SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE

GANDCRAB : LES MALWARES NE SE CACHENT PLUS POUR MOURIR

Quand des groupes cybercriminels disparaissent, c'est souvent - même si parfois très tardivement - à la suite d'opérations - souvent spectaculaires - policières. Cela sauve la morale et confirme le dicton selon lequel "le cybercrime ne paie pas".

Ainsi, il est réconfortant d'apprendre que Bogdan V. R., citoyen roumain et skimmer, a été condamné lundi dernier à 65 mois de détention par un tribunal de Springfield, Massachusetts. Arrêté en 2016, il avait plaidé coupable en décembre 2018 des charges de fraude bancaire et de vol d'identité aggravé dans le cadre de clonage de carte de paiement.

Le 1er juin dernier, le rançongiciel GandCrab se retirait lui-aussi du jeu, mais d'une toute autre façon. Après 18 mois de service et de sévices, ses administrateurs ont annoncé qu'ils prenaient leur retraite.

GandCrab opérait selon un modèle différent de ces prédécesseurs les plus connus comme TeslaCrypt ou CryptoLocker. GandCrab était un Ransomware-as-a-Service : ses clients louaient le binaire de chiffrement, se chargeaient de le diffuser et la plate-forme s'occupait du reste : gestion du paiement des rançons, blanchiment des sommes ainsi extorquées et envoi des

⊙⊙⊙

GANDCRAB : LES MALWARES NE SE CACHENT PLUS POUR MOURIR

clefs de déchiffrement, le tout moyennant une petite commission, toute peine, même malveillante, méritant salaire.

Ce modèle connut un succès commercial fulgurant : la société Kaspersky estimait en mars 2019 que GandCrab détenait 40% du marché de la prise d'otage numérique.

Les clients de GandCrab étaient libres de le diffuser de la façon la plus appropriée : par mail, à l'aide d'Exploit Kits (EK) comme RIG (GandCrab disposant aussi de son propre EK) ou après compromission de l'infrastructure de leur cible, notamment en exploitant des vulnérabilités dans des outils d'accès distant. Ce fut le cas lorsqu'une vulnérabilité fut découverte dans un module édité par Kaseya pour ConnectWise Manage. Une vulnérabilité dans le logiciel GotoAssist aurait elle aussi été exploitée de façon similaire.

D'après Brian Krebs citant le chercheur Joe Stewart, GandCrab pourrait avoir été utilisé dans l'attaque contre la ville de Baltimore.

Dans l'annonce de la prochaine fermeture de leur service, les administrateurs de GandCrab affirment avoir généré près de 2 milliards de dollars de chiffre d'affaires - soit l'équivalent de 2 licornes - pour un bénéfice net de 150 millions après rétribution de leurs clients. Ce bénéfice aurait été blanchi et investi dans des entreprises légales, ce qui relève de ce que, dans un autre temps que les moins de 20 ans ne peuvent pas connaitre, l'on aurait qualifié de gestion en bon père de famille.

Cette apparente success-story, qui se termine sur un pied-de-nez malicieux - "nous avons prouvé qu'on peut gagner en un an suffisamment d'argent pour toute une vie" - cache peut-être une autre réalité. Les 2 milliards de dollars de chiffre d'affaires, pour commencer, semblent une somme exagérée. En outre, à l'instar d'autres rançongiciels, des outils gratuits de déchiffrement ont été fournis aux victimes de GandCrab. Michael Gillespie, grand décortiqueur de rançongiciel et administrateur du site ID-Ransomware.blogpost.com, avait noté une diminution du nombre de clients de la plate-forme avant cette annonce de mise de clef sous la porte.

Même s'il eut été préférable que la fermeture de GandCrab fut le fait d'une visite matinale des forces de l'ordre au domicile de ses auteurs, il ne faut pas se réjouir trop vite non plus. Le cybercrime, tel la nature, a horreur du vide. Le business-model GandCrab inspirera peut-être d'autres fraudeurs.

Références

https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-25-billion/

https://www.kaspersky.com/blog/gandcrab-ransomware-is-back/25854/

https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

https://nakedsecurity.sophos.com/2019/06/04/gandcrab-ransomware-service-shuts-up-shop/

https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[CROWDSTRIKE] **RETOUR SUR LE MODE OPÉRATOIRE « GRIM SPIDER »**

Crowdstrike partage ici les indicateurs observés de façon persistante lors de missions de réponse à incident pour des compromissions réalisées via le mode opératoire GRIM SPIDER. Pour rappel, GRIM SPIDER est l'un des modes opératoires qui peuvent être déployés par l'ensemble d'intrusion WIZARD SPIDER - ce dernier étant responsable de la compromission initiale du réseau - et a pour objectif d'extorquer financièrement une entreprise victime en déployant le ransomware Ryuk sur son parc informatique.

