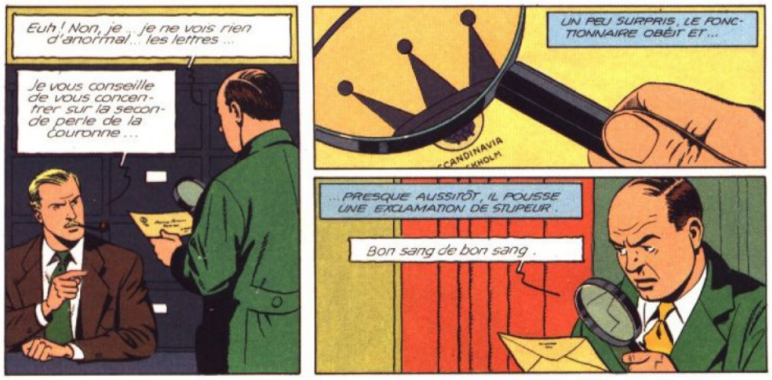
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE



SCADA'CTUALITÉS DE LA SEMAINE

Plusieurs événements ont marqué l'actualité Cyber des systèmes industriels et des infrastructures critiques cette semaine.

Le BND, le BfV et le BSI - dans l'ordre les homologues allemandes de la DGSE, la DGSI et l'ANSSI - ont alerté des entreprises allemandes des secteurs industriels et des infrastructures critiques de la découverte en début d'année de traces de compromissions de longue date dans des entreprises des secteurs de l'énergie et de l'eau.

Le rapport des trois agences fédérales n'est pas publiquement disponible et les entreprises concernées n'ont pas été nommées. Les attaquants auraient compromis des réseaux d'entreprises et dans quelques cas des réseaux OT à la suite d'attaques contre la chaîne logistique (supply chain) de leurs victimes. L'objectif de ces attaques n'a pas été déterminé. Selon toute vraisemblance, elles pourraient s'inscrire dans une phase de reconnaissance et d'espionnage.

Quant à l'identité des attaquants, les trois agences semblent s'accorder pour attribuer ces activités au groupe russophone Berserk Bear. Un rapport similaire avait été rédigé et diffusé en 2018, à peu près à la même époque au sujet des actions hostiles menées par le même groupe contre des entreprises nord-américaines et allemandes.

Le groupe Berserk Bear, qui serait lié aux services de renseignement russes, a fait l'objet de nombreuses alertes ces dernières années et fait donc office de suspect n°1 dès qu'il s'agit d'attaques SCADA et ICS. L'US CERT, le FBI et le DHS ont publié en 2018 une Technical Alert présentant la synthèse des incidents imputés à ce groupe depuis 2016, toutes ciblant des entreprises du secteur de l'énergie aux Etats-Unis ainsi que dans des pays occidentaux.

Comme en 2018, l'ambassade de Russie a nié toute implication de la Fédération de Russie dans ces attaques.

La société Kaspersky a publié une analyse sur des

⊙⊙⊙

LES NOMINÉS POUR LE CÉSAR DE LA MEILLEURE VULNÉRABILITÉ SONT...

attaques ciblées visant des fournisseurs d'équipements et de logiciels destinés aux systèmes industriels et aux infrastructures critiques. Certaines de ces attaques se seraient produites début mai 2020 et auraient touché des entreprises au Japon, en Allemagne, en Italie et au Royaume-Uni.

Le mode opératoire des attaquants repose sur des mails d'hameçonnage comme vecteur initial. Les messages sont rédigés à chaque fois dans la langue des entreprises ciblées et sont accompagnés de pièces jointes malveillantes. L'ouverture de celles-ci provoque l'exécution d'un code malveillant qui vérifie que la configuration du système d'exploitation de l'ordinateur correspond bien à celle de la victime. Cette vérification passe par la détection des variables de localisation. Dans un cas concernant une entreprise nippone, le contenu du mail de phishing, celui du document Excel piégé et des macros malveillantes étaient rédigés en japonais.

