ADVANCED PERSISTENT THREATS
ÉTAT DE L'ART

TANIA MARTIN

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
tte research note
elle 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
Advanced Persistent Threats
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

Récemment, la communauté
officialisé un tendance : les *Advanced Persistent Threats* (APT). Cette terminologie fait référence aux techniques

perpétrer une attaque de longue durée sur une cible bien définie. Selon [1] datant de 2013, 63% des entreprises interrogées

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

peut se baser sur plusieurs méthodes
telles que les interceptions et

développe de plus en plus. Ainsi, les cyber-attaques sont fortement utilisées APT, en particulier celles basées sur la surveillance des connexions I
e 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

:

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

Le 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-
« », 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,

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 .

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

APT », il est
tout ent la signification de ce sigle.

- « *Advanced* »

Le groupuscule met en tout un arsenal de techniques s très poussés pour atteindre son objectif. En regardant plus attentivement chaque , 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].
le groupuscule
composants dans le but unique d e compromettre au mieux
la cible de sûr.

- « *Persistent* »

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 furtive et lente (« *low-and-slow* ») est privilégiée à

- « *Threats* »

être une grande menace pour la cible ou les citoyens de façon générale (p.ex. les plans , les c e 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
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

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.

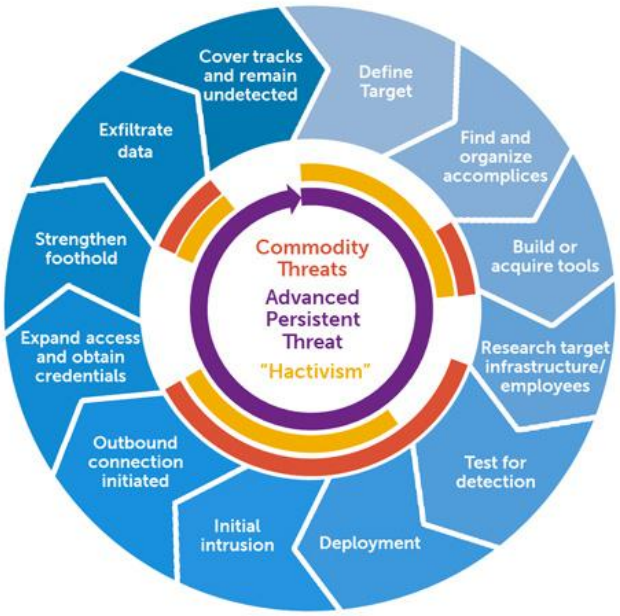


Figure 2 : cycle de vie d'une APT (Crédit : Dell SecureWorks)

2.2.1. Reconnaissance

est certainement la plus importante et la plus cruciale . Elle consiste en une mission de reconnaissance de la cible.

En premier lieu, le groupuscule détermine donc la cible et les objectifs . 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 Ensuite, le groupuscule étudie la cible. Il développe et/ou acquiert les outils nécessaires pour la réussite de l

c.

En second lieu, le groupuscule met en place la deuxième phase de reconnaissance. Un des buts recherchés est de récupérer les *credentials*[7] valides ou plusieurs employés-cibles pour (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* 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 mails, site web falsifié, ou encore SMS.

Le *drive-by download* est aussi une technique très utilisée. Il repose sur le téléchargement accidentel -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 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 simple » cambriolage

- Accès humain

Le groupuscule peut également mettre en place du *social engineering*[13] pour récolter un maximum rmations à propos de certains employés-cibles qui peuvent se révéler très pratiques. Plus précisément, le social engineering se réfère aux techniques de manipulations psychologiques

En effet, la nature même du social engineering se base sur le fait établi que les employés sont souvent le maillon faible de la . Cette méthode vise donc à exploiter les faiblesses de la nature et du comportement humain.

---

[8] Un malware est dit « de type *zero-day*

sécurité informatique.

[9] Un *spyware*
sur lequel il est installé.

