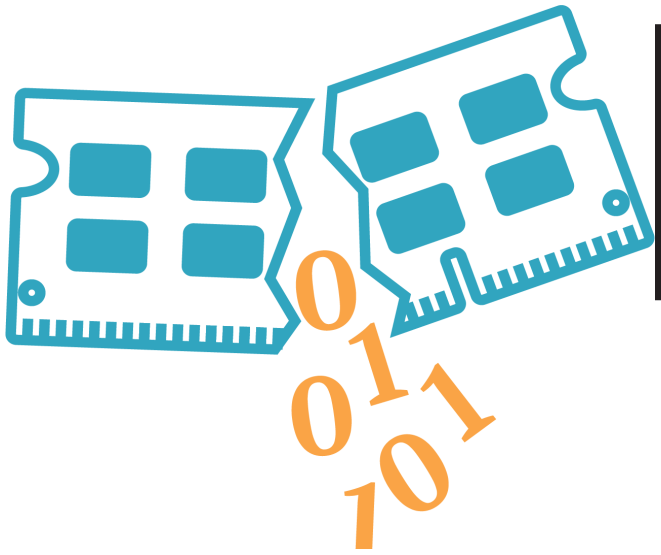
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE



J'AI LA MÉMOIRE QUI FLANCHE...

Heartbleed, Shellshock, Ghost, Badlock, RowHammer, RAMBleed ne sont pas les têtes d'affiche du prochain festival HellFest mais des vulnérabilités qui ont en commun d'avoir un nom, un logo et un site Web dédié. Ce qui en fait des vulnérabilités critiques et la garantie, pour leurs découvreurs, de faire le tour du monde des conférences de sécurité à l'oeil.

RAMBleed sera ainsi présentée au 41st IEEE Symposium on Security and Privacy en mai 2020. Il s'agit d'une vulnérabilité, identifiée par la CVE-2019-0174, qui peut être exploitée dans une side-channel attack, qui se traduit "attaque par canal auxiliaire" (et non "attaque au sac Chanel"). Ce type d'attaque se base sur le fait que le comportement physique d'un composant dépend des données qu'il traite ou manipule et que ce comportement est mesurable d'une façon ou d'une autre : variation de la consommation électrique, vitesse d'exécution ou temps de réponse, émanations électromagnétiques, etc. Nous renvoyons nos lecteurs intéressés par de plus amples détails sur ces attaques à la lecture des actes des conférences de SSTIC où quasiment chaque année ce sujet fait office de marronnier. L'objectif de RAMBleed est de lire arbitrairement le contenu de l'espace-mémoire alloué à des processus en cours d'exécution, y compris - surtout, serait-on tenté de dire - ceux qui n'appartiennent pas à l'utilisateur à l'origine de l'exploitation de cette vulnérabilité. RAMBleed est basée sur RowHammer, une vulnérabilité similaire dont l'exploitation permettait de modifier le contenu de la mémoire. Ironiquement, la rapidité d'accès physique des barrettes de mémoires de types DDR3 et DDR4 facilite ces attaques. Il avait été démontré que RowHammer permettait des élévations de privilèges, de rooter un ordiphone tournant sous Android, de faire fi du cloisonnement entre machines virtuelles et de s'échapper d'une sandbox. Une

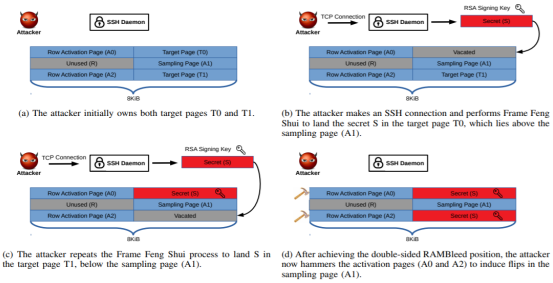
⊙⊙⊙

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

J'AI LA MÉMOIRE QUI FLANCHE...



(a) The attacker initially owns both target pages T0 and T1.

(b) The attacker makes an SSH connection and performs Frame Feng Shui to land the secret S in the target page T0, which lies above the sampling page (A1).

(c) The attacker repeats the Frame Feng Shui process to land S in the target page T1, below the sampling page (A1).

(d) After achieving the double-sided RAMBleed position, the attacker now hammers the activation pages (A0 and A2) to induce flips in the sampling page (A1).