La compromission des ordinateurs repose sur l'exécution des macros contenues dans les fichiers Excel envoyés aux victimes. D'une façon classique, à l'ouverture de ces classeurs, un message informe l'utilisateur qu'il doit activer les macros pour lire de contenu des feuilles Excel. Les macros déchiffrent et exécutent un script PowerShell. Ceux-ci sont lancés avec l'option "–ExecutionPolicy Bypass" qui permet au script de s'affranchir des règles de sécurité relatives à PowerShell. Une autre option provoque l'exécution du script dans une fenêtre cachée.

Le script contient aussi une liste d'URL d'images hébergées sur les domaines imgur.com et imgbox.com. Ces images, d'apparence anodine, contiennent des données chiffrées (RSA) et encodées en Base64. Ces données contiennent, une fois déchiffrées et décodées, une version de Mimikatz en PowerShell. Les attaquants peuvent alors voler des identifiants de connexion pour un usage futur. Les attaquants font appel à la stéganographie pour contourner les antivirus et les systèmes de détection d'intrusion.

L'objectif final de ces attaques n'a pas pu être déterminé mais Kaspersky met l'accent sur la sophistication de ces attaques particulièrement ciblées. L'utilisation de la stéganographie renforce l'opinion des analystes sur le fait que les attaquants sont déterminés et méticuleux.

Dans un autre domaine et une autre partie du cyberespace, Yigal Unna, le directeur général du Israel National Cyber Directorate, a affirmé en fin de semaine que l'Etat hébreu était à l'origine de la cyber attaque qui a visé le port iranien de Shahid Rajaee début mai. Cette attaque a été lancée en représailles à des actions hostiles menées contre des entreprises de distribution d'eau israéliennes qui ont été attribuées à l'Iran. Selon Y. Unna, les activités portuaires ont été fortement perturbées, ce qui s'est traduit par des embouteillages sur les routes menant au port et un nombre de navires qui n'ont pas pu décharger leur cargaison pendant plusieurs heures. Le gouvernement israélien n'a pas souhaité commenter, confirmer ni infirmer cette affirmation.

Sources & Références

https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html

https://ics-cert.kaspersky.com/reports/2020/05/28/steganography-in-targeted-attacks-on-industrial-enterprises/

https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/

https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ESET] NOUVELLE VARIANTE DE COMRAT

La version 4 de ComRAT, un malware déployé par le groupe russophone Turla, utilise des pièces jointes contenues dans des mails envoyés à un compte GMail comme canal de commande et de contrôle. Ce canal vient en complément ou en backup du canal "classique" HTTP par lequel le RAT reçoit ses ordres.

Cette nouvelle version de ComRAT a été analysée par la société ESET dans le cadre d'investigations qui font suite à des attaques contre des parlements de républiques du Caucase et deux ministères des affaires étrangères est-européens.

ESET a également détectée l'exfiltration de journaux d'antivirus à l'aide de ComRAT. L'hypothèse avancée par ESET est que les opérateurs de Turla vérifient ainsi que leurs logiciels n'ont pas été détectés sur les machines compromises.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/turla-hacker-group-steals-antivirus-logs-to-see-if-its-malware-was-detected/
https://www.cyberscoop.com/turla-espionage-russia-eset-eastern-europe/
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

[CYBERSCOOP] LE GROUPE BERSERK BEAR CIBLERAIT DES ENTREPRISES D'INFRASTRUCTURES CRITIQUES ALLEMANDE

Selon un document confidentiel émanant de services gouvernementaux allemands, le groupe russophone Berserk Bear, suspecté d'être lié au FSB, le service de renseignement intérieur russe, ciblerait des entreprises dans les secteurs de l'énergie et de l'eau depuis plusieurs mois.

Le groupe mènerait pour cela des attaques contre la chaîne logistique (supply chain attacks). Les investigations auraient mis en évidence des compromissions dont certaines assez anciennes.

Le BSI avait déjà émis une alerte similaire en juin 2018.

