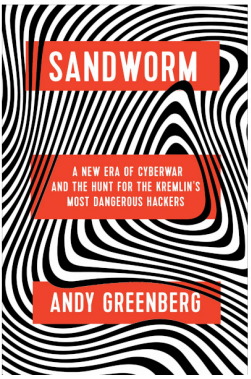
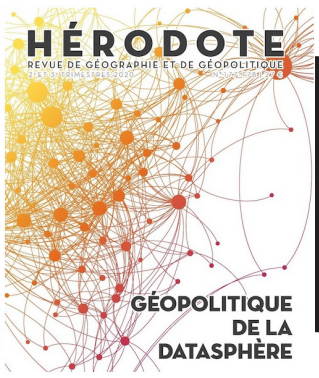
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE





CONSEILS DE LECTURE POUR L'ÉTÉ

Certains de nos lecteurs sont peut-être en train de préparer leurs valises avant un départ pour des congés bien mérités. Pour des vacances apprenantes réussies, voici quelques conseils de lecture à glisser dans votre sac de plage ou votre sac à dos.

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, de Andy Greenberg (Doubleday/Penguin)

Dans cet ouvrage, encore non publié en Français mais que toute bonne librairie indépendante devrait pouvoir fournir, Andy Greenberg, journaliste à Wired, retrace les activités du groupe Sandworm. Ce mode opératoire adverse russophone s'est fait connaître par des cyberattaques contre des infrastructures critiques en Ukraine en 2015 et 2016 au cours desquelles la distribution d'électricité avait été interrompue pendant de nombreuses heures en plein hiver.

Andy Greenberg avait couvert ces incidents et de nombreux autres attribués à différents groupes russophones pour le compte de Wired. Son article sur l'attaque NotPetya, publié en août 2018 dans Wired lui a valu de recevoir un Gerald Loeb Award en 2019 dans la catégorie Journalisme international.

A partir de l'analyse d'un document PowerPoint piégé détecté par la filiale ukrainienne de la société iSight en 2014, A. Greenberg relate les investigations qui ont conduit à la découverte d'une nouvelle variante du malware BlackEnergy. La découverte de chaînes de caractères inspirées par la saga Dune de Frank Herbert durant la rétro-ingénierie de cette version de BlackEnergy conduisit les analyses d'iSight à donner le nom Sandworm au mode opératoire adverse à l'origine de la campagne ciblant l'Ukraine.

A partir des cyberattaques contre les intérêts ukrainiens, imputées au groupe Sandworm, Andy Greenberg décrit comment la nécessaire défense des infrastructures SCADA est passée d'hypothèse de travail pour les organismes gouvernementaux américains à une réalité. Les événements survenus en Ukraine sur fond de conflit avec la Russie ont joué

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

CONSEILS DE LECTURE POUR L'ÉTÉ

le rôle d'accélérateur. Le groupe Sandworm semble particulièrement actif sur le volet Cyber du conflit, qu'il s'agisse de cibler des infrastructures critiques, des entreprises ou plus directement l'armée ukrainienne.

En 2016, le groupe Fancy Bear (APT-28) se retrouve sous le feu des projecteurs après ses actions dans le cadre de la campagne présidentielle américaine et notamment le piratage de la messagerie de John Podesta. La société Dell Secureworks établit un lien entre un compte Gmail utilisé pour compromette J. Podesta et une campagne ciblant des personnalités ukrainiennes. Derrière Fancy Bear se dessine l'ombre de Sandworm.

En 2017, après la deuxième attaque contre des fournisseurs d'énergie ukrainiens, la société ESET mène des investigations sur le code malveillant déployé par les attaquants. Le nouveau malware est appelé Industroyer par la société slovaque qui le décrit comme l'outil le plus complexe développé pour saboter un système SCADA depuis Stuxnet. Un échantillon du code est partagé avec la société Dragos, spécialisée en cybersécurité SCADA. ESET et Dragos publient chacune le fruit de leurs travaux sur ce nouveau malware qu'entre temps Dragos a renommé Crash Override. Sandworm a modernisé son arsenal et s'est doté d'armes plus sophistiquées capables, pour la première fois, d'occasionner des dégâts physiques dans les installations industrielles impactées.

