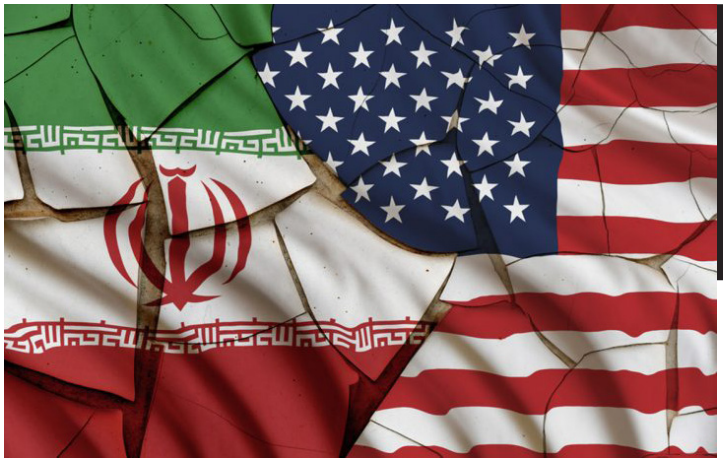
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE



ÉTATS-UNIS VS IRAN : BATAILLE NAVALE À L'HEURE DU CYBERESPACE

Les tensions entre les Etats-Unis et l'Iran s'intensifient depuis plusieurs mois et le cyberespace prend une place prépondérante dans les actions de chaque camp pour provoquer, (tenter de) dissuader ou répliquer aux démonstrations militaires, aux sanctions économiques ou aux tweets de certains protagonistes... Jusqu'à l'escalade ?

Alors que les États-Unis se sont retirés le 4 novembre dernier de l'accord sur le nucléaire iranien (JCPOA) signé en 2015, les tensions avec l'Iran se sont exacerbées.

Même si ni Washington ni Téhéran ne veulent la guerre, leur stratégie respective a pour principal effet de faire monter l'escalade et d'accroître les risques de conflit. L'Iran a ainsi été frappé depuis novembre 2018 par de multiples sanctions économiques américaines pour l'obliger à renoncer durablement à son programme nucléaire et balistique.

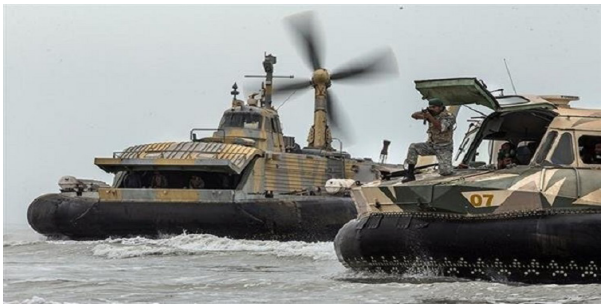
En excercant une pression économique sur le pays, l'administration américaine tente d'obtenir un changement de comportement de son adversaire.
Cette logique est pourtant loin de fonctionner puisqu'elle n'a fait que renforcer la volonté iranienne de défendre sa place sur la scène régionale. Non seulement Hassan Rohani n'a pas renoncé à son programme nucléaire, il a même annoncé vouloir augmenter à partir du 27 juin ses réserves d'uranium enrichi au-delà de la limite fixée par le JCPOA.

A cela s'ajoute une recrudescence des cyberattaques venues de l'Iran. Celles-ci se veulent plus agressives et offensives, soulignant une radicalisation affichée du gouvernement iranien dans sa position. L'objectif étant d'espionner, de perturber voire de mener des opérations d'influence contre les Etats-Unis. Car les

⊙⊙⊙

ÉTATS-UNIS VS IRAN : BATAILLE NAVALE À L'HEURE DU CYBERESPACE

cibles, que ce soit des organisations étatiques ou des entreprises, ont toutes un point commun: elles sont liées à Washington, dans sa propagande ou ses intérêts. D'après CrowdStrike et FireEye, l'Iran a intensifié ses cyberattaques offensives contre le gouvernement américain et ses infrastructures critiques telles que les secteurs pétrolier et gazier. Un communiqué rédigé au cours du weekend par Christopher Krebs, directeur de l'agence de sécurité des infrastructures (CISA) du ministère américain de l'Intérieur (DHS), a par ailleurs confirmé ces propos. D'après lui, l'Iran utiliserait de plus en plus de malwares de type wiper pour mener à bien des attaques destructrices rendant inutilisables les systèmes impactés. On peut par exemple penser au wiper Shamoon utilisé en 2012 contre Saudi Aramco et lors d'une cyberattaque en décembre 2018 contre l'entreprise pétrolière italienne Saipem. La cyber-arme s'ajoute donc aux armes plus conventionnelles utilisées dans la guerre asymétrique opposant les deux adversaires. Car oui, entre char d'assaut, croiseur et offensive cybernétique, le petit jeu entre Téhéran et Washington a tout l'air d'une partie de bataille navale :



- Le 13 juin dernier, les tensions ont grimpé en flèche après que deux pétroliers naviguant en B.4, dans les eaux de la mer d'Oman, ont été attaqués. **Touché**. Malgré les dénégations, l'Iran semble être le suspect principal.

