INFORMATIONS CONCERNANT LES RANÇONGICIELS LOCKERGOGA ET RYUK

NOUVELLE CAMPAGNE D'ATTAQUES ET INDICATEURS TECHNIQUES

Version 1.0

26/03/2019

Sommaire

1 Contexte **3**

2 Investigation **3**
2.1 Échantillon de départ 3
2.2 Échantillons partageant le même certificat 4
2.3 Nouvelle famille de codes malveillants nommée LockerGoga 5
2.4 Script DOS 5
2.5 Infrastructure 5
2.6 Mode opératoire 6

3 Liens avec des modes opératoires d'attaques **7**
3.1 Script DOS 7
3.2 Message de rançon 7
3.3 Grim Spider 8

4 Indicateurs de compromission **9**
4.1 Infrastructure de l'attaquant 9
4.1.1 Adresses IP de serveurs de commande et de contrôle 9
4.1.2 Adresses IP d'administration des serveurs 9
4.2 URL permettant de récupérer du code malveillant 11
4.3 Indicateurs système 11
4.4 Charges malveillantes 11
4.5 Autres indicateurs 11

5 Sources **13**

1 Contexte

L'ANSSI a observé depuis maintenant plusieurs mois des campagnes d'attaques dans lesquelles des rançongiciels nommés « LockerGoga » et « Ryuk » sont déposés sur les systèmes d'information des victimes. Afin de prévenir de futures compromissions et de permettre aux acteurs des chaînes SSI de rechercher cette menace, ce bulletin contient, entre autres, des indicateurs techniques découverts durant les analyses de l'agence.

Les informations présentes dans ce document apportent à la fois des éléments supplémentaires sur ces rançongiciels et détaillent une partie des investigations menées à partir de données internes et externes à la disposition de l'ANSSI.

2 Investigation

2.1 Échantillon de départ

Le 25 janvier 2019, un condensat présent sur VirusTotal a fait l'objet de plusieurs *tweets* le présentant comme un rançongiciel ayant été utilisé dans de récentes attaques :

Condensats	Première vue VT
52340664fe59e030790c48b66924b5bd 73171ffa6dfee5f9264e3d20a1b6926ec1b60897 bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f	2019-01-24 (UTC)

Il s'agit en effet d'un rançongiciel qui, pour chaque fichier, génère une clé de 128 bits et chiffre son contenu en AES avec le mode CTR. La clé de chiffrement, la valeur initiale du compteur ainsi que la taille du fichier original sont ensuite concaténées et chiffrées en RSA-OAEP avec la clé publique de 1024 bits codée en dur dans l'échantillon. Le résultat est ajouté à la fin du fichier chiffré.

Aucune capacité de latéralisation n'a été découverte durant l'analyse de l'échantillon.

Cet échantillon crée un fichier nommé « README-NOW.txt » contenant le message de rançon ci-dessous :

