Cyberwarfare

Stuxnet Malicious Computer Worm, et Autres Virus Stratégiques

Étudiants (M2 IMPAIRS):

FERG Mohamed Amine
KEDJOUR Mohamed Tahar

Sommaire

Introduction

Depuis les temps anciens, le monde a toujours connu des confrontations entre les empires et les nations qui s'étalait sur les quatre coins du monde, le but étant toujours le même: faire osciller la balance du pouvoir en sa faveur.
Dans les relations international, la balance du pouvoir fait référence à l'équilibre entre les pays ou alliances qui empêche une entitée de devenir beaucoup plus puissante que les autres, et ainsi imposer son vouloir sur eux.
Par conséquent, chaque nation doit rester sur la voie de modernité militaire, économique et politique, en prenant conscience de sa position sur l'échelle de puissance mondiale, et en essayant d'escalader les marches de cette dernière.

Tout comme dans les périodes de 1100 avant JC—où le monde a connu le commencement des guerres navales—le XXI^{e} siècle (21^{e}) a donné naissance à un nouveau champ de guerre sur lequel les pays s'échangent les coups en silence depuis des années.
En effet, la technologie moderne a réussi à connecter et automatiser les industrie et les tâches donnant une valeur immense à l'information, et introduisant un nouvel espace qui a ensorcelé les yeux: un espace de guerre cybernétique. C'est le commencement d'une nouvelle ère de guerre, le Cyberwarfare.

Cyberwarfare

Cyberwarfare est un mot qui se compose de deux termes, "Cyber" et "Warfare":

- **Cyber-** est un préfixe dérivé du mot "Cybernetic", défini comme étant l'étude scientifique du contrôle et la communication dans la machine et l'animal.
- **Warefare** représente le processus d'un conflit militaire entre deux nations ou alliances.

Selon une définition générale "Cyberwarfare fait référence à une attaque digitale massivement coordonnée sur un gouvernement par un autre. C'est l'action d'une nation de pénétrer les ordinateurs et les réseaux d'une autre nation dans le but de causer des dommages et des perturbations." [2]
En d'autre termes, il s'agit de l'usage des aptitude cybernétique afin d'accomplir des objectifs militaires, comme définit par le Département de Défense Américaine (DoD).

Cyberspace: le champs de guerre du XXI^{e} siècle

Contrairement à l'espace naturel connu par la terre, la mer, l'air, l'espace ou le spectre électromagnétique, l'espace cybernétique est beaucoup moin concret: il ne fait pas partie de la nature et ne peut pas exister sans les technologies d'information [1].

Cyberspace représent l'ensemble de tous les réseaux informatiques existent dans le monde et tout ce qui est connectable et contrôlable via des câbles (cuivre, fiber-optique, …) ou sans fil. Ainsi, le Cyberspace inclut le réseau internet et autre réseaux privés qui sont inaccessible via l'internet [2].

L'espace cybernétique se compose de trois couches ordonnées par leur niveau de concrétion [1]:

- **La couche d'infrastructure physique:** qui représente l'ensemble des dispositifs et de systèmes de communication (circuits intégrés, infrastructure de communication, processeurs, etc)
- **La couche de logique logicielle:** qui décrit l'ensemble des programmes et des instructions programmées par l'humain afin de contrôler la couche physique.
- **La couche de données:** qui correspond à la totalité d'information manipulé, transmise ou stocké.

Actuellement, l'espace cybernétique se compose de l'intégrité des ordinateurs, serveurs, routeurs, switches et communication câblée ou sans fil qui permettent le fonctionnement des infrastructures critiques.

Les menaces évoquées par le Cyberwarfare

Le Cyberwarfare est caractérisé par les échanges d'attaques au niveau cybernétique, autrement nommée "Cyber-attack", qui est une manoeuvre offensive stratégique visant une cible spécifique en employant des moyens malicieux.

Une attaque cybernétique nécessite un minimum de moyens et d'hommes, ce qui lui donne une importance significative selon le niveau et le type de menace qu'elle implique, et qui peut être classifié sous les catégories suivantes:

- **L'espionnage:** l'espionnage cybernétique consiste à la collection d'information et des données (militaires, politiques, économique, etc) à distance et depuis n'importe quel point du monde.

