheurs de Deloitte, Ryuk serait vendu comme un *toolkit* à des groupes d'attaquants. Il y aurait donc autant de variantes que de groupes d'attaquants qui achètent le code pour générer leurs binaires [4].

Commentaire : Cette hypothèse ne peut être confirmée par l'ANSSI, qui n'a pas observé la promotion de Ryuk à la manière de celle d'Hermès 2.1 sur des forums souterrains.

Un lien avec le mode opératoire des attaquants (MOA) Bluenoroff, réputé lié à la Corée du Nord, avait été momentanément établi par certains éditeurs du fait de l'utilisation du rançongiciel Hermes au cours de l'attaque contre la Far Eastern International Bank taïwanaise en octobre 2017. Néanmoins, il a été conclu que Bluenoroff avait utilisé Hermes parce qu'il l'avait obtenu sur le *Dark Web*.

1.2 Caractéristiques

Ryuk n'a pas la capacité de se latéraliser automatiquement au sein d'un réseau, d'où la nécessité d'un accès *via* une première charge utile [1] ou d'une latéralisation manuelle.

Ryuk se compose d'un *dropper*, déposant sur le poste de la victime l'une des deux versions d'un module de chiffrement de données (32 ou 64 bit). Le *dropper* exécute ensuite la charge utile. Après quelques minutes d'inactivité, Ryuk cherche alors à arrêter plus de 40 processus et 180 services, notamment ceux liés aux logiciels antivirus, aux bases de données et aux sauvegardes. Il assure sa persistance par la création d'une clé de registre [5].

L'utilisation d'une combinaison de l'algorithme de chiffrement symétrique (AES) et de l'algorithme de chiffrement asymétrique (RSA) permet aussi bien de chiffrer les fichiers que de protéger la clé de chiffrement, rendant les données indéchiffrables par un tiers [5].

Après analyse récursive des disques et partages réseau dans le système infecté puis injection de sa charge malveillante au sein de processus fiables, Ryuk chiffre tous les fichiers, à l'exception de certains fichiers Windows, Mozilla, Chrome et Ahnlab [5].

Commentaire : Ahnlab est une société sud-coréenne d'analyse et de réponse à la menace informatique. La raison de sa présence dans la liste blanche de Ryuk, héritée d'Hermes 2.1, n'est pas clairement établie.

Les navigateurs Internet ainsi que les composants de base du système d'exploitation sont laissés intacts pour permettre aux victimes de lire la demande de rançon, d'acheter des cryptomonnaies et de payer la rançon [6]. Il arrive cependant que Ryuk chiffre des fichiers de base Windows ce qui implique le difficile voire impossible *reboot* des machines compromises [7].

Ryuk ajoute l'extension .RYK aux fichiers chiffrés et dépose le fichier RyukReadMe.txt dans les répertoires chiffrés.

Depuis octobre 2019, Ryuk dispose d'une fonctionnalité lui permettant d'allumer les postes éteints présents sur le réseau local (*Wake-on-LAN*) afin d'accroître sa surface de chiffrement [8].

Il détruit ensuite toutes les copies fantômes présentes sur le systèmes afin d'empêcher l'utilisateur de restaurer son système *via* des commandes vssadmin ou le lancement d'un fichier .bat[1] [9].

Commentaire : il existe un binaire disponible sur GitHub, dénommé Raccine, qui permet d'intercepter le recours à vssadmin par les attaquants et d'empêcher la suppression des copies fantômes [10].

En 2018, le format court de demande de rançon de Ryuk était très similaire à celui du rançongiciel BitPaymer, opéré par le groupe cybercriminel Evil Corp depuis 2017 [4]. Le montant des rançons demandées serait en revanche dix fois supérieur à la moyenne des demandes des autres rançongiciels [11].

Ryuk ne dispose pas de fonctionnalité d'exfiltration de données ni de site Internet dédié à la divulgation des données des victimes, à la différence de beaucoup d'autres rançongiciels. Cependant :

- à la mi-2019, un code malveillant de type *stealer*, présentant des similarités de code avec Ryuk, a été identifié par Malware Hunter Team. Ce code viserait à exfiltrer des fichiers en .docs et .xlsx contenant certains mots clés des champs lexicaux financier, militaire ou encore juridique (”tank”, ”defence”, ”military”, ”classified”, ”federal”, ”finance”, ”IBAN”, ”Swift”, *etc.*). Il serait programmé pour éviter les fichiers relatifs à Ryuk, c'est-à-dire la demande de rançon RyukReadMe.txt ainsi que les fichiers ayant .RYK pour extension [12];
- d'après l'éditeur FireEye [13], il arrive que des attaquants utilisant Ryuk exfiltrent des données de leurs victimes par un autre moyen que le rançongiciel lui-même. Cependant, ces données seraient limitées à des données de reconnaissance interne ou extraites de l'Active Directory, permettant aux attaquants de se latéraliser et d'élever leurs privilèges.

1.3 Victimologie

Ryuk est à l'origine de la compromission de nombreuses entités depuis août 2018, qu'il cible pour leur rentabilité et leur capacité à payer des rançons de montants élevés (*Big Game Hunting*).

Bien qu'aucun ciblage sectoriel spécifique ne puisse être identifié, il apparaît cependant que Ryuk cible particulièrement les États-Unis et le Canada.