[10] Un cheval de Troie est un logiciel légitime effectuant des opérations

[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. _____ Cette méthode est la plus 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

   dévoiler naïvement
   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

   de récolter matériellement des informations, telles que des papiers sensibles se trouvant dans les bureaux des victimes ou encore jetés à la poubelle.

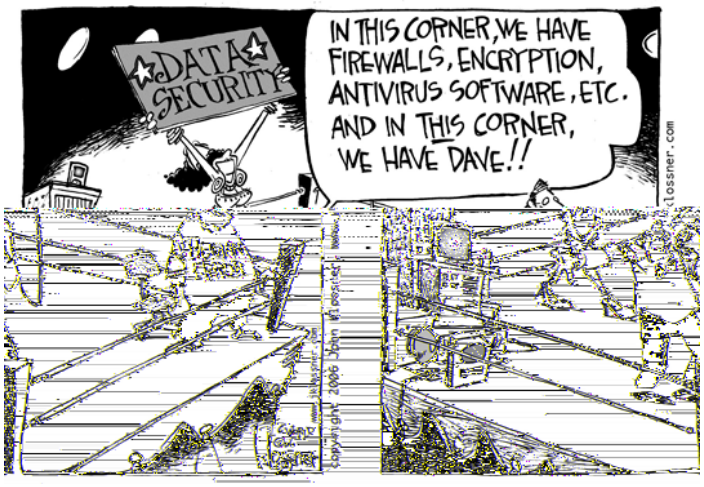
3. Attaque informatique Cette méthode fait référence aux actions groupuscule peut mettre en place pour faciliter son social engineering. Une illustration simple de cette méthode est la récupération de mot de passe. En effet, il semble que beaucoup de personnes utilisent le même mot de passe pour plusieurs 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 -up qui semble teur de ré-entrer

   son login et mot de passe.

4. Phishing Comme expliqué précédemment, cette méthode est Elle peut intervenir durant le social engineering pour forcer la victime à révéler une information sensible ou e
   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.

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. obtenir les credentials valides ou plusieurs employés-cibles pour infiltration. Les victimes de cette attaque ont généralement un poste avec un haut niveau

le système informatique cible (p.ex. manager, administrateur système).



Une autre méthode tout aussi efficace au niveau humain est de p.ex. mise sur écoute).

2.2.2. Infiltration

informatique cible.

le groupuscule effectue un repérage du réseau afin de comprendre et se représenter sa topologie, son architecture, sa

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 déclencha
de sécurité au sein du système.
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 ou plusieurs employés-cibles récupérés durant la phase de reconnaissance. Les machines utilisées à cette étape sont ensuite dites « compromises ».

2.2.3. Implantation

L mplantation du groupuscule dans le système et en la consolidation de cet ancrage.

, le groupuscule
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
Par exemple, le groupuscule peut installer un *sniffer* sur les machines compromises (comme illustré en Figure 3 et Figure 4). Un sniffer est un logiciel
machines situées sur le même réseau local. C
étendre et renforcer son implantation de façon latérale dans le système. Le groupuscule à de nouvelles machines du système qui seront à leur tour dites « compromises ».
être exécutée avec une approche low-and-slow,
compromise à une autre sans générer de trafic réseau supplémentaire, de sécurité. À terme, le groupuscule
ateur système.