- **La propagande:** une attaque très efficace vu qu'elle se base sur les médias et l'alternance de l'opinion publique, ce qui lui qualifie d'être une des plus grandes menaces.
- **Déni de Service (DoS):** la simple stratégie qui se tient derrière ce type d'attaque est d'empêcher des utilisateurs légitimes d'accéder à certains services informatiques, en inondant la cible avec des tâts de données inutiles, ce qui lui rend incapable de répondre aux vrais requêtes.
- **Modification de données:** ce genre d'attaque peut s'étaler d'une simple défiguration de pages web (ce qui peut faire partie d'une propagande) jusqu'aux attaques sur les bases de données destiné à saboter des armes ou des systèmes de contrôles.
- **Manipulation d'infrastructure:** Les infrastructures nationals (secteurs d'énergie, finance, nucléair, etc) sont de plus en plus connecté à internet, ce qui les rend vulnérable. L'incapacitation de ce genre de systèmes peut avoir des effets redoutables, ce qui impose une obligation de renforcer leur sécurité.

Raisons de convergence vers la guerre cybernétique

"*For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.*" Sun Tzu.

Cela dit, la plus grande des ambitions d'une partie dans une guerre est de remporter la victoir avec le minimum de perte et de ressource épuisé.

Le cyberwarfare se tient sur un ensemble de principes avantageux pour les parties et les nations et qui peuvent être résumés comme suit [2]:

- Il ne nécessite pas un large nombre de troupes et d'armes, ce qui réduit les coûts.
- Les coûts de participation sont faibles, avec un ordinateur et une connexion internet n'importe quelle partie peut s'engager.
- La guerre cybernétique peut être délivré depuis n'importe quel point du monde connecté.
- L'acquisition des outils d'attaque ne subit aucun contrôle et sont librement disponible.
- L'attaquant a toujours un avantage: il peut profiter des innovations modernes et exploiter des vulnérabilités inconnus par la victime.
- Le Cyberspace offre l'avantage d'anonymat et d'impunité, vu la difficulté de tracer la source d'attaque (généralement sur le court terme).
- La distribution du pouvoir est disproportionnée sur l'espace cybernétique, donnant l'autorité à des acteurs qui sont parfois non significatifs.
- Perturbe les forces enemy et endurcit l'évaluation des dégâts atteint.
- La neutralization d'une attaque nécessite des équipes d'experts en matériels et logiciels et des dépenses phénoménales.

Cyber-attack

L’attaque cybernétique peut être désigné par un ensemble d’actions planifié qui ont pour but la déception, perturbation ou même la destruction des systèmes ou infrastructures informatiques d’un adversaire.

Tout comme dans toute forme de guerre, les facteurs principales sont les faiblesses dans la défense ennemie (vulnerabilities) et les armes utilisées (types d’attaques).

Les vulnérabilités Informatiques

Les cyber-attacks sont possibles en raison de vulnérabilités au niveau des systèmes et des réseaux informatiques, introduites d’une façon non intentionnelle (ou pas) lors de la conception ou d’implémentation de ces derniers. Le tableau suivant contient quelque types de vulnérabilités exploitables [2]:

Vulnérabilité	**Description**
Logiciel (Software)	Les programmes peuvent contenir des défauts introduits délibérément ou accidentellement, et dont l’exploitation peut altérer le fonctionnement prévu du système.
Matériel (Hardware)	Tout comme les programmes, les matériels informatiques peuvent aussi contenir des défauts de fonctionnement lors de leur fabrication, comprenant les microprocesseurs, les microcontrôleurs, les centrales d'énergie, les périphériques comme les imprimantes, les disques de stockage, les équipements de communication. Toute modification fait sur ces derniers peut produire d’autres fonctionnalitées inattendu.
Les points de jointure entre logiciels et matériels	Tel que le firmware (read-only memory) qui peut être reprogrammé d’une façon clandestine.
Les chaînes de communication	Il est possible d’intercepter la communication qui circule entre les systèmes et le monde extérieur, et ainsi espionner ou même empêcher l'adversaire de la recevoir.
Les fournisseurs de services (Service Providers)	Les fournisseurs de services jouent un rôle important dans le monde de la technologie, ils offrent des services critiques tel que la maintenance et l’accès internet. Une attaque sur les fournisseurs d’un adversaire peut être vue comme une attaque indirecte avec un même niveau d'efficacité qu’une directe.