Fig. 5: Overview of our attack on OpenSSH

implémentation en JavaScript affectant le navigateur Firefox dans sa version 39 avait été également publiée. De quoi jeter un froid et l'effroi notamment parmi les utilisateurs de Cloud. Le professeur Philip Mortimer se serait exclamé "By Jove!" à la lecture de la publication signée Andrew Kwong, Daniel Genkin, Yuval Yarom et Daniel Gruss. Ces chercheurs n'en sont pas leur coup d'essai. Ils s'étaient auparavant impliqués dans les recherches sur l'exploitation des processeurs Intel, recherches qui donnèrent lieu à la publication des vulnérabilités Spectre et Meltdown en janvier 2018.

RAMBleed remet le couvert. Ses découvreurs affirment qu'ils ont pu extraire de la mémoire de l'utilisateur root une clef OpenSSH RSA-2048 sur une machine sous Ubuntu dans ses paramètres de configuration par défaut. Cerise sur le gâteau : le code exécutant l'attaque ne requiert pas de privilèges élevés.

La mémoire exploitée durant les tests était constituée de barrettes de type DDR3 non-ECC. Une barrette dite "ECC" (Error-Correcting Code) est en théorie capable de détecter et corriger des modifications non souhaitées dans la mémoire d'un processus, que ce soit suite à une attaque ou simplement à une erreur. RAMBleed serait cependant capable de contourner cette protection selon ses découvreurs, même si pour leur test, ils se sont montrés prudents façon gazelle en exploitant de la RAM DDR3 non-ECC. Quant à savoir si les barrettes de type DDR4, non vulnérables à l'attaque RowHammer, sont également exposées, les avis divergent (et c'est beaucoup). Pour Intel, elles le sont mais les 4 experts sont moins catégoriques. Si la technologie ECC est utilisée par la barrette de RAM, une observation des temps de latence en lecture permet de déduire le contenu des cellules interrogées. Quoiqu'il en soit, si il vous reste un stock de DDR2, ne les jetez - ou ne les recyclez - pas tout de suite. A court terme, cette nouvelle attaque ne doit pas inquiéter le commun des mortels. Comme dans le cas de RowHammer, le facteur chance joue un rôle non négligeable dans la réussite de l'attaque.

La première phase de l'attaque consiste à localiser les données - en l'occurrence la clef RSA - auxquelles on souhaite accéder dans la mémoire. Cette étape a duré 34 heures dans la démonstration des découvreurs de RAMBleed. Il faut ensuite lire ces données. Dans le cas d'OpenSSH, le précieux Sésame est chargé en mémoire à chaque connexion SSH et n'y reste que 3 secondes environ. Cette limitation peut se contourner en initiant des demandes d'ouverture de sessions SSH en parallèle de l'attaque en elle même. Même dans ces conditions, il a fallu 4 heures pour lire 82% des données et donc récupérer une clef RSA partielle. Pour la reconstituer, les chercheurs ont utilisé une méthode et un algorithme décrits par Nadia Heninger et Hovav Shacham dans "Reconstructing RSA Private Keys from Random Key Bits". Les conditions pour une application en situation réelle - notamment sur une machine où s'exécutent de nombreux processus en même temps - d'une telle attaque ne seront donc probablement pas rassemblées avant un bon bout de temps. RowHammer a été découverte et documentée en 2014 et ses fondements théoriques étaient connus dès la fin 2012. En 2019, cette technique n'est pas utilisée massivement par des codes malveillants ou des groupes d'acteurs de même acabit. Une attaque en hameçonnage ciblé (spear phishing) reste autrement plus simple à conduire et plus efficace et a, selon nous, encore de beaux jours devant elle.

Sources et références

https://arstechnica.com/information-technology/2019/06/researchers-use-rowhammer-bitflips-to-steal-2048-bit-cryp-to-key/
https://www.bleepingcomputer.com/news/security/rambleed-attack-can-steal-sensitive-data-from-computer-memory/
https://www.zdnet.com/article/rambleed-rowhammer-attack-can-now-steal-data-not-just-alter-it/
https://rambleed.com/docs/20190603-rambleed-web.pdf
http://actes.sstic.org/SSTIC19/actes-2019.pdf
https://eprint.iacr.org/2008/510.pdf

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[CYBEREASON] LES SERVEURS EXIM SOUS LINUX CIBLÉS PAR UN VER

Le 5 juin 2019, les chercheurs de Qualys ont découvert une vulnérabilité critique. Identifiée par la CVE-2019-10149, elle impacte les versions 4.87 à 4.91 du logiciel largement répandu d'agent de transfert de courrier (MTA) Exim.

La vulnérabilité permet à un attaquant l'exécution de commandes à distance avec des privilèges root sur le serveur.

Le 14 juin, Microsoft annonce la présence d'un ver exploitant cette vulnérabilité sur des serveurs Exim sous Linux.

Le ver cherche des machines vulnérables puis, après infection, y dépose un logiciel de minage de cryptomonnaie. Il est recommandé de mettre à jour Exim pour la version 4.92.

