STUXNET : une cyberattaque spectaculaire

Découvert en 2010, Stuxnet fait partie des plus grandes cyberattaques. Il a été conçu pour attaquer les systèmes de contrôle industriels. Il est considéré comme l'un des programmes malveillants les plus sophistiqués jamais créés en raison de son utilisation de multiples vulnérabilités pour infiltrer les systèmes cibles et modifier le fonctionnement des centrifugeuses utilisées pour l'enrichissement de l'uranium. Depuis sa découverte, il a suscité des préoccupations, il a été largement étudié par les chercheurs en sécurité informatique pour comprendre son fonctionnement et prévenir des attaques similaires à l'avenir.

Rose-Milca CENAT, M1 (AMSD), Université Paris Cité - UFR des Sciences Fondamentales et Biomédicales, 28 avril 2023.

Introduction

À l'ère où la technologie ne cesse de prendre de l'ampleur, que ce soit à travers le Big data, la connectivité, l'intelligence artificielle et la cybersécurité pour ne citer que ces quatre grands domaines, les entreprises voir accroître leurs chiffres d'affaires et leurs quantités de données. Ce qui engendre parallèlement l'interconnexion des systèmes d'information, et aussi un risque élevé de cyberattaque.

Pour Arnaud Coustillière, vice-amiral chargé de la cyberdéfense française, la cyberattaque se définit comme « une action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support »[1].

Les cyberattaques deviennent de plus en plus nombreuses, et leurs cibles vont bien au-delà des entreprises, en effet, le dysfonctionnement d'un état peut être aussi concerné (figure 1). L'année 2010 a été marquée par l'une des plus célèbres qui fait l'objet de cet article : Stuxnet. Cette cyberattaque a fait beaucoup parlé d'elle et causé pas mal de dégâts. Que ce soit des chercheurs ou des médias, Stuxnet a attiré l'attention de plusieurs, de par sa complexité et son mode d'attaque. Plusieurs articles et livres ont été publiés sur le sujet parmi ceux-ci, on peut citer : « Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon »[2] de Kim Zetter. Cet ouvrage présente Stuxnet comme l'inauguration d'une nouvelle ère de guerre. Et propose de nombreuses explications révélatrices des technologies impliquées.

Un dossier également riche en information, intitulé « W32.Stuxnet Dossier Version 1.4 (February 2011) »[3]. Il a été produit avec la participation de nombreuses personnes de l'équipe Symantec Security Response. Il présente les aspects techniques de Stuxnet et son objectif final qui est de reprogrammer les systèmes de contrôle industriels (de l'anglais : Industrial Control System (ICS)) en modifiant le code sur les contrôleurs logiques programmables (de l'anglais : Programmable Logic Controller (CLP)). Cela permet de faire fonctionner les contrôleurs comme le souhaite l'attaquant tout en cachant ses modifications à l'opérateur de l'équipement.

Le présent article ne traite pas les raisons politiques de cette attaque, mais se limite sur une mise en contexte de sa découverte, ses principaux impacts, une description technique de l'architecture de Stuxnet et de son fonctionnement. Il détaille aussi les dispositions à prendre pour tenter d'éviter le maximum que possible ce genre d'attaque. La conclusion de ce travail portera sur les perspectives envisageables à long terme.

La découverte de Stuxnet

En janvier 2010, suite à des problèmes mécaniques dans une centrale de Natanz en Iran, des inspecteurs de l'Agence internationale de l'énergie atomique (AIEA) ont fait une inspection, les centrifugeuses de l'usine iranienne d'enrichissement d'uranium explosaient sans raison apparente. Le nombre de centrifugeuses qui tombaient en panne était augmenté considérablement.

Plus tard, Sergey Ulasen, un Biélorusse qui travaillait pour VirusBlokAda a reçu un appel de son ami qui était l'expert en cybersécurité d'une entreprise iranienne qui n'avait aucun lien avec le programme nucléaire[4]. L'expert observait sur ses ordinateurs des redémarrages constants et des « BSoD pour Blue Screen of Death », le fameux écran bleu de Windows qui peut apparaître pour diverses raisons : le système qui est infecté par un virus, le signalement d'une erreur lorsque les pilotes ne sont pas mis à jour, l'installation de deux antivirus en même temps, le disque dur qui est défectueux.[5] Même les nouveaux ordinateurs avec Windows fraîchement installés étaient affectés. Et il ne connaissait pas les causes. Les recherches d'Ulasen et de ses collègues lui permettront de réaliser qu'il avait affaire avec un malware très complexe. Dès lors, il partagea l'information avec la communauté de la cybersécurité.

