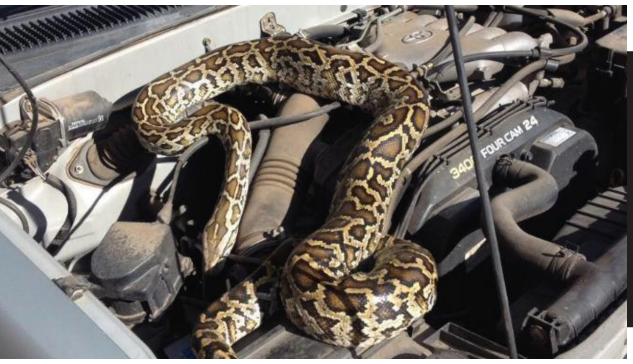
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE



SNAKE ON A CAR

Le géant de l'automobile Honda a été victime d'une cyber attaque par le rançongiciel Snake au début du mois de juin. Le constructeur japonais a été contraint de mettre de nombreux sites à l'arrêt en Europe, en Turquie et en Amérique du Nord.

Snake, également appelé Ekans pour éviter toute confusion avec le malware homonyme attribué au groupe russophone Turla, est un rançongiciel d'un genre un peu particulier. Il a en effet pour particularité de cibler les infrastructures critiques et les systèmes industriels (ICS/SCADA). Ekans a été identifié en janvier 2020 par le chercheur Vitali Kremez (Sentinel One). Il tient son nom Ekans de l'extension ajoutée aux fichiers chiffrés par le malware. Si l'on se fie aux termes mêmes de la demande de rançon affichée après le chiffrement, Ekans s'attaque de façon privilégiée aux réseaux d'entreprises ("We breached your corporate network").

La société Dragos, spécialisée en cybersécurité ICS/SCADA a publié en février une analyse de ce rançongiciel. Selon Dragos, Ekans a fait son apparition en décembre 2019. La société affirme l'avoir analysé en janvier 2020 et n'avoir communiqué le résultat de ces investigations qu'à ses clients. Le rapport de Dragos a été rendu public après que V. Kremez a tweeté sur Ekans.

Ekans contient des fonctionnalités qui permettent au malware d'interférer avec les installations ICS/SCADA. Il contient ainsi une liste de nom de processus à arrêter lors de l'exécution du malware, tous relatifs à des logiciels utilisés dans les infrastructures ICS/SCADA. Parmi les produits ciblés par Ekans on trouve Proficy Historian éditée par General Electric et destiné à collecter et visualiser des données issues de systèmes utilisés dans les secteurs de la production et du transport électriques et dans les industries pétrolières et gazières. Ekans cible aussi des logiciels de gestion de licences comme FLEXNet, Sentinel HASP et ThingWorx Industrial Connectivity Suite. Le malware ne dispose pas de capacité à injecter du code ou modifier des données dans ces logiciels. Il ne peut "que" les arrêter. Dans le cas de Proficy Historian, par exemple, l'arrêt de son processus peut

⊙⊙⊙

SNAKE ON A CAR

avoir de facto un impact sur la surveillance du bon fonctionnement d'une installation industrielle. De même, la mise à l'arrêt de serveurs de licence pourrait entraîner celui des logiciels qui dépendent de ces serveurs.

La "kill list" d'Ekans répertorie 64 processus dans la version analysée par les analystes de Dragos qui rapprochent cette liste et ces fonctionnalités de celles d'un autre ransomware, MegaCortex, dont une version a été analysée par la société Accenture en 2019. Ekans pourrait être un produit dérivé de MegaCortex selon Dragos.

Ces fonctions distinguent Ekans d'autres rançongiciels auxquels ont été attribuées des attaques contre des entreprises de secteurs industriels, comme celle contre la société Norsk Hydro en mars 2019, victime du ransomware LockerGaga. Bapco, l'entreprise pétrolière étatique du Bahreïn aurait été une des premières victimes d'Ekans, sans certitude.

Ekans ne disposant pas de fonctionnalité de propagation autonome, il doit être lancé manuellement ou via un script.

