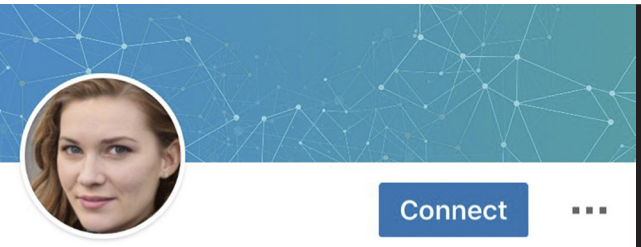
# SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE




## SI C'EST FLOU, C'EST QU'IA UN OURS

**Ce n'est pas la première fois qu'un faux profil LinkedIn est utilisé à des fins douteuses ou franchement frauduleuses. Mais dans le cas de Katie Jones, une étape a été franchie dans la sophistication : la photographie de cette jeune femme aurait été créée à l'aide d'une intelligence artificielle... Bienvenue dans l'ère du « AI-assisted influence operation ».**

Elle s'appelle Katie Jones, elle est américaine, âgée de 30 ans, membre du Center for Strategic and International Studies, un centre de réflexion de Washington DC. Ses centres d'intérêt sont la Russie et l'Eurasie. Elle est rousse, comme Anna Chapman et Maria Butina, deux citoyennes russes accusées d'espionnage. Mais ce doit être une coïncidence. Ou pas. Car la particularité de Katies Jones est qu'elle n'existe pas. Son profil LinkedIn est faux tout comme l'est la photo qui s'y affiche.

Ce n'est pas la première fois qu'un faux profil LinkedIn est utilisé à des fins douteuses ou franchement frauduleuses. Le gouvernement chinois est fortement soupçonné d'avoir créé des faux cabinets de vrais chasseurs de tête. Ceux-ci, via le réseau social professionnel, recrutaient des hauts fonctionnaires ou des collaborateurs gouvernementaux pour leur extorquer des informations confidentielles sous couvert d'études rémunérées. En 2009, deux speakers de la BlackHat ont présenté le résultat d'une expérience. Ils avaient créé de toute pièce un faux profil au nom de Robin Sage, qui se présentait comme une Cyber Threat Analyst âgée de 25 ans, employée au Naval Network Warfare Command, diplômée du MIT et forte de 10 années d'expérience. En quelques mois, elle s'était constitué un réseau de plusieurs centaines de contacts, dont certains V.I.P., dans le secteur de la Défense.

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**

# SI C'EST FLOU, C'EST QU'IA UN OURS

Depuis 2016 il est de notoriété publique que les réseaux sociaux sont devenus le principal vecteur de fausses informations à des fins de déstabilisation, de manipulation ou d'influence. Certains services gouvernementaux ont fait de Twitter et Facebook leur nouveau terrain de Grand Jeu.

Parmi les astuces dont peut user le cyber-quidam pour détecter un faux profil, la recherche inversée à partir de la photographie illustrant le compte suspect est la plus simple et souvent la plus efficace. Elle ne requiert pas de maîtriser un langage de programmation ni une quelconque application de visualisation (sauf si vous désirez illustrer des tweets de graphes à bulles aussi magnifiques qu'incompréhensibles).

Mais dans le cas de Katie Jones, une étape a été franchie dans la sophistication : la photographie de cette jeune femme aurait été créée à l'aide d'une intelligence artificielle. Elle est unique et résiste donc à un examen visuel sommaire et à l'utilisation de moteurs de recherche spécialisés comme TinEye.

Keir Giles est un consultant du Royal Institute of International Affairs (Chatham House), spécialisé sur la Russie. En 2015 il a rédigé une étude pour la Research Division du NATO Defense College sur le concept russe de guerre de l'information (Handbook of Russian Information Warfare). Plus récemment il a publié "Moscow Rules" aux éditions Brookings Institution Press, un ouvrage sur les relations difficiles et conflictuelles entre l'Ouest (Europe et Etats-Unis) et la Russie, dont nous vous recommandons chaudement la lecture (nous ne touchons aucun royalty sur les ventes). C'est lui aussi qui a signalé le profil de Katie Jones après avoir été contacté par cette "personne". K. Giles semble être un habitué des tentatives d'influence : en avril dernier il avait rencontré un monsieur Lambert au sujet de la mise au ban de l'éditeur - russe - Kaspersky par les autorités américaines. Au moins son interlocuteur était-il en chair et en os.

