Lettre trimestrielle - Décembre 2017-disponible sur omc.ceis.eu

Table des matières

L'AIDE DES ETATS-UNIS A L'UKRAINE EN MATIERE DE CYBERSECURITE

En mars 2014, le Congrès américain adopte le *Ukraine Support Act*[1] en réaction à l'annexion de la Crimée par la Russie, puis renforce son soutien avec le *Ukraine Freedom Support Act of 2014*.

La crise ukrainienne a fait de ce pays le théâtre d'expérimentations militaires et de mesures opérationnelles d'un type nouveau. Une place centrale a ainsi été accordée aux mesures informationnelles et aux attaques informatiques dans le conflit, qualifié dès lors de « guerre hybride ». Dès le début du conflit, l'Ukraine a en effet été victime de nombreuses cyberattaques dont l'origine russe a été immédiatement supposée par les commentateurs occidentaux - comme pour celles dont avaient été victimes l'Estonie en 2007 et la Géorgie en 2008 -, notamment d'attaques sur ses infrastructures critiques (en particulier énergétiques), devenant ainsi un quasi- « laboratoire à ciel ouvert en matière de cyber-offensive entre Moscou et Washington »[2].

La plupart des pays et organisations internationales ont fait preuve d'indécision sur les mesures concrètes à adopter face à ce qui pouvait apparaître, soit comme l'éclatement de tensions internes et le passage à un *conflit civil armé*, soit comme une violation du droit international à travers l'annexion de la Crimée par la Russie. Ainsi, si l'Union Européenne est très directement concernée par ce conflit qui se déroule à ses frontières, c'est d'abord Washington qui a décidé d'apporter un soutien accru, notamment militaire, à l'Ukraine à partir de 2014.

Après la Géorgie, l'Ukraine nouveau théâtre d'une guerre hybride ?

De *BlackEnergy* à *Petya/NotPetya* : les soupçons d'ingérences et d'offensives russes dans l'espace cyber ukrainien

La cyberdéfense est devenue un enjeu stratégique pour l'Ukraine en raison des nombreuses attaques informatiques dont elle a été la cible au cours des quatre dernières années.

En effet, dès le mois de février 2014[3], les premières apparitions du *malware BlackEnergy*[4] sont relevées en Ukraine par *BAE Systems*, qui signale alors une forte augmentation du nombre de réseaux ukrainiens touchés par ce virus (attaque « Campagne Serpent », « *Snake Campain* »)[5]. D'après les ingénieurs de l'entreprise, *BlackEnergy* était une version améliorée du ver informatique *Autorun* (« W32/Autorun.worm.dw » ou

[1] "An act to support the independence, sovereignty, and territorial integrity of Ukraine, and for other purposes", https://www.congress.gov/bill/113th-congress/house-bill/4278 : *Sets forth U.S. policy regarding Ukraine, including: (1) support for the sovereignty and territorial integrity of a democratic Ukraine, and (2) condemnation of Russia's armed intervention into Ukraine and its illegal annexation of Crimea*.

[2] *Intelligence Online*, « Les Républicains relancent la cyber-offensive à Kiev », Septembre 2017, N789 p.1, https://www.intelligenceonline.fr/renseignement-d-etat/2017/09/06/les-republicains-relancent-la-cyberoffensive-a-kiev,108260182-eve

[3] A ce sujet, on peut voir l'article de Pierre Sautreuil et Fabrice Deprez, « Ukraine, anatomie d'une cyberguerre », publié le 05/09/2017 sur le site *Numerama* : http://www.numerama.com/politique/283573-en-ukraine-la-cyberguerre-au-quotidien-episode-1-la-menace-permanente.html

[4] Egalement appelé « Uroburos » par *BAE Systems*.

[5] http://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign

Agent.BTZ)[6], dont le mode de propagation reposait au départ sur la contamination de clés USB. *Autorun* correspondait lui-même à une variante améliorée du ver « *SillyFDC* »[7], dont l'utilisation dans une cyberattaque massive à l'encontre de systèmes de l'armée américaine avait été relevée par des ingénieurs militaires en 2008[8].

Depuis, la généalogie du virus a permis de remonter à une souche commune, possiblement créée par le groupe « *Sandworm* »[9] également suspecté d'être à l'origine de *BlackEnergy* en 2014. Celui-ci est fortement soupçonné de liens avec les groupes cybercriminels APT 28 et 29 (aussi surnommés « *Fancy Bear* » et « *Cozy Bear* »), eux-mêmes soupçonnés de collusion avec les services de renseignement russes FSB et GRU.

Outre des fonctions rédigées en russe et en cyrillique dans les programmes malveillants employés par « Sednit »[10], les ingénieurs d'ESET ont en effet découvert le réemploi de parties du code du *malware BlackEnergy* dans des programmes de cyber-espionnage de ce groupe : le système « DOWNDELPH », qui emploie des méthodes de persistance avancées, notamment par le détournement du fonctionnement naturel du *Windows bootkit* et par le biais d'un *rootkit Windows*.[11]

Puis, en mai 2014, ce sont des attaques massives de type *DDoS* (*Distributed Denial of Service*) qui frappent l'Ukraine, avec une ampleur encore jamais observée auparavant. Ainsi, alors que l'entreprise ukrainienne *InfoSafe IT*[12] a toujours réussi à assurer le bon déroulement des élections ukrainiennes depuis 2006 malgré des attaques *DDoS* systématiques pour les perturber, elle ne parvient pas à juguler le flux de connexions lors de l'attaque du 21 mai 2014, quatre jours seulement avant les élections présidentielles. Or, dès le lendemain, cette attaque est revendiquée par le groupe de pirates informatiques « *CyberBerkut* », dont les actions et les publications sur son site internet (https://cyber-berkut.org/) revêtent toujours un caractère ostensiblement « pro-russe ».