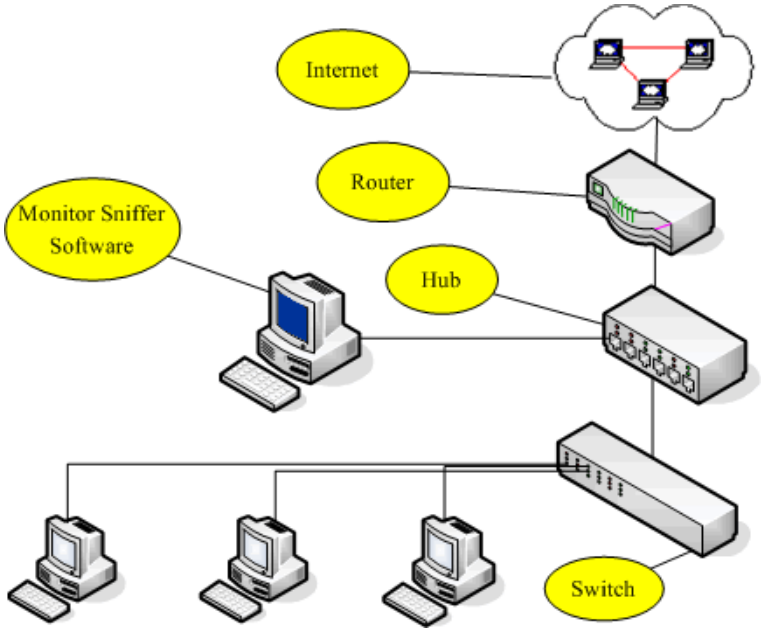


Figure 3: exemple d'architecture système avec un sniffer (Crédit : IM Monitor)

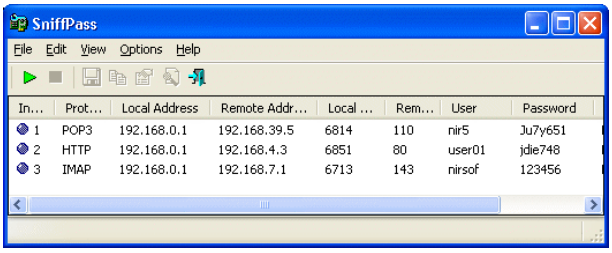


Figure 4 : récupération de credentials avec SniffPass (Crédit: Nir Sofer)

installer un certain nombre de malwares tels que des *backdoors*[14], chevaux de Troie, proxies[15] additionnels. De plus, ces malwares peuvent être polymorphes[16] 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

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

consiste en 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

En second lieu, le groupuscule met en place une partie très délicate et sensible Cette opération difficile car ces données doivent être acheminées à

sécurité. U
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*

[15] De façon générale, un proxy est un composant logiciel agissant en tant aire entre deux entités pour aider ou espionner leurs

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 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 déchiff
qui les rend très difficiles à détecter.

[17] La cryptographie, ou « », est une technique permettant la e, ou « », est une technique permettant de cacher un message secret dans un autre message sans que ce dernier ne soit illisible.

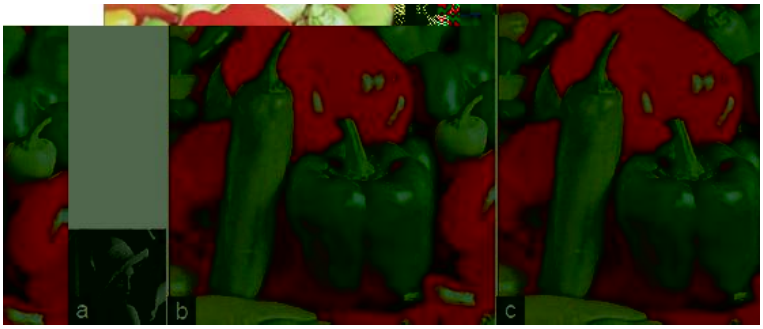


Figure 5 : exemple de stéganographie (Crédit : Atawneh, Almomani et Sumari). L'image (a) est le message à cacher. L'image (b) est l'image dans laquelle le message sera caché. L'image (c) est le résultat de cette stéganographie avec la méthode LSB[18]. Constatation : il n'y a aucune différence remarquable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

t se faire via différentes méthodes (p.ex. email contenant les données à extraire). Une technique très canaux cachés ». canaux de communication établis par le groupuscule entre les machines compromises et le serveur du groupuscule (ces machines clairement pas autorisées à communiquer ensemble par la politique de sécurité du système informatique cible) 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

dans le système cible le plus longtemps possible.

