ADVANCED PERSISTENT THREATS
ÉTAT DE L'ART

TANIA MARTIN

Smals SECTION RECHERCHE 03/2014 • RESEARCH NOTE • 32

Résumé – Depuis quelques années, le monde de la sécurité informatique doit faire face à un nouveau type de cyber-attaques très sophistiquées appelé APT, sigle pour « *Advanced Persistent Threats* ». Au vu des préjudices que peuvent causer les APT, tout organisme et entreprise doit se tenir au courant de cette récente problématique. L'objectif de cette research note est double. Tout d'abord, elle présente un état de l'art des APT, avec leurs caractéristiques et quelques exemples célèbres. Ensuite elle parcourt brièvement les solutions existantes qui permettent potentiellement de se protéger de ces menaces.

Abstract – Sinds enkele jaren moet de wereld van informaticaveiligheid opboksen tegen een nieuw type zeer geavanceerde cyberaanvallen genaamd APT, wat de afkorting is voor "*Advanced Persistent Threats*". Gezien de schade die deze APT's kunnen berokkenen, moeten instellingen en ondernemingen op de hoogte blijven van deze recente problematiek. Deze research note kent twee doelstellingen. Ze stelt in de eerste plaats een overzicht voor van de APT-aanvallen, met hun eigenschappen en enkele bekende voorbeelden. Vervolgens worden de bestaande oplossingen waarmee men zich potentieel kan beschermen tegen deze bedreigingen kort overlopen.

Table des matières

1. Contexte 2

2. Anatomie d'une APT 3
2.1. Vocabulaire 3
2.2. Cycle de vie d'une APT 4

3. Quelques célèbres APT 12
3.1. Un exemple concret : Stuxnet, 2009 12
3.2. Autres exemples d'APT 15

4. Comment se protéger d'une APT 19
4.1. Protéger le système informatique 19
4.2. Former les équipes HelpDesk et sécurité 21
4.3. Former les employés lambda 22

5. Conclusions 23

1. Contexte

Récemment, la communauté d'experts en sécurité informatique a officialisé un nouveau type d'attaques très tendance : les *Advanced Persistent Threats* (APT). Cette terminologie fait référence aux techniques et méthodologies qui peuvent être utilisées par un groupe d'individus pour perpétrer une attaque de longue durée sur une cible bien définie. Selon une enquête d'ISACA[1] datant de 2013, 63% des entreprises interrogées pensent que c'est une simple question de temps avant qu'elles ne soient ciblées par une APT, comme illustré en Figure 1.

Figure 1 : résultat de l'enquête d'ISACA sur la probabilité perçue par une entreprise de devenir la cible d'une APT (Crédit : ISACA)

Pour entrer un peu plus dans les détails, la démarche pour réussir une telle attaque se rapproche fortement de l'espionnage industriel. Une APT peut se baser sur plusieurs méthodes. La plus connue est l'utilisation des techniques d'espionnage traditionnel, telles que les interceptions et écoutes téléphoniques, ou encore l'imagerie satellitaire.

Mais de nos jours, l'espionnage informatique à proprement parler se développe de plus en plus. Ainsi, les cyber-attaques sont fortement utilisées au cours d'une APT, en particulier celles basées sur la surveillance des connexions Internet dans le but d'accumuler un maximum d'informations sensibles. D'autres vecteurs de cyber-attaques reconnus sont aussi bien les virus, vers, rootkits et autres exploits de vulnérabilité, que le social engineering.

[1] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx

But d'une APT :

Une APT vise à ***infiltrer*** un système informatique cible et s'y ***installer*** pour une longue durée sans se faire détecter, pour ensuite ***capturer*** et ***extraire*** des informations sensibles.

Le problème majeur des APT est l'habileté dont les attaquants font preuve pour exécuter ces attaques. Il faut principalement retenir que les attaquants sont généralement très organisés et puissants, avec les moyens/ressources nécessaires et les connaissances suffisantes en cyber-attaques. C'est pourquoi on considère que ce sont plutôt des « groupuscules d'attaquants », tels que des organisations terroristes ou criminelles, des collectifs activistes (p.ex. de hackers), ou encore des États-nations, plutôt que des individus isolés qui sont en mesure de mettre en place une APT.

Les motifs, quant à eux, sont variés : obtenir un avantage financier, éliminer la compétitivité, accumuler des informations sensibles, s'implanter dans la cible pour des exploitations futures, gêner une organisation, endommager une réputation, faire tomber un système informatique, ou encore obtenir un accès indirect à un groupe associé de la cible. Le sentiment général est que la nature du contexte socioéconomique et culturel a clairement évolué ces dernières décennies : la concurrence entre les entreprises et les conflits géopolitiques ont fortement augmenté. Au final, ce ne sont pas tant les attaques de type APT qui sont une nouveauté, mais plutôt leurs motivations et mises en œuvre.

2. Anatomie d'une APT

Cette section présente les caractéristiques qui définissent les attaques de type APT, de leur signification à leur principe de fonctionnement.

2.1. Vocabulaire

Pour donner l'intuition de ce qui se cache derrière le terme « APT », il est tout d'abord important d'expliquer brièvement la signification de ce sigle.

- « *Advanced* »

Le groupuscule d'attaquants met en œuvre tout un arsenal de techniques et d'outils d'attaques très poussés pour atteindre son objectif. En regardant plus attentivement chaque composant d'une APT, on se rend compte que, individuellement, ces derniers ne sont pas forcément très évolués. Par exemple, une APT peut utiliser du *phishing*[2], du *cross-site*

[2] Expliqué en Section 2.2.1.

scripting[3] ou tout simplement un *malware*[4] qui a été généré automatiquement par un « *do-it-yourself* kit »[5]. La force d'une APT est que le groupuscule d'attaquants va combiner, développer et améliorer de tels composants dans le but unique d'atteindre et de compromettre au mieux la cible de l'attaque, ainsi qu'y maintenir un accès sûr.

- « *Persistent* »

Une fois l'accès à la cible établi, le groupuscule n'essaie pas de voler toutes les informations de manière opportuniste en une seule fois. Il va essayer de maintenir cet accès le plus longtemps possible – cela peut se compter en mois – pour récolter divers renseignements sur la cible, et utiliser ces renseignements pour lancer de multiples attaques sur une période de temps étendue. Le mode opératoire du groupuscule implique donc discrétion, évitant ainsi une quelconque suspicion ou détection de la part de la cible. C'est pourquoi une approche furtive et lente (« *low-and-slow* ») est privilégiée à un déferlement d'attaques ponctuelles.

- « *Threats* »

Les renseignements récoltés lors d'une APT peuvent être une grande menace pour la cible ou les citoyens de façon générale (p.ex. les plans d'une centrale nucléaire, les codes d'accès d'un employé d'une agence de renseignements). De plus, une APT ne repose pas sur la simple injection et exécution de malwares dans le système informatique de la cible. Le groupuscule est capable de coordonner méthodiquement, avec une stratégie prédéfinie, les actions des attaquants, ces derniers étant souvent hautement qualifiés et expérimentés, ainsi que motivés car appréciablement financés.