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

To get information on the price of the decoder contact us at:
CottleAkela@protonmail.com;QyavauZehyco1994@o2.pl
The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security
```

De plus, l'échantillon est signé à l'aide d'un certificat appartenant à une société nommée MIKL LIMITED.

2.2 Échantillons partageant le même certificat

Quatre échantillons étant signés par le même certificat ont été découverts :

Condensats	Première vue VT
164f72dfb729ca1e15f99d456b7cf811 f92339e73c7e901c0c852d8e65615cfb588a4ff6 8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29	2019-01-25 (UTC)
9cad8641ac79688e09c5fa350aef2094 3da0a217bbda09561780f52f163a6aafeb721d60 5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c	2019-01-17 (UTC)
3ebca21b1d4e2f482b3eda6634e89211 37cdd1e3225f8da596dc13779e902d8d13637360 6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77	2019-01-25 (UTC)
a5bc1f94e7505a2e73c866551f7996f9 7dea7ff735023418b902d093964028aefbc486a5 14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca	2019-02-06 (UTC)

L'échantillon « `5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c` » contient en chaînes de caractères deux adresses courriel, « `AbbsChevis@protonmail.com` » et « `IjuqodiSunovib98@o2.pl` ». Il s'agit très certainement de deux adresses de contact utilisées pour la demande de rançon.

Une analyse des trois premiers échantillons a montré qu'ils sont similaires à l'échantillon de départ mais possèdent des clés publiques RSA différentes. Le quatrième échantillon n'a pour le moment pas été analysé.

De plus, un cinquième échantillon, non signé par le certificat, mais possédant le même « `imphash` » (« `c226ac4bab6f48634bacbb7a1d34f8f6` ») que l'échantillon de départ a été trouvé :

Condensats	Première vue VT
a1d732aa27e1ca2ae45a189451419ed5 50f5a5ec13d21d4df119140547d63bc40f93b079 c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a	2019-01-27 (UTC)

Une analyse de ce cinquième échantillon montre également un code similaire aux trois autres, avec une clé RSA différente.

Deux échantillons partageant des similarités avec les échantillons signés à l'aide du certificat MIKL LIMITED ont aussi été identifiés. Les caractéristiques de ces échantillons sont présentes ci-dessous :

Condensats	Première vue VT
b3d3da12ca3b9efd042953caa6c3b8cd 34fb03a35e723d27e99776ed3e81967229b3afe1 7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125	2019-02-08 (UTC)
faf4de4e1c5d8e4241088c90cfe8eddd fcd241fdcd462199f2907ca34c73ce9c89b03e5f 47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4	2019-02-05 (UTC)

Ces deux échantillons contiennent toujours un couple d'adresses courriel enregistrées chez « `protonmail.com` » et « `o2.pl` ». Le premier échantillon du tableau utilise les adresses courriel « `RomanchukEyla@protonmail.com` » et « `CouwetIzotofo@o2.pl` », le second les adresses courriel « `PhanthavongsaNeveyah@protonmail.com` » et « `AperywsQaroci@o2.pl` ».

D'après les chaînes de caractères des deux fichiers, le fichier réclamant la rançon semble avoir changé de nom (devenu « `READ-ME-NOW.txt` »), le chemin utilisé pour compiler ces deux échantillons a également été modifié (désormais « `E:\goga\` »), faisant référence au nom de la famille de code **LockerGoga**.

Ces deux échantillons sont signés avec un certificat appartenant à la société KITTY'S LTD. Celui-ci, valide du 1er février 2019 au 1er février 2020, est signé par l'autorité de certification SECTIGO.

2.3 Nouvelle famille de codes malveillants nommée LockerGoga

Le 27 janvier 2019, un chercheur de l'éditeur KASPERSKY publie un *tweet* contenant trois condensats nommés LockerGoga. Les informations concernant ces trois échantillons LockerGoga sont présentes dans le tableau ci-dessous :

Condensats	Première vue VT
174e3d9c7b0380dd7576187c715c4681 31fbfe814628db3b459ddc87bf5ed538700db17a c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4	2019-01-08 (UTC)
a52f26575556d3c4eccd3b51265cb4e6 61fdebb3c9dfa880b54e82579256acfcd4d6d406 97a2ab7a94148d605f3c0a1146a70ba5c436a438b23298a1f02f71866f420c43	2019-01-17 (UTC)
ba53d8910ec3e46864c3c86ebd628796 d1c2dfedc602f5d5f2036b0ba5541cac8f8b4b95 a84171501074bac584348f2942964c8550374c39247ec6af0f4a69756ea9fc7a	2019-01-25 (UTC)

Une analyse a montré que les deux premiers échantillons du tableau ont un lien avec l'échantillon de départ, sans pour autant être identiques. Il pourrait s'agit de variantes (issues de deux branches différentes ayant eu un code commun) ou d'une version antérieure (ces échantillons LockerGoga ont une date de compilation antérieure au premier échantillon).

Le troisième échantillon, d'après les analyses effectuées, est un *dropper* qui contient un code similaire à l'échantillon « `c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4` ».

De plus, le *dropper* contient également des chaînes de caractères spécifiques. Ci-dessous quelques chaînes qui ont pu être extraites :