La mise en place e 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 futurs agissements.

Pour cela, le groupuscule couvre et efface les traces de son passage pour ne pas être détecté 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

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

3. Quelques célèbres APT

Cette section résentant quelques exemples

3.1. Un exemple concret : Stuxnet, 2009

Stuxnet est un *worm*[19] lancé en 2009 NSA[20] [21]. Il fait partie -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 . Il a été découvert le 17 juin 2010 par VirusBlokAda, société biélorusse développant des produits antivirus. À

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 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-
cté, 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 , ce qui contaminait alors les ordinateurs connectés au même réseau privé.

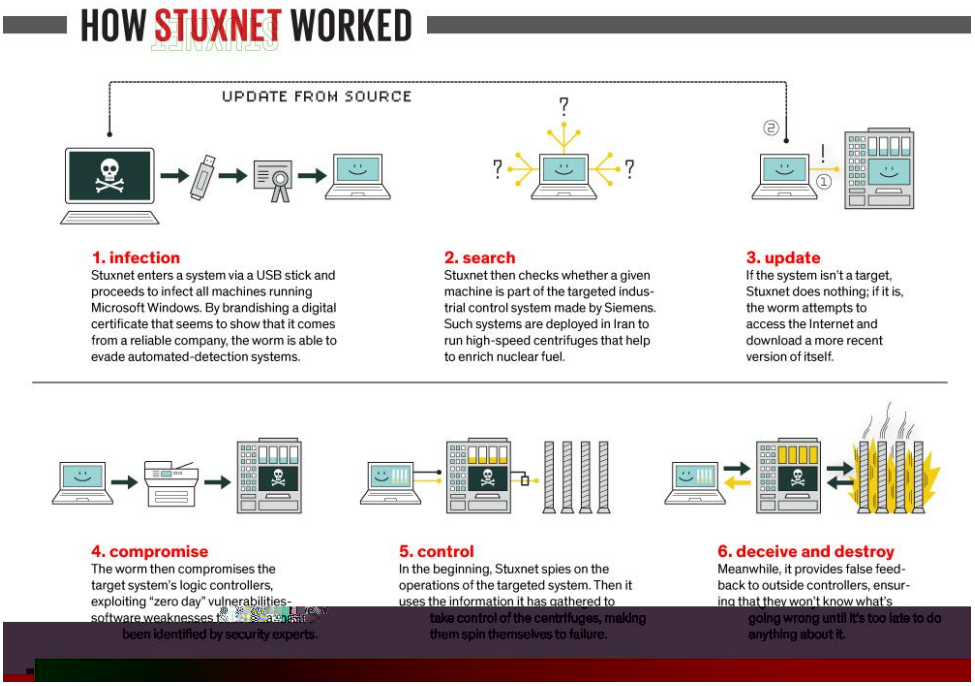


Figure 6 : illustration du mode opératoire de Stuxnet (Crédit : L-Dopa)

- 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 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

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 SCADA de Siemens avec une configuration bien définie, c -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 re 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
utilisation dans Stuxnet.

➢ Les opposants

Les principaux arguments de cette contestation sont au nombre de quatre. Stuxne aucun social engineering dans la phase de . Or ce point semble être, pour certains spécialistes, une caractéristique bien spécifique . Ensuite, sur une propagation en masse du ver pour toucher ordinateur du réseau cible plutôt viser un ordinateur spécifique, en utilisant les données récoltées durant la phase de reconnaissance. Aussi, Stuxnet avait pour but ultime magement du système cible principalement perpétrée que pour récolter des informations sur la cible. Enfin, les spécialistes ont mis en avant le fait e scalpel alors que Stuxnet 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 e groupuscule ayant créé Stuxnet était très organisé et puissant (c.-à-d. coalition entre la NSA et). 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 (s) pour préparer soigneusement implantation du ver pour une longue durée avait également été étudiée par le groupuscule : une fois installé sur un ordinateur cible et ayant accès nternet, Stuxnet -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 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

.