Après cette attaque, il a ainsi fallu deux jours aux experts de *InfoSafe IT*, avec l'aide des services gouvernementaux ukrainiens, pour restaurer le système de décompte des voix. Cependant, le jour des élections, une quarantaine de minutes avant la proclamation des résultats, un faux communiqué apparaît sur le site de la commission électorale annonçant la victoire du candidat d'extrême-droite Dmytro Iaroch, alors que les résultats placent largement en tête Viktor Porochenko[13].

---

[6] https://www.docaufutur.fr/2015/01/19/dagent-btz-a-comrat-7-ans-devolution-du-programme-de-cyber-espionnage/

[7] https://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

[8] Voir l'article "*Under Worm Assault, Military Bans Disks, USB Drives*", publié le 19/11/2008 sur site *Wired*, https://www.wired.com/2008/11/army-bans-usb-d/

[9] Cf. http://www.apexitgroup.com/blog/sandworm-russian-cyber-espionage-campaign-uncovered-after-5-years et https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

[10] Nom donné au groupe APT28 par la firme de sécurité informatique ESET

[11] https://www.welivesecurity.com/2016/10/25/lifting-lid-sednit-closer-look-software-uses/ Pour plus de précisions, on peut consulter les trois rapports détaillés de l'entreprise ESET : https://www.eset.com/int/about/newsroom/research/dissection-of-sednit-espionage-group/

[12] https://www.linkedin.com/company/infosafe-llc

[13] https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaques-trois-piratages-qui-montrent-que-l-ukraine-est-un-terrain-d-entrainement-des-hackers-prorusses_2260721.html

Le système informatique de la commission électorale semble avoir été piraté plusieurs mois auparavant, comme l'indique la présence sur les serveurs, depuis déjà deux mois, d'un fichier comportant la fausse annonce[14]. Cette annonce a été relayée par la télévision russe le soir-même : la chaîne étatique *Pervyj Kanal* a en effet proclamé la victoire de Dmytro Iaroch devant Petro Porochenko, avec 37 % des voix contre 29 %[15]. Ces graves attaques portent directement atteinte à l'intégrité d'un processus électoral interne et constituent ainsi une tentative d'ingérence politique.

L'année suivante, le 23 décembre 2015, une attaque informatique cible simultanément trois distributeurs d'électricité, provoquant une importante coupure d'électricité dans l'ouest de l'Ukraine pendant quelques heures pour plus de 1,4 million d'habitants. Les investigations montreront une fois encore la présence d'une version modifiée de *BlackEnergy,* intégrant en outre un module permettant d'avoir accès aux systèmes de contrôle et d'acquisition de données (SCADA) sur les réseaux des fournisseurs d'électricité[16].

Un an plus tard, le 16 décembre 2016, une autre attaque privait de courant une partie de Kiev en plein milieu de la nuit pendant une heure.

En 2017, le pays subit coup sur coup les attaques des *ransomwares WannaCry, Petya/NotPetya* et *BlackRabbit*, dont le premier a provoqué la paralysie de nombreux acteurs économiques du pays avant de se propager dans le monde entier, affectant des entreprises, des hôpitaux et des institutions.

Si les spécialistes ont depuis indiqué soupçonner l'implication de hackers nord-coréens dans l'attaque *WannaCry (*possiblement rattachés au groupe nord-coréen Lazarus[17]), le mode de propagation du ransomware NotPetya, avec une nette prépondérance en Ukraine[18], a laissé à penser qu'il pouvait s'agir d'une opération d'origine russe. En effet, la contamination le 27 juin 2017 de *NotPetya* était partie d'un logiciel de traitement de données financières russes particulièrement utilisé en Ukraine : le logiciel de comptabilité M. E. Doc[19]. La thèse d'une intervention russe ciblée à l'encontre des milieux économiques et commerciaux ukrainiens a donc d'emblée été soulevée ; d'autant que le *ransomware* ne semblait pas avoir été programmé pour permettre un déchiffrement des données. De nombreux spécialistes ont ainsi supposé qu'il s'agissait plutôt d'un « *wiper* déguisé en *ransomware* » que d'un *ransomware* à proprement parler : en effet, ce dernier n'employait pas seulement des méthodes de chiffrement des données sur les machines qu'il avait infectées, mais bien des méthodes de *destruction* de ces données, semblables à celles utilisées par l'outil *KillDisk* (par réécriture des fichiers et extensions de fichiers des victimes).

---

[14] D'après l'entretien avec Viktor Zhora, directeur général de l'entreprise de sécurité informatique *InfoSafe IT*, relaté dans l'article publié sur le site *Numerama, op. cit.* : « « Les *hackeurs* étaient dans le système depuis deux mois », raconte Viktor Zhora dans les locaux de *InfoSafe*, à Kiev. Personne ne s'attendait à une attaque si minutieusement préparée, c'était une vraie leçon de piratage en temps réel. C'est l'opération qui a marqué le début de la cyber-guerre. »

[15] D'après l'article du site *Numerama, Ibid.*

[16] http://www.numerama.com/tech/137182-un-piratage-serait-a-lorigine-dune-coupure-delectricite-en-ukraine.html.

[17] Voir https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group et http://securityaffairs.co/wordpress/61997/apt/lazarus-apt-us-defense-contractors.html.

[18] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/.

[19] https://www.developpez.com/actu/148341/NotPetya-les-attaquants-ont-incorpore-une-porte-derobee-dans-un-logiciel-comptable-tres-populaire-pour-propager-le-malware/.