En octobre 2020, Ryuk serait responsable de 75% des attaques sur le secteur de la santé [14], secteur qu'il attaquerait depuis le premier semestre 2019.

Selon Prevailion, au 3 novembre 2020, environ 1400 entités communiqueraient avec des serveurs de commande et contrôle (C2) Cobalt Strike associés à UNC1878, l'un des utilisateurs de Ryuk [15]. Ces entités seraient des hôpitaux américains et des agences gouvernementales, des entreprises pharmaceutiques ainsi que des universités dans le reste du monde [14].

[1] Extension d'un fichier de commandes MS-DOS permettant de concevoir des scripts, utilisés ici pour des tâches de maintenance telles que la suppression de fichier.

2 Les chaînes d'infection impliquant Emotet, Trickbot et BazarLoader

2.1 Déroulé des chaînes d'infection initiale

Certaines victimes ont été infectées par TrickBot dès juin 2018, puis compromises par Ryuk à partir d'août [2]. D'après FireEye, la chaîne d'infection TrickBot-Ryuk existerait même depuis décembre 2017 [16].

Commentaire : Cependant, FireEye confirmant que l'apparition publique de Ryuk date d'août 2018, la mention de décembre 2017 suggère qu'il s'agit de la date d'ouverture d'accès par TrickBot, suivi d'un chiffrement par Ryuk à partir d'août 2018.

TrickBot représente depuis le *loader* distribuant le plus Ryuk. TrickBot peut être distribué en amont par le *malware-as-a-service* Emotet. Les chaînes d'infection Emotet-TrickBot-Ryuk et TrickBot-Ryuk ont ainsi couramment été rencontrées, et perdurent au moins jusqu'à septembre en 2020.

Le vecteur d'infection apparaît généralement être un courriel d'hameçonnage délivrant soit Emotet [16], soit TrickBot [17].

Une fois que des outils légitimes de post exploitation sont distribués par TrickBot (Cobalt Strike, Empire, Bloodhound, Mimikatz, Lazagne), les attaquants obtiennent des accès privilégiés à un contrôleur de domaine et déploient Ryuk (par exemple *via* PsExec) au sein du système d'information (SI) de la victime [18].

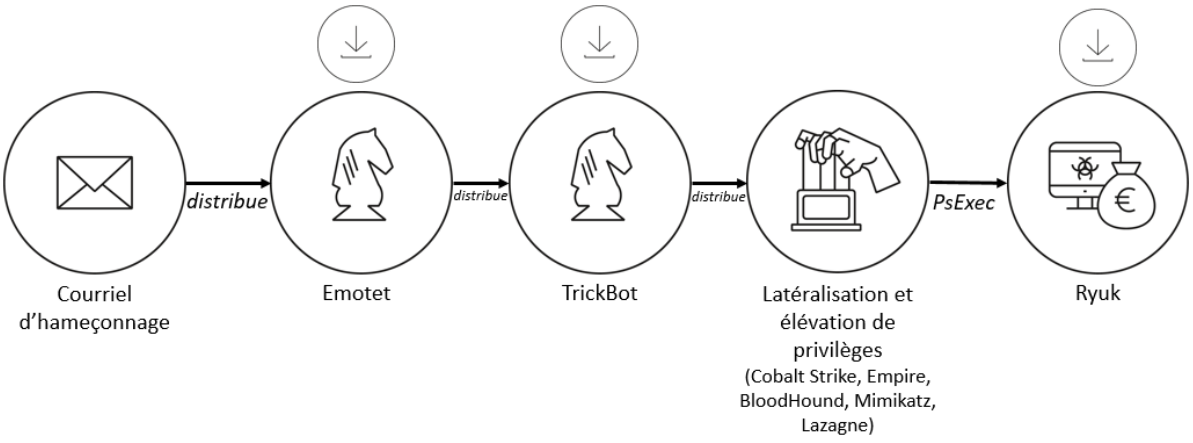

Fig. 2.1 : Déroulé simplifié de la chaîne d'infection Emotet-TrickBot-Ryuk

2.2 Evolution vers la chaîne d'infection Bazar-Ryuk

En mars 2020, les chaînes d'infection impliquant TrickBot auraient été moins nombreuses, voire auraient momentanément cessé. En juillet 2020, la chaîne d'infection Emotet-TrickBot émerge de nouveau, après plusieurs mois d'inactivité d'Emotet. Cette chaîne distribue alors alternativement les rançongiciels Ryuk et Conti [19].

A partir de mi-septembre 2020, la chaîne d'infection BazarLoader-Ryuk semble remplacer les chaînes d'infection impliquant TrickBot.

BazarLoader est généralement distribué par des campagnes d'hameçonnage. Les courriels peuvent être envoyés en utilisant la plateforme de marketing Sendgrid. Ils contiennent des liens pointant vers des pages Google Docs d'aperçus de documents, qui incitent la victime à télécharger le fichier, l'aperçu ne fonctionnant généralement pas [20, 21,

22]. De récentes campagnes identifiées par FireEye [13] n'utilisent plus la plateforme Sengrid mais l'infrastructure des attaquants ou des serveurs de messagerie compromis, pour envoyer des courriels d'hameçonnage contenant des liens vers des documents. Ces documents incluent parfois des références à l'entité pour laquelle travaille la cible. Les fichiers en question sont des exécutables signés avec des certificats révoqués, hébergés sur des services Web légitimes (Google Drive, Basecamp, Slack, Trello, Yougile, JetBrains) [13].

