TLP:WHITE

SYNTHÈSE SUR LE RANÇONGICIEL BITPAYMER/IENCRYPT

21/10/2019

TLP:WHITE

Sommaire

Le rançongiciel connu sous les noms BitPaymer, FriedEx et IEncrypt est utilisé depuis au moins juillet 2017 à l'encontre d'entreprises et institutions, dans le cadre d'attaques ciblées et opérées manuellement [1].

Les recherches de l'éditeur ESET [2] ont permis de lier le rançongiciel au code Dridex (Trojan bancaire[1] particulièrement sophistiqué apparu en 2014 et connu pour cibler le secteur financier) avec lequel il partage de nombreuses similarités techniques. Le groupe cybercriminel utilisant Dridex aurait ainsi diversifié ses activités lucratives, ayant probablement étudié la réussite des rançongiciels déjà existants.

1 Méthodes d'infection et faits opérationnels saillants

Bitpaymer est parfois distribué au travers de sites Internet légitimes compromis proposant le téléchargement de mises à jour Flash et Chrome piégées [3]. BitPaymer a aussi été délivré par la compromission d'accès RDP peu ou pas protégés [1]. En juillet 2019, la compromission des victimes aurait aussi été réalisée au travers de campagnes d'hameçonnage [4]. **Ces différentes méthodes d'infection pourraient signifier que BitPaymer est vendu sur le marché noir en tant que « Ransomware-as-a-Service » et utilisé par différents groupes d'attaquants, dits « affiliés »**.

Dans la majorité des attaques connues de l'ANSSI concernant ce rançongiciel, les attaquants réalisent la propagation au sein du réseau victime de façon manuelle **pendant environ une semaine avant le déclenchement du rançongiciel**. Pour cela, ils cherchent en premier lieu à prendre le contrôle de comptes administrateurs réseau légitimes afin de prendre pied sur des serveurs centraux de type « Active Directory ». Ces comptes leurs servent à cartographier le réseau victime et identifier les ressources importantes. Dans ce cadre, l'utilisation du code malveillant Dridex, de l'outil de test de pénétration Powershell Empire, de l'outil de récupération de mot de passe Mimikatz ainsi que de l'outil d'administration PsExec a été rapportée. Après ces quelques jours de propagation interne, les attaquants déploient, le week-end et au milieu de la nuit, la charge de chiffrement **notamment sur les systèmes de sauvegardes de fichiers restés connectés**. Le code de chiffrement ne possède donc pas de fonctionnalité de propagation automatique.

En plus de chiffrer les fichiers accessibles, BitPaymer a également la capacité de désactiver certaines protections antivirales et de supprimer les copies cachées[2].

Il est également intéressant de noter que le rançongiciel est délivré grâce à un code (« Packer ») spécifiquement créé quelques heures avant l'attaque afin d'empêcher les solutions antivirales de détecter l'attaque. Ainsi, bien que le code de chiffrement ait été compilé plusieurs mois avant et soit connu des éditeurs de solutions de sécurité, il peut tout de même être utilisé par les attaquants.

Enfin, le message de rançon contient le nom de la victime et mentionne en guise de contact des adresses de messagerie utilisant les services Tutanota et Protonmail.

1.1 TTP MITRE ATTACK

Phase	TTP	Commentaires
Initial Access	Spearphishing Attachment	La nature du spearphishing n'est pas connue
Initial Access	Spearphishing link	La nature du spearphishing n'est pas connue
Initial Access	Trusted Relationship	Compromission de sociétés sous-traitantes ou prestataires
Execution	Command-Line Interface	arp / nslookup / etc.
Execution	Service Execution	exécution en tant qu'Alternate Data Stream
Persistence	Hidden Files and Directories	Alternate Data Stream
Persistence	Modify Existing Service	
Privilege Escalation	Bypass User Account Control	
Privilege Escalation	Exploitation for Privilege Escalation	Apple Update 0-day
Defense evasion	Bypass User Account Control	

[1]Code malveillant ayant pour objet initial d'exfiltrer des données bancaires, mais capable également de télécharger d'autres codes malveillants.
[2]Copies de données permettant leur recouvrement lors d'incidents affectant la structure de fichiers d'un système d'exploitation

Defense evasion	Deobfuscate/Decode Files or Information	
Defense evasion	Disabling Security Tools	Windows Defender
Defense evasion	Exploitation for Defense Evasion	Windows Defender
Defense evasion	Obfuscated Files or Information	Chaines de caractères chiffrées avec clé RC4
Defense evasion	Software Packing	Custom Packer Code
Discovery	Account Discovery	
Discovery	System Network Connections Discovery	
Command and Control	Data Obfuscation	Empire
Command and Control	Multilayer Encryption	Empire
Command and Control	Standard Cryptographic Protocol	Empire
Impact	Data Encrypted for Impact	
Impact	Disk Content Wipe	
Impact	Inhibit System Recovery	

2 Victimologie

BitPaymer/FriedEx a notamment compromis le 25 août 2017 plusieurs hôpitaux écossais [5], et a également ciblé les secteurs de la finance et de l'agriculture [4]. Les opérateurs de BitPaymer ne semble pas cibler spécifiquement un secteur d'activité.