2.2. Cycle de vie d'une APT

En 2013, Dell SecureWorks a publié le cycle de vie très détaillé d'une APT que l'on retrouve ici en Figure 2. Cette section explique les cinq étapes majeures qui peuvent être extraites de ce cycle de vie.

1. Reconnaissance
2. Infiltration
3. Implantation
4. Extraction
5. Maintien

[3] Le *cross-site scripting* est un type de faille de sécurité des sites web où il est possible d'injecter des données arbitraires (ou du code malveillant) dans une page web.

[4] Logiciel malveillant.

[5] Un *do-it-yourself* kit est une boite à outils informatique généralement développée par des programmeurs expérimentés, renfermant les failles de sécurité les plus connues et les derniers exploits informatiques, qui permet de générer automatiquement un malware dédié.

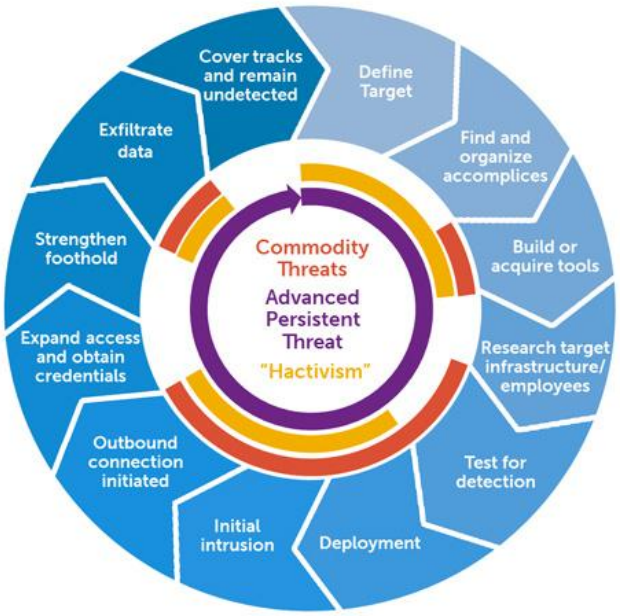


Figure 2 : cycle de vie d'une APT (Crédit : Dell SecureWorks)

2.2.1. Reconnaissance

La première étape d'une APT est certainement la plus importante et la plus cruciale de l'attaque. Elle consiste en une mission de reconnaissance de la cible.

En premier lieu, le groupuscule détermine les bases de l'attaque. Il définit donc tout d'abord la cible et les objectifs de l'APT. Puis, il recrute et organise les attaquants (p.ex. un certain nombre de hackers) et autres potentiels complices (p.ex. un *insider*[6] ou un sous-traitant malicieux) qui feront partie de l'attaque. Ensuite, le groupuscule étudie la cible. Il développe et/ou acquiert les outils nécessaires pour la réussite de l'attaque : malwares spécifiques pour s'implanter dans la cible, pour extraire les données sensibles qui seront récoltées au cours de l'APT, etc.

En second lieu, le groupuscule met en place la deuxième phase de reconnaissance. Un des buts recherchés est de récupérer les *credentials*[7] valides d'un ou plusieurs employés-cibles pour préparer l'étape suivante de l'APT (c.-à-d. l'infiltration dans le système cible). Pour y arriver, plusieurs options sont possibles.

- Accès distant

Le groupuscule peut exploiter différentes techniques qui ne se basent que sur un support informatique.

---

[6] Un *insider* est un membre d'un groupe spécifique, un initié, ou une personne déjà en place dans une organisation, qui a potentiellement accès à des informations privilégiées.

[7] Informations de connexion.

Par exemple, le *phishing* est une des techniques les plus connues pour récolter des informations sensibles en se faisant passer pour une entité de confiance (p.ex. banque, administration). Le phishing peut se perpétrer via envoi d'emails, site web falsifié, ou encore SMS.

Le *drive-by download* est aussi une technique très utilisée. Il repose sur le téléchargement accidentel (p.ex. pièce jointe d'un email, pop-up frauduleux) que peut effectuer un internaute et qui contient un malware *zero-day*[8], *spyware*[9], cheval de Troie[10], ou tout autre logiciel malveillant.

Le *clickjacking*[11], les réseaux sociaux et forums communautaires piégés font également partie de ces techniques ne nécessitant qu'un accès distant.

- Accès physique

Le groupuscule peut tout aussi bien se servir de supports amovibles infectés (p.ex. clés USB, CD/DVD, cartes mémoires), ou du partage de réseau Intranet pour insérer un malware. Par exemple, le groupuscule pourrait contaminer une imprimante via une carte mémoire ; cette imprimante infectée pourrait alors récolter les credentials des PC communiquant avec elle[12].

Concernant les attaques avec accès physique, il est aussi facile d'imaginer que le groupuscule mette en place un « simple » cambriolage pour récupérer les informations intéressantes pour l'APT.

- Accès humain

Le groupuscule peut également mettre en place du *social engineering*[13] pour récolter un maximum d'informations à propos de certains employés-cibles qui peuvent se révéler très pratiques. Plus précisément, le social engineering se réfère aux techniques de manipulations psychologiques permettant d'extirper des informations à une personne sans que cette dernière ne s'en rende compte. En effet, la nature même du social engineering se base sur le fait établi que les employés sont souvent le maillon faible de la chaine de sécurité d'une entreprise. Cette méthode vise donc à exploiter les faiblesses de la nature et du comportement humain. Il est difficile d'énumérer de façon exhaustive toutes les astuces

[8] Un malware est dit « de type *zero-day* » quand il exploite une vulnérabilité d'une application informatique qui n'a pas encore été détectée par la communauté de la sécurité informatique.

[9] Un *spyware* est un logiciel malveillant qui permet d'espionner l'environnement sur lequel il est installé.

[10] Un cheval de Troie est un logiciel légitime effectuant des opérations malveillantes à l'insu de son utilisateur.

[11] Le *clickjacking* est une technique dont le but est de forcer un internaute à cliquer sur un lien malveillant.

[12] Par exemple, une telle vulnérabilité avait été trouvée avec le protocole SMB (Server Message Block) où un attaquant pouvait rejouer des credentials. Cf. http://technet.microsoft.com/en-us/security/bulletin/ms08-068 pour plus de détails.

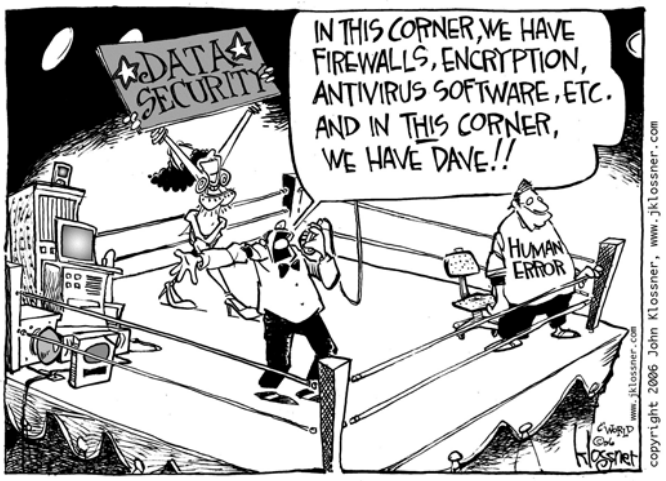
[13] Cf. le blog http://www.smalsresearch.be/archives/6806 pour plus de détails.

pour perpétrer du social engineering, car cette sous-branche des sciences comportementales est bien trop étendue. Il est néanmoins possible de présenter ce qui apparait comme les quatre familles de méthodes les plus répandues.