```
javobohisabi yohoxucojanukazahaviwexepeniwa negikicudosoyihuruyadeyafipihaja

Telawefibudi wuzahibe liga. Caku jakacoza zususezebonuli setusidafohi. Xekaho tiyiwifuvu damonixuxaho togubo
    xisLadoxuna pibifuzida. Goso sepudahemeli bu zevahilipezipa xurotocomupe. Kofe ridimarijoyane. Yeve.
    Tuwipufebedopi yocomujiyezejo su su. Timevumavizase hapezo fogiju. Xonucosegogi li. Bobixayogaci. Kuyi. Leto
    zoyihebezobu wu ciwu. Docadufe ro judewocekodiki
```

Ces chaînes semblant assez discriminantes, une recherche sur celles-ci a permis de trouver un nouvel échantillon.

Condensats	Première vue VT
871aa15f4d61c85e1284e1be3f99f705 236eac0b19f91117b27f1b198a4d8490d99ec2e5 b434bccf0a5ff75b27184e661df751466aef69f35fbd7b8b8692302b8b886262	2019-01-07 (UTC)

2.4 Script DOS

Un fichier nommé « `kill.bat` » a été trouvé lors d'une recherche en source ouverte. Celui-ci a été soumis le même jour par la même clé d'API ayant soumis l'échantillon de départ. Les caractéristiques de ce script sont présentes dans le tableau ci-dessous.

Condensats	Première vue VT
34187a34d0a3c5d63016c26346371b54 ce8209ff9828aa8cb095bd7d1589fc4d394c298c 5f815b8a8e77731c9ca2b3a07a27f880ef24d54e458d77bdabbbaf2269fe96c3	2019-01-24 (UTC)

Le script contient une liste de commandes permettant entre autres de stopper et désactiver des services, de terminer des processus, de désinstaller des logiciels de sécurité, etc.

2.5 Infrastructure

L'ANSSI a identifié une connexion ressemblant à du « `reverse TCP` » vers l'adresse IP « `62.210.136.65` » :

Adresse IP	AS	Nom AS	Pays AS	CIDR	Nom CIDR	Pays CIDR
62.210.136.65	12876	ONLINE S.A.S	France	62.210.0.0/16	ONLINE S.A.S	France

Une deuxième adresse IP, qui télécharge une charge utile METERPRETER ou EMPIRE a été identifiée :

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

Une autre adresse IP appartenant au même sous-réseau a été trouvée :

Adresse IP	AS	Nom AS	Pays AS	CIDR	Nom CIDR	Pays CIDR
185.202.174.86	174	COGENT-174 - Cogent Communications, US	Canada	185.202.174.0/24	H129	Canada

Cette adresse IP a été utilisée pour télécharger une charge malveillante *Powershell* encodée en *base64* avec le *user-agent* : « `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; 360space)` »

De plus, une requête vers l'URL « `https://pastebin.com/raw/7Qmz6q5v` » a été observée qui, après plusieurs traitements, permet de télécharger une charge malveillante depuis l'adresse IP « `93.115.26.171` » :

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

Un échantillon malveillant se connecte à celle-ci sur le port « `443` » :

Condensats	Première vue VT
644087ccca16d2a728ef7685a4106f09 eabd6974ac71efd72d9e0688d5a6131f336d169c 385e31c97e3a07bbb81513f0cd0979e64e6b014943902efd002f57b21eadd41e	2019-01-17 (UTC)

Cet échantillon est soumis sur VIRUSTOTAL avec le nom *cob93.exe*.
Un autre échantillon nommé « `test.bat` » a été trouvé :

Condensats	Première vue VT
7b792de1468a70cfe990b65034d5f3ac 320f1fc66054e98681fd291415ff17b2e1a71b61 a89eac79ff230f3c270b465cd2d8c1225b8937bd4b069ac27872ac883082d82b	2019-02-21 (UTC)

Il réalise une requête similaire à la précédente et permet de récupérer une charge depuis une autre adresse IP :

Adresse IP	AS	Nom AS	Pays AS	CIDR	Nom CIDR	Pays CIDR
176.126.85.207	63473	HOSTHATCH - hostHatch, Inc, US	Allemagne	176.126.85.0/24	HostHatch-LLC	Pays-Bas

2.6 Mode opératoire