Une fois le SI compromis, BazarLoader télécharge depuis le serveur C2[2] une charge utile (chiffrée en XOR) : BazarBackdoor. La porte dérobée télécharge et exécute ensuite des charges de post-exploitation du type Cobalt Strike, Metasploit, Empire, Anchor, PowerTrick[3] [13], BloodHound, Powersploit et ADFind [25]. Des données de reconnaissance (notamment récupérées *via* ADFind) sont exfiltrées *via* FTP [25].

L'élévation de privilèges est réalisée à l'aide de Mimikatz, de Rubeus[4] [13] ou encore de l'exploitation d'une vulnérabilité Zerologon (CVE-2020-1472) [26].

BazarBackdoor, bien que non exclusivement dédiée à cette fin, peut être utilisée pour distribuer le rançongiciel Ryuk.

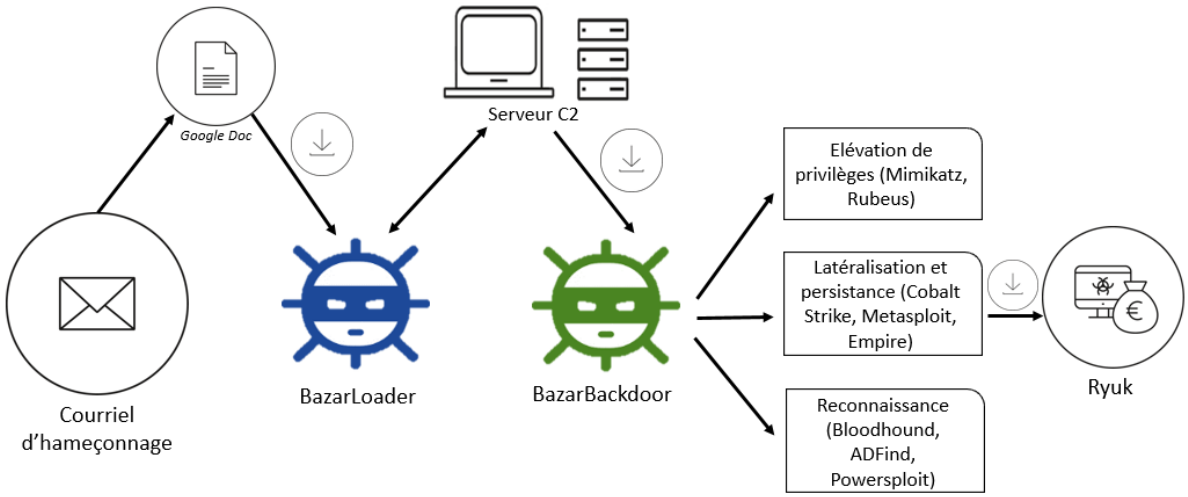

Fig. 2.2 : Déroulé simplifié de la chaîne d'infection Bazar-Ryuk

2.3 Les groupes d'attaquants impliqués

2.3.1 Wizard Spider

Origines

Le groupe opérant le code malveillant TrickBot est dénommé Wizard Spider par l'éditeur Crowdstrike et "the TrickBot gang" par d'autres éditeurs. Il serait aussi à l'origine de la porte dérobée Anchor et de PowerTrick.

Ce groupe comprendrait des membres du groupe Gold BlackBurn, développeurs et opérateurs du cheval de Troie bancaire Dyre [27], qui a cessé ses activités en novembre 2015 suite à une action de la police russe.

Dyre a émergé en juin 2014. Ses particularités étaient les suivantes :

- Dyre aurait disposé du même développeur que Gozi Neverquest (alias Vawtrak) [28]. Gozi Neverquest était basé sur le code source du code malveillant Gozi, qui a fuité en 2010. Le groupe cybercriminel qui l'a déve-

[2] BazarLoader utilise des domaines en .bazar d'EmerDNS pour ses C2. Cela permet l'enregistrement de noms de domaine décentralisé sur une blockchain [23]. Les résolutions DNS des serveurs C2 de Bazar rendent ainsi impossibles le démantèlement et les *sinkholing* [24].
[3] Framework de post-exploitation.
[4] Module Kerberos de Mimikatz.

loppé, Gold Swathmore, est réputé avoir collaboré avec Gold BlackBurn. Cette collaboration se serait poursuivie après l'arrestation de membres de Gold BlackBurn en 2015 et de celle du leader de Gold Swathmore en 2017, au travers de leurs successeurs respectifs Wizard Spider et Lunar Spider [29];

- certaines attaques impliquant Dyre pourraient être connectées au groupe cybercriminel Business Club. Il est alors possible qu'à partir de 2014, ce groupe ait diversifié son activité, en utilisant Dyre pour dérober de l'argent depuis des comptes bancaires de grandes entreprises, et Dridex pour voler de l'argent depuis des comptes bancaires du secteur de la vente (Evil Corp) [28]. Dyre a émergé, tout comme Dridex, deux semaines après le démantèlement du botnet GameOverZeuS, opéré par M. Bogatchev, développeur du cheval de Troie bancaire ZeuS, et le groupe cybercrimel Business Club.