- Pour se défendre, Trump a annoncé H.8 en envoyant 1000 soldats supplémentaires dans la zone du Moyen Orient. **Touché**.

- Le 20 juin, l'Iran a quant à lui annoncé C.5 et a abattu un drone américain survolant ses eaux. **Coulé !**

Ce dernier incident a failli mener à une attaque militaire américaine contre l'Iran d'autant plus que trois jours plus tôt, les forces iraniennes auraient, d'après Reuters, démantelé un réseau de cyber-espions américains. Alors que le cyber peut être un complément à des armes plus conventionnelles, ces dernières sont ici utilisées pour répliquer physiquement à une attaque orchestrée dans le cyberespace par l'élimination de combattants numériques. Même si les Etats-Unis n'ont pas riposté militairement à cette action, ils n'en ont pas pour autant perdu tous leurs navires de combats.

En plus d'établir de nouvelles sanctions visant cette fois notamment le guide suprême iranien Ali Khamenei, ils ont également adopté une approche plus coercitive en employant l'offensive cybernétique comme moyen d'intimidation. Les systèmes informatiques contrôlant la mise à feu des missiles et des roquettes iraniens ont été visés, sans succès d'après l'Iran. Cette stratégie redéfinit la doctrine américaine en matière de cyber puisque celle-ci ne se veut plus purement furtive et défensive mais revendiquée et offensive. Les cyberattaques ne sont plus simplement dissuasives mais un réel moyen d'afficher la position américaine et de dévoiler son jeu - de chat et de la souris. Le fait que l'administration Trump ait choisi de revendiquer l'attaque, alors qu'elle avait nié toute implication dans l'attaque de Stuxnet sur l'Iran en 2010, est d'ailleurs révélateur et permet à Trump de montrer qu'il ne reste pas inactif et en repli.

Reste à savoir si l'un des deux rivaux finira par couler l'ensemble de la flotte ennemie...

Sources et références

https://time.com/5612776/iranian-hackers-cyber-campaign-us/
https://www.lepoint.fr/monde/cyberattaque-americaine-contre-l-iran-le-brouillard-de-la-guerre-sur-le-net-26-06-2019-2321057_24.php
https://www.dhs.gov/cisa/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats
https://news.yahoo.com/pentagon-secretly-struck-back-against-iranian-cyber-spies-targeting-us-ships-234520824.html
https://www.axios.com/irans-history-of-hacking-and-being-hacked-ab1age96-63f1-4974-b75c-b72adc03dc51.html

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[CYBEREASON] **"SOFT CELL", UNE CAMPAGNE CIBLANT PLUSIEURS OPÉRATEURS DE TÉLÉCOMMUNICATIONS**

Dans un rapport publié le 25 juin 2019, des chercheurs de la société américaine Cybereason détaillent une campagne d'attaques ciblant divers opérateurs de télécommunications.

Cette campagne serait active depuis 2017 et est suivie par l'équipe de Cybereason depuis ce début d'année 2019.

Durant les six derniers mois, quatre vagues d'attaques ont été détectées. En analysant les outils et TTPs utilisés, Cybereason suspecte le groupe chinois APT10. Ces derniers ont exfiltré plusieurs gigabytes de métadonnées nommées «Call Detail Records» (CDR) contenant des informations comme la source, la destination et la durée d'un appel; le détail du téléphone utilisé; l'emplacement physique de l'appareil; le fournisseur ainsi que la version du téléphone. Le vol de ces données concerne des individus spécifiques dans plusieurs pays.
Cependant, rien ne prouve pour l'instant que les attaquants aient exfiltré le contenu des communications des victimes.