L'attaquant semble compromettre ses cibles via l'exploitation d'un service exposé sur Internet, cela est réalisé de manière opportuniste puisqu'aucun secteur d'activité ou géographique ne paraît particulièrement visé.

L'attaquant utilise des outils connus tels que « `Metasploit` », « `Empire` » et « `Cobalt Strike` » ainsi que « `psexec` » pour la latéralisation et l'exécution du rançongiciel. Cette exécution est réalisée plusieurs semaines (voire plusieurs mois) après la compromission effective de la cible. Une étude approfondie de la cible et de son infrastructure est donc fortement probable.

L'attaquant prend le contrôle d'au moins un compte administrateur et effectue différents rebonds via le protocole RDP (*Remote Desktop*) dans l'infrastructure ciblée pour ensuite déposer ses outils (entre autres le fichier « `.bat` » et le rançongiciel) dans des serveurs spécifiques. Ces outils sont ensuite exécutés sur les cibles finales.

Ces cibles finales sont choisies en amont par l'attaquant et leurs adresses IP sont listées dans un script. Les adresses IP n'étant pas consécutives, une sélection est réalisée préalablement au déclenchement de la charge utile.

Voici un schéma représentant le chemin de compromission effectué par l'attaquant sur la cible :

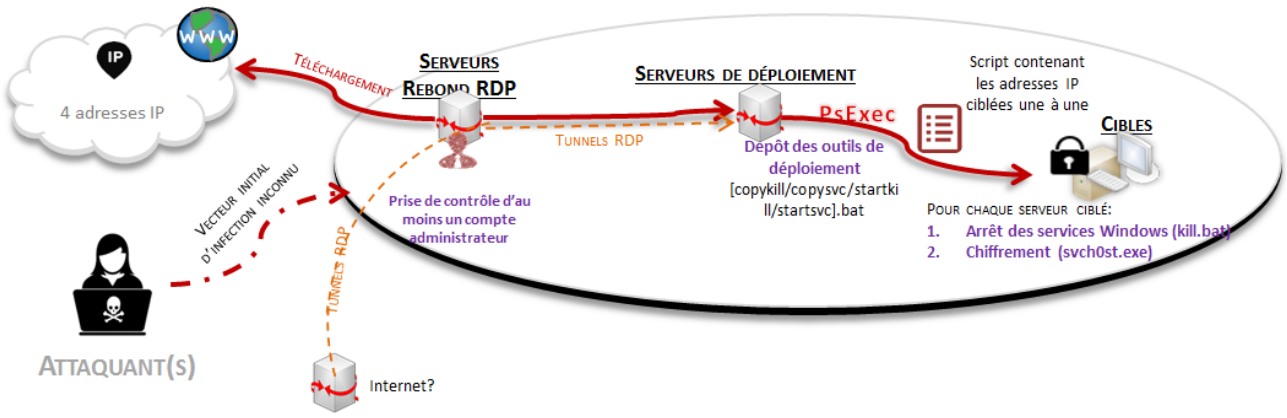

Fig. 2.1 : Chemin de compromission

3 Liens avec des modes opératoires d'attaques

Des liens avec des modes opératoires d'attaques d'origine cybercriminelle ont pu être identifiés.

3.1 Script DOS

Le fichier « `kill.bat` » rappelle celui utilisé par le groupe d'attaquants *Grim Spider* [2]. D'après CROWDSTRIKE, ce groupe utilise également un fichier « `kill.bat` » afin de stopper et désactiver des services, terminer les processus, etc.

3.2 Message de rançon

Le message de rançon possède plusieurs similarités avec des messages issus d'autres familles de rançongiciels.
Le texte coloré en bleu signifie que ce texte est presque le même que celui d'autres messages de rançon (même idée, presque les mêmes phrases). Le texte coloré en rouge signifie que le texte est exactement le même que sur les autres messages de rançon.

(Supposé) LockerGoga	BitPaymer	Ryuk (version courte)	Ryuk (version longue)
Greetings! There was a significant flaw in the security system of your company. You should be thankful that the flaw was exploited by serious people and not some rookies. They would have damaged all of your data by mistake or for fun. Your files are encrypted with the strongest military algorithms RSA4096 and AES-256. Without our special decoder it is impossible to restore the data. Attempts to restore your data with third party software as Photorec, RannohDecryptor etc. will lead to irreversible destruction of your data. To confirm our honest intentions. Send us 2-3 different random files and you will get them decrypted. It can be from different computers on your network to be sure that our decoder decrypts everything. Sample files we unlock for free (files should not be related to any kind of backups). We exclusively have decryption software for your situations DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT RENAME the encrypted files. DO NOT MOVE the encrypted files. This may lead to the impossibility of recovery of the certain files. To get information on the price of the decoder contact us at: [first