A cela s'ajoute le fait que la propagation exponentielle de *WannaCry* en mai 2017s'était accompagnée en Ukraine du déploiement d'un *ransomware* plus agressif, mais visiblement codé à partir de *NotPetya* : le *malware* XData[20]. Ce dernier avait été attribué au groupe *TeleBots*, en raison de l'emploi par le groupe de différentes variantes de l'outil *KillDisk* ; emploi qui aurait ainsi permis de faire la supposition d'un lien avec les attaques de *NotPetya* (XData et ce dernier ayant donc apparemment été réalisés pour mettre en œuvre une infrastructure de type *KillDisk*)[21]. Or, selon les chercheurs d'ESET, le groupe *TeleBots* entretiendrait des relations avec le groupe supposé russe (russophone du moins) à l'origine du *malware BlackEnergy* (évoqué auparavant)[22].

L'ensemble de ces attaques contre l'Ukraine utilisant des méthodes avancées, spécialistes et commentateurs ont été amenés à supposer une implication directe ou indirecte, par le biais de financements ou de formation par exemple, d'acteurs militaires et/ou étatiques russes : le GRU et le FSB[23]. D'autres attaques encore laissent à penser que la Russie fournit aux combattants séparatistes ukrainiens une assistance tactique sur le terrain : l'infection des téléphones Android de militaires ukrainiens depuis fin 2014 a permis de récupérer des données de communication et de localisation et de les utiliser pour frapper les unités d'artillerie de Kiev, qui ont ainsi subi de fortes pertes[24].

2017 : augmentation des aides américaines à l'Ukraine et durcissement du discours officiel américain face à la Russie

Les premières aides de Washington à Kiev

Les Etats-Unis n'ont pas attendu 2014 et les événements en Crimée pour soutenir l'Ukraine. Leur soutien remonte, nous l'avons vu, à 1992, avec la mise en place du *FREEDOM Support Act ("Freedom for Russia and Emerging Eurasian Democracies and Open Markets Support Act"*) dont ont bénéficié la plupart des Etats de l'ancien bloc soviétique. Puis, en 2008, les gouvernements de Washington et de Kiev ont signé une charte pour un « Partenariat Stratégique ».

Le texte du Comité des Affaires Etrangères, adopté en soutien de l'*Ukraine Support Act* de 2014, prévoyait une « aide à la démocratie et à la société civile en Ukraine, en favorisant la transparence, le respect de la loi, les efforts anti-corruption, et en renforçant les organisations politiques et protégeant les médias indépendants, alors que l'Ukraine se prépa[rait] pour des élections libres et équitables au mois de mai », qui incluait notamment de la formation dans le domaine militaire.

Au fil des années, cette aide a été augmentée, mais disséminée au sein de plusieurs programmes et lois, tels que le *Department of Defense Appropriations Act*, l'*Ukraine Security Assistance Initiative*, le *State Foreign Operations Program* et des programmes liés, ou encore le *National Defense Authorization Act*. Cette

[20] https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/.

[21] https://www.datasecuritybreach.fr/cyberattaque-petya-telebots/.

[22] https://www.welivesecurity.com/fr/2017/07/04/telebots-de-nouveau-ukraine/.

[23] https://www.scientificamerican.com/article/tracing-the-sources-of-today-rsquo-s-russian-cyberthreat/ et https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[24] Voir http://www.numerama.com/politique/218963-la-russie-aurait-piste-lartillerie-ukrainienne-avec-un-malware-android.html et https://siecledigital.fr/2017/10/05/russie-pirate-smartphones-soldats-otan/, « La Russie pirate les *smartphones* des soldats de l'OTAN » et « La Russie aurait pisté l'artillerie ukrainienne avec un *malware Android* ».

dissémination des aides a pu être un moyen, pour le Congrès, d'atteindre une somme totale conséquente tout en la masquant en raison des réticences formulées par certaines institutions gouvernementales ou pour limiter les tensions avec la Russie.

Néanmoins, le *National Defense Authorization Act* signé par le Président Obama en 2015 avait tout de même permis d'allouer à l'Ukraine 300 millions de dollars d'aide en matière de sécurité, dont 50 millions de dollars destinés à la fourniture d'armes létales.

Ainsi, malgré des précautions prises pour des raisons de politique intérieure ou internationale, ces divers soutiens à l'Ukraine devraient atteindre à terme, en 2018, près d'1 milliard de dollars ; dont une large part devrait être allouée aux réformes de l'appareil de sécurité du pays, et - en particulier - à ses efforts en matière de cybersécurité[25].

Les derniers développements de l'aide des Etats-Unis à l'Ukraine en matière de cybersécurité

Suite aux cyberattaques de décembre 2015 contre des infrastructures énergétiques ukrainiennes, les Etats-Unis ont envoyé sur place des équipes comprenant des membres du Ministère de l'Energie, du Bureau Fédéral d'Investigation (FBI) et de l'organisation North American Electric Reliability Corporation (NERC), afin d'aider à sécuriser les infrastructures et de participer à l'enquête.

Cette délégation interministérielle s'est de nouveau rendue en Ukraine en mars 2017, tandis qu'un exercice de cyberdéfense des infrastructures ukrainiennes a été mené conjointement par les Etats-Unis et l'Ukraine au mois de mai de la même année.

Par la suite, le *DoD Appropriation Act 2017* a permis de mettre 150 millions de dollars à la disposition de l'Ukraine dans le cadre du programme d'assistance en matière de sécurité ''*Ukraine Security Assistance Initiative*''[26]*.* Ce programme avait été créé en 2016 par le *National Defense Authorization Act* afin de fournir différents types d'assistance à l'Ukraine, dont de la formation, des équipements, du support logistique, des fournitures et des services, du renseignement et du soutien aux forces de sécurité militaires et civiles, ainsi que de remplacer toutes les équipements de défense fournis par les Etats-Unis à l'Ukraine au cours des précédents programmes de soutien.