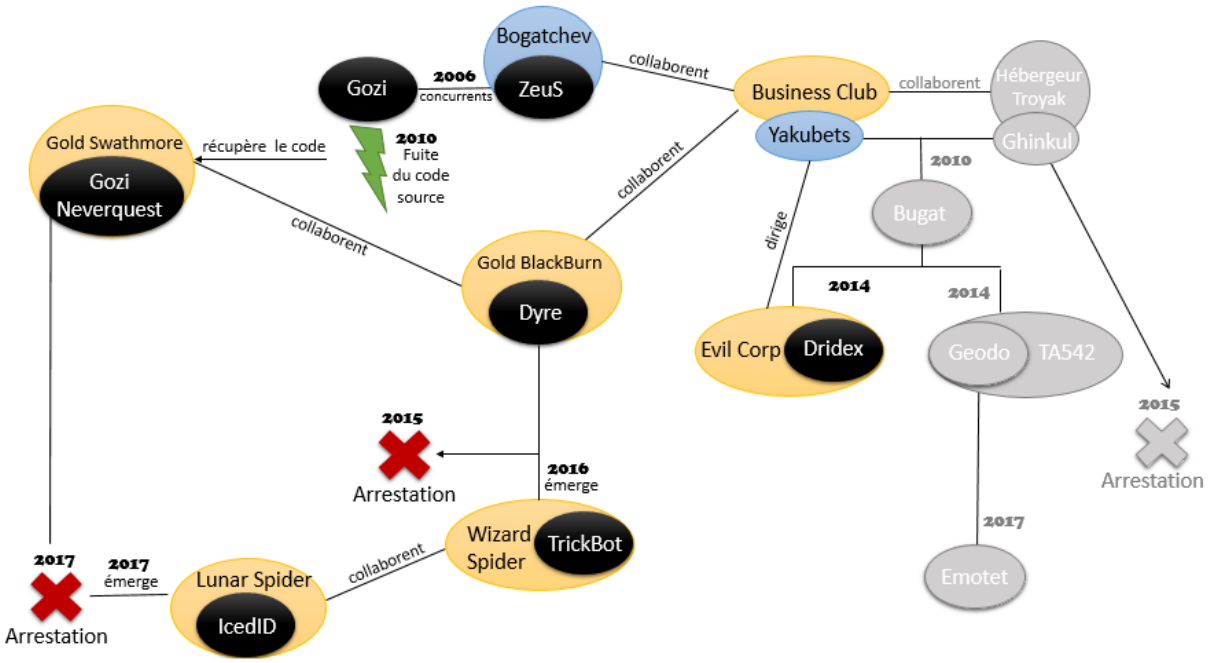

Fig. 2.3 : Origines de Wizard Spider

Le cheval de Troie bancaire et *loader* TrickBot

TrickBot, apparu un an après le démantèlement de Dyre, est opéré sur la base d'un modèle d'affiliés, impliquant sa distribution par des groupes indépendants [30]. Bien que les affiliés de TrickBot ne soient pas identifiables, les campagnes impliquant TrickBot se différencient par leur vecteur d'infection et un paramètre dans lequel il est codé en dur : le *Group Tag* ou Gtag [31].

Les différents Gtags associés aux chaînes d'infection TrickBot-Ryuk sont au minimum :

- "serXXX" (ser0918us par exemple) [18];
- "libXXX", "totXXX" et "jimXXX" : plusieurs Gtags peuvent cohabiter sur un même SI infecté ; c'est par exemple le cas des Gtags "libXXX", "totXXX" et "jimXXX" (373 et 369 ou encore 371) qui peuvent ainsi être retrouvés à la suite d'un Gtag "serXXX" et/ou d'un courriel d'hameçonnage [16, 18];
- "morXXX" : c'est le Gtag associé aux primo-infections par Emotet depuis septembre 2019 (mor 84 [32] ou mor114 [33] par exemple).

  Commentaire : Néanmoins, Ryuk étant actif depuis au moins août 2018, et déjà distribué en tant que charge finale de la chaîne d'infection Emotet-TrickBot, d'autres Gtags que les morXXX ont participé à des attaques par ce rançongiciel sans qu'il ne puisse être identifié si ces attaques, perpétuées depuis maintenant plus de deux ans, sont le fait d'un unique groupe d'attaquants, ou de plusieurs qui auraient vu leur Gtag évoluer.

Le *loader* BazarLoader et la porte dérobée BazarBackdoor

Wizard Spider aurait commencé à distribuer les codes malveillants BazarLoader et BazarBackdoor en mars 2020 [30]. Plusieurs éléments techniques suggèrent qu'il en serait le développeur :

- utilisation du même *crypter* par TrickBot et BazarBackdoor et de routines de déchiffrement très similaires entre les *loaders* Bazar et TrickBot (utilisation des mêmes WinAPIs, *custom* RC4, *API-hammering*) ;
- utilisation par Anchor et Bazar de la résolution DNS Emercoin pour les communications C2 ;
- réutilisation de domaines compromis, par exemple machunion[.]com, bakedbuns[.]com et ruths-brownies[.]com, qui ont par le passé hébergé TrickBot puis plus récemment BazarLoader.

Bazar serait, tout comme TrickBot, utilisé comme *access-as-a-service* pour compromettre voire qualifier un SI pour le compte d'autres groupes d'attaquants. Il n'est pas connu si BazarLoader fonctionne, là aussi tout comme TrickBot, également sur un modèle d'affiliés.