contact email];[second contact email] The payment has to be made in Bitcoins. The final price depends on how fast you contact us. As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security	Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorythm. Backups were either encrypted or deleted or backup disks were formatted. We exclusively have decryption software for your situation. DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT RENAME the encrypted files. DO NOT MOVE the encrypted files. This may lead to the impossibility of recovery of the certain files. To get info(pay-to-decrypt your files) contact us at: [first contact email] or [second contact email] BTC wallet: [bitcoin address] KEY:[key]	Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover. We exclusively have decryption software for your situation No decryption software is available in the public. DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT RENAME OR MOVE the encrypted and readme files. DO NOT DELETE readme files. This may lead to the impossibility of recovery of the certain files. To get info (decrypt your files) contact us at [first contactemail] or [second contact email] BTC wallet: [bitcoin wallet] Ryuk No system is safe	Gentlemen! Your business is at serious risk. There is a significant hole in the security system of your company. We've easily penetrated your network. You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks. They can damage all your important data just for fun. Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256. No one can help you to restore files without our special decoder. Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly. If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files (Less than 5 Mb each, non-archived and your files should not contain valuable information (Databases, backups, large excel sheets, etc.)). You will receive decrypted samples and our conditions how to get the decoder. Please don't forget to write the name of your company in the subject of your e-mail. You have to pay for decryption in Bitcoins. The final price depends on how fast you write to us. Every day of delay will cost you additional +0.5 BTC Nothing personal just business As soon as we get bitcoins you'll get all your decrypted data back. Moreover you will get instructions how to close the hole in security and how to avoid such problems in the future + we will recommend you special software that makes the most problems to hackers. Attention! One more time ! Do not rename encrypted files. Do not try to decrypt your data using third party software. P.S. Remember, we are not scammers. We don't need your files and your information. But after 2 weeks all your files and keys will be deleted automatically. Just send a request immediately after infection. All data will be restored absolutely. Your warranty - decrypted samples. contact emails [first contact email] or [second contact email] BTC wallet: [bitcoin wallet] Ryuk No system is safe

Le rançongiciel Ryuk est connu pour avoir deux types de messages de rançon, en fonction de l'importance qu'il accorde à la société victime.

3.3 Grim Spider

L'éditeur CROWDSTRIKE liste plusieurs caractéristiques du mode opératoire utilisé par *Grim Spider* qui semblent similaires à celui employé lors des attaques par rançongiciels « `LockerGoga` » :