En février 2017, l'entreprise américaine *Black Box Network Corporation* (BBNC) avait notamment annoncé avoir été sélectionnée par les forces armées américaines dans le cadre de l'*Ukraine Security Assistance Initiative*[27] *:* l'entreprise serait en charge de l'installation en Ukraine d'un système informatique ultra-sécurisé par fibre optique au profit notamment du Ministère de la Défense, de l'état-major des Armées et du *Cyber Security Operation Center* créé en 2016. L'ensemble du projet soutenu par les Etats-Unis vise à mettre en

[25] *Intelligence Online*, « Les Républicains relancent la cyber offensive à Kiev », Septembre 2017, N789 p.1.

[26] https://www.congress.gov/ et https://securityassistance.org

(Dans le DOD Appropriation Act de 2016, 200 millions de dollars avaient été débloqués pour venir en aide à l'armée et aux forces de sécurité ukrainiennes ; de plus, l'année précédente il avait été décidé que 30 millions de dollars du milliard alloué à la *European Reassurance Initiative* seraient destinés à l'Ukraine).

[27] https://www.blackbox.com

place des systèmes communs d'information relatifs à la cybersécurité, des systèmes C&C et de commandement logistique et médical[28].

Par ailleurs, en avril 2017, une proposition de loi portant sur le renforcement de la coopération entre les Etats-Unis et l'Ukraine en matière de cybersécurité, l'*Ukraine Cybersecurity Cooperation Act of 2017*[29] a été présentée devant le Congrès. Le processus législatif est toujours en cours. La proposition se concentre sur trois points principaux :

(1) Fournir à l'Ukraine le soutien nécessaire à l'amélioration des protections les plus avancées sur les systèmes informatiques gouvernementaux, en particulier dans le cas des systèmes défendant ses infrastructures critiques ;
(2) L'assister dans la réduction de sa dépendance à des technologies russes ;
(3) L'assister dans le renforcement de ses compétences, augmenter sa participation à la coopération internationale en vue de répondre aux attaques informatiques, et partager avec ses services les informations dont disposent les Etats-Unis en matière de cybersécurité.

A ces initiatives, s'est ajoutée une annonce conjointe de l'Ukraine et des Etats-Unis le 9 juillet 2017, indiquant que les deux pays étaient parvenus à des accords sur la lutte contre la cybercriminalité lors de la visite du Secrétaire d'Etat de l'Administration Présidentielle Rex Tillerson à Kiev. Le détail de ces accords n'a cependant pas été rendu public[30].

Suite au premier Dialogue Bilatéral en matière de cybersécurité (*Bilateral Cybersecurity Dialogue*) qui s'est tenu à Kiev, l'Ambassadrice des Etats-Unis en Ukraine a déclaré le 27 septembre que les Etats-Unis alloueraient plus de 5 millions de dollars au renforcement des capacités de l'Ukraine en vue de prévenir les cyberattaques, d'en minimiser les conséquences, et d'y répondre[31]. Les échanges ont notamment porté sur les stratégies de protection des infrastructures critiques et militaires du pays, ainsi que sur le thème de la confiance dans le cyberespace au sein de l'Organisation pour la Sécurité et la Coopération en Europe[32].

On peut également noter que l'ONG américaine *World Learning* recrutait, en octobre dernier, 3 consultants en cybersécurité, afin de fournir un soutien technique au *State Service for Special Communication and Information Protection* (SSSCIP) et au *State Center for Cyber Protection and Counteraction to Cyber Threats* (SCCPCCT) ukrainiens, dans le cadre du projet d'assistance technique financé par l'USAID[33].

---

[28] https://globenewswire.com/

[29] "*A bill to encourage United States-Ukraine cybersecurity cooperation and require a report regarding such cooperation, and for other purposes*", https://www.congress.gov/bill/115th-congress/house-bill/1997

[30] https://www.unian.info/.

[31] https://ua.usembassy.gov/.

[32] https://www.kyivpost.com/.

[33] https://www.devex.com.

Déploiement des aides des Etats-Unis à l'Ukraine par le biais d'institutions tierces (OTAN, OSCE)

En outre, les Etats-Unis ont soutenu les efforts du gouvernement ukrainien en matière de sécurité par le biais de l'OTAN et de programmes de coopération avec des acteurs tiers. L'importance du numérique dans ce soutien a été croissante au cours des dernières années.

L'OTAN a ainsi établi 6 fonds pour soutenir l'Ukraine dans différents domaines[34], dont un spécifiquement dédié à la cyberdéfense, ouvert dès décembre 2014 avec un budget initial de 560 000€[35]. Ce fonds a notamment pour objectif de fournir à l'Ukraine le soutien nécessaire au développement de ses capacités défensives, notamment celles de type CERT, et comprend la création de laboratoires pour étudier les incidents de cybersécurité[36]. Si le pays directeur du programme est officiellement la Roumanie, la participation financière des Etats-Unis s'est avérée être la plus importante.

En mars 2017, suite à l'adoption de ces programmes, l'OTAN a alimenté ces fonds de soutien à l'Ukraine de plus de 14 millions d'euros, dont près d'un million pour la cybersécurité[37].

Enfin, le 5 avril 2017, le service de presse officiel de l'Etat ukrainien a annoncé la création d'un Centre de cybersécurité à Kiev avec l'aide de l'OTAN, inspiré de « l'expérience turque »[38], et en partenariat avec l'Université Technique Nationale d'Ukraine (*NTU*) et l'Institut Polytechnique de Kiev (*KPI*).

Ces modes de soutien mettant en œuvre des collaborations multiples ont également permis, en juin 2017, la coopération des Services de renseignement ukrainiens (SBU) avec Europol, la National Crime Agency britannique et le FBI, afin de tenter d'attribuer l'attaque du *ransomware NotPetya*[39].

Notons également que le Commandement militaire américain pour l'Europe (US EUCOM) avait organisé en août et septembre 2014, avec 31 pays dont l'Ukraine, un grand exercice en matière de sécurité informatique et d'interopérabilité des réseaux de communication, *Combined Endeavour 14*[40].