1. Récolte classique d'information – Cette méthode est la plus basique qu'un groupuscule peut perpétrer sans se faire repérer. Le groupuscule utilise tous les moyens légaux et publics qui lui sont offerts pour récolter des informations, comme une simple recherche sur Internet. De nos jours, cette méthode peut être vraiment efficace avec le développement des réseaux et autres médias sociaux. Par exemple, il n'est pas rare de voir un employé dévoiler naïvement un certain nombre d'informations sensibles sur son compte Facebook.
2. Attaque physique – Cette méthode se rapporte plus aux actions concrètes que peut tenter un groupuscule pour son attaque. Par exemple, le groupuscule essaie de rentrer dans un immeuble surveillé sans aucun badge. S'il réussit, il est alors possible pour lui de récolter matériellement des informations, telles que des papiers sensibles se trouvant dans les bureaux des victimes ou encore jetés à la poubelle.
3. Attaque informatique – Cette méthode fait référence aux actions informatiques qu'un groupuscule peut mettre en place pour faciliter son social engineering. Une illustration simple de cette méthode est la récupération de mot de passe. En effet, il semble que beaucoup de personnes utilisent le même mot de passe pour plusieurs comptes (p.ex. pour Gmail, eBay, Facebook ou Twitter). Le groupuscule peut donc essayer de retrouver ce mot de passe (p.ex. avec une attaque du dictionnaire) et ainsi accéder aux autres comptes de cet utilisateur. Un autre exemple un peu plus poussé que l'on peut citer est l'utilisation de pop-up qui semble faire partie du réseau et qui demande à l'utilisateur de ré-entrer son login et mot de passe.
4. Phishing – Comme expliqué précédemment, cette méthode est une des plus connues à l'heure actuelle. Elle peut intervenir durant le social engineering pour forcer la victime à révéler une information sensible ou encore de la persuader d'ouvrir une pièce jointe malveillante. Le vishing est une variante où le groupuscule utilise le téléphone. Par exemple, il appelle un employé en se faisant passer pour une personne du HelpDesk pour un problème urgent et demander un accès immédiat au réseau.

Une fois la récolte d'informations terminée, le groupuscule peut lancer une attaque de *spear-phishing* sur les employés-cibles les plus vulnérables. Le spear-phishing est une variante du phishing classique qui vise une personne en particulier : le message envoyé à la victime est donc très personnalisé. Le but ultime de cette attaque est d'obtenir les credentials valides d'un ou plusieurs employés-cibles pour l'étape d'infiltration. Les victimes de cette attaque ont généralement un poste avec un haut niveau

d'accréditation dans le système informatique cible (p.ex. manager, administrateur système).



Une autre méthode tout aussi efficace au niveau humain est de simplement faire de l'espionnage classique (p.ex. mise sur écoute).

2.2.2. Infiltration

La deuxième étape d'une APT consiste en l'infiltration dans le système informatique cible.

Tout d'abord, le groupuscule effectue un repérage du réseau afin de comprendre et se représenter sa topologie, son architecture, sa complexité et ses potentiels points d'entrée. Ceci peut se faire via la vérification des adresses IP actives, le scan des ports ouverts, etc. Par exemple, les ports 80 (pour le http) et 443 (pour le https) sont des ports génériques généralement ouverts ne déclenchant pas forcément d'alerte de sécurité au sein du système. Le but de la manœuvre est d'initialiser des points de connexions entrantes et sortantes entre le système cible et le groupuscule.

Ensuite, le groupuscule effectue une intrusion initiale avec les credentials valides d'un ou plusieurs employés-cibles récupérés durant la phase de reconnaissance. Les machines utilisées à cette étape sont ensuite dites « compromises ».

2.2.3. Implantation

La troisième étape d'une APT consiste en l'implantation du groupuscule dans le système et en la consolidation de cet ancrage.

Une fois l'infiltration réussie, le groupuscule établit l'inventaire du parc logiciel du système. Il explore les divers services et applications qui tournent sur le système cible, ainsi que leurs potentielles failles de sécurité.

Le groupuscule cherche ensuite à étendre ses privilèges au système en obtenant de nouveaux credentials, de préférence ceux permettant un accès *root* à une des machines compromises.

À partir de là, cet accès root est utilisé pour examiner le réseau plus en profondeur et récolter de nouvelles informations utiles pour l'APT. Par exemple, le groupuscule peut installer un *sniffer* sur les machines compromises dont il a l'accès root (comme illustré en Figure 3 et Figure 4). Un sniffer est un logiciel capable d'écouter tout le trafic réseau des machines situées sur le même réseau local. Cette manœuvre a pour but d'étendre et renforcer son implantation de façon latérale dans le système. Le groupuscule peut ainsi obtenir l'accès root à de nouvelles machines du système qui seront à leur tour dites « compromises ». La manœuvre doit être exécutée avec une approche low-and-slow, d'une machine compromise à une autre sans générer de trafic réseau supplémentaire, pour ne pas faire sonner d'alarme de sécurité. À terme, le groupuscule peut acquérir autant de pouvoirs et droits que l'administrateur système.

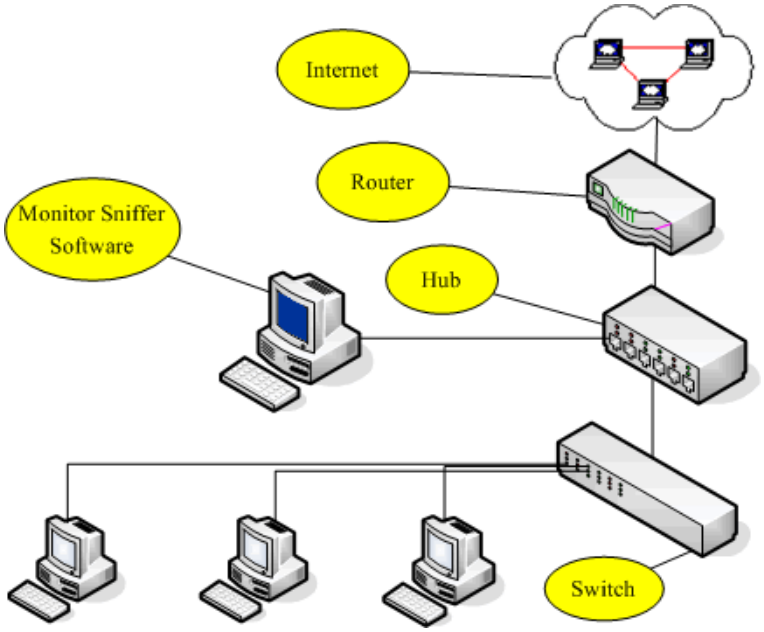


Figure 3: exemple d'architecture système avec un sniffer (Crédit : IM Monitor)

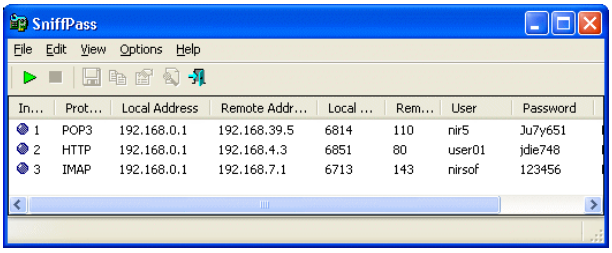


Figure 4 : récupération de credentials avec SniffPass (Crédit: Nir Sofer)

Durant cette phase, l'accès root aux machines compromises permet au groupuscule d'installer un certain nombre de malwares utiles pour l'APT, tels que des *backdoors*[14], chevaux de Troie, proxies[15] additionnels. De plus, ces malwares peuvent être polymorphes[16] pour prolonger l'APT et ne pas éveiller les soupçons du système cible.