- utilise systématiquement deux services d'enregistrement d'adresses courriel pour les demandes de rançon ;
- crée un « `reverse shell` », notamment en utilisant METASPLOIT ou COBALT STRIKE ;
- utilise PSEXEC pour copier et exécuter le rançongiciel afin de chiffrer les machines cibles.

4 Indicateurs de compromission

4.1 Infrastructure de l'attaquant

4.1.1 Adresses IP de serveurs de commande et de contrôle

Adresse IP
62.210.136.65
185.202.174.91
93.115.26.171
185.202.174.86

4.1.2 Adresses IP d'administration des serveurs

Adresses IP	
185.238.0.217	185.70.105.158
185.70.105.43	185.70.187.21
185.70.187.88	31.192.108.122
31.192.108.123	31.207.44.186
31.207.44.83	5.39.219.168
5.39.219.185	185.70.184.134
185.70.184.250	185.70.187.22
185.70.187.23	185.70.187.38
185.70.187.46	185.70.187.51
185.70.187.53	185.70.187.56
185.70.187.65	185.70.187.77
185.70.187.79	185.70.187.86
185.70.187.92	31.207.44.118
31.207.44.77	31.207.44.80
31.207.44.84	31.207.45.251
31.207.45.45	5.39.219.172
5.39.219.183	5.39.219.184
5.39.219.187	5.39.219.188

Certaines adresses IP hébergent des certificats X.509 (les certificats en rouge sont auto signés).

Adresse IP	SHA-1 du certificat	Première vue	Dernière vue
185.70.105.43	5286a5ed1288e7c54f1ca04d097f17c1d6aea32b	2018-10-14	2018-10-23
185.70.105.43	6dc00843f313690075612ee5ce770cae067cd37f	2018-06-05	2018-06-19
31.207.44.186	ee4c9567c9a072e1d8ed8a78cb06d6ce1a81dd11	2019-02-12	2019-02-12
31.207.44.186	2200eb3303e448a52404128458e87f3248d4612c	2018-09-25	2018-11-06
5.39.219.159	f0e07b689caa5c7b3767bb3b4cfe4cba2aecb5f8	2019-01-29	2019-01-29
5.39.219.159	cc9aa7e71ce04b893bcdf49a1da2f0e20e45faf2	2019-01-22	2019-01-22
5.39.219.159	840963454567b38a5f1d1df7cd202629804e4c61	2018-11-06	2018-11-20
185.58.204.177	dc8f3c31906c01d077c614809bb1195af2393dc1	2018-01-02	2019-02-12
185.58.204.177	02faf3e291435468607857694df5e45b68851868	2017-08-29	2017-12-05
185.58.204.177	28a4481f8138c889367f9112ef48e4f17fb69944	2017-08-29	2017-12-05
185.58.204.177	339cdd57cfd5b141169b615ff31428782d1da639	2017-08-29	2017-12-05
185.58.204.177	f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0	2017-08-29	2017-12-05
185.58.204.177	3712786dd9d1d8ac7db60ba2f989280c7257a3a9	2017-04-10	2017-07-18

185.58.204.177	736a4dc679d682da321563647c60f699f0dfc268	2017-04-10	2017-07-18
185.58.204.177	b1bc968bd4f49d622aa89a81f2150152a41d829c	2017-04-10	2017-07-18
185.58.204.177	02faf3e291435468607857694df5e45b68851868	2017-04-03	2017-04-03
185.58.204.177	28a4481f8138c889367f9112ef48e4f17fb69944	2017-04-03	2017-04-03
185.58.204.177	339cdd57cfd5b141169b615ff31428782d1da639	2017-04-03	2017-04-03
185.58.204.177	f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0	2017-04-03	2017-04-03
185.58.204.177	15abccaae3920046f55293e25f5f931a6581e00f	2016-12-26	2017-01-02
185.58.204.177	736a4dc679d682da321563647c60f699f0dfc268	2016-12-26	2017-01-02
185.58.204.177	b1bc968bd4f49d622aa89a81f2150152a41d829c	2016-12-26	2017-01-02

Le tableau ci-dessous décrit, pour chaque certificat, son émetteur et son sujet.

SHA-1 du certificat	Émetteur	Sujet
5286a5ed1288e7c54f1ca04d097f17c1d6aea32b	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = vds23392, emailAddress = root@vds23392	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = vds23392, emailAddress = root@vds23392
6dc00843f313690075612ee5ce770cae067cd37f	CN = scourketchupfries.cn.com	CN = scourketchupfries.cn.com