Le scénario le plus commun d'une attaque cybernétique nécessite une vulnérabilité dans le système de l'adversaire, un accès à cette vulnérabilité afin de l'exploiter et un payload à exécuter.

Un payload est un terme utilisé pour décrire l'action qui sera faite après l'exploitation d'une vulnérabilité. Les payloads peuvent se trouver dans plusieurs formes, tout dépend du type de vulnérabilité et de la méthode d'attaque.

Les méthodes d'attaques (Cyber Weapons)

Il existe plusieurs types et outils d'attaques cybernétiques, nommé généralement Cyber Weapons (les armes cybernétiques), qui sont de plus en plus sophistiqués, avec des capabilities avancées, sans infrastructure nécessaire ou limitations de matériaux et du savoir. Le tableau suivant décrit quelque méthodes d'attaques [2]:

Attaque	Description
Déni de Service (DoS)	
Inondation (Flooding)	Envoi d'énormes flux de données inutiles afin de bloquer un service hôte.
Nuking	Forger des messages afin de réinitialiser les connections actives.
Les attaques avec des programmes malveillant	
Worm	Un programme qui pénètre les systèmes d'exploitation et les réseaux afin de propager des instructions malveillant.
Virus	Un code qui se reproduit dans les applications existantes sur le système ou le réseau.
Backdoor	Une fenêtre à travers laquelle des commandes à distance peuvent être exécutées.
Trojan	Un code ou programme qui peut exécuter des commandes, et qui est caché dans un autre programme légitime.
Exploits	
Overflows	Écrire un code arbitraire au-delà de la taille d'un tampon afin de l'exécuter (Buffer

	Overflows, Heap Overflows, Integer Overflows, …).
Brute force	Essaie répétitif des combinaisons différentes de caractères afin de d'accéder à un système protégé par un mot de passe.
Race Conditions	Exploiter les conditions non sécurisé dans les différent programmes.
Privilege escalations	L'action d'obtenir un accès élevé aux ressources d'un système qui sont protégés contre les applications et les utilisateurs.
Manipulations des paquets d'IP	
Remote Session hijacking	Faire du spoofing afin d'intercepter et rediriger les connections.
Blind IP spoofing	Changer l'adresse IP de la source pour accéder à certains services sans qu'un mot de passe soit exigé
Insider Attack	
Camouflage (Cloaking)	Faire remplacer des fichiers systèmes afin de cacher les accès non autorisées.
Reniflement (Sniffing)	Capturer les données transmises qui circulent sur le réseau afin de trouver des information sensibles.
Backdoor daemons	Il s'agit d'ouvrir un port caché afin de permettre un accès à distance.
Manipulation des fichiers logs	Supprimer les traces d'une attaque ou un accès non autorisé.

Stuxnet: L'Iran sous la cible, Opération Jeux Olympiques

Durant la présidence de George W. Bush, les Etats-Unis a mené une campagne d'attaques cybernétiques nommé "Opération Olympic Games" (avec la coopération probable l'Agence de Sécurité Nationale (NSA) américaine ainsi que les forces Israéliennes) sur l'Iran, dans le but d'endommager et causer des perturbation au niveau des centrales nucléaires iraniènnes. Cette

dernière était une opération clandestine classifié et non reconnu par le gouvernement américain, et dont l'arme principale était un logicielle malveillant (Worm) connu couramment dans la communauté informatique par Stuxnet.
L'Opération Jeux Olympique est considéré une des plus grande attaques manipulatives depuis la deuxième guerre mondiale en vue de son effet dévastateur qui a atteint environ 5000 centrifuges iraniens [3].

Historique

Lors d'une visite d'inspection sur la centrale d'enrichissement de l'uranium en mois de Janvier 2010 à Natanz (Figure 1), Iran, les inspecteurs de l'Agence International de l'Energie Atomique (IAEA) ont remarqué que le taux de pannes au niveau des centrifuges était trop élevé. Par conséquent, l'entreprise de sécurité informatique VirusBlokAda a été invoqué afin d'intervenir pour régler le problème. En juin 2010, les chercheurs de "VirusBlokAda" ont trouvé des fichiers malicieux sur un des systèmes, ce qui a mené à la découverte de "Rootkit.Tmphider", le nom original du virus connu aujourd'hui par Stuxnet, qui s'agit d'une combinaison des termes ".stub" et "mrxnet.sys".