Pour Raphael Satter (Associated Press), auteur d'un article sur le cas K. Jones, la création de faux profils est entrée dans l'ère du Machine Learning et de l'Intelligence Artificielle. D'où un nouveau terme : AI-assisted influence operation. Cette photographie aurait été réalisée à l'aide de réseaux adverses génératifs (generative adversarial networks ou GAN). Cette classe de Machine Learning permet de créer des images fictives à partir d'échantillons réels. Elle a été utilisée par le collectif d'artistes Obvious pour générer le Portrait d'Edmond de Belamy, une oeuvre d'art vendue 432 500 dollars chez Christie's le 25 octobre 2018. Dans le domaine de la recherche pharmaceutique, l'Institut de Physique et de Technologie de Moscou développe des GAN pour créer de nouvelles structures moléculaires.

Il était bon au siècle dernier de se doter de solutions de sécurité "military grade" : les réseaux étaient protégés par des military grade firewalls. Le chiffrement était basé sur la military grade encryption - terme plus military hype qu'AES - ou sur la snake oil cryptography.

**Les opérations d'influence sont-elles condamnées à être de nos jours AI-assisted ?**

Le sujet, qui englobe aussi les deepfakes, ces fausses vidéos plus vraies que nature, est pris au sérieux aux Etats-Unis. Le comité pour le renseignement de la chambre des représentants américaine a ainsi tenu cette semaine une audience publique sur le défi que représente, pour la sécurité nationale, l'intelligence artificielle appliquée à la manipulation des médias et les «Deepfakes».

**Sources et références**

https://www.apnews.com/bc2f19097a4c4fffaa00de6770b8a60d

https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=657

## L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

### [TREND MICRO] **NOUVELLES ACTIVITÉS DU GROUPE MUDDYWATER**

**TrendMicro dévoile de nouvelles activités du groupe iranien MuddyWater (aka Seedworm, Temp.Zagros).**

Jusqu'à présent ce groupe concentrait ses tentatives de compromission sur des entités gouvernementales et des groupes de télécommunication ou d'infrastructure Internet du Proche-Orient et du Moyen-Orient. Fait nouveau, TrendMicro a observé des campagnes contre des organisations européennes et américaines. Cependant, la Turquie, le Pakistan, l'Afghanistan et la Jordanie sont toujours parmi les cibles privilégiées du groupe iranien : en plus de ses habituelles campagnes d'infection à partir d'e-mails contenant des documents exécutant des macros malveillantes qui installent une porte dérobée basée sur Powershell, TrendMicro a identifié de nouveaux modes d'infection à partir de malware Android distribués par SMS et via des sites officiels compromis qui ciblent ces pays. Lorsqu'une compromission aboutit, le groupe déploie des outils de post-exploitation, et plus rarement un second malware. Les comptes email compromis des victimes sont ensuite utilisés pour envoyer de nouveaux emails piégés, un mode opératoire particulièrement efficace lorsque les victimes sont des entités gouvernementales. MuddyWater place ses pions dans son grand jeu d'espionnage.

SOURCES ET RÉFÉRENCES :
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/
https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

MOTS CLEFS : **IRAN / MUDDYWATER / GOUVERNEMENT / TÉLÉCOM**

### [MORPHISEC] **RETOUR DU GROUPE FIN8**

**D'après Morphisec, le groupe cybercriminel FIN8 a lancé une nouvelle campagne d'attaques ciblant le secteur américain de l'hôtellerie entre mars et mai 2019.**

Connu pour mener des attaques motivées par des intérêts financiers, FIN8 cible plus particulièrement les entreprises exploitant des systèmes de points de vente (POS). Ceux-ci se font infecter par une variante plus sophistiquée de la porte dérobée ShellTea/PunchBuggy. Une fois la backdoor en place, FIN8 explore le réseau à la recherche des POS, et y installe un POS-scrapper, qui peut voler les numéros de carte bancaire en mémoire avant leur chiffrement. Ceux-ci seront ensuite vendus sur des forums de marché noir.