Commentaire : TrickBot et Bazar sont régulièrement utilisés pour distribuer Ryuk. Cependant, il n'est pas possible pour l'ANSSI de déterminer si ces attaques, ou certaines d'entre elles, sont le fait de Wizard Spider, d'affiliés de TrickBot, de clients de Bazar, ou d'un opérateur final de Ryuk qui ferait appel à des attaquants spécialisés dans l'access-as-a-service ou achèterait des accès compromis ou qualifiés sur le Dark Web.

2.3.2 UNC1878

UNC1878, alias One group [34], est un *cluster* d'activité, découvert par FireEye fin janvier 2020, et impliqué dans des chaînes d'infection TrickBot-Ryuk depuis janvier 2020, puis dans des chaînes d'infection Bazar-Ryuk à partir de septembre 2020. UNC1878 ne correspondrait pas exactement à Wizard Spider [35, 36].

Son ciblage est indiscrimé, et ses infections sont opportunistes [35, 36]. Elles sont caractérisées par :

- leur vecteur d'infection qui repose sur des courriels d'hameçonnage contenant généralement des liens ;
- leur rapidité d'exécution, le délai entre l'infection initiale et le chiffrement s'étant récemment réduit de quelques jours (2 à 5) à trois heures [25] ;
- l'utilisation constante d'échantillons Cobalt Strike auto-signés [35] ;
- l'utilisation d'outils légitimes tout au long de la chaîne d'infection post-compromission (Cobalt Strike Beacon, Empire, Meterpreter, Mimikatz, Lazagne, Kerbrute, Kerberoast, Bloodhound, ADFind, Powersploit) [35] ;
- l'absence d'exfiltration d'informations depuis le SI de ses victimes [35].

D'après FireEye, un cinquième des intrusions liées à des rançongiciels en 2020 sont dues à Ryuk. 83% d'entre elles sont le fait d'UNC1878, parmi lesquelles 27% ont été un succès [35].

UNC1878 ne serait donc pas responsable de toutes les attaques impliquant le rançongiciel Ryuk, ni même des codes TrickBot et Bazar [37], mais serait en revanche bien à l'origine des attaques à l'encontre d'hôpitaux américains depuis octobre 2020 [35].

Commentaire : UNC1878 pourrait s'appuyer sur différents affiliés de TrickBot ou différents attaquants ayant accès à BazarLoader dans l'ouverture d'accès à ses victimes. Il pourrait lui-même être un affilié/client de ces deux loaders, mais cela n'expliquerait pas pourquoi différents Gtags pourraient être rencontrés au cours d'infections TrickBot-Ryuk alors qu'il est communément admis que chaque Gtag (au moins le préfixe composé de lettres) correspond à un affilié.

3 Autres chaînes d'infection identifiées et groupes d'attaquants associés

Emotet-TrickBot-Ryuk, TrickBot-Ryuk et Bazar-Ryuk ne sont pas les uniques chaînes d'infection aboutissant ou ayant abouti par le passé au déploiement du rançongiciel Ryuk.

3.1 Buer et SilentNight

D'après l'éditeur Sophos, Ryuk aurait été distribué par Buer loader en septembre 2020 [38]. Buer est un *malware-as-a-service* utilisé pour distribuer des chevaux de Troie bancaires et des rançongiciels. Il est proposé sur le *Dark Web* pour 350 dollars. Les *droppers* Buer loader et Ryuk utilisent le même *shellcode loader* pour injecter le code malveillant décompressé en mémoire [38]. Enfin, Buer aurait déjà distribué TrickBot [20], sans que la chaîne d'infection Buer-TrickBot-Ryuk ne puisse être identifiée.

SilentNight est également impliqué dans des attaques visant à distribuer le rançongiciel Ryuk. Ce cheval de Troie, vendu sur des forums russophones souterrains depuis fin 2019, est une variante du code malveillant Zloader (issu du code source de ZeuS) dont la dernière activité remonte à 2018 [39].

Ces deux codes malveillants, de même que BazarLoader, ont été observés distribués par des courriels d'hameçonnage envoyés *via* Sengrid puis au travers d'un hébergeur russe, et pointant vers des Google Docs malveillants [38].

Commentaire : Un même utilisateur de Ryuk pourrait par exemple utiliser ces trois services de distribution pour mener à bien ses attaques.

3.2 Chaîne d'infection impliquant le groupe cybercriminel FIN6

3.2.1 Implication de FIN6 ou d'acteurs qui lui sont affiliés dans des incidents Ryuk

L'implication du groupe cybercriminel russophone FIN6, ou des acteurs qui lui sont affiliés, dans des incidents Ryuk remonterait à juillet 2018 d'après FireEye [40, 4].

Actif depuis 2015, FIN6 ciblait traditionnellement les terminaux de points de vente (TPV) et les serveurs de paiement d'eCommerce, à des fins d'exfiltration et de revente de données bancaires. A partir de la mi-2018, des éléments techniques et opérationnels suggèrent que FIN6 ou des acteurs qui lui sont affiliés distribuaient les rançongiciels Ryuk et LockerGoga (apparu en janvier 2019).

L'éditeur Morphisec [41] a fait état d'intrusions menées début 2019, en Inde, au Japon et aux États-Unis, dans les systèmes de TPV des secteurs de la finance et de la santé, au moyen de Cobalt Strike et du code malveillant FrameworkPOS. D'après l'éditeur, cette campagne pourrait être attribuée à FIN6 du fait de TTPs similaires.