Notons aussi que le groupuscule peut installer des *rootkits* sur les machines compromises avec accès root. Ces malwares permettent de remplacer les outils d'administration d'un système par des versions modifiées. Ils peuvent donc masquer la présence du groupuscule sur le système cible et tromper l'administrateur système en lui masquant la réalité.

2.2.4. Extraction

La quatrième étape d'une APT consiste en l'extraction des informations qui intéressent le groupuscule dans le système cible.

En premier lieu, le groupuscule installe sur les machines compromises des malwares personnalisés (de type chevaux de Troie ou spywares) qui vont collecter de façon automatique les données visées par l'APT.

En second lieu, le groupuscule met en place une partie très délicate et sensible de l'APT : l'extraction des données collectées. Cette opération peut s'avérer très difficile car ces données doivent être acheminées à l'extérieur de l'infrastructure cible sans se faire détecter par le système de sécurité. Une telle extraction peut se faire en deux étapes. Tout d'abord, le groupuscule installe des outils cryptographiques ou stéganographiques[17] (cf. Figure 5) sur les machines compromises. Les données collectées sont ensuite chiffrées ou cachées dans des messages anodins par ces outils, minimisant ainsi la suspicion du système de sécurité.

---

[14] Une *backdoor* est une fonctionnalité d'un logiciel inconnue de l'utilisateur permettant un accès illégitime à l'environnement sur lequel le logiciel est installé.

[15] De façon générale, un proxy est un composant logiciel agissant en tant qu'intermédiaire entre deux entités pour aider ou espionner leurs communications. Dans le cadre d'une APT, un proxy peut aider le groupuscule à déjouer la politique de sécurité de la cible, par exemple en contournant les filtrages des sites web imposés par la cible.

[16] Un malware est dit « polymorphe » s'il prend une forme différente (c.-à-d. une partie de son code se modifie de lui-même) à chaque contamination tout en effectuant le même type de dégâts. La majorité des malwares polymorphes sont chiffrés et ne se déchiffrent que lorsqu'ils doivent contaminer un nouvel hôte, ce qui les rend très difficiles à détecter.

[17] La cryptographie, ou « l'art du secret », est une technique permettant la protection d'un message, le rendant inintelligible. En revanche, la stéganographie, ou « l'art de la dissimulation », est une technique permettant de cacher un message secret dans un autre message sans que ce dernier ne soit illisible.

Figure 5 : exemple de stéganographie (Crédit : Atawneh, Almomani et Sumari). L'image (a) est le message à cacher. L'image (b) est l'image dans laquelle le message sera caché. L'image (c) est le résultat de cette stéganographie avec la méthode LSB[18]. Constatation : il n'y a aucune différence remarquable à l'œil nu entre l'image (b) et l'image (c).

Enfin, l'extraction des données peut se faire via différentes méthodes (p.ex. envoi d'email contenant les données à extraire). Une technique très prisée pour l'extraction de données est l'utilisation de « canaux cachés ». Dans le cadre d'une APT, ces canaux correspondent aux canaux de communication établis par le groupuscule entre les machines compromises et le serveur du groupuscule (ces machines n'étant clairement pas autorisées à communiquer ensemble par la politique de sécurité du système informatique cible) pour l'extraction des données collectées. Il existe deux principaux types de canaux cachés :

- les « canaux de stockage » où la machine émettrice modifie une donnée spécifique, ainsi la machine réceptrice détecte et interprète directement la donnée modifiée ;
- les « canaux temporels » où la machine émettrice fait varier les temps de réponse du système informatique, ainsi la machine réceptrice interprète directement ces variations comme des données.

2.2.5. Maintien

Enfin, la dernière étape d'une APT consiste en maintenir l'implantation dans le système cible le plus longtemps possible.

La mise en place d'une APT est une opération de longue haleine, et le groupuscule a dû fournir un travail relativement poussé et faire preuve de patience pour atteindre son objectif. Une fois sa mission accomplie, le groupuscule peut néanmoins souhaiter garder l'accès à la cible, pour de futurs agissements.

Pour cela, le groupuscule couvre et efface les traces de son passage pour ne pas être détecté par le système de sécurité de l'infrastructure cible. Il supprime les fichiers qu'il a créés et nettoie les fichiers de logs des

[18] La méthode LSB (*Least Significant Bit*) est une des techniques de stéganographie les plus simples à utiliser sur les images : les bits de poids faible de chaque octet d'une image sont remplacés par les bits de l'image à cacher.

machines dans lesquelles il s'est introduit : en résumé, il supprime les lignes d'activité concernant ses actions.

3. Quelques célèbres APT

Cette section illustre le fonctionnement d'une APT en présentant quelques exemples d'attaques déployées dans le passé.

3.1. Un exemple concret : Stuxnet, 2009

Stuxnet est un *worm*[19] lancé en 2009 d'une supposée coopération entre la NSA[20] et l'ISNU[21]. Il fait partie d'un programme de cyber-attaques de grande envergure connu sous le nom de « Operation Olympic Games ».

Le but de Stuxnet était de contaminer les installations nucléaires iraniennes, dont les équipements sont gérés par le système SCADA[22] de Siemens, via plusieurs failles informatiques spécifiques au système d'exploitation Windows. Il a été découvert le 17 juin 2010 par VirusBlokAda, société biélorusse développant des produits antivirus. À l'heure actuelle, il est reconnu comme le premier malware à s'attaquer explicitement à une cible industrielle prédéfinie.

> *« This is the first direct example of weaponized software, highly customized and designed to find a particular target. »*
> (Michael Assante[23])

3.1.1. Cycle de vie de Stuxnet

Cette section présente le mode opératoire du ver pour contaminer sa cible, illustré en Figure 6.

- Propagation

Stuxnet a été le premier ver informatique à exploiter trois vulnérabilités zero-day (maintenant identifiées) afin de se propager.

La première est la vulnérabilité dans la gestion des fichiers de raccourcis de type .lnk/.pif de Microsoft Windows[24]. Elle permettait au ver de déposer

[19] Ver informatique.

[20] *National Security Agency*, organisme gouvernemental américain responsable du renseignement d'origine électromagnétique.

[21] *Israeli SIGINT National Unit*, unité de renseignement de l'armée israélienne, équivalent de la NSA américaine.