SOURCES ET RÉFÉRENCES :
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability
https://duo.com/decipher/linux-worm-hits-unpatched-exim-servers

MOTS CLEFS : **EXIM / VULNÉRABILITÉ / VER**

[ZDNET] DES USINES DU SOUS-TRAITANT AÉRONAUTIQUE ASCO INDUSTRIES À L'ARRÊT DEPUIS PLUS D'UNE SEMAINE À CAUSE D'UN RANSOMWARE

La société Asco Industries, sous-traitant aéronautique, a été victime d'une attaque par ransomware le vendredi 7 juin 2019.

La compromission a commencé par une usine en Belgique et a provoqué l'arrêt de la production dans d'autres usines aux Etats-Unis, en Allemagne et au Canada.

Le redémarrage des services informatiques est toujours en cours mais la société a annoncé que de nombreux employés resteront au chômage technique jusqu'à dimanche.

Aucun élément technique n'a été communiqué publiquement sur cet incident et sur le ransomware utilisé.

SOURCES ET RÉFÉRENCES:
https://www.zdnet.com/article/ransomware-halts-production-for-days-at-major-airplane-parts-manufacturer/
https://www.lalibre.be/economie/libre-entreprise/l-arret-de-travail-chez-asco-prolonge-jusqu-a-dimanche-5d08d10f9978e27796543bd0
https://www.lalibre.be/economie/libre-entreprise/victime-de-piratage-informatique-asco-devrait-redemarrer-ses-activites-5d07a8c2d8ad580bf06596de

MOTS CLEFS : **RANSOMWARE / AÉRONAUTIQUE / USINES**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[TREND MICRO] **DÉPLOIEMENT DE CRYPTO-MINEURS VIA DES OUTILS D'ATTAQUES AVANCÉS**

Depuis mars 2019 se déroule une campagne d'attaques de cybercriminels visant à installer des crypto-mineurs Monero.

Les acteurs malveillants utilisent un panel d'outils tels que ceux publiés par le groupe The Shadow Brokers pour compromettre un large nombre de machines Windows.

Le crypto-mineur utilisé est une variante d'un mineur open-source fréquemment utilisé par les cybercriminels. Etant donné la diversité de secteurs d'activité et de pays impactés, les attaquants semblent ne pas avoir de cibles particulières si ce n'est des machines encore vulnérables. Cette campagne semble suivre la tendance d'attaquants peu expérimentés utilisant des outils avancés, parfois fournis «clé en main», disponibles publiquement sur Internet.

SOURCES ET RÉFÉRENCES :
https://blog.trendmicro.com/trendlabs-security-intelligence/advanced-targeted-attack-tools-used-to-distribute-cryptocurrency-miners/

MOTS CLEFS : **CRYPTOMINEUR / OPEN SOURCE**

[TREND MICRO] **NOUVELLE CAMPAGNE DE CYBERESPIONNAGE CIBLANT DES APPAREILS ANDROID**

D'après la société de cybersécurité Trend Micro, une nouvelle campagne d'espionnage appelée "Bouncing Golf" a été repérée au Moyen-Orient, infectant plus de 660 téléphones sous Android.

Le logiciel malveillant AndroidOS_GolfSpy.HRX est intégré dans des applications que les attaquants reconditionnent à partir d'applications légitimes. Les types de données volées concernent majoritairement des informations militaires et comprennent entre autre les informations de contact, les messages texte, les photos, les données de compte d'applications ainsi que le contenu du presse papier. Alors qu'en général les hackers recourent à la plateforme Google Play pour diffuser leurs applications malveillantes de manière globale, ceux à la tête de Bouncing Golf se servent plutôt des réseaux sociaux pour promouvoir le site web hôte du malware. Même si la campagne n'a pas encore été attribuée à un attaquant, la structure du code utilisé et les données ciblées présenteraient, d'après Trend Micro, des similitudes avec le mode opératoire avancé d'origine iranienne Domestic Kitten.

SOURCES ET RÉFÉRENCES :
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east

MOTS CLEFS : **ANDROID / DOMESTIC KITTEN / IRAN**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[WIRED] **INDISPONIBILITÉ DE TELEGRAM : LA CHINE A BON DDOS**

Le 12 juin 2019, l'application de messagerie chiffrée Telegram a été victime d'une attaque DDoS. Aucune donnée d'utilisateurs n'aurait été compromise durant l'interruption de service.

Selon Pavel Durov, CEO de Telegram, l'analyse des adresses IP employées pour mener le DDoS semblent indiquer que la Chine est à l'origine de l'attaque.
À la suite de la proposition de loi qui permettrait l'extradition vers la Chine de toute personne incarcérée à Hong Kong, une vague de contestation a secoué la région spéciale de Chine.