Les groupes russophones seront très actifs durant cette année 2017 : en juin, NotPetya, code malveillant inséré dans une mise à jour d'un logiciel comptable ukrainien, touche de nombreuses entreprises en Ukraine et dans le monde, occasionnant plusieurs centaines de millions de dollars de dommages. Le cas de la société Maersk fait figure d'exemple. La campagne présidentielle française est également ciblée : l'équipe du candidat Emmanuel Macron est victime d'une compromission et d'un vol de données qui seront diffusées à la veille du second tour.

En 2018, la cérémonie d'ouverture des Jeux olympique d'hiver fait l'objet d'une cyberattaque, attribuée dans un premier temps à des acteurs nord-coréens. Après une analyse poussée des codes malveillants déployés pour saboter des serveurs, c'est, une fois encore, le groupe Sandworm ou un sous-groupe qui se profilent. Il faudra attendre janvier 2018 pour qu'un article du Washington Post, citant des sources anonymes de la CIA, avance que le GRU, le service de renseignement militaire russe, est à l'origine de l'attaque NotPetya. Il en découlerait que les groupes Sandworm et Fancy Bear seraient des équipes du GRU ou ne feraient qu'un. Au sein du GRU, les membres de Sandworm appartiendraient à l'unité 74455.

La lecture de l'ouvrage d'Andy Greenberg constitue un excellent récapitulatif des cyberattaques attribuées à la Russie depuis 2014 et pourrait faire l'objet d'une mise à jour ou d'un nouveau volume : en effet, le 25 juillet, Andy Greenberg a publié un article sur de nouvelles campagnes contre des entreprises de production et de distribution d'énergie américaines dont le GRU serait responsable. Dans un communiqué, la NSA alertait sur des tentatives par le groupe Sandworm d'exploitation de la CVE-2019-10149 affectant le MTA Exim.

Géopolitique de la datasphère, revue Hérodote

La revue de référence de géographie et de géopolitique Hérodote publie un numéro double sur le thème "Géopolitique de la #Datasphere". La même revue avait publié en 2014 un dossier consacré à la Géopolitique du cyberespace.

Dans son éditorial, Frédérick Douzet, professeur et directrice à l'Institut français de géopolitique (université Paris 8), définit la datasphère comme le "lien entre la sphère du monde physique et les données". La datasphère "peut se concevoir comme la représentation d'un nouvel ensemble spatial formé par la totalité des données numériques et des technologies qui la sous-tendent, ainsi que de leurs interactions avec le monde physique, humain et politique dans lequel elle est ancrée"

Sont abordés dans ce numéro des thèmes comme les campagnes d'influence sur les réseaux sociaux attribuées à la Russie en 2016, la place de ces réseaux dans la stratégie électorale du Premier ministre indien Narendra Modi ou bien encore le développement des stratégies d'influence russe et chinoise à destination des internautes africains dans le cadre du développement de leur présence et de leurs activités sur le continent africain. Ces stratégies s'appuient sur des médias internationaux russes et chinois implantés en Afrique,

CONSEILS DE LECTURE POUR L'ÉTÉ

dont les publications sont reprises et relayées sur les réseaux sociaux. Les auteurs de l'article "Cartographier la propagation des contenus russes et chinois sur le Web africain francophone" montrent que les internautes de la Guinée, pays riche en bauxite, ressource à laquelle s'intéresse la Chine, relaient activement les contenus favorables aux intérêts chinois. Il en est de même en Côte d'Ivoire, pays dans lequel la Chine, à travers des entreprises ou des aides au développement est très active et présente.

Rédigé avant le confinement lié à la pandémie de la Covid-19, un article sur l'informatique nuagique (cloud computing) montre comment cette technologie et ses usages, y compris dans la sphère économique privée, sont devenus un enjeu géopolitique et l'objet du développement d'une politique publique dédiée au cloud computing. Rappelant les échecs des clouds souverains, les auteurs montrent comment la notion de cloud de confiance, basée sur la sécurité des données, s'est imposée comme un sujet stratégique aux autorités gouvernementales.