Enfin, selon Dragos, Ekans ne semble pas être le fruit du travail d'équipes d'acteurs étatiques mais celui de cybercriminels qui ne cherchent que le profit financier, d'où le choix de cibler des entreprises, à l'instar des autres acteurs du marché (Ryuk, Maze, etc), ses fonctionnalités anti-ICS/SCADA en faisant un produit de "niche".

Dans l'attaque attribuée à Ekans contre Honda, les codes malveillants utilisés par les cybercriminels se sont assurés de l'identité de leur cible en émettant des requêtes DNS vers des noms de machines et des domaines internes à leur victime, c'est-à-dire non accessibles depuis Internet. Dans le cas de Honda, le malware tentait de résoudre le sous-domaine "mds.honda.com".

La même semaine, une autre entreprise a été victime d'une attaque en tous points similaires : la filiale argentine du groupe Enel. Dans ce cas aussi, les attaquants ont utilisé un nom de domaine interne pour s'assurer d'être au bon endroit.

Cette utilisation d'un nom interne avait également été identifiée lors d'une attaque contre le groupe allemand de santé Fresenius en mai 2020.

Dans ces trois cas, cela laisse supposer qu'une compromission antérieure au déclenchement de la charge finale a eu lieu, durant laquelle les attaquants auront pu mener des actions de reconnaissance avant de construire et déployer une version sur-mesure du rançongiciel, propre à chaque victime. Une autre hypothèse est que les attaquants ont préalablement cherché et trouvé ces noms dans le détails de certificats TLS émis pour les sociétés visées.

Le vecteur initial de compromission n'est pas encore clairement identifié, mais un serveur d'accès distant RDP fait figure de suspect idéal.

Si le mode opératoire est très proche de celui d'autres rançongiciels, l'utilisation de fonctionnalités spécifiques aux installations ICS/SCADA et la capacité d'Ekans de bloquer des chaînes de production constituent des leviers de pression supplémentaires pour inciter les victimes à verser les rançons demandées. La remise en route de solutions logicielles industrielles qui auraient été impactées par Ekans peut aussi demander des procédures moins éprouvées que celles qui consistent à restaurer des données préalablement sauvegardées ou à reconstituer des ressources IT telles que les annuaires Active Directory.

Références :

https://arstechnica.com/information-technology/2020/06/honda-halts-production-at-some-plants-after-being-hit-by-a-cyberattack/

https://www.zdnet.com/article/honda-confirms-its-network-has-been-hit-by-cyber-attack/

https://threatpost.com/snake-ransomware-honda-energy/156462/

https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[RECORDED FUTURE] RAPPORT SUR LE RANSOMWARE THANOS

La société Recorded Future a publié un rapport sur un nouveau rançongiciel appelé Thanos. Thanos a été proposé à la vente sur un forum par un acteur identifié par le pseudonyme "Nosophoros."

Nosophoros présente Thanos comme un générateur de rançongiciels proposant 43 options de configuration. C'est aussi le premier rançongiciel qui intègre la technique RIPlace. Cette technique d'évasion, présentée sous forme de preuve de concept, permet de contourner les mesures de protection anti-rançongiciels fournies par les logiciels antivirus et les solutions de type EDR.

Thanos présente des similarités et réutilise des fonctionnalités avec un rançongiciel nommé Hakbit par d'autres sociétés de sécurité.

Selon RecordedFuture, les clés de chiffrement et de déchiffrement peuvent, dans certains cas, être extraites de la mémoire d'un ordinateur victime de Thanos, ce qui pourrait permettre de ne pas avoir à payer de rançon.

SOURCES ET RÉFÉRENCES :
https://www.recordedfuture.com/thanos-ransomware-builder/

[ZDNET] CLOUDEYE SUSPECTÉE DE LAXISME

La société italienne CloudEye fournit un service nuagique de protection de binaires contre la rétro-ingénierie.

Elle est suspectée d'avoir fait une promotion discrète mais efficace de ses services auprès d'auteurs de malware et d'avoir fait 500 000 dollars de chiffre d'affaires avec eux. Les activités floues de CloudEye ont été mises en évidence après que la société CheckPoint a découvert des indices dans le malware GuLoader d'utilisation des services de CloudEye.