SOURCES ET RÉFÉRENCES :
https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

[ZDNET] DÉMANTÈLEMENT DU BOTNET DOUBLEGUNS

Les sociétés chinoises Qihoo et Baidu ont annoncé avoir démantelé le botnet DoubleGuns. Ce botnet a été détecté pour la première fois en 2017 et n'a pas cessé de grandir pendant les 3 années suivant son apparition. Il avait comme particularité de ne cibler qu'exclusivement des ordinateurs en Chine.

Aucune activité de DoubleGuns au-delà du grand Pare-feu n'a été décelée.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/qihoo-baidu-disrupt-malware-botnet-with-hundreds-of-thousands-of-victims/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[CYBERSCOOP] **ARRESTATION D'UN MEMBRE DU GROUPE FIN7**

Un ressortissant ukrainien, membre du groupe cybercriminel FIN7 a été arrêté la semaine dernière à Seattle.

Le groupe FIN7 est suspecté d'avoir volé 1 milliard de dollars à ses victimes aux Etats-Unis. FIN7 s'est spécialisé dans la compromission de points de vente électroniques (Point of Sale) et cible des chaînes de restauration et d'hôtellerie.

Depuis quelques semaines, il cible également des cabinets d'avocats. Adepte du phishing, le groupe a également adopté une nouvelle technique : l'envoi de clés USB piégées.

En septembre dernier, un autre membre du groupe a plaidé coupable des charges pesant contre lui devant un juge de Washington.

SOURCES ET RÉFÉRENCES :
https://www.cyberscoop.com/fin7-hacking-arrest-financial/
https://www.documentcloud.org/documents/6928399-Iarmak-Fin7-Indictment.html

[ZDNET] **GOOGLE PUBLIE SON PREMIER RAPPORT TRIMESTRIEL SUR LES MENACES**

Le groupe d'analyse des menaces de Google (TAG) a publié son premier rapport trimestriel dans lequel les analystes de Google mettent en avant deux tendances à la hausse au cours des trois premiers mois de 2020.

La première est la montée en puissance des entreprises de piratage informatique qui opèrent depuis l'Inde, un pays où ces services n'étaient pas très répandus jusqu'à présent. Les attaques sous-traitées à ces acteurs utilisent la pandémie de la Covid-19 comme leurre. Des attaquants ont ainsi créé des comptes GMail usurpant l'identité de l'OMS.

La seconde tendance est le nombre croissant d'opérations d'influence politique menées par des gouvernements à travers le monde.

C'est également la première fois que Google publie des révélations officielles sur des opérations d'influence coordonnées qui ont abusé des plateformes de l'entreprise.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/google-highlights-indian-hack-for-hire-companies-in-new-tag-report/
https://blog.google/threat-analysis-group/updates-about-government-backed-hacking-and-disinformation

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

Les opérateurs du rançongiciel **RagnarLocker** déploient des machines virtuelles VirtualBox sous Windows XP pour camoufler leur présence sur une machine compromise.

L'université du Michigan (MSU) a été victime d'une attaque par le rançongiciel **NetWalker**. Les fraudeurs laissent une semaine à l'université pour verser la rançon et menacent de publier des fichiers volés à la MSU.

L'équipe de sécurité de Microsoft a publié une alerte au sujet d'un nouveau rançongiciel appelé **PonyFinal.** Il s'agit d'un ransomware en Java qui est déployé manuellement après la compromission initiale. Dans les attaques analysées par Microsoft, celle-ci résultait d'attaque par dictionnaire.

Un nouveau rançongiciel appelé **[F] Unicorn** cible l'Italie. Il se présente sous la forme d'une fausse application de traçage des infections Covid-19. Les fraudeurs usurpent l'identité de l'Italian Pharmacist Federation (FOFI) pour inciter leurs victimes à installer le logiciel malveillant.

Les opérateurs du rançongiciel **Netfilim** mettent leur menace à exécution et publie 200 Go de données volées au groupe Toll.

La filiale congolaise de Bolloré Transport & Logistics, la municipalité autrichienne de Weiz, la société australienne Stellar ont été victimes de **NetWalker**.