ee4c9567c9a072e1d8ed8a78cb06d6ce1a81dd11	CN = Endway Cisco VPN, O = Endway	CN = Endway Cisco VPN, O = Endway
2200eb3303e448a52404128458e87f3248d4612c	C = XX, L = Default City, O = Default Company Ltd	C = XX, L = Default City, O = Default Company Ltd
f0e07b689caa5c7b3767bb3b4cfe4cba2aecb5f8	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = unknown58339, emailAddress = root@unknown58339	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = unknown58339, emailAddress = root@unknown58339
cc9aa7e71ce04b893bcdf49a1da2f0e20e45faf2	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = vds58339.localdomain, emailAddress = root@vds58339.localdomain	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = vds58339.localdomain, emailAddress = root@vds58339.localdomain
840963454567b38a5f1d1df7cd202629804e4c61	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = localhost.localdomain, emailAddress = root@localhost.localdomain	C = –, ST = SomeState, L = SomeCity, O = SomeOrganization, OU = SomeOrganizationalUnit, CN = localhost.localdomain, emailAddress = root@localhost.localdomain
dc8f3c31906c01d077c614809bb1195af2393dc1	C = AU, ST = Some-State, O = Internet Widgits Pty Ltd	C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
3712786dd9d1d8ac7db60ba2f989280c7257a3a9	C = BE, O = GlobalSign nv-sa, CN = GlobalSign Domain Validation CA - SHA256 - G2	OU = Domain Control Validated, CN = www.csgolite.ru
02faf3e291435468607857694df5e45b68851868	C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTrust External CA Root	C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTrust External CA Root
28a4481f8138c889367f9112ef48e4f17fb69944	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA	OU = Domain Control Validated, OU = PositiveSSL, CN = tcp.csgolite.ru
339cdd57cfd5b141169b615ff31428782d1da639	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Domain Validation Secure Server CA
f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0	C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTrust External CA Root	C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA Certification Authority
15abccaae3920046f55293e25f5f931a6581e00f	C = BE, O = GlobalSign nv-sa, CN = GlobalSign Domain Validation CA - SHA256 - G2	OU = Domain Control Validated, CN = bendermoney.com
736a4dc679d682da321563647c60f699f0dfc268	C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA	C = BE, O = GlobalSign nv-sa, CN = GlobalSign Domain Validation CA - SHA256 - G2
b1bc968bd4f49d622aa89a81f2150152a41d829c	C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA	C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA

4.2 URL permettant de récupérer du code malveillant

URL malveillante
https://pastebin.com/raw/wdcq0Tda
https://pastebin.com/raw/9ditgTZh
https://pastebin.com/Mzd1HFrN

4.3 Indicateurs système

Un utilisateur local nommé « `terminal` » peut être créé sur la machine compromise.

4.4 Charges malveillantes

MD5	Nom	Taille
06457b317d5624590803a77d3770bff2	AD.zip	472243

SHA1	Nom	Taille
2a030cc6d84d5785f5e84d0f5888a411d4b06d01	soft.exe	45568
2abae839362edfe52d9ebe282fb61113d22b331f	sttager.exe	20480
6995a32e0a4d4f6d0c9b2a00a96d69bff4b83ea7	test443.exe	373911
87b1f17fbb4a1e8eef4cb31c1c0194b1426c868c	veil.exe	345761
afc36916a4df934446681ea28bef6add4decb98a	80_http.exe.exe	411850