Sur la base d'analyses menées aussi bien par l'ANSSI que par ses partenaires, deux IOCs retrouvés au cours de cette campagne ciblant les TPV, les adresses IP 185.202.174.91 et 93.115.26.171, sont communs à des incidents traités par l'ANSSI impliquant les rançongiciels Ryuk et LockerGoga. Ainsi :

- L'analyse par l'ANSSI de l'infrastructure de commande et de contrôle liée à LockerGoga a permis de retrouver l'adresse IP 185.202.174.91, comme téléchargeant des charges utiles Metasploit ou liées au *framework* d'attaque Empire :

Adresse IP	AS	Nom AS	Pays AS	CIDR	Nom CIDR	Pays CIDR
185.202.174.91	174	COGENT-174- Cogent Communications	US	185.202.174.0/24	H129	Canada

- L'adresse IP 93.115.26.171 a également été retrouvée lors de ces investigations, téléchargeant aussi une charge utile sur la machine compromise. Elle se retrouve lors d'un incident LockerGoga et d'un incident Ryuk traités

par l'ANSSI.

Adresse IP	AS	Nom AS	Pays AS	CIDR	Nom CIDR	Pays CIDR
93.115.26.171	16125	CHERRYSERVERS1-AS	LT	93.115.26.0/24	CHERRYSERVERS-LT-DEDICATED	Lithuania

Les liens techniques identifiés, ici non exhaustifs, appuient l'hypothèse de FireEye selon laquelle des acteurs affiliés à FIN6 ont participé à des attaques mettant en œuvre les rançongiciels Ryuk et LockerGoga.

Le vecteur d'infection constaté lors des incidents traités par l'ANSSI est également le même que celui identifié par FireEye : les attaquants auraient compromis leurs cibles *via* l'exploitation d'un service exposé sur Internet. Après la compromission initiale, ils auraient utilisé des couples identifiants/authentifiants dérobés pour se latéraliser au moyen du protocole RDP [40].

Commentaire : Il est cependant difficile de savoir si FIN6 a été l'opérateur final des rançongiciels LockerGoga et Ryuk lors de ces chaînes d'infection ou un attaquant intermédiaire chargé par l'opérateur final de qualifier l'accès au SI.

3.2.2 Liens supposés entre FIN6 et Wizard Spider

D'après IBM [42], FIN6 et Wizard Spider collaboreraient. Les raisons à l'appui de cette hypothèse sont les suivantes :

- fin 2019-début 2020, TrickBot et la porte dérobée Anchor ont été utilisés au cours d'intrusions au sein d'entreprises, dont certaines disposaient de TPV, intrusions présentant des similitudes avec le mode opératoire traditionnel de FIN6 ;
- il a été constaté qu'au cours de chaînes d'infection impliquant PowerTrick et Anchor, TerraLoader avait installé la porte dérobée More_Eggs[5], dont FIN6 est l'un des principaux utilisateurs (avec le groupe cybercriminel Cobalt Gang). De plus, les attaquants auraient utilisé PowerShell pour télécharger et exécuter TerraLoader, chargé à son tour d'installer More_Eggs, méthode spécifique à FIN6 d'après IBM ;
- la *Rkey* de l'un des échantillons contenait la mention "wearenotcobaltthanks", message similaire à d'autres trouvés dans des échantillons More_Eggs attribués à FIN6 ("We are not cobalt gang, stop associating us with such skids !").

Commentaire : Etant donné que FIN6 semble avoir utilisé les services d'accès de Wizard Spider, il est possible d'envisager qu'il les ait également utilisés pour distribuer Ryuk. Cependant, cela n'expliquerait pas pourquoi TrickBot a distribué Ryuk mais jamais LockerGoga alors que FIN6 aurait distribué ces deux rançongiciels ainsi que MegaCortex et Maze.

3.3 Liens entre Ryuk et le rançongiciel Conti

Apparu en décembre 2019 [43], le rançongiciel Conti serait mis à la disposition d'affiliés selon le modèle de *ransomware-as-a-service* (RaaS). Il a notamment été déployé en parallèle de Ryuk au cours de chaînes d'infection Emotet-TrickBot-Ryuk/Conti ou BazarLoader-Ryuk/Conti.

De plus, FireEye a observé des intrusions impliquant la porte dérobée Anchor et la distribution des rançongiciels Conti et Maze [13]. Conti, qui, à la différence de Ryuk, dispose d'un site dédié de divulgations de données dérobées aux victimes, a même publié les données de deux victimes listées sur le site de divulgations de Maze.

Commentaire : les similarités de codes et de message de demande de rançon ainsi que la distribution par TrickBot, suggèrent que Conti a pu être créé par les développeurs de Ryuk. Cependant, aucun lien ne semble exister entre Ryuk et Maze alors que Maze a aussi été distribué par TrickBot. Ainsi, il est possible qu'un même utilisateur de Ryuk et de Conti utilise le service de distribution de TrickBot ou en soit affilié.

[5] Alias SpicyOmelette et Skid, More_Eggs est une porte dérobée Javascript mise à disposition de certains affiliés par le prestataire en *malware-as-a-service* Venom Spider (alias badbullzvenom), actif depuis 2012.