[22] *Supervisory Control and Data Acquisition*.

[23] Ancien chef de la recherche sur la cyber-sécurité des systèmes de contrôle industriel au *U.S. Department of Energy's Idaho National Laboratory*.

une copie de lui-même ainsi qu'un lien vers cette copie sur n'importe quel disque amovible connecté à l'ordinateur infecté, contaminant ainsi le disque amovible.

Les deuxième et troisième vulnérabilités sont celle du service d'impression Spooler de Windows[25] et celle du service Serveur de Windows[26]. Chacune permettait l'exécution de code à distance sur un ordinateur infecté, ce qui contaminait alors les ordinateurs connectés au même réseau privé.

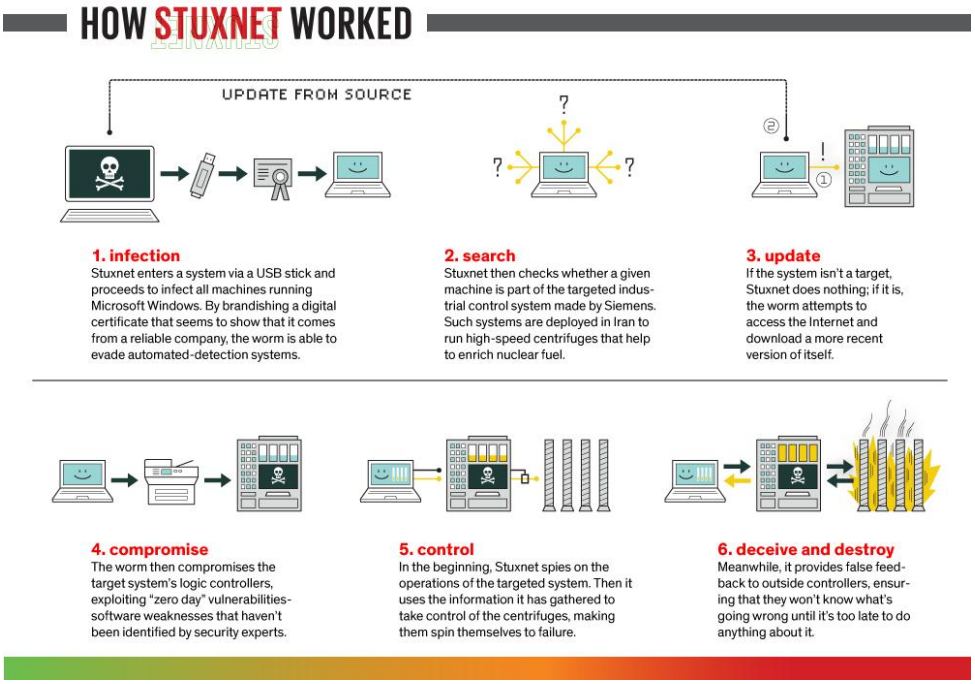


Figure 6 : illustration du mode opératoire de Stuxnet (Crédit : L-Dopa)

- Installation

Quand il avait atteint un nouvel ordinateur, Stuxnet se servait de vulnérabilités dans les pilotes en mode noyau de Windows[27] qui permettaient une élévation des privilèges. Grâce à ces vulnérabilités, Stuxnet était capable d'installer sur ce nouvel ordinateur deux rootkits (un en mode utilisateur et un en mode noyau) lui permettant de tromper les antivirus.

La particularité de cette étape était que les drivers utilisés par Stuxnet pour installer ces deux rootkits étaient signés avec les clés privées de

[24] Cette vulnérabilité est maintenant répertoriée sous le BugTraq IDentifier (BID) 41732.

[25] Cette vulnérabilité est maintenant répertoriée sous le BID 43073.

[26] Cette vulnérabilité est maintenant répertoriée sous le BID 31874. Elle avait déjà été utilisée avec succès par le ver Conficker.

[27] Ces vulnérabilités sont maintenant répertoriées dans le Bulletin de sécurité Microsoft MS10-073.

deux certificats légitimement reconnus par Windows[28] (cf. Figure 7). Ces signatures légitimes facilitaient donc l'installation des rootkits sans l'approbation de l'utilisateur, ni sa notification.

Figure 7 : un des certificats légitimes utilisé par Stuxnet (Crédit : Symantec)

- Détection et compromission de la cible

Pour chaque ordinateur infecté, Stuxnet analysait si celui-ci faisait partie d'un système SCADA de Siemens avec une configuration bien définie, c'est-à-dire qui correspondait à celle des ordinateurs utilisés dans les installations nucléaires iraniennes.

La description complète de cette configuration dépasse le cadre de ce rapport. Notons néanmoins que les ordinateurs des installations nucléaires iraniennes exécutaient les applications de supervision WinCC/PCS7 du système SCADA de Siemens. Ces applications géraient en particulier la vitesse de rotation des centrifugeuses et des turbines à vapeur du site nucléaire. Stuxnet avait donc pour but de prendre le contrôle de ces équipements pour les endommager sans que le système puisse s'en rendre compte. Cette cyber-attaque a ainsi permis de ralentir le programme nucléaire iranien sans faire intervenir de forces armées.

3.1.2. Stuxnet, une fausse APT ?

Au vu de la médiatisation de Stuxnet, un certain nombre de spécialistes en sécurité informatique ont contesté le fait que Stuxnet soit présenté au grand public comme une APT.

[28] VeriSign a révoqué ces certificats quelques jours après l'annonce relative à leur utilisation dans Stuxnet.

- Les opposants

Les principaux arguments de cette contestation sont au nombre de quatre. Tout d'abord, Stuxnet n'utilisait aucun social engineering dans la phase de reconnaissance de l'attaque. Or ce point semble être, pour certains spécialistes, une caractéristique bien spécifique d'une APT. Ensuite, l'attaque se basait sur une propagation en masse du ver pour toucher n'importe quel ordinateur du réseau cible. Or l'infiltration d'une APT va plutôt viser un ordinateur spécifique, en utilisant les données récoltées durant la phase de reconnaissance. Aussi, Stuxnet avait pour but ultime l'endommagement du système cible : une APT n'est principalement perpétrée que pour récolter des informations sur la cible. Enfin, les spécialistes ont mis en avant le fait qu'une APT a plutôt la précision d'un scalpel alors que Stuxnet s'apparentait davantage à un marteau, étant donné le nombre conséquent de vulnérabilités zero-day exploitées.

- Les partisans

Malgré ces arguments, Stuxnet avait également des caractéristiques très proches d'une APT. Tout d'abord, le groupuscule ayant créé Stuxnet était très organisé et puissant (c.-à-d. coalition entre la NSA et l'ISNU). Le ver mettait avant tout en place une attaque très ciblée visant les installations nucléaires iraniennes. Pour se faire, plusieurs experts ont affirmé que le groupuscule avait indubitablement reçu l'aide et les connaissances poussées d'insider(s) pour préparer soigneusement l'attaque. L'implantation du ver pour une longue durée avait également été étudiée par le groupuscule : une fois installé sur un ordinateur cible et ayant accès à l'Internet, Stuxnet avait une procédure d'auto-mise à jour programmée. Enfin, le groupuscule avait pris soin de programmer Stuxnet pour être le moins détectable possible.