Enfin, l'OSCE a mis en place un programme de coordination du trafic ferroviaire par assistance informatique, ainsi qu'un programme d'équipement de la « cyber police » ukrainienne[41] en juillet 2017.

---

[34] https://www.nato.int/cps/en/natolive/topics_37750.htm#.

[35] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf

[36] http://www.uadn.net/2017/07/10/nato-allocates-e1-million-to-support-ukraines-cyber-security/

[37] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170302_170301-trust-funds.pdf

[38] ''*Ukraine, within the framework of countering modern cyber threats, is preparing a single national cyber security center, which will be created with the assistance of NATO based on the experience of Turkey. State-owned firm* Ukrinmash*, which is part of Ukroboronprom, is the coordinator of the project, which will be implemented with the participation of the National Technical University of Ukraine (NTU) Kyiv Polytechnic Institute (KPI), the press service of the state concern Ukroboronprom said on April 5.*'', https://www.kyivpost.com/ukraine-politics/ukraine-natos-support-prepares-creation-cyber-security-centre.html.

[39] http://securityaffairs.co/wordpress/60562/intelligence/sbu-investigation-notpetya.html : *Security Affairs*, "*Ukraine Secret Service announces joint investigation with Europol, FBI, and NCA to attribute the recent NotPetya massive attack.*", 30/06/2017.

[40] http://www.eucom.mil/media-library/article/27834/worlds-largest-multilateral-c4-exercise-concludes.

[41] http://www.osce.org/project-coordinator-in-ukraine/330471

Conclusion

Les opérations cyber-offensives à l'encontre de l'Ukraine attribuées à la Russie ont provoqué un soutien américain allant crescendo, notamment dans le domaine de la cybersécurité. L'Ukraine est ainsi devenu un véritable « laboratoire à ciel ouvert en matière de cyber-offensive entre Moscou et Washington »[42].

L'élection de Donald Trump, qui affichait à la fois le souhait d'une normalisation des relations avec la Russie et une moindre participation des Etats-Unis aux actions de l'OTAN, n'a pas modifié cette dynamique de soutien numérique à l'Ukraine.

[42] *Intelligence Online*, « Les Républicains relancent la cyber-offensive à Kiev », Septembre 2017, N789 p.1, https://www.intelligenceonline.fr/renseignement-d-etat/2017/09/06/les-republicains-relancent-la-cyberoffensive-a-kiev,108260182-eve.

THE SHADOW BROKERS

En août 2016, un mystérieux groupe de hackers, The *Shadow Brokers* ("Les courtiers de l'ombre"), inconnu jusqu'alors, acquiert très rapidement une notoriété mondiale. Il vient en effet de mettre en ligne sur différents sites Internet des outils d'attaque informatique qu'il dit avoir volés à un autre groupe de hackers, l'*Equation Group*, soupçonné d'être lié à la *National Security Agency* (NSA) américaine. Et il annonce en même temps mettre aux enchères des outils d'attaque bien plus puissants également volés à l'*Equation Group*. Dans les mois qui suivent, les *Shadow Brokers* multiplient les divulgations sur les outils et les actions de la NSA, les accompagnant de messages souvent étonnants, rédigés dans un anglais approximatif, sur des sujets divers comme la compromission des élites, la lutte des classes ou la politique américaine.

Qui est ce groupe ? Quels sont ses objectifs réels ? Pour qui agit-il ? Comment a-t-il volé de informations hautement classifiées de la NSA ? Personne ne semble savoir répondre à ces questions. Mais des soupçons très variés circulent, sans qu'aucun ne parvienne à convaincre.

Voyons d'abord ce que l'on sait de ce groupe, avant de détailler les principales conséquences de ses actions. Nous explorerons ensuite les hypothèses qui circulent, et tenterons d'émettre un avis sur chacune d'entre elles.

Les faits

La première manifestation publique des *Shadow Brokers* date du 13 août 2016. Un Tweet adressé à de grands media américains depuis le compte "@shadowbrokerss"[43] annonce que des outils d'attaque informatique utilisés par l'*Equation Group,* comprenant des vulnérabilités et les outils pour les exploiter, peuvent être obtenus sur les sites *Pastebin, Tumblr* et *GitHub*. Sur ces sites[44], les *Shadow Brokers* déclarent avoir piraté les serveurs de l'*Equation Group*, nom donné par la société de sécurité informatique russe Kaspersky aux auteurs des attaques *stuxnet*, *duqu* et *flame,* et mettre aux enchères les très nombreux outils d'attaque qu'il lui a dérobé, et que remportera celui qui versera la plus grosse somme en Bitcoins sur un compte désigné. Les *Shadow Brokers* promettent par ailleurs qu'ils mettront tous les outils d'attaques librement en ligne si le total des sommes déposées sur le compte atteint 1 million de Bitcoins. A titre de preuve, ils fournissent librement une quinzaine d'outils d'attaque utilisés par l'*Equation Group.* Et concluent par une violente diatribe dénonçant les crimes des "élites fortunées".

Dès le 16 août, Kaspersky confirme la similitude des outils diffusées par les *Shadow Brokers* avec les programmes de l'*Equation Group.* Et le 19, *The Intercept*, un site dédié au journalisme d'investigation, qui dénonce notamment les programme US de surveillance globale, et héberge les révélations d'Edward

[43] https://twitter.com/shadowbrokerss

[44] Voir le texte publié sur les sites Pastebin.com (https://web.archive.org/web/20160816004542/http://pastebin.com/NDTU5kJQ), Tumblr.com (http://web.archive.org/web/20160815192545/https://theshadowbrokers.tumblr.com) et Github.com (http://web.archive.org/web/20160815124425/https://github.com/theshadowbrokers/EQGRP-AUCTION).