Les victimes françaises identifiées par l'ANSSI lors de ses investigations ont été prévenues.

3 Variante DoppelPaymer

En juillet 2019, une nouvelle variante du rançongiciel (DoppelPaymer), présentant des différences notables avec Bitpaymer, a été détectée par l'éditeur Crowdstrike [6] lors d'une attaque contre la municipalité d'Edcouch au Texas. Crowdstrike avance l'hypothèse d'une séparation au sein de l'équipe cybercriminelle, Bitpaymer étant toujours utilisé.

Cette nouvelle variante donne des indications intéressantes sur la volonté des cybercriminels d'adapter leurs attaques à leurs cibles, et notamment à leur capacité financière. Ainsi, des attaques impliquant DoppelPaymer ont pu être associées à des rançons de 2, 40 et 100 Bitcoins (soit d'environ 25 000 à 1 200 000 dollars).

4 Recommandations

Lors de son chargement, BitPaymer vérifie l'existence du fichier "`C:\\aaa_TouchMeNot_.txt`" afin de s'assurer de ne pas s'exécuter au sein de l'environnement d'émulation de Windows Defender [4]. En créant ce fichier au préalable, il est possible d'empêcher l'infection d'une machine.

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 »).

5 Moyens de détection

L'éditeur Morphisec a publié en juillet 2019 une règle Yara permettant de détecter le « Packer » de BitPaymer [4]. L'ANSSI confirme que cette règle permet de détecter la couche d'obscurcissement contenant le code de chiffrement.

```
rule BitPaymer {
        meta:
                description = "Rule to detect newer Bitpaymer samples. Rule is based on BitPaymer custom packer"
                author = "Morphisec labs"
        strings:
                $opcodes1 = {B9 ?? 00 00 00 FF 14 0F B8 FF 00 00 00 C3 89 45 FC}
                $opcodes2 = {61 55 FF 54 B7 01 B0 FF C9 C3 CC 89 45 FC}
        condition:
                (uint16(0) == 0x5a4d) and ($opcodes1 or $opcodes2)
}
```

Extrait de code 5.1: Règle yara sur le Packer de BitPaymer. Source : Morphisec

De plus, les actions de propagation au sein du SI victime par l'attaquant à l'aide de comptes possédant des droits d'administrateurs réseau peuvent être détectés par le changement comportemental important de ces derniers. L'ANSSI a pu constater l'usage intensif du protocole RDP par les comptes compromis la semaine avant le déclenchement du code de chiffrement.

Enfin, les attaquants étant susceptibles d'utiliser Powershell Empire et Dridex dans les premières phases de leurs attaques et avant le déclenchement du code de chiffrement, il peut être pertinent de porter ses efforts de détection sur ces codes afin de stopper l'attaque à ses débuts. Les dernières investigations de l'ANSSI ont permis de découvrir un certain nombre d'adresses IP associées à des serveurs Powershell Empire actifs. Ils ne le restent habituellement que quelques semaines.

6 Bibliographie

[1] NJCCIC. *Bit Paymer*. 29 août 2017. URL : https://www.cyber.nj.gov/threat-profiles/ransomware-variants/bitpaymer (visité le 29/01/2019).

[2] ESET. *Dridex Authors Return with a New Chapter in Their Malware Story*. 26 jan. 2018. URL : https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/ (visité le 29/01/2019).

[3] CrowdStrike. *Big Game Hunting : The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware*. 14 nov. 2018. URL : https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/ (visité le 29/01/2019).

[4] Morphisec. *BitPaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S.* 19 juil. 2019. URL : http://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework (visité le 19/07/2019).

[5] BleepingComputer. *Bit Paymer Ransomware Hits Scottish Hospitals*. 29 août 2017. URL : https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/ (visité le 24/07/2019).

[6] Crowdstrike. *CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant*. 12 juil. 2019. URL : https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/ (visité le 24/07/2019).

- 21/10/2019

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