3.2. Autres exemples d'APT

Cette section présente succinctement une liste non-exhaustive des APT les plus connues.

3.2.1. Moonlight Maze, 1998

À la fin des années 2000, une série étendue de cyber-attaques contre des sites gouvernementaux a été découverte par le gouvernement américain. Ces attaques, baptisées Moonlight Maze, se sont perpétrées incognito pendant près de deux ans. Elles ont servi à pénétrer les systèmes du Pentagone, de la NASA, du Département de l'Énergie des États-Unis, ainsi que les universités et les laboratoires de recherche impliqués dans la recherche militaire. Moonlight Maze a volé des dizaines de milliers de fichiers, y compris des cartes d'installations militaires, des configurations de troupes militaires déployées et des designs de matériel militaire, causant des dommages s'élevant à plusieurs millions de dollars.

Le Département de la Défense des États-Unis a identifié un ordinateur de l'ex-Union soviétique comme origine de Moonlight Maze, bien que le gouvernement russe ait nié toute implication. Certains experts considèrent

Moonlight Maze comme étant le premier exemple majeur d'APT, bien que le terme n'ait pas encore été inventé à l'époque.

3.2.2. Titan Rain, 2003

Titan Rain est le nom de code donné par le gouvernement américain à une série d'attaques de cyber-espionnage lancées en 2003 contre les entrepreneurs de la défense des États-Unis (p.ex. Lockheed Martin, Sandia National Laboratories, Redstone Arsenal ou encore la NASA). Titan Rain a été étiqueté d'origine chinoise, bien que le gouvernement chinois ait nié toute implication.

La principale nouveauté apportée par Titan Rain était l'utilisation de multiples vecteurs d'attaques très élevées combinant :

- un social engineering poussé et bien documenté sur des individus cibles spécifiques avec
- des attaques furtives utilisant chevaux de Troie, backdoors et autres malwares étudiés pour contourner les mesures de sécurité implémentées à l'époque.

3.2.3. Sykipot, 2006

Sykipot fait référence à une série d'attaques de type APT perpétrées depuis 2006 (mais détectés bien plus tard). Sykipot a collecté et volé de nombreux secrets et propriétés intellectuelles, y compris des données financières, de fabrication ou de planification stratégique. Sykipot utilisait principalement du spear-phishing avec pièce jointe malveillante (comme illustré en Figure 8) ou lien vers un site infecté, ainsi que les exploits zero-day (p.ex. la vulnérabilité BID 38615 d'Internet Explorer).

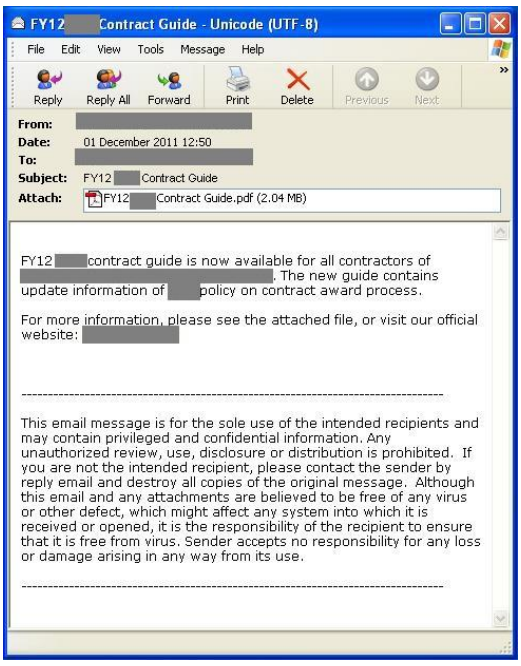


Figure 8 : exemple d'email spear-phishing envoyé par Sykipot (Crédit : Helloblog)

Sykipot a ciblé de nombreuses entreprises américaines et britanniques, en particulier celles opérant dans la défense informatique, les télécommunications, l'énergie, les produits chimiques et les secteurs gouvernementaux. Une analyse de Sykipot menée en 2011 par AlienVault Labs a indiqué que la grande majorité des serveurs utilisés par l'APT étaient basés en Chine. Les objectifs, les moyens déployés et les informations recueillies ont fortement suggéré qu'une agence de renseignement serait le bénéficiaire de cette APT.

3.2.4. GhostNet, 2009

GhostNet est le nom d'une opération de cyber-espionnage à grande échelle découverte en Mars 2009. Comme Sykipot, GhostNet utilisait du spear-phishing avec pièce jointe malveillante qui uploadait un cheval de Troie sur l'ordinateur de la cible, permettant ainsi l'exécution de commandes à partir d'un centre de contrôle distant. Ce cheval de Troie favorisait par la suite le téléchargement de malwares additionnels permettant de prendre le plein contrôle de l'ordinateur compromis. GhostNet incluait aussi la possibilité d'utiliser les périphériques audio et vidéo pour surveiller les locaux où se trouvait l'ordinateur compromis.

GhostNet aurait infiltré les ordinateurs de cibles politiques, économiques et médiatiques dans plus de cent pays, tels que les ambassades d'Inde, de Corée du Sud, d'Indonésie, de Roumanie, de Chypre, de Malte, de Thaïlande, de Taïwan, du Portugal, d'Allemagne, du Pakistan et du bureau du Premier ministre du Laos. Les ministères des Affaires étrangères d'Iran, du Bangladesh, de Lettonie, d'Indonésie, des Philippines, du Brunei, de la Barbade et du Bhoutan ont également été ciblés. Des ordinateurs dans les centres d'exil tibétains du dalaï-lama en Inde, à Londres et à New York ont également été compromis.

Le centre de contrôle de GhostNet a été signalé comme étant basé en grande partie en Chine, bien que le gouvernement chinois ait – encore – nié toute implication. Certains experts ont suggéré que GhostNet aurait pu être une opération perpétrée par des citoyens en Chine (pour des questions de profit ou de simple patriotisme). Une autre hypothèse est qu'il ait pu avoir été créé par les services de renseignement d'autres pays tels que la Russie ou les États-Unis.

3.2.5. Opération Aurora, 2009

L'opération Aurora fait référence à une série de cyber-attaques lancées en 2009 présumées d'origine chinoise. Aurora était une APT très bien coordonnée qui se déroulait en six grandes étapes comme illustré en Figure 9. Tout d'abord, Aurora utilisait du spear-phishing avec un lien vers un site malveillant (se trouvant le plus souvent sur un serveur à Taiwan, au Texas ou dans l'Illinois). Une fois sur ce site, le navigateur de l'utilisateur cible téléchargeait et exécutait un cheval de Troie nommé Hydraq[29] incluant un exploit zero-day sur Internet Explorer. Cet exploit se

[29] Cf. http://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit pour une explication claire du fonctionnement d'Hydraq.

basait sur le téléchargement et l'exécution d'un binaire déguisé en image depuis le serveur malveillant. Ce binaire mettait ensuite en place une backdoor reliée au serveur malveillant permettant de contrôler à distance l'ordinateur cible. Ainsi Aurora permettait au groupuscule d'avoir l'accès complet au système cible. Le but final d'Aurora était de récolter un maximum d'informations soumises à la propriété intellectuelle sur les systèmes cibles.