Snowden[45], affirme que ces outils font partie du puissant arsenal utilisé par la NSA pour ses opérations d'espionnage dans le monde entier[46]. Il a en effet retrouvé, dans les lignes de code diffusées par les *Shadow Brokers,* l'empreinte numérique que la NSA, dans un manuel hautement classifié volé par Snowden et à l'époque non encore rendu public, demandait d'inscrire dans tous les développements utilisant son outil d'attaque SECONDDATE[47] afin d'en suivre l'utilisation[48].

Également le 19 août 2016, les sociétés informatiques Cisco et Fortinet confirment publiquement que leurs produits présentent effectivement les vulnérabilités extrêmement critiques – zero day, c'est-à-dire inconnues jusqu'alors – que viennent de divulguer les *Shadow Brokers*[49]. Elles publient les correctifs nécessaires dans les jours suivants.

Le 31 octobre 2016, après plus de 2 mois d'un silence presque total, les *Shadow Brokers* publient plusieurs centaines de noms de domaine et d'adresses IP qui auraient été piratés par l'*Equation Group* entre 2000 et 2010 dans 49 pays afin de permettre à la NSA de lancer des attaques ciblées[50]. Cette révélation s'accompagne d'un étrange discours sur la liberté de la presse, la corruption des politiques, les attaques informatiques sur les processus électoraux et les élections présidentielles américaines prévues 8 jours plus tard.

Le 14 décembre, dans un article "Are the Shadow Brokers selling NSA tools on ZeroNet?" publié sur le site *Medium* sous le pseudo Boceffus Cleetus[51], les *Shadow Brokers* fournissent une nouvelle liste d'outils d'attaque de la NSA, qu'ils vendent désormais à l'unité, ou en totalité pour 1000 Bitcoins, en regrettant le peu de succès de leur vente aux enchères et de leur appel aux dons.

Le 12 janvier 2017, dans un message posté sur le site ZeroNet[52], les *Shadow Brokers* annonce l'arrêt de leur activité, trop peu rentable et désormais trop risquée, et la fermeture de leur compte de messagerie, tout en précisant que l'offre reste valable et leur compte en Bitcoins ouvert. Ils mettent également en ligne une soixantaine de données, jugées sans intérêts par les experts.

Ils réapparaissent le 8 avril suivant, en publiant sur Medium[53] un long message dénonçant la politique du Président Trump, qu'ils affirment avoir soutenu lors de son élection, et plus précisément le bombardement, 2 jours auparavant, de la base aérienne syrienne d'Al-Chaayrate, base utilisée aussi par les forces aériennes russes. Ils rendent publics divers outils d'attaque sur les environnements Linux et Unix, ainsi que des

---

[45] https://theintercept.com/snowden-sidtoday/

[46] https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/

[47] SECONDDATE est un outil de la NSA destiné à infecter des ordinateurs en interceptant leurs requêtes web puis en redirigeant leur navigateur vers un serveur piégé. L'article de *The Intercept* signale un document de la NSA de 2013 présentant deux utilisations réussies de cet outil, au Liban et au Pakistan (https://www.documentcloud.org/documents/3031638-Select-Slides-FINAL-PMR-4-24-13-Redacted.html). SECONDDATE aurait en fait permis d'infecter des millions d'ordinateurs dans le monde.

[48] Cette empreinte numérique était constituée par une chaîne spécifique de 16 caractères ("ace02468bdf13579").

[49] https://www.silicon.fr/cisco-fortinet-valident-serieux-shadow-brokers-hackers-nsa-155390.html?inf_by=58d3b1882ad0a1a13a7ca620

[50] https://medium.com/@shadowbrokerss/message-5-trick-or-treat-e43f946f93e6 et https://www.reddit.com/r/DarkNetMarkets/comments/5a9wnc/message_5_trick_or_treat/

[51] https://medium.com/@CleetusBocefus/are-the-shadow-brokers-selling-nsa-tools-on-zeronet-6c335891d62a

[52] https://medium.com/@msuiche/summary-of-the-latest-shadowbrokers-released-iocs-2d0718841644

[53] https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

informations montrant la compromission par la NSA de la messagerie CaraMail depuis 2001 et de 900 serveurs d'entreprises et d'universités.

Le 14 avril 2017, un Tweet fournit un lien sur le site Steemit[54], sur lequel est divulguée une nouvelle série d'outils dérobés à la NSA, certains destinés à espionner le réseau interbancaire SWIFT, les autres à compromettre les environnements Windows et Windows Server. Microsoft déclare aussitôt avoir déjà corrigé les vulnérabilités exploitées par ces derniers outils, notamment un mois auparavant la faille *EternalBlue*[55].

Les conséquences des actions des *Shadow Brokers*

La mise en difficulté des Etats-Unis et de la NSA

Les premières victimes des révélations des *Shadow Brokers* sont bien évidemment les Etats-Unis d'Amérique, dont la position a été affaiblie sur la scène internationale, et son agence de renseignement, la NSA, dont la capacité de cyber espionnage a été fortement diminuée. Alors que l'impact des informations dévoilées par Edward Snowden en 2013 commençait à l'estomper, les Shadow Brokers ont vivement remis en lumière l'étendue de la surveillance globale exercée par la NSA, apportant en outre une compréhension bien plus concrète de la puissance de l'arsenal cyber-offensif américain que celle qu'apportaient les documents divulgués par Snowden. Dans une enquête qu'il a mené sur l'agence américaine de sécurité en novembre 2017, le *New York Times* a montré que l'action des *Shadow Brokers* a été plus néfaste que celle d'Edward Snowden[56].

La forte pression exercée sur le gouvernement américain a conduit la Maison Blanche à prévoir plus de transparence dans l'utilisation et la divulgation des vulnérabilités logicielles que la NSA et les autres agences gouvernementales pourraient découvrir. C'est l'objet de la nouvelle charte, publiée mi-novembre 2017, sur le processus d'évaluation des vulnérabilités[57].