Ces modes opératoires agissent de la façon suivante : WIZARD SPIDER réalise des campagnes d'e-mails malveillants qui installent le plus souvent le malware Emotet. Lorsque le mode opératoire GRIM SPIDER s'ensuit, Emotet déploie TrickBot, puis ce dernier exécute des modules d'exploration et de mouvement latéral jusqu'à compromettre le contrôleur de domaine de la victime (d'autres modes opératoires utilisant TrickBot existent, par exemple la recherche de systèmes de point de vente).

Il est intéressant de noter que CrowdStrike observe que cette étape peut durer plusieurs jours, voire plusieurs semaines. Une fois cet objectif atteint, les opérateurs peuvent ensuite déployer et exécuter le ransomware Ryuk sur tout le réseau.

Cet article fournit essentiellement des indicateurs de compromission observables lorsque TrickBot exécute ses modules de vol de mot de passe et de mouvement latéral. Il souligne également une des faiblesses de ce mode opératoire : la longue durée nécessaire à la compromission du contrôleur de domaine, ce qui favorise ici la défense en offrant une longue fenêtre de détection.

Cet article peut également être un bon exemple de modélisation d'un ensemble d'intrusion d'après la base ATT&CK.

SOURCES ET RÉFÉRENCES :
https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/
https://pastebin.com/u/jroosen
https://urlhaus.abuse.ch/browse/tag/emotet/

MOTS CLEFS : **EMOTET / TRICKBOT / RYUK / RANSOMWARE / GRIM SPIDER / WIZARD SPIDER**

[BLEEPINGCOMPUTER] **NOUVELLE FUITE POUR UN OUTIL D'ESPIONNAGE DU MODE OPÉRATOIRE « OILRIG »**

Les outils d'espionnage de plusieurs groupes supposés oeuvrer pour le compte du gouvernement iranien font l'objet de fuites d'information depuis quelques semaines. Le dernier outil à avoir fuité serait utilisé par l'acteur OilRig (APT34).

Nommé Jason et décrit succinctement dans cet article, il paraît être un simple outil de compromission de compte Exchange par force brute. Les signatures de détection pour Jason (absentes initialement) ont été mises à jour, et 25 antivirus le détectent au moment où nous écrivons ces lignes. Néanmoins, la capture d'écran montre que Jason semble cibler Exchange Web Services et il n'est pas encore clair si cet outil se déploie également sur un réseau compromis pour attaquer un serveur Exchange interne.
Une solution d'authentification à deux facteurs ou une politique de mot de passe complexe (plus une sensibilisation sur la réutilisation des mots de passe) peuvent être efficaces contre ce type d'attaque automatisé, mais OilRig (ainsi que

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

d'autres acteurs) a déjà démontré sa capacité à contourner l'authentification forte en réalisant des attaques man-in-the-middle. En effet, la messagerie Outlook est l'un des objectifs privilégiés d'OilRig et Jason vient s'ajouter aux stratégies de compromissions diverses déjà utilisées par OilRig afin de compromettre les comptes email de ces cibles: phishing, exploitation de vulnérabilités dans les règles, formulaires et pages d'accueil de Outlook, attaques man-in-the-middle par compromission de serveurs DNS, etc.
La diffusion anonyme d'outils peut nuire temporairement aux opérations iraniennes, mais elle pourrait également leur permettre de se fondre dans un bruit créé par la réutilisation de ces outils par d'autres groupes, ou bien permettre à un autre groupe de se faire passer pour OilRig, dans le but par exemple de prendre des mesures de représailles contre l'Iran ou bien de faire que l'Iran en soit le bouc émissaire.

SOURCES ET RÉFÉRENCES:
https://www.bleepingcomputer.com/news/security/new-email-hacking-tool-from-oilrig-apt-group-leaked-online/#.XPWA3sHCqJI.twitter

MOTS CLEFS : **OILRIG / LEAKS / IRAN / EXCHANGE / APT34**

[GUARDICORE] PLUS DE 50 000 SERVEURS WINDOWS MS-SQL ET PHPMYADMIN COMPROMIS AVEC UN MALWARE CRYPTO-MINEUR

Une campagne basée en Chine, nommée Nansh0u, et visant l'installation de crypto-mineurs a infecté plus de 50 000 serveurs appartenant à diverses organisations des secteurs de la santé, des télécommunications, des médias et de l'informatique.