Pour plus de détails : FLINT. **#69**

SOURCES ET RÉFÉRENCES :
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

MOTS CLEFS : **TÉLÉCOMMUNICATIONS / APT / CHINE**

[REUTERS] **L'IDENTITÉ DES VICTIMES DE LA CAMPAGNE "CLOUD HOPPER" D'APT10 RÉVÉLÉE**

Une investigation publiée par Reuters revient sur l'opération Cloud Hopper attribuée au groupe chinois APT10 (dont 2 membres ont été inculpés par le Department of Justice américain en décembre 2018).
Elle révèle notamment l'identité des grandes entreprises victimes de cette campagne de cyberespionnage.

Selon Reuters, Hewlett Packard Entreprise, IBM, Fujitsu, Tata Consultancy Services, NTT Data, Dimension, CSC et DXC Technology ont été victimes d'APT10.

Mais le groupe d'attaquants avait d'autres objectifs en vue en compromettant ces géants de l'infogérance : leurs clients. Parmi eux, on retrouve Ericsson, grand concurrent de Huawei dans le secteur des équipementiers télécoms (5G notamment) mais également Sabre, un leader de la réservation de voyages ou encore Huntington Ingalls Industries, constructeur naval qui construit des sous-marins nucléaires pour l'US Navy.

SOURCES ET RÉFÉRENCES:
https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

MOTS CLEFS : **APT10 / MSP / CHINE**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[NASA] UN RAPPORT D'AUDIT RECENSE LES NOMBREUSES CYBERATTAQUES (RÉUSSIES) CONTRE UN CENTRE R&D DE LA NASA

Un rapport d'audit du bureau de l'inspecteur général de la NASA recense les très nombreuses faiblesses en matière de sécurité informatique du Jet Propulsion Laboratory (JPL), un centre de R&D de la NASA financé par le gouvernement fédéral situé à Pasadena, en Californie et géré par Caltech (California Institute of Technology).

Depuis 2009, les réseaux de JPL ont été compromis par au moins 6 différentes cyberattaques, occasionnant la fuite de centaines de gigaoctets de données confidentielles. Le dernier incident a été détecté en avril 2018 mais l'attaque était en cours depuis presque un an. Grâce à un compte d'un utilisateur externe compromis, les attaquants ont ensuite pu accéder aux réseaux de JPL via un Raspberry Pi non autorisé qui y était connecté et se latéraliser facilement pour atteindre leurs objectifs.

Le rapport identifie les manquements en matière de sécurité informatique qui sont à l'origine de ces nombreuses cyberattaques réussies contre les réseaux de JPL :

- inventaire de son parc informatique non exhaustif ;
- mauvaise segmentation des réseaux ;
- mauvaise gestion du patch management ;
- absence d'analyse des logs de sécurité ;
- manque de formation à la sécurité pour les administrateurs informatiques.

SOURCES ET RÉFÉRENCES :
https://oig.nasa.gov/docs/IG-19-022.pdf
https://www.zdnet.com/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network/https://oig.nasa.gov/docs/IG-19-022.pdf

MOTS CLEFS : **NASA / AUDIT / JPL / INCIDENTS**

[ZDNET] UTILISATION DE FAILLES ZERO-DAY SUR FIREFOX POUR ATTAQUER LES EMPLOYÉS DE COINBASE

En combinant deux failles zero-day de Firefox, des attaquants ont pu, via un mail de phishing, pénétrer dans le système de Coinbase, portefeuille et plateforme d'échanges de cryptomonnaies.

Après avoir été notifié par Coinbase d'une vulnérabilité sur Firefox, Mozilla a publié un correctif. L'équipe avait alors alerté que la faille pourrait permettre à un attaquant d'exécuter à distance du code dans le navigateur de la victime, mais qu'une autre faille était nécessaire pour exécuter du code sur l'OS. Deux mois après ces révélations, la faille a été exploitée en combinaison avec une autre vulnérabilité pour mener à bout des attaques sur les employés Coinbase. La manière dont les attaquants ont acquis les détails concernant l'utilisation de cette faille en la combinant avec une deuxième est inconnue. Aucune preuve d'exploitation ciblant les clients n'a par ailleurs pu être détectée.

SOURCES ET RÉFÉRENCES :
https://www.zdnet.com/article/firefox-zero-day-was-used-in-attack-against-coinbase-employees-not-its-users/

MOTS CLEFS : **FIREFOX / 0-DAY / CRYPTOMONNAIE**

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

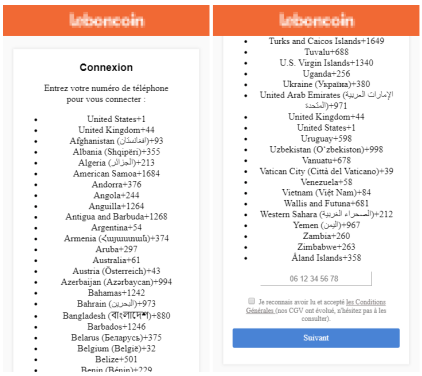
[SECURELIST] LE TROJAN ANDROID RILTOK SE DÉPLOIE SUR L'EUROPE

Initialement distribué principalement sur le territoire russe, le trojan Riltok ciblant les smartphones sous Android a été adapté et distribué en Europe.