SOURCES ET RÉFÉRENCES:
http://blog.morphisec.com/security-alert-fin8-is-back

MOTS CLEFS : **FIN8 / POS / SHELLTEA / HOTELLERIE**

## L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

### [BLEEPING COMPUTER] DES MILLIONS DE SERVEURS MAIL EXIM VULNÉRABLES À UNE FAILLE DE SÉCURITÉ CRITIQUE

**Une faille de sécurité critique présente dans les versions 4.87 à 4.91 de l'agent de transfert de mail Exim (MTA) permet l'exécution de commandes à distance avec des privilèges «root».**

La faille est exploitable de façon triviale par un attaquant local et par un attaquant à distance dans le cas de certaines configurations spécifiques du serveur. Une attaque à distance dans le cas d'une configuration par défaut est faisable mais plus compliquée.

Le code d'attaque est disponible publiquement sur internet et plus de 4.8 millions de machines sont vulnérables à ce jour.

Les développeurs d'Exim ont mis à disposition une correction de cette faille.

Il est recommandé de passer à la dernière version d'Exim (version 4.92) - les précédentes étant considérées comme obsolètes.

SOURCES ET RÉFÉRENCES :
https://www.bleepingcomputer.com/news/security/millions-of-exim-mail-servers-exposed-to-local-remote-attacks/
https://www.openwall.com/lists/oss-security/2019/06/05/3
https://securityaffairs.co/wordpress/86864/hacking/exim-flaw-cve-2019-10149.html

MOTS CLEFS : **EXIM / MTA / RCE / VULNÉRABILITÉ**

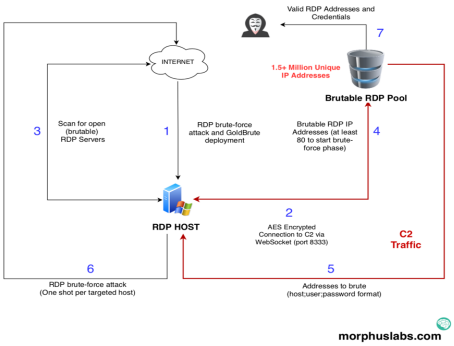
### [ISC SANS] LE BOTNET GOLDBRUTE S'ATTAQUE À DES MILLIONS DE SERVEURS RDP

**Découvert par un chercheur en sécurité de la société Morphus Labs, le botnet GoldBrute cible les systèmes Windows exposés sur Internet via le service RDP.**

Il tente des attaques par force brute pour s'y connecter et les enrôler dans le botnet.

Ce type d'attaque par force brute, généralement facilement détectable et blocable, est ici mené de façon «distribuée» afin de contourner les mesures de sécurité classiques : chaque bot teste, avec une seule combinaison de nom d'utilisateur et de mot de passe, des millions de serveurs.

Des recherches sur Shodan montrent que près de 3 millions de serveurs seraient exposés à ce type d'attaque. Les identifiants RDP compromis risquent également d'être revendus à d'autres groupes de cybercriminels, notamment ceux spécialisés dans la demande de rançon.




SOURCES ET RÉFÉRENCES :
https://isc.sans.edu/diary/GoldBrute+Botnet+Brute+Forcing+1.5+Million+RDP+Servers/25002
https://www.shodan.io/search?query=Remote+desktop

MOTS CLEFS : **RDP / BOTNET / FORCE BRUTE**

## L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

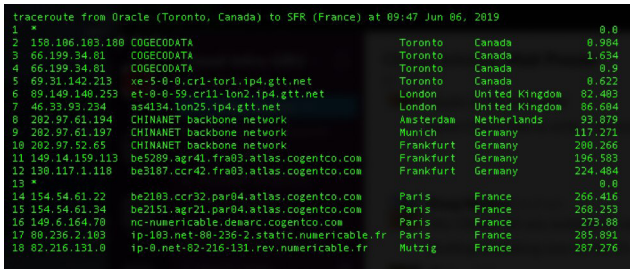
### [ORACLE] **UNE ERREUR DE ROUTAGE BGP DÉVIE UNE GRANDE PARTIE DU TRAFIC**

**Dans un incident qui reste encore non expliqué, l'opérateur suisse Safe Host a annoncé des routes erronées.**

Cet opérateur ayant un partenariat avec China Telecom, ce dernier a repris et diffusé ces routes plus largement, captant alors le trafic vers les 368 millions d'adresses IP incluses dans ces routes. Ceci a eu pour effet d'augmenter la latence de certains paquets, voire pour certains de subir la censure du Grand Firewall de Chine.