La raison qui conduit à la découverte de ce virus était une erreur de programmation introduite lors de la mise à jour de ce dernier, menant vers une propagation incontrôlable vers autres machines que celle du central de Natanz, à commencer par l'ordinateur d'un ingénieur qui a joué le rôle d'un porteur de virus depuis le centrifuge vers le réseau internet.

Les chercheurs de la corporation de logiciels de sécurité américaine Symantec ont révélé une version plus ancienne de Stuxnet—utilisé pour attaquer la même cible—qui datée de Novembre 2007, et qui était en développement quand l'Iran faisait la mise en place de ces centrales en 2005 [3].

Figure 1 - La centrale d'enrichissement de l'uranium - Natanz, Iran

Mode d'opération

D'après les aspects techniques découvert lors de l'analyse de Stuxnet, il est possible de spéculer un scénario d'attaque de ce dernier:

Afin de pouvoir manipuler ou endommager une centrale industriel (tel qu'une centrale d'enrichissement de l'uranium) l'attaquant doit pouvoir accéder aux Systèmes de Contrôle Industriel (ICS) qui sont opérés par un ensemble de Contrôleurs Logiques Programmables (PLC)—généralement programmés par des ordinateurs Windows isolés—qui s'occupe du contrôle des processus de manufacturation.

La configuration des PLC diffère selon les tâches qu'ils doivent effectuer, par conséquent, l'attaquant doit tout d'abord obtenir les schémas de l'ICS physiquement ou à travers une autre attaque cybernétique. Cela donnera la possibilité de développer une version de Stuxnet avec des caractéristiques spécifique au système industriel visé, afin d'infiltrer et manipuler les PLC et saboter l'ICS.

L'attaquant doit aussi mettre au point un environnement de test, conçu à partir des schémas obtenus en utilisant les même périphériques et architectures.

Les fichiers malicieux (contenant des pilotes) doivent être signé digitalement afin d'éviter les soupçons, en obtention des certificats digitales d'une ou plusieurs entreprises reconnus et digne de confiance.

Afin d'installer la version final de Stuxnet sur l'environnement ciblé, il est indispensable d'exploiter une partie tierce (volontaires ou pas) qui a un accès directe au central (à travers un flash disque par exemple).

Les PLC sont programmés par des ordinateurs Windows (appelés Field PGs) qui ne sont pas connectés au réseau. Afin de les atteindre, l'attaquant doit se propager sur les autres noeuds du LAN en exploitant une zero-day vulnerability au niveau des projets Step 7 de Siemens, ce qui augmente les chances de transporter le virus Stuxnet d'une machine infectée vers un Field PG.

La logique requise pour le sabotage du système de la central doit être incorporé dans l'exécutable de Stuxnet, vu que les Field PGs sont des machines isolées du net. Les mise à jours de Stuxnet sont introduites à travers un réseau pair-à-pair entre toutes les machines infectées (connectées à internet ou pas).

Le Stuxnet doit finalement pouvoir modifier le code des PLC d'une façon secrète et indétectable [4]. Les figures 2 et 3 représentent le fonctionnement des PLC avant et après l'infection respectivement:

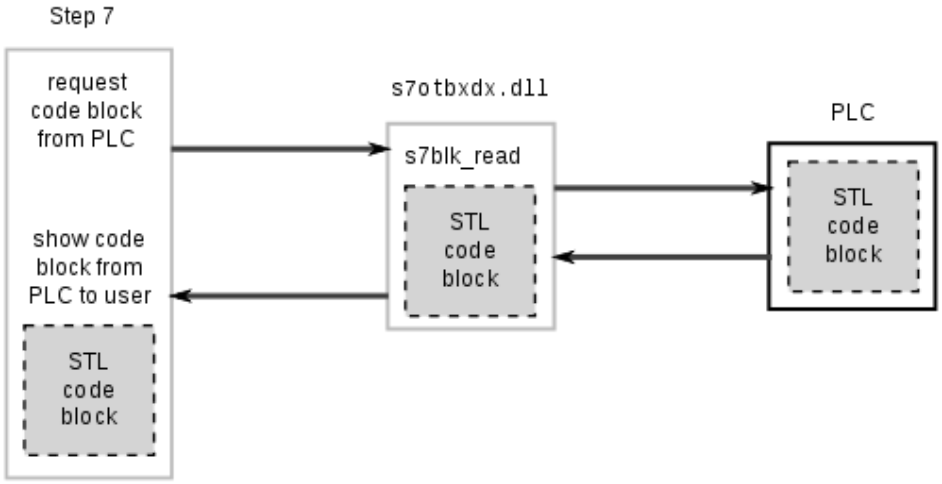

Figure 2 - Fonctionnement des PLC avant l'infection par Stuxnet [8]