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ZDNET] LE FBI ALERTE LES ENTREPRISES AMÉRICAINES CONTRE UNE PORTE DÉROBÉE DANS UN LOGICIEL COMPTABLE CHINOIS

La société Trustwave a publié en juin 2020 un rapport dévoilant la présence de codes malveillants - GoldenHelper et GoldenSpy - embarqués dans un logiciel comptable dont l'installation est requise pour le règlement des taxes sur la valeur ajoutée en Chine.

Dans une note diffusée mardi, le FBI a mis en garde les entreprises américaines contre le risque que présente ce logiciel et sa potentielle utilisation à des fins d'espionnage économique. Le FBI indique avoir eu vent d'au moins deux incidents, en 2018 et en 2020, dans lesquels les deux codes malveillants ont été exploités pour des vols de données sensibles.

Selon le FBI, deux éditeurs de solutions comptables dans lesquelles GoldenHelper et GoldenSpy ont été détectés travaillent sous la supervision du National Information Security Engineering Center, une entreprise en lien avec l'Armée Populaire de Libération, faisant craindre que l'insertion de ces codes ait été faite dans le cadre d'une campagne étatique d'espionnage.

https://www.zdnet.com/article/fbi-warns-us-companies-about-backdoors-in-chinese-tax-software/

[THREAPOST] LA NSA ALERTE SUR UNE POTENTIELLE EXPLOITATION D'UNE FAILLE DANS UN COMPOSANT SCADA CRITIQUE

L'Agence de sécurité nationale américaine (NSA) et l'Agence de cybersécurité et de sécurité des infrastructures (CISA) ont mis en garde contre des attaques pouvant viser des infrastructures critiques à travers les États-Unis.

L'ICS-CERT a émis un bulletin sur une faille de sécurité critique trouvée dans le logiciel TriStation et le module de communication Triconex de Schneider Electric. Ces contrôleurs du système d'instrumentation de sécurité sont utilisés pour déclencher l'arrêt d'équipements industriels en cas de problème avant que surviennent des accidents tels que des explosions ou des incendies. Ces deux composants ont déjà été ciblés par le code malveillant TRITON en 2017.

Le bulletin rédigé conjointement par la NSA et la CISA fait état de deux incidents ayant affecté un pipeline en février 2020 et des éoliennes en novembre 2019. Dans ces deux cas, le contrôle et la supervision des équipements industriels impliqués avaient été momentanément perdus par les opérateurs.

https://threatpost.com/nsa-urgent-warning-industrial-cyberattacks-triconex/157723/
https://us-cert.cisa.gov/ics/advisories/icsa-20-205-01

[BLEEPINGCOMPUTER] UN "JUSTICIER" PERTURBE LA DISTRIBUTION DE MALWARE PAR EMOTET

Le botnet Emotet a été victime d'une intrusion non revendiquée qui a perturbé la distribution par de codes malveillants.

Un intrus dont l'identité n'a pas été révélée a piraté des sites préalablement compromis par les opérateurs d'Emotet

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

et a remplacé les malware par des images reprenant de célèbres mêmes. Cet intrus aurait tout simplement exploité la faiblesse de certains mots de passe et leur réutilisation par les opérateurs d'Emotet sur de nombreux sites de distribution.

https://www.bleepingcomputer.com/news/security/emotet-malware-operation-hacked-to-show-memes-to-victims/

[CYBERSCOOP] LA FAILLE CRITIQUE CVE-2020-5902 EST ACTIVEMENT EXPLOITÉE SELON LA CISA

La CISA a communiqué sur deux incidents impliquant une organisation gouvernementale et une entreprise américaines, dans lesquels les attaquants ont exploité la faille critique CVE-2020-5902 affectant les équipements BIG-IP de la société F5 Networks.