3.2.3. Sykipot, 2006

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).

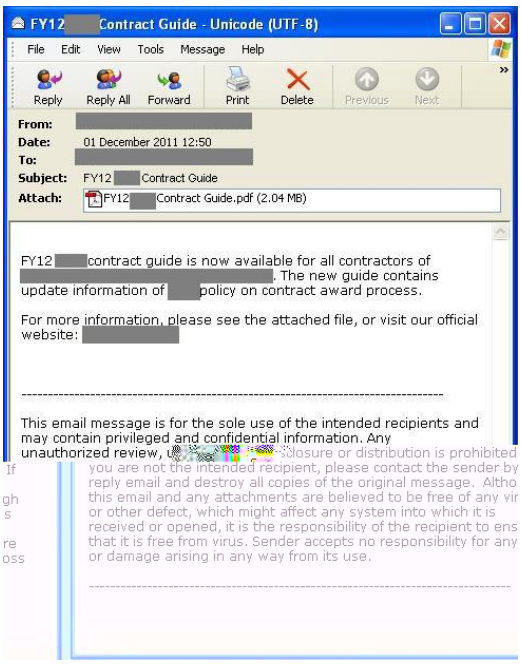


Figure 8 : exemple d'email spear-phishing envoyé par Sykipot (Crédit : Helloblog)

Sykipot a ciblé de nombreuses entreprises américaines et britanniques, en particulier celles opérant dans la défense informatique, les télécommunications, 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 étaient basés en Chine. Les objectifs, les moyens déployés et les informations recueillies ont fortement suggéré agence de renseignement serait le bénéficiaire de cette APT.

3.2.4. GhostNet, 2009

GhostNet -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 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 compromis.
GhostNet incluait aussi la possibilité d'utiliser les périphériques audio et vidéo pour surveiller les locaux où se trouvait .

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

pération Aurora fait référence à une série de cyber-attaques lancées en 2009 présumées origine chinoise. Aurora était une APT très bien coordonnée qui se déroulait en six grandes étapes comme illustré en Figure 9. Aurora utilisait du spear-phishing avec un lien vers un site malveillant (se trouvant le plus souvent sur un serveur à Taiwan, . Une fois sur ce site, le navigateur de

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 u

basait sur le téléchargement et exécut 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 Ainsi Aurora permettait au grou complet au système cible.

soumises à la propriété intellectuelle sur les systèmes cibles.

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

Les victimes 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. Google qui a dévoilé anvier 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.

Force est de constater
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

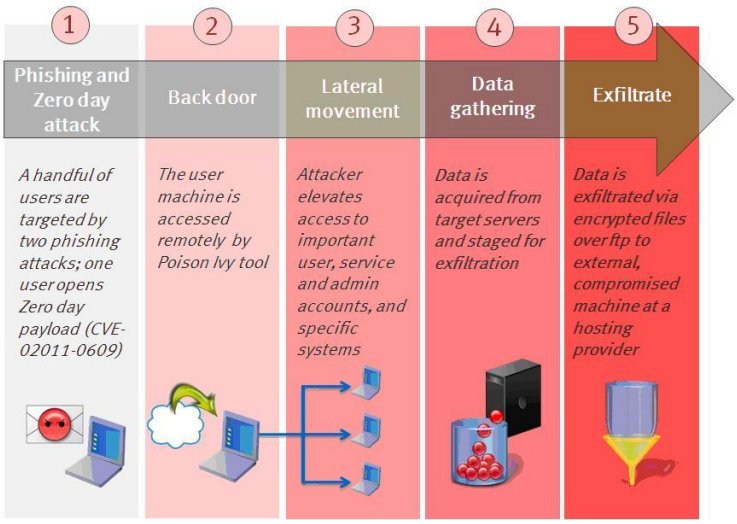


Figure 10 : schéma simplifié de l'APT contre RSA SecureID (Crédit : RSA)

En résumé à identifier de 2012 sur les intrusions de systèmes informatiques établi par Verizon[31], 92% des organisations ont été mises au externe.