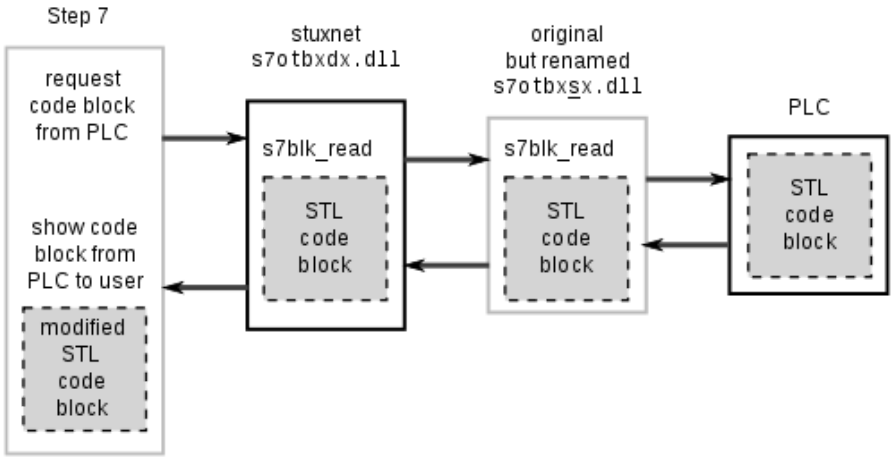

Figure 3 - Le fonctionnement des PLCs après l'infection par Stuxnet [8]

Les méthodes de propagation

La propagation de Stuxnet est très rapide, mais reste limité par des contraintes afin de le garder sous contrôle (il n'infecte que trois ordinateurs à travers un flash disque, et s'auto-effacer à partir du 24 juin 2012).
Stuxnet utilise plusieurs méthodes et vulnérabilités pour se propager:

Propagation à travers les flash disques

La propagation via flash disques se base sur l'exploitation de deux vulnérabilités principals qui sont Windows LNK pour les versions les plus récentes de Stuxnet, et autorun.inf pour les versions les plus anciennes.

- **La vulnérabilité Windows LNK (CVE-2010-2568):** Lors de l'insertion d'un flash disque dans un port USB d'un ordinateur infecté, Stuxnet crée une copie sur le lecteur (le DLL de Stuxnet et quatre fichiers .lnk pour charger le virus sur la machine quand un utilisateur insère le flash disque dans une autre machine).

- **Le fichier autorun.inf:** ce type de fichiers s'exécute automatiquement sur un flash disque lors de son insertion. Les versions précédentes de Stuxnet placé un tel fichier sur les flash disques, contenant le code du virus lui même ainsi qu'une liste de commandes pour infecter la cible [5].

Propagation via la vulnérabilité "MS10-061 Print Spooler 0-day"

Une autre manière dans laquelle Stuxnet utilise pour se propager sur le réseau est d'exploiter la vulnérabilité qui se trouve dans le service Windows Spooler (MS10-061). Toutes les machines qui partagent des fichiers et des périphériques (imprimante) sont vulnérables par cette attaque. Cette vulnérabilité peut permettre à un attaquant d'exécuter à distance un code arbitraire en envoyant une requête d'impression forgée vers le système vulnérable qui a l'interface Print Spooler exposé sur RPC (Remote Procedure Call) [6].

L'application Siemens WinCC

Stuxnet cherche les ordinateurs qui exécutent l'interface des systèmes SCADA Siemens WinCC, et utilise un mot de passe prédéfini afin de pouvoir attaquer la base de données du système en utilisant des commandes SQL et téléchargeant une version de Stuxnet sur l'ordinateur victime [5].

Propagation via la vulnérabilité “MS08-067 SMB”

Stuxnet peut se propager en envoyant un chemin malformé sur SMB (un protocole de partage des fichiers et autres ressources entre les machines), ce qui lui permet d'exécuter un code arbitraire sur la machine victime [7].