Le malware utilisé est conçu pour miner une crypto-monnaie appelée TurtleCoin. Pour déployer le crypto-mineur, les attaquants cherchent dans un premier temps les ports MS-SQL ouverts puis exécutent une attaque par brute force en utilisant un dictionnaire contenant des dizaines de milliers de mots de passe fréquents. Une fois dans le système, les attaquants exécutent un script MS-SQL qui télécharge et exécute la charge malveillante.

La charge utilise une vulnérabilité pour élever ses privilèges et obtenir celui du compte SYSTEM, exécute le mineur de crypto-monnaie, crée une persistance en écrivant des clés d'exécution dans le base de registre, protège le processus du mineur contre sa terminaison à l'aide d'un rootkit signé et garantit l'exécution continue du mineur en utilisant un mécanisme de surveillance.

Ces attaquants utilisent des techniques avancées observées précédemment par des APTs, telles que des vrais certificats mais de sociétés fictives et les vulnérabilités d'élévation de privilèges, ce qui est rarement le cas lors d'une attaque concernant les crypto-mineurs.

Cependant, diverses fautes de frappe et erreurs indiquent que, malgré son succès, l'opération n'a pas été testée avec soin.

SOURCES ET RÉFÉRENCES :
https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/

MOTS CLEFS : **NANSH0U, CRYPTO-MINEUR, CHINE, MS-SQL, PHPMYADMIN**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ECONINFOSEC] SEULEMENT 5,5% DES VULNÉRABILITÉS SERAIENT EXPLOITÉES POUR MENER DES CYBERATTAQUES

Une nouvelle étude a montré que 5,5% des vulnérabilités de sécurité connues seraient réellement exploitées par des attaquants.

Sur les 76000 failles découvertes entre 2009 et 2018, seules 4183 ont été utilisées pour mener à bien des cyberattaques.

Par ailleurs, la plupart des vulnérabilités exploitées dans la nature ont un indice de gravité CVSS de 9 ou 10. Les failles à plus haut risque étant les plus exploitées, il est donc plus facile de définir quelles vulnérabilités devraient être corrigées en priorité.

Fait intéressant, aucun lien n'a été trouvé entre la publication d'un code d'exploitation de preuve de concept (PoC) pour une faille donnée et le début d'une attaque exploitant cette vulnérabilité.

Comme seulement la moitié des 4183 vulnérabilités avaient un code d'exploitation disponible publiquement, cela pourrait signifier que les acteurs de la menace ont probablement développé eux-même leur propre code d'exploitation.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/
https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf

MOTS CLEFS : **VULNÉRABILITÉS / POC / CVSS**

FL INT. SEKOIA THREAT **INTEL**LIGENCE **FLASH** REPORT

Extraits de nos derniers rapports Flash Intelligence réservés à nos clients :

FL—INT #66
SandboxEscaper's Windows zero-day exploits

Type: 0-day
Date: 28/05/2019
Keywords: 0-day, CVE-2019-0863, CVE-2019-0841, Sandbox-escape, LPE

FL—INT #65
CVE-2019-0708 - Remote Desktop Services vulnerability

Type: Vulnerability
Date: 15/05/2019
Keywords: CVE-2019-0708, Remote Desktop Services, Remote Code Execution

FL—INT #64
TA505 new activities on financial enterprises

Type: Crimeware
Date: 29/04/2019
Keywords: ServHelper, LOLBins

NOS DERNIERS BILLETS **MEDIUM**

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

Focus adversaire : MuddyWater

MuddyWater, aussi connu sous le nom de Seedworm et TEMP.Zagros, est un mode opératoire supposé étatique, actif depuis au moins 2017. Même s'il semblerait que le groupe ait pour donneur d'ordre la République islamique d'Iran, cette affiliation reste à confirmer.

—> Le billet complet

Introduction to STIX and TAXII

Introduction aux standards internationaux STIX et TAXII qui permettent de décrire et partager de façon structurée du renseignement sur les cybermenaces.

—> Le billet complet

Threat Intelligence 101—Splendeurs et misères de la Kill Chain

Le concept de Kill Chain a été introduit au sein de l'Armée de l'air américaine à partir de 1973. Il décrit et modélise les étapes à suivre pour mener à bien une action militaire offensive ou défensive. Hasard ou simple coïncidence, ce concept a été transposé dans le cyberespace en 2011 par Eric M. Hutchins, Michael J. Cloppert et Rohan M. Amin de la société Lockheed Martin Corporation, grand fournisseur de l'U.S. Air Force.

—> 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 de 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
—