La Northwest Atlantic Fisheries Organization, qui gère les quotas de pêche dans les eaux internationales de l'Atlantique du Nord-Ouest pour une douzaine de membres, dont le Canada, l'Union européenne et la Russie, a été victime d'une attaque par rançongiciel le 24 mai.

Des affiliés du rançongiciel **Maze** publient 2Go de données volées à la banque publient Banco de Costa Rica. Ils menacent de continuer à publier de nouvelles données chaque semaine jusqu'au versement d'une rançon.

La municipalité de Columbus, en Géorgie (Etats-Unis) a été victime d'une attaque par rançongiciel.

SOURCES ET RÉFÉRENCES :

https://www.zdnet.com/article/ransomware-deploys-virtual-machines-to-hide-itself-from-antivirus-software/
https://www.zdnet.com/article/michigan-state-university-hit-by-ransomware-gang/
https://www.zdnet.com/article/microsoft-warns-about-attacks-with-the-ponyfinal-ransomware/
https://threatpost.com/funicorn-ransomwarecovid-19-contact-tracing-app/156069/
https://www.bleepingcomputer.com/news/security/hackers-tried-to-use-sophos-firewall-zero-day-to-deploy-ransomware/
https://www.seafoodsource.com/news/business-finance/northwest-atlantic-fisheries-organization-hit-by-ransomware-attack
https://edscoop.com/michigan-state-hit-by-ransomware-threatening-leak-of-student-and-financial-data/
https://webcache.googleusercontent.com/search?q=cache:MSeGhuoAMOIJ:https://www.wrbl.com/news/local-news/columbus-mayor-confirms-ransomware-attack-on-city-government-yesterday/+&cd=1&hl=en&ct=clnk&gl=fr
https://www.ibtimes.sg/netfilm-ransomware-operators-leak-massive-data-global-logistic-group-45390
https://www.itwire.com/security/australian-customer-experience-firm-stellar-hit-by-ransomware.html
http://www.leparisien.fr/high-tech/une-filiale-du-groupe-bollore-touchee-par-un-intrigant-rancongiciel-24-05-2020-8322495.php
https://www.heise.de/news/Hacker-veroeffentlichen-Daten-nach-Cyberangriff-auf-staedtische-IT-in-Oesterreich-4727538.html

NOS DERNIERS BILLETS **MEDIUM**

| **medium**.com/**@sekoia_team** | **medium**.com/**cyberthreatintel** | **medium**.com/**sekoia-io-blog** |

Les nominés pour le César de la meilleure vulnérabilité sont...

La Cybersecurity and Infrastructure Security Agency (DHS CISA) et le FBI ont publié la liste des 10 vulnérabilités les plus couramment exploitées entre 2016 et 2019 par les attaquants. Les dix CVE mentionnées dans le document mis en ligne par les deux agences fédérales le 12 mai 2020 ont un point commun : elles sont toutes couvertes par des mises à jour et des correctifs disponibles.

—> Le billet complet

A la découverte du FLINT, le bulletin quotidien de veille et d'analyse des cybermenaces de SEKOIA

Le SEKOIA Threat Intelligence FLASH Report ou FLINT est un bulletin quotidien de veille et d'analyse des dernières cybermenaces et vulnérabilités critiques.

Transmis par e-mail, il est également disponible dans un format STIX2.1, structuré et actionnable, dans l'Intelligence Center de SEKOIA.IO, notre base de Cyber Theat Intelligence (CTI), accessible via API REST, feed MISP et bientôt sur un portail web.

—> Le billet complet

FL INT. **SEKOIA** THREAT INTELLIGENCE **FLASH** REPORT (RÉSERVÉ À NOS **CLIENTS CTI**)

EXTRAITS DE NOS DERNIERS FLINT :

29/05/2020 - FL|INT.2020-101
Exim Mail Transfer Agent known vulnerability exploited by Sandworm Team

28/05/2020 - FL|INT.2020-100
Valak malware: recent developments make it more than just a loader

27/05/2020 - FL|INT.2019-099
Energetic Bear targets German critical infrastructures

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
—