Exploitation des projets Step7

Sur les ordinateurs contaminé par Stuxnet, le virus cherche les projets de contrôle industriel de Siemens SIMATIC Step7 seront infecté en modifiant leurs fichiers DLLs ainsi qu’un fichier exécutable .exe dans le WinCC Simatic Manager, afin qu’ils exécutent le code de Stuxnet lors de l’exécution de ces projets [5].

La figure 4 illustre les différentes méthodes de propagation utilisées par Stuxnet:

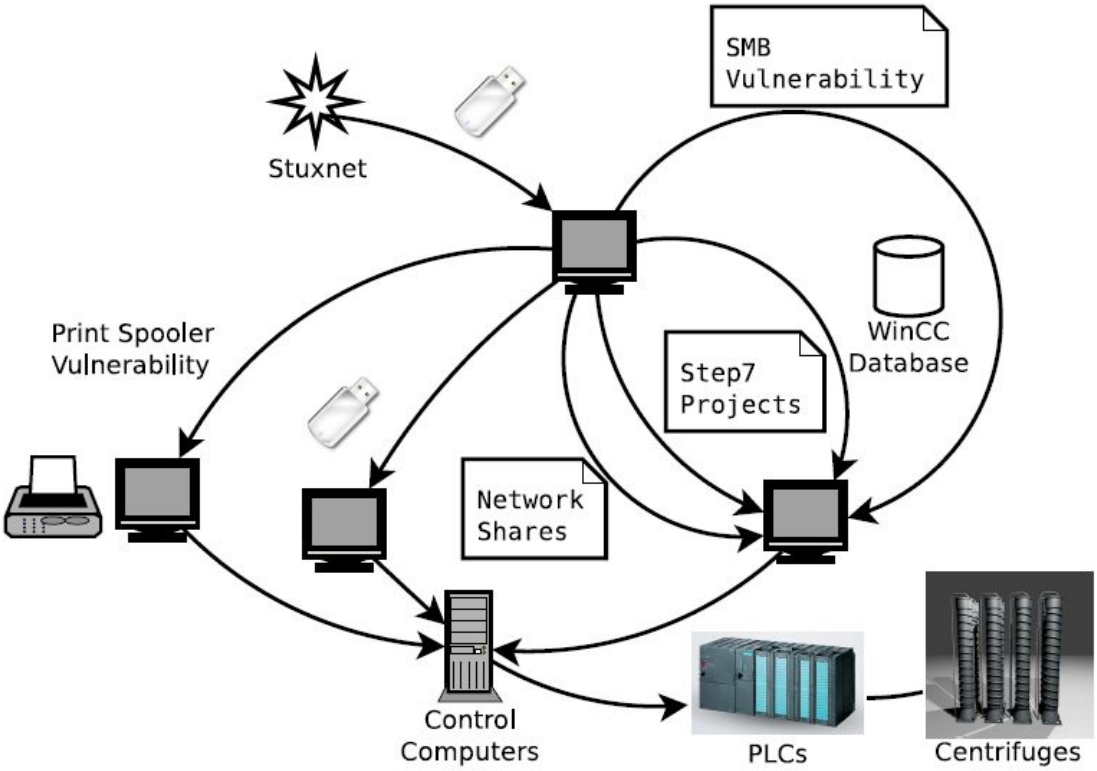

Figure 4 - Les différentes méthodes de propagation utilisées par Stuxnet [5]

Les pays infectés par Stuxnet:

Une étude effectué par la corporation de logiciels de sécurité américaine Symantec a démontré le taux de propagation du virus dans plusieurs pays (figure 5):