CheckPoint a trouvé un lien entre CloudEye et un service de "protection" de logiciels malveillants nommé DarkEye, annoncé sur les forums de piratage dès 2014.

Selon CheckPoint, GuLoader est le principal client de CloudEye.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/italian-company-exposed-as-a-front-for-malware-operations/
https://research.checkpoint.com/2020/guloader-cloudeye/

[THREATPOST] UTILISATION DU MOUVEMENT BLACKLIVESMATTER PAR TRICKBOT

Selon Abuse.ch, les opérateurs du malware Trickbot exploitent le mouvement BlackLivesMatter et les manifestations contre le racisme pour diffuser des mails malveillants propageant le malware.

Les messages envoyés ont pour sujet "Vote anonymous about Black Lives Matter" ou "Leave a review confidentially about Black Lives Matter" et sont accompagnés d'une pièce jointe malveillante qui se présente comme un formulaire de sondage.

Le malware s'exécute quand, après avoir ouvert ce document, les utilisateurs activent les macros comme cela leur est demandé.

SOURCES ET RÉFÉRENCES :
https://threatpost.com/black-lives-matter-emails-trickbot-malware/156497/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ZDNET] **FERMETURE DE 32.000 COMPTES TWITTER**

La société Twitter a fermé 32 242 comptes utilisés par des acteurs étatiques chinois, russes et turcs pour mener des campagnes de désinformation et de communication politiques.

Le plus grand de ces réseaux de comptes était basé en Chine. Selon Twitter, 23 750 comptes formaient le coeur de ce réseau et étaient responsables de la majorité des diffusions de contenus. Les contenus postés depuis ces comptes étaient relayés par 150 000 comptes jouant le rôle d'amplificateurs.

Selon Twitter, la Chine utilisait son réseau de comptes pour diffuser des messages à caractère géopolitique et contre les manifestations à Hong Kong. La Russie et la Turquie ciblaient leurs opposants internes respectifs.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/twitter-bans-32k-accounts-pushing-chinese-russian-and-turkish-propaganda/

[CYBERSCOOP] **DE NOUVEAUX OUTILS POUR LE GROUPE RUSSOPHONE GAMAREDON**

Le groupe russophone Gamaredon, connu pour des campagnes de cyber espionnage, utiliserait de nouveaux outils dans le cadre d'une campagne menée depuis plusieurs mois et visant à infiltrer des organisations gouvernementales. Le groupe diffuserait depuis au moins 6 mois des mails d'hameçonnage ciblé, sans prendre la peine de camoufler ses traces, selon la société ESET. Les chercheurs ont refusé de nommer le gouvernement visé mais historiquement, Gamaredon est l'un des nombreux groupes liés à la Russie et a ciblé le gouvernement ukrainien par le passé.

Parmi les nouveaux outils exploités par Gamaredon se trouve une macro VBA qui cible Microsoft Outlook dans le but d'automatiser l'envoi de nouveaux messages d'hameçonnage aux contacts du carnet d'adresses de l'utilisateur compromis.

Un autre outil permet d'injecter des macros malveillantes dans des documents Office présents sur le poste infecté.

SOURCES ET RÉFÉRENCES :
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/
https://www.cyberscoop.com/gamaredon-russia-ukraine-eset/

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

MAZE

La société américaine de maintenance aéronautique VT San Antonio Aerospace (VT SAA) a été victime du rançongiciel Maze.

La société de services informatiques américaine Conduent a été victime du groupe Maze.

MAZE / RAGNAR LOCKER

Les opérateurs du rançongiciel RagnarLocker rejoignent le cartel formé par le groupe Maze.

EKANS

Le géant de l'automobile japonais Honda a été victime du rançongiciel Ekans. L'attaque a été très ciblée : avant de déclencher sa charge finale, le malware lançait une requête DNS vers un domaine interne à l'entreprise non accessible depuis Internet. De nombreuses filiales de Honda en Europe, en Turquie et en Amérique du Nord ont été mises à l'arrêt après cette attaque. La filiale argentine du fournisseur d'énergie italien Enel a également été victime du même rançongiciel.