Les analystes, les médias, les chercheurs commencèrent à publier sur l'incident. Il y a eu

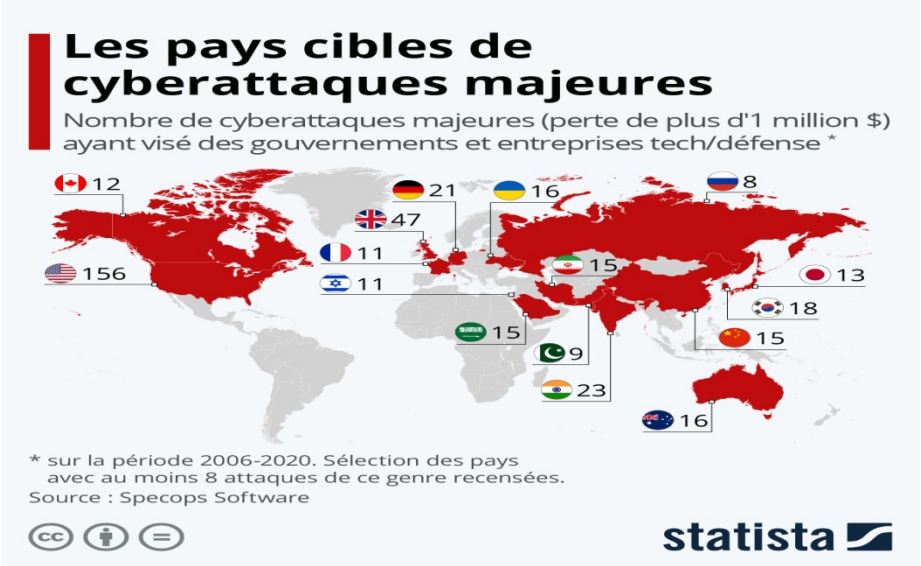

Figure 1. Source: Statista, Tristan Gaudiaut.

Brian Krebs et ensuite Frank Boldewin qui établi un lien entre Stuxnet et les systèmes de contrôle industriels Siemens WinCC SCADA. Et plus tard vinrent des théories qui relièrent le ver au programme nucléaire Iranien.

Comment fonctionne Stuxnet?

Stuxnet s'appuie sur l'attaque de l'homme du milieu (man-in-the-middle), consistant en une longue durée d'espionnage qui le permet d'intercepter les communications entre deux parties prenantes au moment opportun.[6]

Sa manière de fonctionner est très complexe. D'une part, il y a la propagation du virus, qui utilise les failles de Windows. D'autre part, l'attaque des systèmes SCADA (Supervisory Control And Data Acquisition)[7] qui repose sur le logiciel WinCC et PCS7. WinCC est un outil de télésurveillance et d'acquisition de données développé par Siemens. Il est utilisé pour contrôler un système automatique comme PLC (Programmable Logic Controler).[8]

Pour se propager, Stuxnet utilise les quatre vulnérabilités 0-day de Windows. Les points d'entrée principaux utilisés par ses développeurs pour pénétrer l'infrastructure ciblée sont les supports de stockage amovibles comme les clefs USB et autres disques durs portables. Ils utilisent la faille de raccourci Windows. Ce type de fichiers est d'extension .LNK et .PIF. La faille provient précisément du chargement de l'icône associé au lien. L'image est chargée à partir d'un fichier CPL (Windows Control Panel File) grâce à la fonction système LoadLibraryW().

En spécifiant les informations adéquates comme le chemin d'accès à une DLL malveillante dans la section File LocationInfo d'un fichier LNK, un pirate peut forcer le système Windows à exécuter du code en affichant

simplement le contenu d'un dossier.[8]

Stuxnet peut aussi se répandre sans l'aide d'utilisateurs. Il utilise alors les failles de sécurité exploitables à distance au sein d'un réseau local, qui proviennent du spouleur d'impression Microsoft et du service serveur (MS08-067).[8]

Pour s'attaquer aux systèmes SCADA, le malware utilise un mot de passe défini par défaut au sein de certains systèmes SCADA pour accéder aux systèmes. Ensuite, il remplace la librairie provenant de la suite de logiciel Simatic de Siemens "s7otbxdx.dll" qui est utilisée pour faire communiquer un PC tournant sous Windows avec un PLC de la famille Simatic. Il change le nom de la librairie en "s7otbxsx.dll", puis place sa propre version de la librairie qui lui permet d'intercepter tous les appels aux fonctions exportées par la librairie originale. En effet, la fonction équivalente "s7otbxsx.dll" reçoit la plupart des appels aux fonctions de "s7otbxdx.dll", ce qui signifie que seul le comportement de quelques fonctions est trafiqué.[8]

Cependant, tous les PLC ne sont pas ciblés par Stuxnet, la librairie recherche précisément les appareils Siemens 6ES7-315-2 et 6ES7-417.

