SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE

ÉLECTIONS US 2020 : ON PREND LES MÊMES ET ON RECOMMENCE ?

On ne saura peut-être jamais si les cyber attaques attribuées aux services de renseignement russes ont permis à l'actuel locataire de la Maison blanche de signer en 2016 le bail qui arrive à échéance prochainement. Si les interventions des différents influenceurs - hackers ursidés, ouvriers des usines à trolls de Saint-Pétersbourg, experts en Big Data et profileurs de Cambridge Analytica, whistleblower de Wikileaks - ne sont plus remises en doute, leur efficacité n'a jamais été prouvée et fait encore débat.

Les actions des hackers russes, notamment, ont été largement couvertes, médiatiquement et judiciairement. Quand bien même n'auraient-elles rien changé au résultat des élections, le fait qu'on leur ait donné - ou prêté - une telle importance est déjà une victoire en soi pour leurs auteurs et leur commanditaire présumé. La campagne qui s'ouvrira incessamment sous peu aux Etats-Unis pourrait donc avoir un air de déjà vu.

Le président Donald Trump ne s'étant pas fait que des amis, en dehors de Kim Jong Un, au cours de son premier mandat, et l'Histoire aimant bégayer, la question de possibles nouvelles ingérences se pose, à quelques mois du prochain scrutin.

Le mode opératoire des actions Cyber menées en 2016 a été décortiqué et analysé, en long, en large et en travers. La documentation technique sur les cyber attaques est facilement disponible. Les sociétés de cybersécurité - FireEye, CrowdStrike, Fidelis Cybersecurity, Mandiant, SecureWorks, liste non exhaustive - qui ont enquêté sur le piratage du Democratic Congressional Campaign Committee (DCCC), sur les vols de données du Democratic National Committee (DNC) ou la diffusion de fake news sur les réseaux sociaux Twitter et Facebook ont publié de nombreux rapports suite à leurs investigations. Les services de renseignement américains ont confirmé tout ou partie des soupçons pesant sur deux principaux services de renseignement russes. En mai 2019, le procureur spécial Robert Mueller, chargé d'enquêter sur les accusations d'ingérences de ces services a publié un rapport de 448 pages sur l'affaire. Nous

⊙⊙⊙

WE INT.

*Le **THREAT INTELLIGENCE WEEKLY REPORT** est publié publiquement et gratuitement chaque semaine pour faciliter la compréhension des cybermenaces dans ses dimensions tant techniques que géopolitiques. Abonnez-vous pour le recevoir automatiquement par e-mail.*

Vous retrouverez en dernière page des détails sur nos offres de Cyber Threat Intelligence. Ces publications sont réservées à nos clients, adaptées à leur secteur d'activité et à leurs besoins spécifiques. Pour plus d'informations : threatintel@sekoia.fr

HUMAN **BEHIND BINARY**

ÉLECTIONS US 2020 : ON PREND LES MÊMES ET ON RECOMMENCE ?

renvoyons le lecteur désireux d'approfondir le sujet aux chapitres 28, 29 et 30 de l'excellent ouvrage de Thomas Rid "Active Measures - The Secret History of Disinformation and Politcal Warfare", non traduit à ce jour. La recette pour (re)produire les mêmes effets est à la portée de tous.

Selon Microsoft et Google, la prochaine campagne présidentielle américaine est dans le collimateur de plusieurs groupes d'attaquants, qui s'y préparent activement.

Shane Huntley, directeur du Google Threat Analysis Group (TAG) indique dans un tweet publié le 4 juin 2020 que deux groupes d'acteurs visent les équipes de campagne des deux candidats et plus particulièrement leurs comptes GMail. Le groupe APT31 (Chine) cible George Biden, le candidat démocrate. Le groupe APT35 (Iran), quant à lui, concentre ses efforts sur Donald Trump. Dans les deux cas, ce sont des campagnes d'hameçonnage ciblé qui sont lancées. Les équipes des deux candidats affirment avoir été briefées sur ces menaces et s'y préparer.

Le groupe APT31 est connu pour ses campagnes d'espionnage contre le secteur des télécommunications ou contre des associations humanitaires. Selon Microsoft, le groupe est très très actif ("very very busy") depuis un mois et demi.

Le groupe APT35 a déjà commencé à cibler des comptes associés à la campagne de Donald Trump en octobre 2019. Il s'était précédemment illustré dans des cyber attaques contre le secteur de l'énergie et celui des technologies et des gouvernements.

Les motivations de ces deux acteurs ne sont pas clairement identifiées : s'agit-il pour eux d'influencer la campagne d'un ou des deux candidats, en volant et diffusant des données, à la Russe ? Ou simplement, de mener des actions d'espionnage ?

Quant aux groupes russophones, ils sont dans tous les esprits mais ne semblent pas être encore sur le pied de cyber guerre. Il faut toutefois se méfier de l'eau qui dort.

Le contexte actuel - pandémie de la Covid-19, conséquences de celle-ci sur l'économie et, plus récemment, les protestations contre les violences policières et contre le racisme - peut aussi aisément servir de support à des campagnes de désinformation. Certains médias russophones, sans pour autant faire de l'infox, soufflent sur les braises en relayant les contenus relatifs à la répression des manifestations américaines. Le président tchétchène s'est même fendu d'une déclaration à la presse pour exprimer son sentiment horrifié (sic) sur les violences policières aux Etats-Unis. Seul SouthFront, un site pro-Russe en anglais, couvre les événements de façon outrancière et présente les manifestations comme une révolution de couleur menée par le parti Démocrate américain.

Twitter et Facebook ont pris des mesures pour limiter l'abus de leurs plateformes - fermeture de comptes identifiés comme participant à la diffusion de fake news, marquage de contenus dont la véracité ou l'honnêteté prêtent à réflexion - mais les deux réseaux sociaux ne semblent pas faire front commun ou avoir adopté une ligne de conduite homogène.

L'année 2020 promet d'être et de rester mouvementée aux Etats-Unis sur le plan Cyber.

Sources & Références

https://www.cyberscoop.com/biden-trump-china-iran-hacking-spearphishing-2020-elections/

https://www.zdnet.com/article/google-chinese-and-iranian-hackers-targeted-biden-and-trump-campaign-staffers/

https://www.zdnet.com/article/china-iran-and-russia-worked-together-to-call-out-us-hypocrisy-on-blm-protests/

https://arstechnica.com/tech-policy/2020/06/iran-and-china-backed-phishers-try-to-hook-the-trump-and-biden-campaigns/

https://www.theatlantic.com/magazine/archive/2020/06/putin-american-democracy/610570/

https://profilebooks.com/active-measures-hb.html

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[NSA] NOUVELLE VARIANTE DE COMRAT

La NSA a publié un communiqué indiquant que le groupe d'attaquants russophones Sandworm exploite activement la CVE-2019-10149. Cette faille, rendue publique en juin 2019, touche le MTA Exim largement utilisé sur Internet pour le transport et la distribution du courrier électronique. L'exploitation de cette vulnérabilité permet à un attaquant d'exécuter du code à distance sur un serveur vulnérable.

Au 1er mai 2020, seule une moitié des serveurs impactés par la faille ont été patchés. Le groupe Sandworm, qui serait rattaché à l'unité 74455 du GRU, exploite cette vulnérabilité pour installer des portes dérobées.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/nsa-warns-of-new-sandworm-attacks-on-email-servers/
https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf

[ZDNET] VULNÉRABILITÉ DANS VMWARE CLOUD DIRECTOR

VMware a publié un correctif pour la solution Cloud Director afin de couvrir la vulnérabilité CVE-2020-3956.

Celle-ci a été découverte par la société Citadelo lors d'un audit réalisé pour le compte d'une entreprise du Fortune 500. L'exploitation de cette CVE permet à un attaquant authentifié d'exécuter du code et dans certaines conditions de prendre le contrôle de machines virtuelles hébergées sur le même système hôte.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/vmware-cloud-director-vulnerability-could-be-exploited-to-hijack-full-server-infrastructure/

[GITHUB] DÉCOUVERTE DU MALWARE OCTOPUS SCANNER

Des chercheurs de GitHub Security Lab ont découvert en mars dernier un malware appelé Octopus Scanner qui a été utilisé pour des attaques sur la chaîne logistique (supply chain attacks) contre des dépôts Github.

Octopus Scanner cible l'environnement de développement intégré Java Apache NetBeans Il a infecté au moins 26 dépôts dans lesquels il a installé des portes dérobées.

Le serveur de contrôle (C2) du malware n'était plus actif quand les chercheurs de GitHub ont mené leurs investigations.

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

[ANSSI/CERT-FR] **RECOMMANDATIONS DE DURCISSEMENT POUR ACTIVE DIRECTORY**

Le CERT-FR a publié une liste de recommandations de durcissement des annuaires Active Directory. Ceux-ci sont des cibles privilégiées car la sécurité d'un réseau Windows repose majoritairement sur cette solution. La compromission d'un annuaire AD par un attaquant conduit dans la plupart des cas à la compromission de l'ensemble des machines qui y sont rattachées.

Le guide publié par le CERT-FR a pour vocation d'accompagner les entreprises dans leur processus d'amélioration du niveau de sécurité des annuaires Active Directory.

SOURCES ET RÉFÉRENCES :
https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/

[ZDNET] **CISCO PATCHE 4 VULNÉRABILITÉS CRITIQUES**

Cisco a dévoilé quatre failles de sécurité critiques affectant les routeurs sous IOS XE et IOS. Les quatre failles critiques font partie du bulletin semestriel de Cisco du 3 juin pour les logiciels de réseau IOS XE et IOS, qui comprend 23 avis décrivant 25 vulnérabilités.

L'exploitation de ces vulnérabilités permet une exécution de code à distance et une prise de contrôle des routeurs affectés.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

MAZE

La société Sparboe Companies, producteur d'oeufs du Minnesota, et la société Westech International, fournisseur du département américain de la défense et du département de l'énergie, ont été victimes d'une attaque par le groupe Maze.

Les opérateurs de la plateforme Maze se seraient associés à d'autres rançongiciels dont LockBit pour mettre en commun certains de leurs moyens.

Maze a ainsi publié sur son site des données volées à la société américaine Total Property Management par LockBit. Maze fait profiter d'autres attaques de sa "réputation", ses retours d'expériences et de sa visibilité.

REvil/Sodinokibi

Le groupe REvil/Sodinokibi a publié 1280 fichiers contenant des données personnelles de dirigeants d'Elexon volés lors de l'attaque dont a été victime le fournisseur d'électricité britannique le mois dernier.

Il a également créé une place de marché sur laquelle il propose à la vente les données volées à ses victimes qui refusent de payer les rançons exigées par les fraudeurs. Cela constitue un nouveau moyen de pression sur celles-ci et une nouvelle source de revenus pour les opérateurs du rançongiciel. Le site de vente aux enchères est présenté comme l'eBay des données volées.

Sekhmet

La société de services informatiques Excis a été victime d'une attaque par le rançongiciel Sekhmet.

DoppelPaymer

La société Digital Management Inc., fournisseur de service de la NASA, a été victime d'une attaque par le rançongiciel DoppelPaymer.

Netwalker

Après l'université de l'Etat du Michigan et le Columbia College of Chicago, l'University of California San Francisco a été victime du rançongiciel NetWalker.

Divers

L'administration de la communauté amérindienne canadienne de la Nipissing First Nation (NFN) a confirmé avoir été victime d'une attaque par rançongiciel.

SOURCES ET RÉFÉRENCES :
https://www.infosecurity-magazine.com/news/maze-claims-ransomware-attack-on-us/
https://www.bleepingcomputer.com/news/security/ransomware-locks-down-the-nipissing-first-nation/
https://www.bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/
https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/
https://www.databreaches.net/sekhmet-ransomware-team-claims-to-have-hit-international-it-firm-very-hard/
https://arstechnica.com/information-technology/2020/06/ransomware-gang-is-auctioning-off-victims-confidential-data/
https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/
https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/
https://www.bleepingcomputer.com/news/security/netwalker-ransomware-continues-assault-on-us-colleges-hits-ucsf/
https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack/

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 :

05/06/2020 - FL|INT.2020-105
Tycoon ransomware leverages an uncommon Java image format to fly under the radar

04/06/2020 - FL|INT.2020-104
Metamorfo banking trojan gains stealth using DLL hijacking

03/06/2020 - FL|INT.2019-099
USBCulprit: a Goblin Panda tool used in attacks against South East Asian governments

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
—