L'agence note une recrudescence de tentatives des activités de reconnaissance par balayage et d'exploitation de cette vulnérabilité qui permet l'exécution de code à distance. La CISA incite vivement les utilisateurs des solutions impactées à appliquer les correctifs fournis par F5 dans les plus brefs délais.

https://www.cyberscoop.com/cisa-f5-vulnerability-exploitation-incident-response/
https://us-cert.cisa.gov/ncas/alerts/aa20-206a

[ARS TECHNICA] LE GRU CIBLE DES ORGANISATIONS GOUVERNEMENTALES ET LE SECTEUR DE L'ÉNERGIE AMÉRICAINS

Selon le FBI, le groupe Fancy Bear tenterait de compromettre des serveurs de messagerie, des comptes Office 365 et des serveurs VPN. Fancy Bear, qui serait lié au GRU, le service de renseignement militaire russe, ciblerait des Etats américains et des organisation fédérales, ainsi que des universités. Le groupe ciblerait aussi le secteur de l'énergie.

https://arstechnica.com/information-technology/2020/07/russias-gru-hackers-hit-us-government-and-energy-targets/

[ARS TECHNICA] DEUX RESSORTISSANTS CHINOIS POURSUIVIS POUR ESPIONNAGE

Le ministère de la Justice américain a publié un acte d'accusation à l'encontre de deux ressortissants chinois soupçonnés de s'être livrés à des actes d'espionnage depuis au moins 10 ans. Les dommages causés par ces actes se chiffrent en centaines de millions de dollars selon le DoJ.

https://arstechnica.com/tech-policy/2020/07/doj-accuses-chinese-hackers-of-trying-to-steal-covid-19-research-data/

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

WASTEDLOCKER

La société Garmin a été victime d'une attaque par le rançongiciel WastedLocker. Les solutions de géolocalisation proposées par la société ont été fortement impactées par cette attaque qui a provoqué des arrêts de services pour les clients grand public mais aussi professionnels de la société. Les lignes de production de l'équipementier taïwanais ont également été touchées par cette attaque. Il n'est pas encore clairement établi que des données utilisateurs aient été volées durant cette attaque.

SODINOKIBI / REVIL

La société Arete a publié un rapport de ses activités en réponse aux incidents dans des cas d'attaques par Sodinokibi. Le rapport se base sur 41 interventions de l'équipe Arete IR, majoritairement dans le secteur de l'éducation.

18.000 ordinateurs du fournisseur de service argentin Telecom Argentina ont été compromis par une attaque revendiquée par le groupe Sodinokibi. L'attaque s'est produite le samedi 18 juillet et les fraudeurs demandent 7,5 millions de dollars de rançon à l'opérateur Télécom. Les opérations de Telecom Argentina n'ont pas été impactées par cette attaque.

Autre victime du groupe Sodinokibi : la société ferroviaire espagnole ADIF. Les attaquants affirment avoir volé 800 Go de données à l'opérateur espagnol. Cette attaque n'a pas perturbé ses services.

AUTRES

Dans un rapport sur les cybermenaces liées à l'industrie du sport, le NCSC britannique indique que les attaques par rançongiciels font partie des trois principales menaces auxquelles font face les clubs sportifs. Le rapport fait mention d'une compromission d'un club de l'English Football League dont l'origine n'a pas été déterminée mais pourrait être un hameçonnage ou une intrusion dans le réseau de caméras d'un stade.

Le fournisseur de solutions et d'infrastructures nuagiques Blackbaud a reconnu avoir dû verser une rançon à la suite d'une attaque dont il a été la cible. Blackbaud avait réussi à stopper l'attaque avant le chiffrement de ces machines mais n'avait pas pu empêcher le vol préalable de données. La rançon a été versée pour que ces données ne soient pas publiées. Des données appartenant à des clients de Blackbaud, dont des universités et des organisations humanitaires, auraient été dérobées par les attaquants.

https://www.zdnet.com/article/garmins-outage-ransomware-attack-response-lacking-as-earnings-loom/

https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/

https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf

https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/

https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/

https://www.techtimes.com/articles/251345/20200724/blackbaud-security-breach-impacted-6-uk-universities-ransomware-attack-worse.htm

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