Des attaques violentes utilisant les outils de la NSA publiés par les *Shadow Brokers*

Mais les conséquences les plus graves de l'action des *Shadow Brokers* ont été les trois cyberattaques qui ont frappé le cyberespace en moins de 2 mois en utilisant les outils d'attaques qu'ils ont rendus publics.

Le 12 mai 2017, un malware nommé *WannaCry*, combinaison d'un rançongiciel et d'un ver informatique qui exploite la faille de sécurité *EternalBlue* volée par les *Shadow Brokers* à la NSA, commence à bloquer les ordinateurs d'utilisateurs publics et privés à travers le monde, un message demandant une rançon en Bitcoins pour effectuer le déblocage. Cette cyberattaque, considérée comme le plus grand rançonnage de l'histoire d'Internet, touchera plus de 300 000 ordinateurs dans plus de 150 pays. Dès la première nuit, 100 000 ordinateurs sont infectés. Le *National Health System* du Royaume-Uni est l'une des principales victimes, avec plus de 20% d'hôpitaux du pays touchés. Malgré la panique provoquée par WannaCry, la plupart des

[54] https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation

[55] https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/

[56] https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

[57] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Voir aussi https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process

utilisateurs n'ont pas cédé au chantage et n'ont pas payé. Les auteurs de l'attaque n'auraient gagné que 41 Bitcoins, soit environ 60 000 $. D'après Europol, aucun pays en particulier n'a été ciblé [58].

Au même moment, une autre cyberattaque d'ampleur similaire, *Adylkuzz*, contamine des centaines de milliers d'ordinateurs, en exploitant les mêmes failles de sécurité que *WannaCry*. Mais à l'inverse de cette dernière, *Adylkuzz* est restée furtive, son but étant de créer de la crypto-monnaie - le Monero - en utilisant les capacités de calcul des ordinateurs infectés sans éveiller les soupçons de leurs utilisateurs légitimes. Elle a été découverte par hasard lors d'investigations sur *WannaCry*. N'ayant provoqué au plus que des baisses de performances, elle a été moins médiatisée que WannaCry, malgré son ampleur a priori plus forte. Les auteurs de l'attaque en auraient tiré un bénéfice de l'ordre d'un million de dollars.

Enfin, une troisième attaque exploitant des outils publiés par les *Shadow Brokers, NotPetya,* commence le 27 juin 2017. Initialement considérée comme une nouvelle version de *Petya*, un rançongiciel apparu en mars 2016, en raison du message s'affichant sur l'écran de l'ordinateur et réclamant une rançon, elle n'en avait en fait que l'apparence, détruisant les fichiers au lieu de les chiffrer. Cette attaque semble avoir visé l'Ukraine, mais elle s'est répandue dans bien d'autres pays, faisant d'importants dégâts dans de nombreuses entreprises, avec un préjudice global de plusieurs milliards de dollars.

Un maigre butin pour les *Shadow Brokers*, mais un potentiel de nuisance encore très important

D'après des analyses effectuées en traçant les sommes versées sur le compte en Bitcoins qu'ils avaient indiqué, les *Shadow Brokers* n'auraient fait que très peu de profits depuis le mois d'août 2016. Espérant cependant profiter du succès du ransomware WannaCry pour vendre le reste de leur butin volé à la NSA, ils ont mis en place un abonnement mensuel, le *TheShadowBrokers Data Dump of the Month*, qui offrira aux abonnés des outils d'attaque pour navigateur web, routeurs ou Windows 10 (épargné jusqu'ici), mais aussi des données subtilisées au réseau bancaire SWIFT, à des banques centrales, et à des États. Ils assurent en effet disposer encore en réserve de "*75% de l'arsenal cyber offensif américain*", et avoir acquis des informations sur les programmes d'armement nucléaire russe, chinois, iranien ou encore nord-coréen. De quoi attiser la convoitise de nombreux cybercriminels, voire aussi de groupes terroristes. Et les *Shadow Brokers* ont renoncé aux Bitcoins, dont les mouvements sont exposés publiquement, pour se faire payer en ZEC[59], une crypto-monnaie beaucoup plus discrète créée en 2016[60].

Les diverses hypothèses circulant sur les *Shadow Brokers*

Hypothèse I : une action russe

La « cyberguerre froide » entre la Russie et les Etats-Unis donne lieu à l'utilisation de techniques et moyens de plus en plus raffinés. Après les accusations des Etats-Unis contre les Russes qui, selon les Américains, ont été à l'origine du piratage des comptes du Parti démocrate pendant la campagne présidentielle, l'apparition

[58] https://www.francetvinfo.fr/sante/affaires/cyberattaque-le-logiciel-malveillant-wannacry-met-en-difficulte-les-hopitaux-britanniques_2192065.html

[59] https://btcmanager.com/the-shadow-brokers-release-price-adjustment-to-data-dumps/

[60] https://z.cash/blog/helloworld.html

des Shadow Brokers suscite de nouveau des rumeurs sur l'implication de la Russie dans le piratage des cyber-espions américains. Selon Edward Snowden, exilé en Russie, l'opération menée par les Shadow Brokers serait en fait un avertissement de Moscou aux Etats-Unis.

Certaines sources d'informations anglo-saxonnes, telles que *The Telegraph*, affirment qu'à travers The Shadow Brokers, la Russie cherche également à se venger pour des frappes aériennes en Syrie[61], en citant même un message adressé au Président des Etats-Unis, Donald Trump, rédigé en mauvais anglais[62]. Les messages diffusés par les Shadow Brokers sont effectivement systématiquement écrits dans un anglais très approximatif avec de nombreuses fautes de grammaire, ce qui pourrait laisser à penser qu'ils ont été rédigés par des non anglophones.