Toujours d'après Telegram, les autorités chinoises sont susceptibles d'avoir compromis l'application pour entraver les communications des manifestants qui ont également recours à WhatsApp et Signal pour communiquer. Permettant d'échapper à la censure et à l'espionnage étatique, ces applications sont devenues un outil incontournable pour l'organisation de rassemblements à l'encontre de régimes autoritaires.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/telegram-says-whopper-ddos-attack-launched-mostly-from-china/
https://www.wired.com/story/telegram-says-china-behind-ddos/

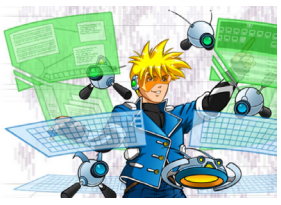
MOTS CLEFS : **TELEGRAM / DDOS / CHINE**

[RECORDED FUTURE] **DÉTECTION DE SERVEURS COBALT STRIKE MALVEILLANTS**

Cobalt Strike est une plateforme d'exploitation commercialisée par la société américaine Strategic Cyber LLC. Destinée aux Red Teams, elle permet de simuler des attaques reproduisant le mode opératoire de groupes d'adversaires connus.

Même si l'éditeur de cette plateforme exerce un contrôle scrupuleux sur les clients de son produit, certaines versions de l'outil ont fuité et se sont retrouvées entre de mauvaises mains, notamment les groupes APT-32 et Cobalt Group qui tirent son nom du logiciel de Strategic Cyber.

Insikt Group, l'équipe Threat Intelligence de Recorded Future, à qui l'on doit des analyses aussi pertinentes sur le plan géopolitique que sur le plan technique, fait le point dans cet article sur les différentes méthodes de détection des instances malveillantes de serveurs Cobalt Strike.



SOURCES ET RÉFÉRENCES :
https://www.recordedfuture.com/cobalt-strike-servers/
https://www.recordedfuture.com/identifying-cobalt-strike-servers/

MOTS CLEFS : **COBALT STRIKE / DÉTÉCTION / APT**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[SYMANTEC] **ATTENTION, UNE APT PEUT EN CACHER UNE AUTRE**

Symantec aurait découvert des éléments indiquant que le mode opératoire avancé russe Turla, affilié au gouvernement russe, aurait détourné l'infrastructure d'un autre groupe d'espionnage lors d'une attaque en novembre 2017 au Moyen Orient.

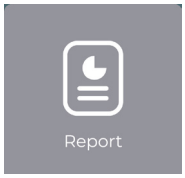
Le groupe d'attaquants APT34, également connu sous le nom d'Oilrig et ayant des liens avec le gouvernement iranien, en était la cible.

Turla a utilisé les serveurs de commande et de contrôle d'APT34 pour pirater l'infrastructure de la victime. En effet, en déposant des logiciels malveillants sur des ordinateurs précédemment compromis par APT34, les hackers russes ont pu avoir accès à son réseau. Même s'il semblerait qu'APT34 n'ait pas détecté l'intrusion, le groupe iranien s'est servi jusqu'à fin 2018 d'autres infrastructures de C2 pour rester actif dans le réseau compromis. Les groupes d'attaquants n'ont pas fini de jouer au chat et à la souris.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/telegram-says-whopper-ddos-attack-launched-mostly-from-china/
https://www.wired.com/story/telegram-says-china-behind-ddos/

MOTS CLEFS : **TURLA / APT / APT34**

[LE RAPPORT DE LA SEMAINE] **UNE ENCYCLOPÉDIE DES GROUPES D'APT**



Le 12 juin, ThaiCert, le CERT gouvernemental thaïlandais a publié un document de 275 pages recensant et décrivant un très grand nombre de groupes d'attaquants informatiques.

A télécharger ici :
https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0

NOS DERNIERS BILLETS **MEDIUM**

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

Augmented SOC—How to rethink your security center?

Facing the constant changing tactics of attackers and the endless growing number of log data, the SOC need to evolve to better anticipate the threats.

—> Le billet complet

The Pyramid of Pain ou l'échelle de la cyber-douleur

En 2013, David Bianco publiait sur le concept de « Pyramid of Pain » (PoP) que l'on peut traduire en français en « échelle de la cyber-douleur ». Cette échelle définit le degré et le niveau de dommages qu'il est possible d'infliger à un adversaire en fonction de ses capacités détruites, neutralisées ou dégradées par les actions des équipes de cyberdéfense de ses cibles.

—> Le billet complet

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**

- **flux d'IoCs :**

IN THREAT
SEKOIA THREAT INTELLIGENCE **FEED**

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