TLP:WHITE

INFORMATIONS CONCERNANT LE RANÇONGICIEL CLOP

1.0

22/11/2019

TLP:WHITE

Ces dernières semaines, l'ANSSI a observé plusieurs attaques impliquant le déploiement du rançongiciel Clop sur des systèmes d'information en France. Ce code malveillant chiffre les documents présents sur les SI et leur ajoute, suivant les versions, l'extension « `.CIop` » ou « `.Clop` ». Les analyses réalisées par l'ANSSI et ses partenaires montrent que le chiffrement des postes est précédé par des actions de propagation manuelle réalisées par l'attaquant au sein du réseau victime. **Cette phase en amont du chiffrement dure plusieurs jours et signifie qu'il est possible de détecter certains signes de l'attaque avant le déclenchement du rançongiciel sur une grande partie du SI.**

Ces attaques semblent être le résultat d'une vaste campagne d'hameçonnage ayant eu lieu autour du 16 octobre 2019 et liée au groupe cybercriminel TA505.

1 Le rançongiciel Clop

Ce rançongiciel a été observé pour la première fois en février 2019. Son code est l'objet de fréquentes modifications mineures, qui semblent principalement avoir pour objectif de complexifier sa détection [1]. Il est une variante de la famille de rançongiciels CryptoMix, elle-même dérivée des familles CryptXXX et CryptoWall.

Les attaques impliquant Clop ne se limitent pas à une zone géographique ni un secteur d'activité particuliers. L'éditeur McAfee mentionne ainsi des attaques ayant majoritairement ciblé les États-Unis, mais également une douzaine d'autres pays[1]. Durant le premier semestre 2019, Clop aurait également ciblé des agences gouvernementales en Corée du Sud [2].

Méthodes d'infection connues et faits opérationnels saillants

Le rançongiciel Clop semble être majoritairement distribué au travers de campagnes d'hameçonnage, qui n'apparaissent pas ciblées mais plutôt massives.

Le rançongiciel étant dépourvu de fonctionnalités de propagation automatique, les attaquants s'attachent en premier lieu à se propager au sein du réseau de la victime à l'aide de plusieurs codes malveillants. Ainsi, l'éditeur Ahnlab[2] [2] et le CERT gouvernemental sud-coréen [3] rapportent l'usage de la porte dérobée FlawedAmmyy[3] (parfois renommée wsus.exe) et de l'outil d'attaque Cobalt Strike lors de cette phase. L'objectif des attaquants est d'acquérir des droits d'administration réseau afin de faciliter le déploiement du code de chiffrement sur l'ensemble du système d'information à partir de serveurs centraux.

En outre, des certificats sont utilisés pour signer le code malveillant Clop afin de lui donner une apparence légitime. Les entités suivantes ont été observées à plusieurs reprises dans le champ « Sujet » des certificats associés aux attaques déployant le rançongiciel Clop : "ALISA L LIMITED"[4], "THE COMPANY OF WORDS LTD" et "MISHA LONDON LTD".

Enfin, afin d'entraver les actions des équipes de sécurité informatique de la victime, le rançongiciel est souvent déployé en début ou veille de week-end et comporte une fonction de suppression des copies cachés Windows (*Volume Shadow copies*).

[1] Suisse, Royaume-Uni, Belgique, Pays-Bas, Croatie, Allemagne, Danemark, République Dominicaine, Porto Rico, Turquie, Russie
[2] Ahnlab a observé deux méthodes distinctes de déploiement du rançongiciel Clop au sein d'entités gouvernementales sud-coréennes.
[3] FlawedAmmyy est un outil d'accès à distance basé sur la fuite du code source du logiciel légitime Ammyy Admin en 2016, et contenant un downloader et une porte dérobée.
[4] Ce nom de certificat se rapproche fortement d'un certificat utilisé pour signer LockerGoga, nommé ALISA LTD.

2 Liens entre TA505 et le déploiement du rançongiciel Clop

Outre l'utilisation dans la chaîne de compromission d'outils connus pour être associés au groupe TA505 (en particulier FlawedAmmyy), plusieurs liens techniques rattachent le rançongiciel Clop à ce groupe cybercriminel. Notamment, une souche du rançongiciel a été signée avec le même certificat qu'une souche de FlawedAmmyy [4, 5, 6, 7].

Un lien similaire a aussi été constaté par le CERT sud-coréen [3] entre une souche du rançongiciel et une souche du code Amadey qui, bien que vendu sur certains forum d'attaquants, est aussi utilisé par TA505.

Aussi il apparaît intéressant de prendre en compte les informations connues sur TA505, et notamment le fait que ce groupe pratique aussi l'exfiltration de données bancaires et qu'il puisse ainsi réaliser ce type d'action en marge de l'utilisation du rançongiciel Clop.

Le groupe cybercriminel TA505

TA505 est un groupe cybercriminel actif depuis 2014, ciblant principalement le secteurs de la finance [8] mais aussi de la distribution, des institutions gouvernementales et également depuis 2019 des entités des secteurs de la recherche, de l'énergie, de l'aviation et de la santé. Une campagne d'attaques a notamment ciblé en septembre 2019 des institutions financières en Grèce, à Singapour, aux Émirats Arabes Unis, en Géorgie, en Suède et en Lituanie.