Hypothèse II : une action américaine

Il ressort cependant d'analyses linguistiques poussées menées par des chercheurs et du constat que le ou les rédacteurs ont une bonne connaissance de la culture américaine, que les auteurs pourraient plus sûrement être des anglophones cherchant à brouiller les pistes et à faire accuser la Russie.

Certains imaginent du coup que l'opération pourrait avoir été menée par les Etats-Unis en guise de représailles après le piratage des emails du Parti démocrate. Les Américains auraient également surtout voulu mettre en cause la Russie et profiter du chaos pour masquer une attaque plus ciblée. La fuite des outils de la NSA n'aurait ainsi été qu'un feu de paille concernant des outils qui n'auraient déjà plus été sous son contrôle ou exploitaient des failles vieillissantes…

Ces hypothèses semblent particulièrement improbables. En effet, les Etats-Unis ont été les plus impactés par les actions du groupe Shadow Brokers, qu'il s'agisse de la perte de contrôle de leur arsenal cyber offensif, de l'image du pays ou de ses entreprises (Microsoft, Cisco, etc.) ou encore de la vulnérabilité du pays aux exploits (les administrations et entreprises américaines sont les premières à être équipées des produits ciblés par les exploits publiés).

Hypothèse III : une action idéologique indépendante

L'opération pourrait aussi avoir été menée par des individus indépendants, sans contrôle ni des autorités russes ou américaines, par exemple pour lutter contre la militarisation du cyberespace. Aucune preuve factuelle ne permet en effet d'affirmer avec certitude que l'opération s'inscrit dans le cadre d'une démarche stratégique sur le champ de bataille cyber russo-américain.

Un élément milite en faveur de la thèse de l'action indépendante et non contrôlée : si les Etats-Unis ont été la principale victime de l'opération en termes d'impact opérationnel sur ses capacités de renseignement et d'image de marque, la Russie aurait, elle, été l'une des principales victimes du ransomware, sans que l'on ait beaucoup de précisions sur les conséquences réelles pour le pays. L'éditeur Avast a notamment constaté que « la moitié des tentatives d'attaque sur l'ensemble de la base de données d'utilisateurs Avast [avaient] été bloquées en Russie »[63].

---

[61] http://www.telegraph.co.uk/news/2017/05/12/russian-linked-cyber-gang-shadow-brokers-blamed-nhs-computer/

[62] https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

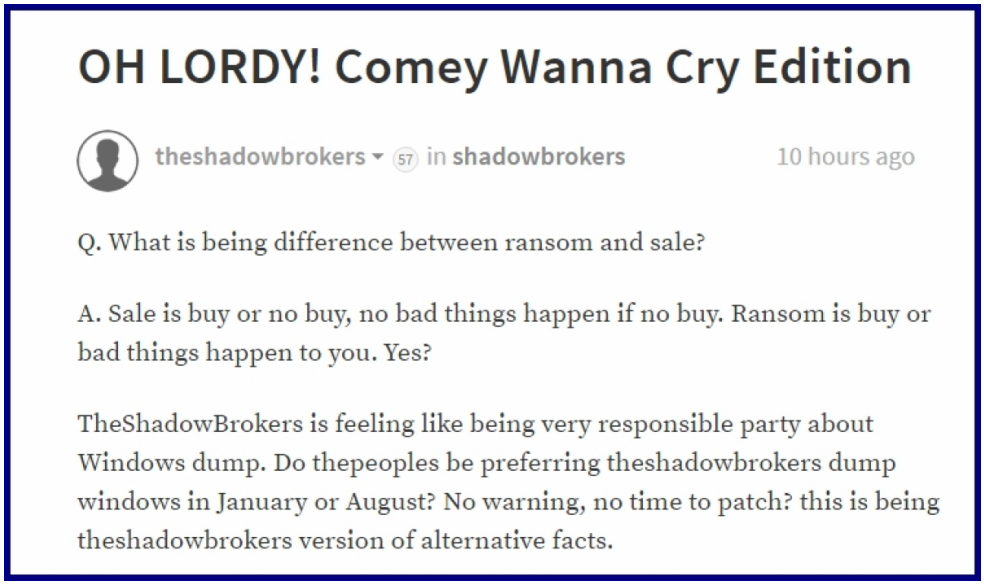
[63] https://blog.avast.com/fr/wannacry-pire-epidemie-de-ransomwares-de-lhistoire

Hypothèse IV : une opération à but lucratif

La très grande majorité des communications de Shadow Brokers met en avant un intérêt financier, prétextant parfois, à la marge, des motivations politiques.

On relève cependant dès la première « vente aux enchères » une incohérence significative : le groupe annonce que les outils seront remis à l'acheteur ayant versé la plus grande somme, mais également que l'ensemble des outils seraient mis en ligne à disposition de tous si le montant dépasse un million de dollars. Ceci est incohérent puisque la valeur objective de ces outils tient au fait qu'ils concernent des failles zero day que seul l'acheteur (et la NSA bien entendu) ait connaissance de ces failles.

Une autre hypothèse concerne la manipulation du cours du Bitcoin. La Corée du Nord serait ainsi montrée du doigt, récemment accusée de pirater des plateformes d'échange bitcoin en vue de dérober des fonds d'une monnaie « étrangère ». Néanmoins, la théorie n'a pas reçu beaucoup de soutien pour une simple raison : si les motivations des Shadow Brokers étaient purement financières, l'effet de cette démarche ne justifie pas les efforts investis dans l'affaire.



Message de groupe The Shadow Brokers. Source : Steemit64

Si les hypothèses I et III paraissent les moins improbables, aucune ne parait totalement vraisemblable. Difficile, en effet, de savoir à qui profite réellement le crime…

[64] https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées

Direction Générale des Relations Internationales et de la Stratégie

60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS

Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15

Téléphone : 01 45 55 00 20

E-mail : omc@ceis-strat.com