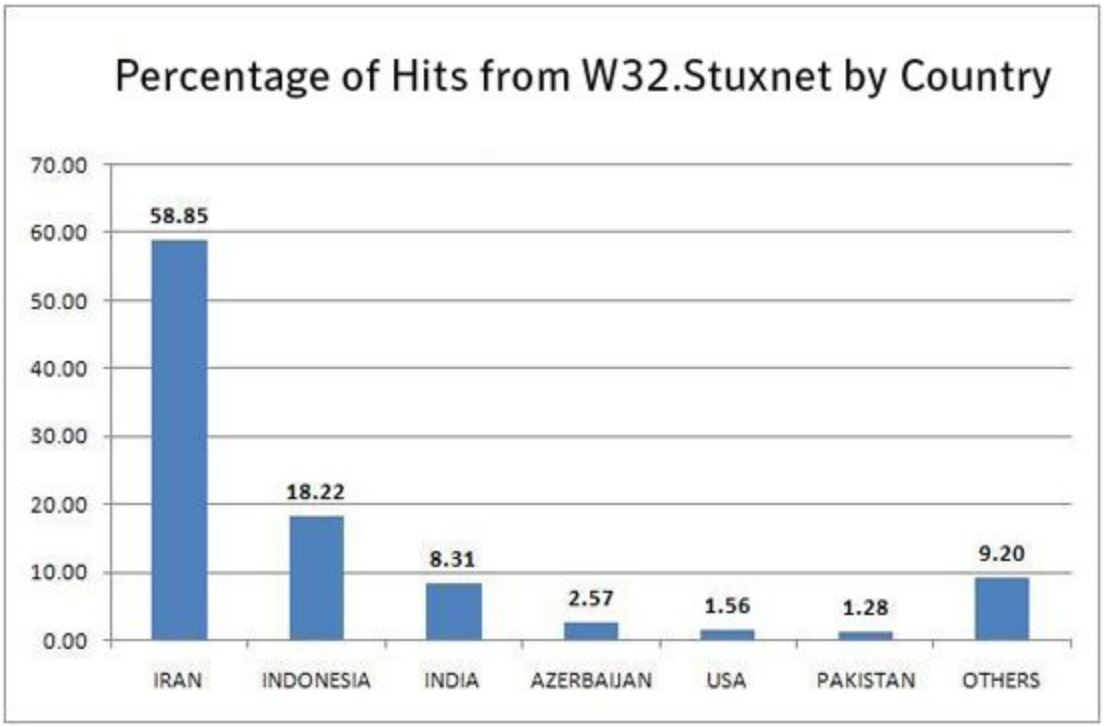

Figure 5 - Taux d'infection par Stuxnet dans différents pays [4]

Autres armes cybernétiques

Stuxnet a marqué le début d'une nouvelle ère de sécurité informatique, où le sense des malwares et le but de leurs existences ont été altérés. En effet, Stuxnet a réussi à produire des dégâts physiques (endommagement des centrifuges Iraniennes) ce qui est considéré comme un act sans précédent pour un malware informatique.
Depuis, des nouvelles générations de virus dévastateurs émergent sans cesse, utilisés généralement comme des armes stratégiques. Nous comptons ce qui suit:

Duqu

En septembre 2011, le Laboratoir de Cryptographie et Sécurité des Systèmes (CrySyS) ont publié un rapport qui dévoile l'existence d'un nouveau malware comportant des

ressemblances frappantes avec Stuxnet sur le niveau technique (il se base sur plusieurs modules de Stuxnet) et le but de sa création (espionnage sur le programme nucléaire Iranien). Duqu utilise les même méthode de propagation en exploitant une différente faille de type Zero-Day [9] (MS11-087) qui se trouve sur un pilote Kernel-Mode de Windows. En effet, Duqu utilise un fichier word spécial qui exploite le moteur de parsing TrueType du module Win32K de kernel Windows afin d'exécuter un code arbitraire et gagner un accès privilégié au système [10][11].

Les victimes de Duqu ont été trouvées dans plusieur endroits, comprenant l'Europe de l'ouest, les Moyen-Orient et l'Asie.

Flame

En Mai 2012, Kaspersky Lab, MAHER Center of Iranian National CERT et CrySyS Lab ont découvert une autre arme cybernétique—classifié comme l'arme cybernétique la plus large qui n'a jamais été détectée auparavant—qui a été nommée Flame ou Da Flame (figure 6).
Flame est considéré comme étant un des programmes malicieux les plus sophistiqués. Tout comme le fameux Stuxnet, Flame est considéré comme étant une arme cybernétique qui est spéculé d'être opérationnel depuis Mars 2010.
Ce malware était conçu d'une façon qui le rend presque indétectable, avec des modules qui le permet d'effectuer des acts d'espionnage (collecte d'information critiques, de données stockées, les conversations, etc), et une complexité qui dépasse toutes les cyber weapons connus [12].