Certains services comme WhatsApp ont donc subi une interruption de service pendant plus de deux heures.

Il est reproché ici à China Telecom de n'avoir pas mis en place de moyens de filtrage des annonces de routes erronées ni de capacité de détection et de remédiation rapide de ces incidents. Cet incident vient rappeler la faible robustesse du protocole de routage BGP.



```
traceroute from Oracle (Toronto, Canada) to SFR (France) at 09:47 Jun 06, 2019
1  *                                                                        0.0
2  158.106.103.180 COGECODATA                          Toronto    Canada    0.984
3  66.199.34.81    COGECODATA                          Toronto    Canada    1.634
4  66.199.34.81    COGECODATA                          Toronto    Canada    0.9
5  69.31.142.213   xe-5-0-0.cr1-tor1.ip4.gtt.net       Toronto    Canada    0.622
6  89.149.148.253  et-0-0-59.cr11-lon2.ip4.gtt.net     London     United Kingdom  82.403
7  46.33.93.234    as4134.lon25.ip4.gtt.net            London     United Kingdom  86.604
8  202.97.61.194   CHINANET backbone network           Amsterdam  Netherlands     93.879
9  202.97.61.197   CHINANET backbone network           Munich     Germany         117.271
10 202.97.52.65    CHINANET backbone network           Frankfurt  Germany         200.266
11 149.14.159.113  be5289.agr41.fra03.atlas.cogentco.com  Frankfurt  Germany      196.583
12 130.117.1.118   be3187.ccr42.fra03.atlas.cogentco.com  Frankfurt  Germany      224.484
13 *                                                                        0.0
14 154.54.61.22    be2103.ccr32.par04.atlas.cogentco.com  Paris      France       266.416
15 154.54.61.34    be2151.agr21.par04.atlas.cogentco.com  Paris      France       260.253
16 149.6.164.70    nc-numericable.demarc.cogentco.com     Paris      France       273.88
17 80.236.2.103    ip-103.net-80-236-2.static.numericable.fr  Paris  France      285.891
18 82.216.131.0    ip-0.net-82-216-131.rev.numericable.fr  Mutzig    France       287.276
```

SOURCES ET RÉFÉRENCES :
https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom
https://blog.thousandeyes.com/whatsapp-disruption-just-one-symptom-of-broader-route-leak/

MOTS CLEFS : **BGP / CHINE**

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

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

**[UPDATE] SANDBOXESCAPER'S WINDOWS ZERO-DAY EXPLOITS**

Type: 0-day
Date: 12/06/2019
Keywords: 0-day, CVE-2019-0863, CVE-2019-0841, Sandbox-escape, LPE

**CRITICAL VULNERABILITY ON EXIM MAIL SERVERS**

Type: Vulnerability
Date: 14/06/2019
Keywords: Vulnerability CVE-2019-10149, Exim, MTA

**FIN8 IS BACK IN BUSINESS, TARGETING THE HOSPITALITY INDUSTRY**

Type: Malware
Date: 14/06/2019
Keywords: PunchBuggy, ShellTea, POS

NOS DERNIERS BILLETS **MEDIUM**

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

**Threat Intelligence data storage: make it easy with ArangoDB!**

At SEKOIA we heavily use STIX (Structured Threat Information eXpression) to manipulate Threat Intelligence information. As soon as a piece of information enters our system it is converted to the STIX format. Using a common standard presents some advantages but raises a few issues. In this blog post we are going to study how ArangoDB helps us store STIX data in an easy and efficient manner.

—> Le billet complet

**Dernières évolutions de MITRE ATT&CK**

La dernière mise à jour du framework ATT&CK date d'avril 2019 et apporte son lot de nouveautés. Elle intègre notamment 7 nouvelles techniques, la mise à jour de 11 techniques existantes, un nouveau concept de « sous-techniques » mais également et surtout une nouvelle « tactique» (Impact).

—> Le billet complet

**Threat Intel 101—CoA faire en cas d'intrusion ?**

Une des qualités du renseignement sur les menaces est d'être actionnable. Cet anglicisme signifie "qui permet et guide l'action". Dans le contexte de la réponse aux incidents ou celui de l'adaptation de la politique de sécurité et des défenses numériques d'une organisation, la Threat Intelligence doit permettre de répondre à la question posée en 1901 par Vladimir Ilitch Oulianov : "Que Faire" ?

—> 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