Comme beaucoup de malwares de cette catégorie, le trojan se dissimule en une application populaire (même icone, même nom, etc.). En France, il usurpe, par exemple, le logo de l'application LeBonCoin.

La distribution de ce malware se fait au travers de campagnes SMS invitant l'utilisateur à suivre un lien qui, une fois cliqué, proposera à la victime d'installer une «nouvelle version» de l'application.

Une fois installé, le trojan espionnera la messagerie de l'utilisateur et fera apparaître des pages de phishing afin de collecter les informations bancaires de la victime.



SOURCES ET RÉFÉRENCES :
https://securelist.com/mobile-banker-riltok/91374/

MOTS CLEFS : **ANDROID / TROJAN / EUROPE**

[THREATPOST] DEUX VILLES DE FLORIDE PARALYSÉES PAR UN RANSOMWARE EN UNE SEMAINE

En l'espace d'une semaine, les villes de Riviera City et Lake City ont partagé bien plus que le doux soleil de Floride.

Si l'on ignore si les deux incidents sont liés, les services numériques de ces municipalités ont été verrouillés par un ransomware. Ces attaques semblent entrer dans le cadre d'une vaste campagne de ransomwares visant les autorités des Etats et des municipalités des États-Unis.

Paralysées par ce ransomware qui a aussi bien touché la mairie que la police et n'ayant pas de sauvegardes des disques durs, les autorités se sont résolues dans les deux cas à payer une rançon.

Pour Riviera City, qui n'avait plus accès à ses données depuis près d'un mois, la rançon s'est élevée à 65 bitcoins, soit environ 600 000$.

Ajoutons à cela le renouvellement de son parc informatique pour la somme de 941 000$, l'addition est salée. Quant à Lake City, 42 bitcoins, soit environ 460 000$, ont été versés.

SOURCES ET RÉFÉRENCES :
https://threatpost.com/second-florida-city-pays-hackers-500k-post-ransomware-attack/146018/
https://www.lemondeinformatique.fr/actualites/lire-ransomware-riveira-beach-verse-600-000-$-aux-pirates-75696.html
https://www.zdnet.fr/actualites/ransomware-cette-ville-de-floride-paie-600-000-pour-recuperer-ses-donnees-39886265.htm

MOTS CLEFS : **RANSOMWARE / BITCOIN / FLORIDE**

NOS DERNIERS BILLETS **MEDIUM**

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

IACD and the Quest for an Orchestrated Cyber Defense

Our journey takes us through the operationalization of the Integrated and Adaptive Cyber Defense (IACD) framework to guide security operational teams on the path towards security automation. After a short summary of the main issues encountered with traditional defense strategies, the article describes the IACD framework and details the orchestration services it models.

—> Le billet complet

Security Operations at a new pace

SEKOIA.IO will integrate the next Cyber@StationF program lead by Thales. We are very proud of that! The whole team is delighted to meet new colleagues there and to tune our ideas with technical experts and business leaders. Of course, the pitch focused on SEKOIA.IO but with a special angle: the acceleration of an operational security: "Bring security operations to a new pace"

—> Le billet complet

Threat Intel 101—Le cycle du renseignement appliqué à la (Cyber) Threat Intelligence

Ce modèle, qui nous vient du monde militaire, représente sous la forme d'un cycle assez simple le processus de création du renseignement. S'il est évidemment perfectible et critiquable, ce cycle du renseignement reste une représentation logique, pragmatique et pleine de bon sens de comment transformer des données puis des informations en renseignement qui va aider à la prise de décision stratégique et opérationnelle et donc à agir pour réduire un risque, une incertitude (dans notre thématique cybersécurité, de détecter ou de bloquer une attaque informatique).

—> Le billet complet

Threat Intel 101—Le modèle en Diamant

Tout analyste en Threat Intel reconnaîtra sa forme entre mille. Le modèle en Diamant : on l'adore, ou on le déteste. Pourquoi ? Souvent critiqué, le modèle en Diamant trouve sa valeur ajoutée dans la matérialisation visuelle d'axes relationnels et analytiques.

—> 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