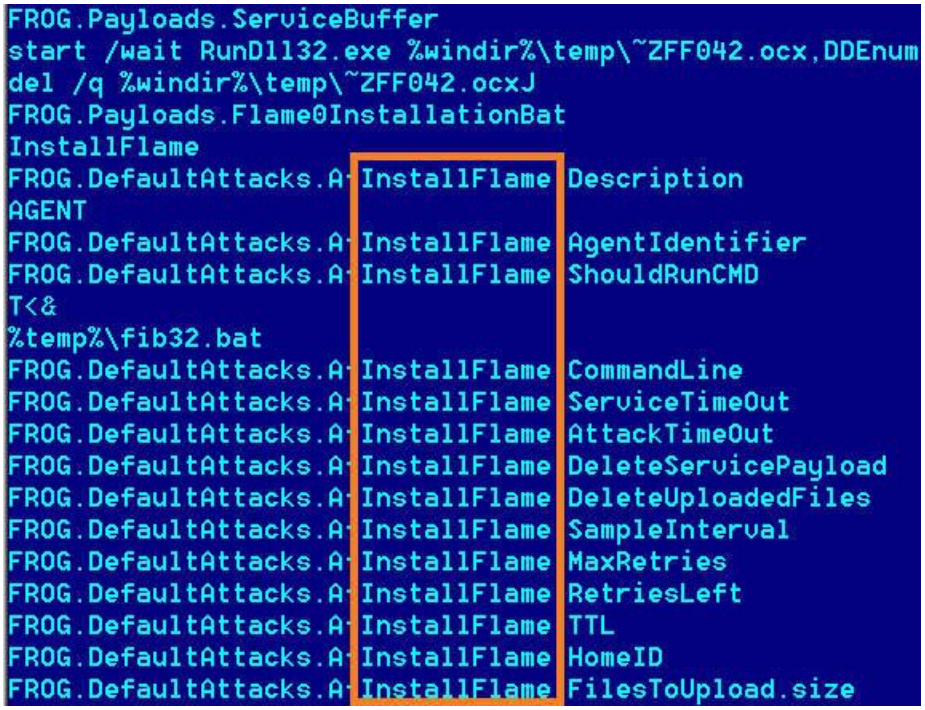

Figure 6 - Flame a été nommé après l'un de ces modules principaux [13]

Conclusion

Le Cyberwarfare est un domaine récent qui ne cesse d'attirer l'attention des nations et des individus ces dernières années. L'évolution des armes utilisées dans ce champs de batail s'accroît rapidement, ce qui introduit une inquiétude ainsi qu'une friction entre les groupes, organisations et même les gouvernements.

Plusieur experts et politiciens aujourd'hui se mettent d'accord que l'exploitation des armes cybernétiques ne s'élève pas aux actes de guerre. Par Contre, les derniers développements notés lors de la fameuse opération Jeux Olympique sur l'Iran a remis le débat sur la table, après l'apparition d'un virus informatique si sophistiqué qu'il peut causer des dégâts physiques qui peuvent toucher les infrastructures critiques des pays, et re-distribuant les cartes du pouvoir.

Actuellement, la course vers l'armement cybernétique est toujours en marche sous les ombres de confidentialité, et le renforcement des défense est devenus plus qu'une simple obligation. L'agitation dans le cyberespace continu, et le future ne pourra être prédit, seulement révélé avec le temps.

Références

[1] Lior Tabansky, Basic Concepts in Cyber Warfare
[2] Fred Schreier, (2015), On Cyberwarfare
[3] Kim Zetter, (2014), An Unprecedented Look at Stuxnet, the World's First Digital Weapon. wired.com
[4] Nicolas Falliere, Liam O Murchu et Eric Chien, (2011), W32.Stuxnet Dossier. Symantec
[5] Paul Mueller et Babak Yadegari, (2012), The Stuxnet Worm. Université d'Arizona
[6] https://technet.microsoft.com/en-us/library/security/ms10-061.aspx
[7] https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
[8] https://en.wikipedia.org/wiki/Stuxnet
[9] https://technet.microsoft.com/en-us/library/security/ms11-087.aspx
[10] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, Márk Félegyházi, 14 Octobre 2011, Duqu: A Stuxnet-like malware found in the wild, Laboratory of Cryptography and System Security (CrySyS)
[11] (11 juin 2015), THE DUQU 2.0 Technical Details, Kaspersky Lab
[12] https://www.kaspersky.com/flame
[13] https://www.wired.com/2012/05/flame/