La dernière étape de la modification de Stuxnet se traduit par une conséquence physique sur le système ciblé qui est difficile à détecter, mais elle détruit progressivement le système de manière discrète. Dès qu'il parvient à prendre le contrôle du PLC, Stuxnet provoque une altération de la vitesse de rotation des centrifugeuses qui deviennent rapidement inutilisables.

Quelles ont été les conséquences de Stuxnet ?

Symantec Corporation devenu **Gen Digital Inc**, a mis en place, le 20 juillet 2010, un système de surveillance du trafic vers les serveurs de commande et de contrôle (C&C) Stuxnet. Le système a seulement détecté le trafic des ordinateurs qui ont réussi à se connecter aux serveurs C&C. Les informations envoyées aux serveurs C&C étaient cryptées et comprenaient des données telles que l'adresse IP interne et externe, le nom de l'ordinateur, la version du système d'exploitation, et si le logiciel de contrôle industriel Siemens SIMATIC Step 7 était en cours d'exécution. Le 29 septembre 2010, les données ont montré qu'il y avait environ 100 000 hôtes infectés.[3]

Près de 58 % des hôtes infectés se trouvaient en Iran, une observation de plus de 40 000 adresses IP externes uniques, provenant de plus de 155 pays.

Les dommages causés aux centrifugeuses iraniennes par Stuxnet ont été estimés à plusieurs centaines de millions de dollars. Ce qui conduit à penser que Stuxnet avait pu viser délibérément une infrastructure de grande valeur en Iran (figure 2), vraisemblablement liée au programme de recherche nucléaire.[3]

Les dispositions et perspectives à long terme

Suite à l'attaque de Stuxnet, nombreux sont ceux qui se sentaient concernés par les dispositions à prendre soit pour éviter ou pour faire face à ce genre d'attaque.

Le 15 juillet 2010, Siemens met à disposition de ses clients un outil capable de détecter Stuxnet et de le supprimer.[9] European Union Agency for Cybersecurity, à travers le Dr. Helmbrecht qui stipulait que les infrastructures de l'information devront être protégées, qu'il doit y avoir une reconsidération intégrale des théories répandues en matière de CIIP (Critical Information Infrastructure Protection),

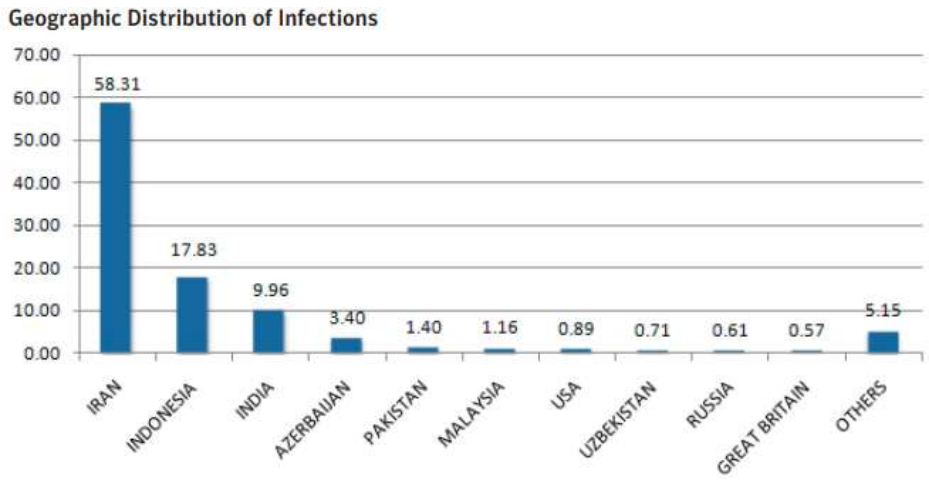

Figure 2. Source: W32.Stuxnet Dossier Version 1.4 (February 2011), Symantec.