Figure 9 : illustration de l'opération Aurora (Crédit : McAfee)

Les victimes de l'opération Aurora ont été assez réticentes à se faire connaître ou à confronter les auteurs présumés, généralement par peur de contrarier les agresseurs ou de bouleverser leurs clients et actionnaires. L'exception à cette loi du silence a été Google qui a dévoilé l'APT en janvier 2010 dans un blog officiel[30], affirmant que vingt autres entreprises avaient également été attaquées. Maintenant, il est largement admis que le nombre est beaucoup plus élevé, incluant Adobe Systems, Juniper Networks et Rackspace. Beaucoup d'autres entreprises attaquées ont préféré rester anonyme, bien que plusieurs rapports ont indiqué qu'ils comprenaient de grandes banques, des entrepreneurs de la défense, des éditeurs de sécurité informatique, des compagnies pétrolières et gazières ainsi qu'un certain nombre d'autres sociétés technologiques.

3.2.6. Et encore plein d'autres…

Force est de constater que des dizaines d'autres APT ont été mises en place depuis les années 2000. On peut par exemple citer celle contre RSA SecureID en 2011 illustrée en Figure 10, ou encore Duqu, Flame et Red October découverts respectivement en 2011, 2012 et 2013.

[30] http://googleblog.blogspot.be/2010/01/new-approach-to-china.html

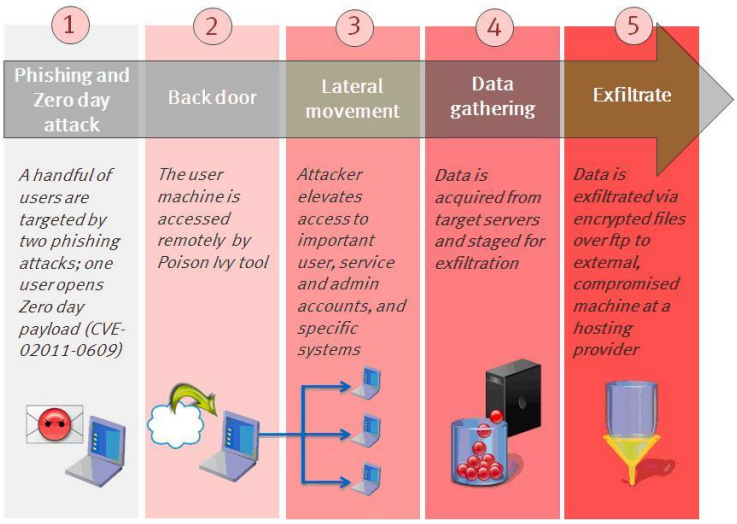


Figure 10 : schéma simplifié de l'APT contre RSA SecureID (Crédit : RSA)

En résumé, le nombre d'APT déployées ou en création ne cesse d'augmenter. Ce type d'attaque est réellement difficile à identifier : d'après le rapport d'investigation de 2012 sur les intrusions de systèmes informatiques établi par Verizon[31], 92% des organisations ont été mises au courant d'une brèche de sécurité dans leur système par une entité externe.

4. Comment se protéger d'une APT

La première leçon à retenir est qu'aucun produit de sécurité réseau vendu sur le marché ne peut garantir à 100% une protection contre les APT. Étant donné l'arsenal de techniques et d'outils d'attaques mis en place, il existe clairement toujours un moyen d'infiltrer n'importe quel système cible, soit directement via des failles informatiques, soit avec l'aide (involontaire ?) des utilisateurs. Rien n'est complètement impénétrable pour un groupuscule motivé et plein de ressources. La bataille contre les APT vient juste de commencer et elle s'annonce très longue.

Une fois ce fait accepté et intégré, les organisations/entreprises peuvent néanmoins mettre en place un certain nombre de protections pour limiter et réduire au maximum la réussite de ce type d'attaques, à défaut de pouvoir les bloquer.

4.1. Protéger le système informatique

La ligne de défense générique contre les APT concerne bien entendu le système informatique en lui-même. Tout d'abord, de simples dispositions peuvent être prises : sécuriser l'accès à distance avec un mécanisme d'authentification forte et un chiffrement des communications, partitionner

[31] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

les données clés de l'entreprise et les protéger grâce à du cloisonnement stratégique et efficace.

Ensuite, la deuxième étape – qui semble évidente – est de maintenir à jour toute l'infrastructure, en particulier les patchs de sécurité des systèmes et applications (p.ex. pour Java ou Internet Explorer). L'opération Aurora aurait pu être stoppée ou ralentie si les utilisateurs n'avaient pas utilisé Internet Explorer 6. Il est également important de maintenir à jour l'infrastructure à clés publiques interne et les certificats des CA[32] externes utilisés. Cela aurait pu, par exemple, limiter la propagation d'APT telles que Stuxnet.

Les organisations et entreprises peuvent aussi déployer un certain nombre de protections périmétriques standards telles que les antivirus, pare-feux permettant de contrôler le trafic entrant et sortant du réseau, IDS/IPS[33] surveillant le réseau et les hôtes du système, à la recherche d'activités anormales, ou bacs-à-sable testant des logiciels externes non vérifiés. Les organisations peuvent également installer des logiciels DLP[34], outils très utile pour découvrir, surveiller, protéger et gérer les données de l'entreprise, peu importe leur localisation dans le système. Des logiciels de *content-filtering*, comme illustré en Figure 11, sont aussi disponibles pour restreindre et contrôler ce qu'un utilisateur est autorisé à consulter, en particulier sur le réseau Internet. Par exemple, les pages d'Hotmail pourraient être interdites d'accès depuis le réseau interne d'une entreprise, ce qui éviterait une potentielle attaque par phishing via ce type de boites aux lettres personnelles.

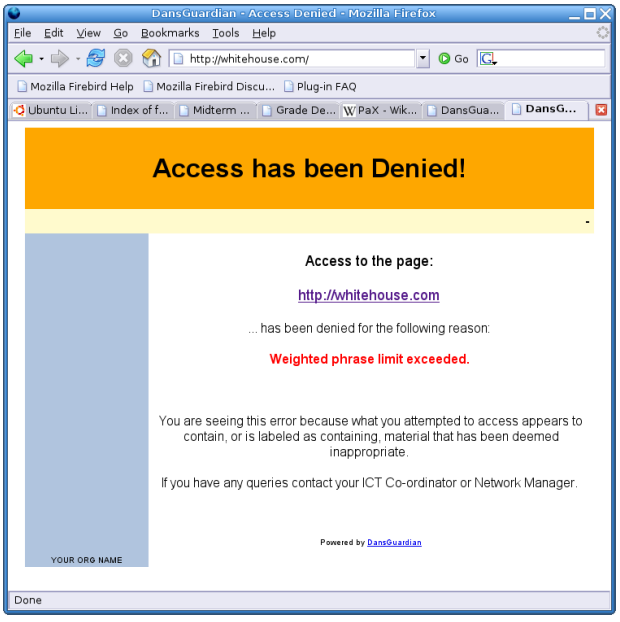


Figure 11 : exemple de page Internet bloquée avec le logiciel de content-filtering DansGuardian (Crédit : Bluefoxicy)

[32] *Certificate Authority*.