f832d94391a8d2d5cf92773e6c912905ec7c40c7	test1.exe	406636
056823c7891a04b2fec8903eb401ae3291743a54	beca.exe.exe	23808
b7afa7acf1b7ded2c4e3d0884b5cdaa230d9f82e	shell1.exe	24576
4b50b6b9157026ab408d966ece02d1cef8045f82	starggge.exe	27136
6042dfd50d33da40e383baec4a7ef7c75bf17481	8_32.exe	24064
9b50fae63f4d8d402f30c487ca7216f610413642	payload.exe	6144
781778f789185889259d2a8dec981e80098fa490	443_12.exe	28904
153d37f0f0660734a1e05cb67721c4ceff54919f	test.exe	370807
2d038fcd5987b2e7008b2e269b0a9ff968063ee8	test_1.exe	601039
9d2148cd22c245fc3ba7861a560d223f72f34414	synack_network_noinject_x86.ps1	302611
c8207144f89c9d775ff5565888dbbc8167e09330	synack_network_noinject_x64.ps1	390311
5131a7a011041e88b32a2a98e5170c42d5c57250	synack_network_x64.ps1	423995
e925c3ba15f007363ad32b84df7da9b299b9b100	synack_x64.ps1	423995
481b18bcbd9d32c5363bb56ab212d57d78497c05	synack_network_x86.ps1	327187
2bcfd0679726f0110545b47b4512a8a4ddcb830f	synack_x86.ps1	327187
eaefb5e9ea2e0d301ee594e6358ea136442cd075	test.exe	529477
237b19af7c867b21f46793dd7257dff2f3be1513	encryptor.zip	18211
f5619064f2d8aebfdba0fc3f566cb60f599f9f6e	encryptor.exe	29696
399d4d5ab0bdbe0b1a61bac007d56adff005486d	tung2901_AU3_EXE_6cr22.rar	277412

4.5 Autres indicateurs

MD5	SHA1	SHA256
644087ccca16d2a728ef7685a4106f09	eabd6974ac71efd72d9e0688d5a6131f336d169c	385e31c97e3a07bbb81513f0cd0979e64e6b014943902efd002f57b21eadd41e
34187a34d0a3c5d63016c26346371b54	ce8209ff9828aa8cb095bd7d1589fc4d394c298c	5f815b8a8e77731c9ca2b3a07a27f880ef24d54e458d77bdabbbaf2269fe96c3
871aa15f4d61c85e1284e1be3f99f705	236eac0b19f91117b27f1b198a4d8490d99ec2e5	b434bccf0a5ff75b27184e661df751466aef69f35fbd7b8b8692302b8b886262
a1d732aa27e1ca2ae45a189451419ed5	50f5a5ec13d21d4df119140547d63bc40f93b079	c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a
164f72dfb729ca1e15f99d456b7cf811	f92339e73c7e901c0c852d8e65615cfb588a4ff6	8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29
9cad8641ac79688e09c5fa350aef2094	3da0a217bbda09561780f52f163a6aafeb721d60	5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c
3ebca21b1d4e2f482b3eda6634e89211	37cdd1e3225f8da596dc13779e902d8d13637360	6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77

52340664fe59e030790c48b66924b5bd	73171ffa6dfee5f9264e3d20a1b6926ec1b60897	bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f
a5bc1f94e7505a2e73c866551f7996f9	7dea7ff735023418b902d093964028aefbc486a5	14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca
b3d3da12ca3b9efd042953caa6c3b8cd	34fb03a35e723d27e99776ed3e81967229b3afe1	7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125
faf4de4e1c5d8e4241088c90cfe8eddd	fcd241fdcd462199f2907ca34c73ce9c89b03e5f	47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4
7b792de1468a70cfe990b65034d5f3ac	320f1fc66054e98681fd291415ff17b2e1a71b61	a89eac79ff230f3c270b465cd2d8c1225b8937bd4b069ac27872ac883082d82b

Adresse IP
176.126.85.207

IMPHASH
c226ac4bab6f48634bacbb7a1d34f8f6

5 Sources

[1] *Tweet de @vxsh4d0w*, TWITTER, 2019-01-25.
https://twitter.com/vxsh4d0w/status/1088866607441629184

[2] *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*, CROWDSTRIKE, 2019-01-10.
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative...

[3] *Bulletin d'alerte du CERT-FR*, ANSSI, 2019-01-31.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-003

Version 1.0 - 26/03/2019

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