qu'elles doivent être en mesure de résister à ces nouvelles attaques sophistiquées. Qu'il doit y avoir une collaboration entre les acteurs de la sécurité, et qu'ils doivent mettre en place de meilleures stratégies.[10]

Microsoft a rapidement réagi en annonçant le bulletin de sécurité MS10-046, le 2 août 2010, et les correctifs associés. BitDefender et Microsoft mettent à disposition des outils gratuits pour se débarrasser des malwares les plus en vogue du moment. Parmi les outils de BitDefender, il y en a un qui permet de supprimer Stuxnet, qui a été mis à disposition le 8 octobre 2010.[9] Le 19 août 2010, un outil de suppression est mis à disposition par FSB Security Labs en France.[9]

De façon générale, certains principes sont à préconiser pour se protéger des virus qui sont des programmes malveillants qui se propagent en infectant des fichiers exécutables sur un ordinateur ou un réseau, ils ont besoin d'un hôte pour se propager et se répliquer, et sont généralement cachés à l'intérieur d'autres programmes ou fichiers. Des vers qui eux sont des programmes malveillants qui se propagent en utilisant des réseaux informatiques, mais qui n'ont pas besoin d'un hôte ou d'une intervention humaine pour se propager et tous les autres logiciels malveillants.

– Utiliser un réseau avec pare-feu afin de protéger votre réseau.

– Mettre en place des politiques strictes pour les périphériques afin de prévenir l'infection des appareils par des clés USB malveillantes.

– Utiliser les anti-virus et les VPN (Virtual Private Network).

- Utiliser des mots de passe complexes et éviter d'avoir un même mot de passe.

– Surveiller de façon optimale afin de détecter toute réaction inhabituelle.

– Ne cliquez jamais sur un lien douteux envoyé par e-mail.[11]

Conclusion

Cet article fait une présentation de Stuxnet, son historicité, ses conséquences, son fonctionnement et présente certaines mesures qui ont été prises et certaines à prendre pour faire face à des attaques similaires.

Stuxnet est un malware spécialisé qui vise les systèmes SCADA utilisant les logiciels Siemens SIMATIC® WinCC ou Siemens STEP 7 pour la visualisation des processus et le contrôle du système. Il utilise plusieurs vulnérabilités du système d'exploitation Windows® pour infecter et se propager. Le malware se propage par l'intermédiaire de clés USB ou de partages réseaux ouverts et est conçu pour rester caché sur les systèmes infectés pendant très longtemps grâce à un composant rootkit. L'attaquant peut ensuite prendre le contrôle total du système infecté à distance.

Stuxnet a été l'une des plus grandes cyberattaques, et d'autres s'ensuivirent. Des mesures ont été prises, des recherches ont été faites, cependant, nous aurons toujours à faire face à des attaques de cyber. Il serait important de garder les bons principes et de rénover à chaque fois. Car, comme disait Albert Einstein, "agir intelligemment dans les affaires humaines n'est possible que si l'on essaie de comprendre les pensées, les motifs et l'appréhension de son adversaire de telle manière que l'on puisse voir le monde à travers ses yeux".[12]

Référence

[1] *Cyberattaque, Wikipédia.*

[2] *Countdown to Zero Day, Kim Zetter.*

[3] *W32.Stuxnet Dossier, version 1.4 (February 2011), Nicolas Falliere, Liam O Murchu, and Eric Chie.*

[4] *The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight, 2 novembre 2011, Eugene Kaspersky.*

[5] *L'écran bleu, d'où vient-il ? Comment se débarrasser des "écrans bleus de la mort" ?, 22 mai 2016, Mathilde.*

[6] *Qu'est-ce que le ver Stuxnet?, 14 Septembre 2022, Delphine Lacour.*

[7] *Tout savoir sur les systèmes SCADA, FactoryFuture.*

[8] *STUXNET: Analyse, Mythes et Réalités, L'ACTUSÉCU 27, David Helan.*

[9] *Stuxnet, Wikipédia.*

[10] *L'analyse du logiciel malveillant «Stuxnet» par l'agence Européenne, 07 octobre 2010, ENISA.*

[11] *Stuxnet : zoom sur la « cyber-arme » et comment s'en protéger, 21 Novembre, 2022, Adriana L.*

[12] *Citation célèbre, Le Parisien, Albert Einstein.*

Le ver Stuxnet est-il la première cyber-arme ?, 22 septembre 2010, La Rédaction.