Divers

Les opérateurs du rançongiciel **STOP Djvu** fournissent à leurs victimes un logiciel qui, au lieu de déchiffrer les données volées, les chiffrent une nouvelle fois. L'objectif pourrait être de dissuader les victimes d'utiliser des logiciels gratuits de déchiffrement fournis par certains éditeurs d'antivirus.

La société Lion, fabricant de boissons australien, a annoncé avoir été victime d'un rançongiciel. Cette attaque intervient au moment où Lion reprend ses activités à l'issue du confinement lié à la pandémie. La distribution et la production sont affectées par cet incident. Lion met en garde contre une possible pénurie de bière suite à cette attaque.

Depuis le 1er juin 2020, les activités du groupe **eCh0raix** ont repris. Ce groupe cible les serveurs de stockage (NAS) Qnap pour déployer un rançongiciel en exploitant des vulnérabilités présentes sur des équipements non mis à jour.

Un nouveau rançongiciel appelé **Kupidon** a été détecté en mai 2020. Il cible indifféremment les utilisateurs grand public et les entreprises. Il est déployé après la compromission de serveurs d'accès distants RDP.

La ville de Knoxville dans l'Etat du Tennessee a été contrainte de stopper son système d'information à la suite d'une attaque par rançongiciel. Knoxville est la 51e ville américaine à avoir été victime d'un rançongiciel.

SOURCES ET RÉFÉRENCES :

https://www.bleepingcomputer.com/news/security/business-services-giant-conduent-hit-by-maze-ransomware/
https://www.bleepingcomputer.com/news/security/ongoing-ech0raix-ransomware-campaign-targets-qnap-nas-devices/
https://www.bleepingcomputer.com/news/security/kupidon-is-the-latest-ransomware-targeting-your-data/
https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/
https://www.bleepingcomputer.com/news/security/fake-ransomware-decryptor-double-encrypts-desperate-victims-files/
https://www.zdnet.com/article/lion-warns-of-beer-shortages-following-ransomware-attack/
https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/
https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-partnered-with-maze-ransomware-cartel/
https://arstechnica.com/information-technology/2020/06/knoxville-shuts-down-parts-of-its-network-after-being-hit-by-ransomware/

INTELLIGENCE-DRIVEN CYBERSECURITY

POUR SIGNALER UN INCIDENT

Si vous êtes victime d'une attaque, si vous avez un doute ou si vous désirez revenir et investiguer sur un incident de sécurité, prenez contact avec le CERT SEKOIA.

cert@sekoia.fr
+33 (0) 805 692 142

SEKOIA accompagne les premières sociétés du CAC40 dans la mise en place de leurs CERTs internes.

Depuis 2013 SEKOIA active son CERT inter-entreprises et offre ses services à des OIV et autres acteurs du CAC40 et du SBF120.

LA THREAT INTELLIGENCE, PIERRE ANGULAIRE DE LA LUTTE INFORMATIQUE DEFENSIVE

SEKOIA dispose d'une offre complète en matière de Cyber Threat Intelligence :

- **conseil & accompagnement**,
- **formation**,
- **veille et rapport sur les cybermenaces** :

BR INT. SEKOIA THREAT INTELLIGENCE **BRIEFING REPORT**

FL INT. SEKOIA THREAT INTELLIGENCE **FLASH REPORT**

SP INT. SEKOIA THREAT INTELLIGENCE **SPECIAL REPORT**

- **base & feed de renseignements cyber :**
  SEKOIA THREAT **INTELLIGENCE CENTER**

A PROPOS DE SEKOIA

Pure player et acteur français majeur de la cybersécurité, SEKOIA accompagne au quotidien grands comptes, institutions et entreprises innovantes pour les conseiller sur leur stratégie, les préparer et leur offrir support et assistance dans l'exercice de leurs métiers comme dans les phases les plus critiques d'exposition aux menaces.

Découvrez une structure, un modèle et une stratégie innovante dans le secteur de la cybersécurité.

SEKOIA

SEKOIA — PARIS
18-20,
Place de la Madeleine,
75008 Paris

SEKOIA — RENNES
1137A
Avenue des Champs Blancs
35510 CESSON-SÉVIGNÉ
—
Tél. +33 1 44 43 54 13
—