4 Conclusion

Ryuk n'est pas officiellement un RaaS. Cependant, il apparaît que plusieurs attaquants différents sont impliqués dans des chaînes d'infection aboutissant au déploiement de Ryuk. Plusieurs arguments pèsent en faveur de cette hypothèse :

- Le kit Hermès vendu sur le *Dark Web* ne contenait pas d'outil d'exploitation, obligeant ses acheteurs à compromettre les victimes par leurs propres moyens ou ceux d'un intermédiaire. Ce pourrait être le même cas de figure pour Ryuk . Parmi les intermédiaires potentiellement employés se trouveraient notamment TrickBot, Bazar, Buer et SilentNight. Ces *loaders* seraient utilisés par l'opérateur final de Ryuk ou par des attaquants chargés de lui ouvrir des accès ;
- FIN6 ou des acteurs qui lui sont affiliés auraient manifestement été impliqués dans des incidents Ryuk en 2019 lors desquels aucune charge intermédiaire du type des *loaders* précédents n'a été observée ;
- Les différentes demandes de rançon Ryuk suggèrent selon MalwareBytes qu'il pourrait y avoir plus d'un groupe ayant accès au rançongiciel [44] ;
- D'après FireEye, UNC1878 est responsable de 83% des infections Ryuk en 2020 et n'exfiltrerait pas d'informations hormis celle de reconnaissance interne depuis le SI de ses victimes, à la différence d'autres opérateurs de Ryuk [35].

Au vu de ces éléments et de l'utilisation exclusive d'outils légitimes de post-compromission au cours des chaînes d'infection aboutissant au déploiement de Ryuk, empêchant l'identification de TTPs distinctes, il est envisageable :

- qu'un unique opérateur de Ryuk mette le rançongiciel à disposition de partenaires de confiance. Les partenaires de confiance auraient alors la possibilité de distribuer Ryuk *via* les services de distribution de Wizard Spider (TrickBot et Bazar) ou par leurs propres moyens. Cette hypothèse pourrait être renforcée par la collaboration qui existerait entre FIN6 et Wizard Spider ;
- que plusieurs acteurs malveillants utilisent Ryuk (dont FIN6 en 2019) de manière indépendante, et qu'un ou plusieurs d'entre eux soient affiliés de TrickBot ou au moins client de son service de distribution et/ou de celui de Bazar (dont UNC1878) ;
- qu'un unique opérateur de Ryuk fasse appel à différents services de distribution (TrickBot, Bazar, Buer, SilentNight) ou à un ou plusieurs *hacker-for-hire* (dont FIN6 pourrait faire partie), ce qui expliquerait les différences de TTPs entre incidents aboutissant au chiffrement par Ryuk.

Ryuk demeure un rançongiciel particulièrement actif au cours du second semestre 2020. Il se distingue de la majorité des autres rançongiciels par le fait qu'au moins l'un de ses opérateurs a attaqué des hôpitaux en période de pandémie, par l'absence de site dédié de divulgations de données et par l'extrême rapidité d'exécution (de l'ordre de quelques heures) de la chaîne d'infection Bazar-Ryuk.

5 Bibliographie

[1] NCSC-UK. *Advisory : Ryuk Ransomware Targeting Organisations Globally*. 22 juin 2019.

[2] Kivu Threat Intelligence. *Kivu Myth Busters : Ryuk vs. North Korea*. 1er fév. 2019. URL : https://kivuconsulting.com/kivu-myth-busters-ryuk-vs-north-korea/.

[3] Xakep. *Operators of the New Ransomware Ryuk Have Already Earned over $640,000*. 22 août 2018. URL : https://xakep.ru.

[4] Virus Bulletin. *The Long Tail of the Ryuk Malware*. 1er jan. 2019. URL : https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-shinigamis-revenge-long-tail-ryuk-malware/.

[5] CERT Nazionale Italia. *Il Nuovo Ransomware Ryuk Diffuso in Attacchi Mirati*. 23 août 2018. URL : https://www.certnazionale.it/news/2018/08/23/il-nuovo-ransomware-ryuk-diffuso-in-attacchi-mirati/.

[6] Sophos. *After SamSam, Ryuk Shows Targeted Ransomware Is Still Evolving*. 18 déc. 2018. URL : https://nakedsecurity.sophos.com/2018/12/18/after-samsam-ryuk-shows-targeted-ransomware-is-still-evolving/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29.

[7] Red Canary. *Detecting Ryuk Ransomware*. 1er fév. 2020. URL : https://redcanary.com/blog/ryuk-ransomware-attack/.

[8] Crowdstrike. *WIZARD SPIDER Adds New Features to Ryuk*. 1er nov. 2019.

[9] Bank Info Security. *Alert : « Ryuk » Ransomware Attacks the Latest Threat*. 7 sept. 2018. URL : https://www.bankinfosecurity.com/alert-ryuk-ransomware-attacks-latest-threat-a-11475.

[10] Github. *Raccine*. 1er jan. 2020. URL : https://github.com/Neo23x0/Raccine.

[11] Coveware. *Ryuk Ransomware Recovery, Payment & Decryption Statistics*. URL : https://www.coveware.com/ryuk-ransomware.

[12] Bleeping Computer. *Ryuk Related Malware Steals Confidential Military, Financial Files*. 11 sept. 2019. URL : https://www.bleepingcomputer.com/news/security/ryuk-related-malware-steals-confidential-military-financial-files/.