4. Comment se protéger d'une APT

ucun produit de sécurité réseau vendu sur le marché ne peut garantir à 100% une protection contre les APT. Étant donné mis en place, il existe clairement

(involontaire ?) des utilisateurs complètement impénétrable pour un groupuscule motivé et plein de ressources. La bataille contre les APT vient juste de commencer et elle 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 , 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. , de simples dispositions peuvent être prises : s un mécanisme 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 et les protéger grâce à du cloisonnement stratégique et efficace.

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

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 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 ntreprise, peu importe leur localisation dans le système. Des logiciels de *content-filtering*, comme illustré en Figure 11, sont aussi disponibles pour est autorisé à consulter, en particulier sur le réseau Internet. Par exemple, les pages Hotmail

entreprise, ce qui éviterait une potentielle attaque par phishing via ce type de boites aux lettres personnelles.

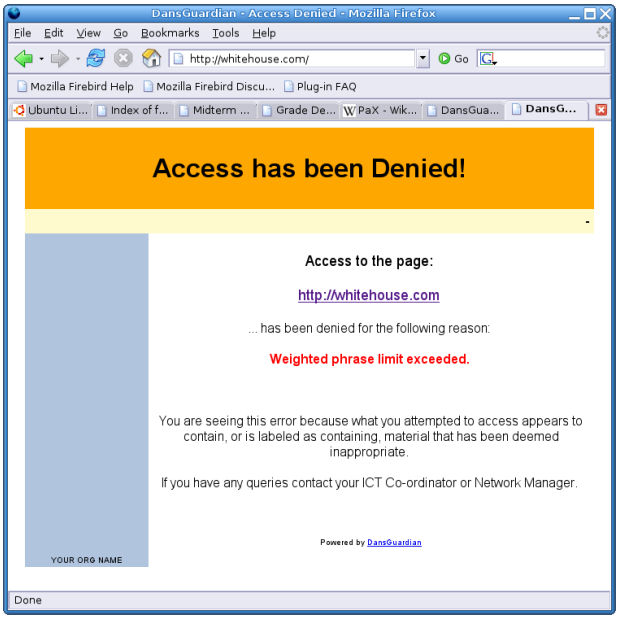


Figure 11 : exemple de page Internet bloquée avec le logiciel de content-filtering DansGuardian (Crédit : Bluefoxicy)

[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 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

dégâts que peuvent engendrer les APT.

uivre de très près toutes les dernières menaces publiées et toutes les nouveautés concernant la sécurité (p.ex. via la participation à des cours, conférences).
Ceci leur permettra de connaitre et maitriser toutes les dernières techniques pour se prémunir des APT. Elles doivent également se plonger

déployées (p.ex. comprendre comment les zero-day exploits sont mis en) et des types de vulnérabilités généralement exploitées. Garder à jour une documentation précise des menaces est clairement un atout contre les APT.

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

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).

si les comptes de plusieurs utilisateurs se bloquent simultanément.

Les équipes HelpDesk et sécurité doivent sans cesse être proactives quant amélioration d
(*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 . Ces plateformes sont ainsi identifier « botte de foin » qui indiquerait une attaque de type APT en action dans le système.

Le 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

qui en fait la demande. Elle doit aussi fixer certains points fondamentaux

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 entreprises. Le but 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

4.3. Former les employés lambda

Enfin, la toute première ligne de défense contre les APT est clairement le personnel non- 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 La campagne du DHS[41] « *If You See Something, Say Something* », dont le la connaissance et la compréhension du grand public

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 une APT. 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 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 américaine responsable de la sécurité intérieure.

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 hacktivistes[42], ou des État-nations. vaccin » 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 ».