La motivation première de TA505 est lucrative : principalement à la recherche d'entités détenant de l'argent, ils auraient récemment cherché à monétiser de la propriété intellectuelle qu'ils auraient dérobée [9]. A ce titre, ils utiliseraient soit des trojans bancaires (notamment Dridex et TrickBot jusqu'à début 2018), soit des rançongiciels (notamment Locky, GlobeImposter et Philadelphia) [10].

TA505 apparaît être un groupe très actif, capable de mener de nombreuses opérations. Ils seraient à l'origine d'au moins 9 campagnes d'attaques depuis juin 2019 ayant un impact dans le monde entier [9]. Ces importantes capacités d'action interrogent sur la structure du groupe qui pourrait regrouper plusieurs sous-groupes ou impliquer une collaboration avec d'autres.

3 Recommandations

Afin d'éviter autant que possible le déclenchement de la charge de chiffrement, un durcissement du poste de travail doit être effectué (contrôle d'exécution de fichier, outils d'analyse comportementale).

Il est important de noter que les architectures « backup-less » qui protègent efficacement contre la destruction de données isolées ne protègent pas contre les attaques ciblées par rançongiciel, les attaquants s'employant à chiffrer les données sur l'ensemble des serveurs de réplication. Ainsi, il est important de continuer à considérer les systèmes de sauvegardes déconnectées (« à froid ») pour les données les plus critiques.

Enfin, le chiffrement de l'Active Directory, en tant que cœur de l'authentification du réseau, peut porter gravement atteinte à l'intégrité de ce dernier. Un système de cloisonnement des niveaux d'administration peut être mis en place afin d'assurer au maximum que les niveaux d'administration les plus hauts sont difficilement atteignables par les attaquants (voir la fiche Microsoft : « Modèle de niveau administratif Active Directory »).

4 Moyens de détection

Les actions de propagation au sein du SI de la victime et en amont du déploiement du rançongiciel Clop étant réalisées manuellement et à l'aide de comptes administrateurs de domaine, il peut être intéressant de réduire leur nombre et de vérifier le comportement de ces comptes et notamment la mise en place de règles de déploiement de

codes sur le réseau.

Afin de s'assurer que la machine sur lequel il se trouve n'a pas déjà été chiffrée, le rançongiciel Clop vérifie la présence d'un « mutex » sur celle-ci et ne s'exécutera pas s'il est présent. Bien que ce dernier soit spécifique à la victime, il peut être utile pour une victime dont le système d'information est en cours de chiffrement, d'éxécuter un script de création de ce mutex sur les machines encore saines. Pour autant, il s'agit d'une manœuvre de dernier recours.

5 Indicateurs de compromission

5.1 Exemples de mutex créés par le rançongiciel Clop

« `MoneyP#666` »; « `CLOP#666` »; [1]
« `HappyLife^_-` » [1]
« `Fany-Fany-6-6-6` » [1]

6 Bibliographie

[1] McAfee. *Clop Ransomware*. 1er août 2019. URL : https://securingtomorrow.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/.

[2] Ahnlab. *ASEC Report Vol.96 Q3 2019*. Quarterly Reports. 7 juil. 2019.

[3] Korea Internet & Security Agency. *KISA Cyber Security Issue Report : Q2 2019*. 13 août 2019.

[4] Virus Total. *A1d8dfcea46dcaf2e5faab857389a6fa2bf19a29a4dbb7a31e8aecffcf468bdc*. 22 juil. 2019. URL : https://www.virustotal.com/gui/file/a1d8dfcea46dcaf2e5faab857389a6fa2bf19a29a4dbb7a31e8aecffcf468bdc/detection.

[5] Virus Total. *0e58ff6dfb839f1df933b8d999832f98d8b53ea48d49bebf861161b5bf957433*. 25 août 2019. URL : https://www.virustotal.com/gui/file/0e58ff6dfb839f1df933b8d999832f98d8b53ea48d49bebf861161b5bf957433/detection.

[6] *Vitali Kremez sur Twitter : "@KorbenD_Intel @James_inthe_box @malwrhunterteam @Malwageddon Nice find. Indeed, another #signed #FlawedAmmyy malware with #Thawte cert for [MISHA LONDON LTD]. Seems like more and more Thawte certs are leveraged in malware signing lately ????." / Twitter*. 19 nov. 2019. URL : https://twitter.com/vk_intel/status/1139512108943650822.

[7] *Vitali Kremez sur Twitter : "2019-08-17 :????#CryptoMix #Clop #Ransomware ????| #Signed [MISHA LONDON LTD] #Thawte Same Company Cert Used by #FlawedAmmyy https ://t.co/D4qR5vQDsD h/t @malwrhunterteam ???? Note : "The faster you write, the cheaper the price will be" | AV Proc Kill MD5 :4c7590305e7212225ad31c3b339c0516 https ://t.co/mvbPi9DsTC" / Twitter*. 19 nov. 2019. URL : https://twitter.com/vk_intel/status/1162810558774747137.

[8] Proofpoint. *TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader*. 15 oct. 2019. URL : https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader.

[9] Positive Technologies. *Positive Technologies : TA505 Rising to Become World's Most Dangerous Cybercriminal Group*. 3 oct. 2019. URL : https://www.ptsecurity.com/ww-en/about/news/ta505-rising-to-become-worlds-most-dangerous-cybercriminal-group/.

[10] Proofpoint. *Threat Actor Profile : TA505, From Dridex to GlobeImposter | Proofpoint US*. 27 sept. 2017. URL : https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter.

1.0 - 22/11/2019
Licence ouverte (Étalab - v2.0)

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