[13] FireEye. *Unhappy Hour Special : KEGTAP and SINGLEMALT With a Ransomware Chaser*. 28 oct. 2020.

[14] Bloomberg. *Hackers Bearing Down on U.S. Hospitals Have More Attacks Planned*. 30 oct. 2020. URL : https://www.bloomberg.com/news/articles/2020-10-30/hackers-bearing-down-on-u-s-hospitals-have-more-attacks-planned.

[15] Prevailion. *On the Trail of UNC1878*. 3 nov. 2020. URL : https://www.prevailion.com/on-the-trail-of-unc1878/.

[16] FireEye. *A Nasty Trick : From Credential Theft Malware to Business Disruption*. 11 jan. 2019. URL : https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html.

[17] ANSSI. *Le Malware-as-a-Service Emotet*. 29 oct. 2020.

[18] Intel 471. *Understanding the Relationship between Emotet, TrickBot and Ryuk*. 14 avr. 2020.

[19] Bleeping Computer. *Emotet-TrickBot Malware Duo Is Back Infecting Windows Machines*. 20 juil. 2020. URL : https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/.

[20] AT&T cybersecurity. *TrickBot BazarLoader In-Depth*. 19 mai 2020. URL : https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth.

[21] The DFIR Report. *Ryuk's Return*. 8 oct. 2020. URL : https://thedfirreport.com/2020/10/08/ryuks-return/.

[22] Cybereason. *A Bazar of Tricks : Following Team9's Development Cycles*. 16 juil. 2020. URL : https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles.

[23] Medium. *5 Features Making EmerDNS the Only Truly Decentralized DNS*. 20 fév. 2020. URL : https://medium.com/@emer.tech/5-features-making-emerdns-the-only-truly-decentralized-dns-4c513bb13850.

[24] ADVANCED-INTEL. *"Front Door" into BazarBackdoor : Stealthy Cybercrime Weapon*. 13 oct. 2020. URL : https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon.

[25] THE DFIR REPORT. *Ryuk Speed Run, 2 Hours to Ransom*. 5 nov. 2020. URL : https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/.

[26] BLEEPING COMPUTER. *Hacking Group Is Targeting US Hospitals with Ryuk Ransomware*. 29 oct. 2020. URL : https://www.bleepingcomputer.com/news/security/hacking-group-is-targeting-us-hospitals-with-ryuk-ransomware/.

[27] CROWDSTRIKE. *"Sin"-Ful SPIDERS : WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web*. 15 fév. 2019. URL : https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/.

[28] DELL SECUREWORKS. *Evolution of the GOLD EVERGREEN Threat Group*. 15 mai 2017. URL : https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

[29] DELL SECUREWORKS. *Gold Swathmore*. URL : https://www.secureworks.com/research/threat-profiles/gold-swathmore.

[30] DELL SECUREWORKS. *Gold Blackburn*. URL : https://www.secureworks.com/research/threat-profiles/gold-blackburn.

[31] SANS INTERNET STORM CENTER. *InfoSec Handlers Diary Blog - Trickbot*. 11 déc. 2019. URL : https://isc.sans.edu/diary.html?storyid=25594.

[32] SANS INTERNET STORM CENTER. *Emotet Epoch 1 Infection with Trickbot Gtag Mor84*. 28 jan. 2020. URL : https://isc.sans.edu/forums/diary/25752/.

[33] TWITTER. *@cryptolaemus1*. 26 août 2020. URL : https://twitter.com/GossiTheDog/status/1298486442159677440.

[34] ADVINTEL. *Anatomy of Attack : Inside BazarBackdoor to Ryuk Ransomware "One" Group via Cobalt Strike*. 6 nov. 2020. URL : https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike.

[35] FIREEYE. *STAR Webcast : Spooky RYUKy : The Return of UNC1878*. 28 oct. 2020. URL : https://www.youtube.com/watch?v=BhjQ6zsCVSc.

[36] FIREEYE. "It's Your Money and They Want It Now — The Cycle of Adversary Pursuit". 31 mar. 2020. In : (31 mar. 2020).

[37] TWITTER. *@anthomsec*. 29 oct. 2020. URL : https://twitter.com/anthomsec.

[38] SOPHOS. *Hacks for Sale : Inside the Buer Loader Malware-as-a-Service*. 28 oct. 2020. URL : https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/.

[39] INFOSEC INSTITUTE. *ZLoader : What It Is, How It Works and How to Prevent It*. 19 août 2020. URL : https://resources.infosecinstitute.com/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/.

[40] FIREEYE. *Pick-Six : Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware*. 5 avr. 2019. URL : https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html.

[41] MORPHISEC. *New Global Attack on Point of Sale Systems-FIN6*. 27 fév. 2019. URL : http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems.

[42] SECURITY INTELLIGENCE. *ITG08 (Aka FIN6) Partners with TrickBot Gang, Uses Anchor Framework*. 7 avr. 2020. URL : https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/.

[43] BLEEPING COMPUTER. *Conti Ransomware Shows Signs of Being Ryuk's Successor*. 9 juil. 2020. URL : https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/.

[44] MALWAREBYTES LABS. *The Curious Case of Ryuk Ransomware*. 12 déc. 2019. URL : https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/.

- 27/11/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN