SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE

LA VENGEANCE CYBER EST UN PLAT QUI SE MANGE FROID

Le 10 juillet, le président américain Trump a confirmé que les Etats-Unis ont lancé en 2018 des cyberattaques contre la ferme à trolls russe de l'Internet Research Agency. Le rôle de cette agence avait été pointé du doigt dans les opérations de désinformation et de manipulation menées en parallèle des actions Cyber attribuées aux services de renseignement russes lors de la campagne présidentielle de 2016.

Cette opération a été lancée après que Donald Trump eut signé en août 2018 le National Security Presidential Memorandum 13 (NSPM-13) autorisant la CIA à mener des actions clandestines dans le domaine Cyber, sans que l'agence ait le besoin de demander d'autorisation préalable. Le NSPM-13 - qui aurait pu s'appeler le Patriot Hack - définit les conditions d'engagement de l'agence de renseignement quand elle dispose de suffisamment de preuves ou d'indices forts que des puissances étrangères ciblent ou nuisent aux intérêts américains et à la sécurité nationale. Les pays désignés dans ce mémorandum sont la Russie, la Chine, l'Iran et la Corée du Nord. La première application du NSPM-13 consista à s'attaquer à l'Internet Research Agency au moment des élections de mi-mandat en 2018.

La CIA se voit donc officiellement autorisée non seulement à collecter du renseignement à l'aide d'opérations de cyberespionnage mais aussi à mener des actions offensives dans le domaine Cyber dans un but de sabotage ou de destruction de capacités adverses, y compris celles en dehors du domaine cybernétique. Les infrastructures critiques comme les centrales électriques, les installations nucléaires, les raffineries, les réseaux de distribution d'énergie et d'eau sont inclus dans le périmètre d'action de la centrale de Langley, ainsi que des banques ou des institutions financières. Des vols de documents, suivis de leur publication en ligne ou leur communication à des journalistes, à la manière des opérations de hack-and-dump menées par les hackers russes en 2016 ou Wikileaks sont également au catalogue des actions cyber que pourrait mener la CIA dans le cadre de ce mémorandum.

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**

LA VENGEANCE CYBER EST UN PLAT QUI SE MANGE FROID

Enfin, le NSPM-13 entérine le droit pour la CIA de cibler des organisations humanitaires, des institutions religieuses ou des sociétés suspectées d'agir au bénéfice d'adversaires des Etats-Unis.

En résumé : le cyber Rubicon semble avoir été franchi.

Ne nous voilons pas la face : les services de renseignement de tous bords n'avaient pas l'interdiction de mener de telles campagnes jusqu'à peu : ils avaient celle de se faire prendre. Sans Edward Snowden, on spéculerait sûrement encore sur l'identité des auteurs et celle de leurs commanditaires d'attaques comme celle menée contre l'usine iranienne de Natanz à l'aide de Stuxnet. Et tant que les membres des groupes russophones APT28 et APT29 n'auront pas été formellement identifiés, le président russe pourra continuer à plaisanter sur ces hackers qui sont "des gens libres, comme les artistes qui se réveillent le matin de bonne humeur et commencent à peindre". Et qui, quand ils lèvent du pied gauche, sabotent des installations électriques ukrainiennes, interfèrent dans des campagnes électorales ou espionnent des laboratoires impliqués dans la recherche d'un vaccin contre la Covid-19.

Selon une source anonyme, le personnel de la CIA aurait salué la signature de ce mémorandum par des cris de joie, même s'il existe des dissensions au sein de l'agence sur ce tournant dans la doctrine régissant l'emploi des forces Cyber.

Une douzaine d'opérations auraient déjà été menées dans le cadre du NSPM-13.

La publication de données volées à la société russe SyTech, sous-traitant du FSB, pourrait être la conséquence d'une opération de la CIA conduite selon les règles du mémorandum. 7,5 To de données avaient été communiquées à divers organes de presse à l'issue de cette action de hack-and-dump en juillet 2019. Quelques mois avant, des fuites d'informations et de données savamment orchestrées, concernant des membres des services de renseignement Cyber iraniens seraient également le résultat d'une campagne conduite dans le même cadre. En novembre 2019, enfin, la diffusion des données de 15 millions de clients de trois banques iraniennes liées au corps des Gardiens de la Révolution Islamique démontrerait que la CIA n'hésite plus à s'attaquer au système bancaire d'un Etat. Les précédentes administrations américaines, y compris quand un président Républicain occupait le bureau oval, considéraient ce type d'action trop dangereux pour la stabilité du système financier mondial.

Le ministère de la Défense américain a adopté un nouveau concept : celui d'engagement permanent, selon lequel les forces Cyber américaines doivent rester en contact au jour le jour avec les forces adverses et pas seulement en cas de conflit ouvert.

Ce débat sur l'emploi de cyber armes n'est pas propre aux seuls Etats-Unis même si l'administration Trump est la première à opter officiellement pour une posture et une doctrine Cyber agressives.

De notre côté de l'Atlantique, dans un entretien accordé au journal Le Monde, le général François Lecointre, chef d'état major des armées, assume pleinement l'emploi par les forces armées "des armes cyber comme des armes du champ de bataille sur nos théâtres d'opérations, pour attaquer des réseaux de combat ennemis comme des centres de propagande".

En Iran, des explosions et des incendies dont l'origine reste indéterminée ont frappé l'usine de Natanz et des installations électriques au cours des dernières semaines. Le nombre et la fréquence de ces incidents serait le signe, selon le gouvernement iranien, qu'un Etat hostile en est responsable. Israël, impliqué dans Stuxnet aux côtés des Etats-Unis, fait figure de suspect idéal.

Le cyberespace, qui depuis quelques années est considéré comme un espace géopolitique, devient également un théâtre d'opérations à portée géopolitique. Dans "The Hacker and the State - Cyber Attacks and the New Normal of Geopolitics", Ben Buchanan, professeur à la Georgetown University School of Foreign Service, décrit le changement de portée des actions Cyber menées par des acteurs étatiques. Ces opérations étaient destinées à envoyer un signal ou un message d'avertissement de façon plus ou moins déguisée ou discrète à un adversaire. Elles deviennent de plus en plus souvent des outils "modificateurs", dont le but est de changer, à distance, une situation ou un équilibre, en faveur de celui qui les mène.

LA VENGEANCE CYBER EST UN PLAT QUI SE MANGE FROID

Le danger d'une escalade dans le domaine Cyber est une crainte exprimée par certains experts. Des Etats comme la Russie ou l'Iran pourraient s'appuyer sur la publicité faite par les Etats-Unis à ce changement de doctrine pour se poser en victimes ou comme cibles. Ils pourraient justifier des mesures de rétorsion ou les pousser à se lancer dans une course aux cyber armements. Cela pourrait également conduire à des attaques ayant des conséquences dans le monde physique, comme celles dénoncées par l'Iran contre ses infrastructures, et faire peser le risque de dommages humains.

Références

https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

https://www.lawfareblog.com/cia-covert-action-and-operations-cyberspace

https://www.zdnet.com/article/report-cia-received-more-offensive-hacking-powers-in-2018/

https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[CYBERSCOOP] MICROSOFT CORRIGE UNE VULNÉRABILITÉ CRITIQUE DE WINDOWS DNS SERVER

Microsoft a publié un correctif pour la vulnérabilité SIGRed qui touche le composant Windows DNS Server présent dans Microsoft Windows Server dans les versions 2003 à 2019.

Cette vulnérabilité critique a été découverte par Check Point et permet une exécution de code à distance avec les droits SYSTEM. Elle est déclenchée par l'envoi d'une réponse DNS malveillante. SIGRed pourrait être intégrée à un ver et se propager à des machines vulnérables sans action d'un utilisateur.

https://www.cyberscoop.com/microsoft-dns-patch-check-point-july-2020/
https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/

[NCSC] APT29 AURAIT CIBLÉ DES ORGANISATIONS IMPLIQUÉES DANS LA RECHERCHE D'UN VACCIN CONTRE LE COVID-19

La NSA, le DHS, le GCHQ et le CSE ont publié un communiqué conjoint qui attribue au groupe APT29 - également connu sous les noms de The Dukes ou Cozy Bear - la responsabilité de campagnes de cyberespionnage ayant visé des laboratoires anglo-saxons impliqués dans la recherche d'un vaccin contre la Covid-19 au Canada, aux États-Unis et au Royaume-Uni.

Le groupe APT29 aurait exploité des vulnérabilités présentes dans les solutions VPN Citrix, Pulse et FortiGate, ainsi qu'une vulnérabilité dans le webmail Zimbra pour compromettre des machines de leurs cibles, sur lesquelles ont été déployés les codes malveillants WellMess et WellMail. C'est la première fois que ces deux codes sont formellement attribués au groupe APT29.

https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

[BLEEPINGCOMPUTER] SAP CORRIGE LA VULNÉRABILITÉ CRITIQUE RECON

SAP a publié un correctif pour la vulnérabilité RECON présente dans le composant NetWeaver AS JAVA (LM Configuration Wizard) dans les versions 7.30 à 7.50. Cette vulnérabilité peut être exploitée par un attaquant distant non authentifié et permettre une prise de contrôle complète des systèmes vulnérables.

40 000 clients de SAP seraient concernés par RECON et il y aurait au moins 2500 serveurs vulnérables exposés sur Internet.

https://www.bleepingcomputer.com/news/security/critical-sap-recon-flaw-exposes-thousands-of-customers-to-attacks/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[THE REGISTER] DÉTOURNEMENT DU SERVICE GOOGLE ANALYTICS POUR VOLER DES DONNÉES DE PAIEMENT

Le pirate responsable du vol de plus de 200 millions de données appartenant aux société LinkedIn, Dropbox et Formspring a été reconnu coupable vendredi par un tribunal de San Francisco.

Yevgeniy Nikulin, un citoyen russe, a plaidé coupable des charges pesant contre lui et notamment du vol de 117 millions de données de comptes LinkedIn, 68 millions de données Dropbox et 28 millions de Formspring. La vente du fruit de ces cyber larcins lui aurait rapporté plusieurs centaines de milliers de dollars. Le pirate n'hésitait pas à faire étalage de cette richesse mal acquise.

Il avait été arrêté à Prague en 2015 avant d'être extradé vers les Etats-Unis, trahi par son train de vie luxueux et des dépenses somptueuses.

https://www.theregister.com/2020/07/14/russian_hacker_guilty/

[GEMINI ADVISORY] ETUDE SUR LES ACTIVITÉS DU GROUPE KEEPER

Selon une étude de la société Gemini Advisory, le groupe cybercriminel Keeper, spécialisé dans le web skimming, aurait volé 184 000 données de cartes bancaires et engrangé 7 millions de dollars entre juillet 2018 et avril 2019.

Affilié à Magecart, le groupe aurait compromis 570 sites en exploitant des failles du CMS Magento. Les victimes de Keeper sont majoritairement des internautes anglo-saxons.

https://geminiadvisory.io/keeper-magecart-group-infects-570-sites/

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

MAZE

Le fabricant de puces informatiques X-Fab a été victime d'une attaque par rançongiciel revendiquée par le groupe Maze sur son blog. Le déclenchement de la charge finale de l'attaque s'est produit alors que le Premier ministre français visitait le site français du fondeur le 5 juillet dernier.

NEFILIM

Orange a confirmé que sa branche Orange Business Services a été victime d'une attaque par rançongiciel qui a touché une vingtaine d'entreprises clientes. Le groupe Nefilim a revendiqué cette attaque dans un communiqué publié le 15 juillet sur son blog.

La société de services informatiques Collabera a subie une attaque le 8 juillet.

AUTRES

Un nouveau rançongiciel appelé AgeLocker utilise un outil de chiffrement développé par un employé de Google.

La société Check Point a détecté que le botnet Phorpiex a connu une hausse d'activité ces derniers mois et a été utilisé pour distribuer le rançongiciel Avadon.

L'US Secret Service a créé la Cyber Fraud Task Force, une unité dédiée à la lutte contre la cybercriminalité financière. Cette unité s'attachera à enquêter sur les attaques de type BEC et par rançongiciels. Présente dans 42 États américains, cette Task Force aura à terme 160 antennes aux Etats-Unis et dans le monde.

Le rançongiciel Conti, dont la diffusion est en augmentation depuis quelques mois, partagerait des échantillons de code avec Ryuk. Conti cible des entreprises et a été détecté fin 2019. Le nombre de détection de Conti aurait sensiblement progressé en juin dernier. Pour le chercheur Vitali Kremez, Conti serait tout simplement une version rebrandée de Ryuk.

https://www.businesswire.com/news/home/20200712005045/en/X-FAB-Track-Resume-Production-Cyber-Attack

https://www.bleepingcomputer.com/news/security/orange-confirms-ransomware-attack-exposing-business-customers-data/

https://www.theregister.com/2020/07/14/collabera_ransomware/

https://www.bleepingcomputer.com/news/security/new-agelocker-ransomware-uses-googlers-utility-to-encrypt-files/

https://www.zdnet.com/article/this-botnet-has-surged-back-into-action-spreading-a-new-ransomware-campaign-via-phishing-emails/

https://www.bankinfosecurity.com/us-secret-service-forms-cyber-fraud-task-force-a-14602

https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/

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.IO **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