[33] *Intrusion Detection System / Intrusion Prevention System*.

[34] *Data Loss Prevention*.

Enfin, les organisations peuvent tout aussi bien investir dans des « plateformes de protection » spécialement conçues pour les APT (p.ex. FireEye[35], TrendMicro[36], Symantec[37] ou PaloAlto Networks[38])[39] et combinant certaines protections périmétriques de prochaine génération. Il faut cependant garder en tête que ces plateformes ne servent généralement qu'à préparer des réponses plus ou moins immédiates aux incidents et attaques, mais ne forment pas en soi un bouclier infranchissable contre les APT.

4.2. Former les équipes HelpDesk et sécurité

Une autre ligne de défense contre les APT est le personnel technique et sécurité d'une organisation. Leur formation est primordiale pour limiter les dégâts que peuvent engendrer les APT.

Tout d'abord, ces équipes doivent suivre de très près toutes les dernières menaces publiées et toutes les nouveautés concernant la sécurité (p.ex. via la participation à des cours, conférences ou séances d'information). Ceci leur permettra de connaitre et maitriser toutes les dernières techniques pour se prémunir des APT. Elles doivent également se plonger dans la rédaction d'analyses détaillées des techniques d'attaques déployées (p.ex. comprendre comment les zero-day exploits sont mis en œuvre) et des types de vulnérabilités généralement exploitées. Garder à jour une documentation précise des menaces est clairement un atout contre les APT.

De plus, par son accès très étendu aux données de l'entreprise, le HelpDesk est généralement une cible favorite du social engineering. Une attention particulière doit donc être apportée à sa formation sur le sujet. La règle fondamentale du HelpDesk doit être de ne jamais divulguer d'information sans une autorisation préalable de la hiérarchie.

Pour les aspects plus pratiques, le HelpDesk doit être sensibilisé à reconnaitre, remonter et signaler toute anomalie dans les logs collectés du système informatique. Par exemple, il doit surveiller si des connexions se produisent depuis des zones ou des heures inhabituelles (p.ex. depuis un autre pays ou au beau milieu de la nuit). Le cas d'une anomalie récurrente doit aussi sonner l'alarme du HelpDesk, par exemple si les comptes de plusieurs utilisateurs se bloquent simultanément.

Les équipes HelpDesk et sécurité doivent sans cesse être proactives quant à l'amélioration des techniques d'investigation numérique (*forensics*) et des capacités de réponse aux incidents et anomalies détectés. Pour ce dernier, ces équipes peuvent alors mettre en place des

[35] http://www.fireeye.com/products-and-solutions/threat-prevention-platform.html

[36] http://www.trendmicro.com/us/business/cyber-security/index.html

[37] http://www.symantec.com/endpoint-protection

[38] https://www.paloaltonetworks.com/products/features/apt-prevention.html

[39] Détailler ces produits est hors du cadre de ce rapport.

plateformes SIEM[40] pour consolider et corréler les données de sécurité de diverses sources au sein de l'infrastructure informatique. Ces plateformes sont ainsi capables d'identifier « l'aiguille dans une botte de foin » qui indiquerait une attaque de type APT en action dans le système.

Le résultat d'une formation poussée des équipes HelpDesk et sécurité est la mise en place de politiques de sécurité robustes et adéquates, en particulier sur le comportement des utilisateurs. Ainsi, une politique de sécurité peut interdire aux employés de communiquer (p.ex. par téléphone) un certain type d'information, et ce, peu importe la personne qui en fait la demande. Elle doit aussi fixer certains points fondamentaux du système informatique, tels que le contrôle d'accès aux informations, la création des comptes utilisateurs, ou encore les changements réguliers (mais pas trop contraignants du point de vue utilisateur) de mot de passe.

Enfin, de façon plus générale, les équipes HelpDesk et sécurité devraient être poussées à participer à une synergie avec d'autres organisations et entreprises. Le but d'une telle démarche serait de partager et accroitre leurs connaissances et expériences sur les problèmes de sécurité dans les entreprises, et faire émerger de nouvelles initiatives en matière de protection des systèmes d'information.

4.3. Former les employés lambda

Enfin, la toute première ligne de défense contre les APT est clairement le personnel non-technique d'une organisation ou entreprise. Là aussi, leur formation est vitale pour limiter les dégâts que peuvent engendrer les APT, en particulier car ces utilisateurs ne sont pas forcément des spécialistes en informatique ni des experts en sécurité.

Ainsi, la première mesure à prendre est de sensibiliser les utilisateurs à remonter toute anomalie, aussi petite soit-elle, comme un compte bloqué ou encore un problème à l'ouverture d'un fichier reçu par email. La campagne du DHS[41] « *If You See Something, Say Something*™ », dont le but est d'augmenter la connaissance et la compréhension du grand public des actes de terrorisme et de violence, peut également s'appliquer au sein des organisations et entreprises dans le cadre des APT. Les employés doivent aussi être formés à accroitre leur vigilance, que ce soit pour garder secret leurs mots de passe, sécuriser leurs documents, ou connaitre les techniques de social engineering et de spear-phishing.

Enfin, il est important de responsabiliser le personnel non-technique face aux potentielles menaces : ils sont tout aussi coupables que les équipes HelpDesk et sécurité en cas d'infiltration d'une APT. C'est pourquoi il faut intégrer tous les employés dans la solution déployée pour faire face aux APT. Les employés doivent être formés aux bonnes pratiques de sécurité, comme celles décrites dans la politique. Ils doivent garder à l'esprit que la

[40] *Security Information and Event Management*, cf. la research note http://www.smalsresearch.be/publications/document?docid=30 pour plus de détails sur le sujet.

[41] *Department of Homeland Security*, département de l'administration fédérale américaine responsable de la sécurité intérieure.

sécurité de l'entreprise est une priorité, et comprendre que leur rôle à jouer est essentiel pour transformer des politiques de sécurité théoriques en une culture de la sécurité réelle et efficace.

5. Conclusions

Les APT sont bien une menace réelle pour toute organisation ou entreprise dont les activités pourraient fortement intéresser des groupuscules d'attaquants tels que des organisations criminelles, des hacktivistes[42], ou des État-nations. Or, à l'heure actuelle, aucun « vaccin » informatique ne peut protéger un système contre ce type d'attaques. C'est pourquoi les organismes et entreprises doivent mettre en place toute une ligne de défense pour se prémunir au mieux des APT, tant des outils de sécurité informatique classiques (p.ex. pare-feux, IDS/IPS) que des plateformes SIEM. Ils doivent également rester *up-to-date* sur tous ces mécanismes de protection. Enfin, former tous les employés à détecter toute anomalie et potentielle menace de type social engineering reste le meilleur rempart contre les APT.

La section Recherche de Smals produit régulièrement des publications couvrant de nombreux domaines du marché IT actuel. Vous pouvez obtenir ces publications via le site web de la section Recherche :

http://www.smalsresearch.be

[42] Mot-valise formé à partir de « hack » et « activisme ».