Province de Liège

Enseignement

Haute Ecole de la Province de Liège

CATEGORIE TECHNIQUE

Parc des Marêts - Rue Peetermans, 80 - 4100 Seraing

Étude et analyse de solutions de détection, prévention et protection contre des menaces avancées et persistantes sur un système d'information

Benjamin Nicodème

Travail de fin d'études présenté en vue de l'obtention du grade de Bachelier en informatique et systèmes finalité réseaux et télécommunications

Année académique : 2015 - 2016

Siège social :
Avenue Montesquieu, 6
4101 Jemeppe (Seraing)
Belgique

www.hepl.be

Editeur responsable : Province de Liège, Place Saint-Lambert 18A , 4000 Liège

Remerciements

Je tiens à remercier tous ceux qui ont contribué, de près ou de loin, à la réalisation de mon travail de fin d'études, à savoir :

Monsieur Alexandre Lienard pour m'avoir permis de réaliser mon stage de fin d'études au sein de la société Nethys.

Messieurs Raphaël Prys et Jean-Louis Timsonet pour m'avoir encadré durant mon stage.

Monsieur Ignace Caria pour ses nombreux conseils ainsi que la motivation qu'il ma transmise.

Monsieur Xavier Mertens pour ses conseils en matière de test d'intrusion.

Monsieur Pierre De Fooz pour son investissement au bon déroulement de ce travail.

Messieurs Raphaël Prys, Ignace Caria et Xavier Mertens pour la relecture de mon travail.

Enfin, un remerciement particulier à ma mère pour son soutien, ses conseils, et pour la relecture de mon travail

First release, May 2016

Table des matières

Table des figures

Glossaire

Acronyme	Signification anglaise	Signification française
API	Application Programming Interface	Interface de programmation applicative
APK	Android PacKage	Format de fichiers pour Android
APT	Advanced Persistent Threat	Menace avancée et persistante
ARM	Advanced RISC (reduced instruction set computer) Machine	Processeur possédant une architecture spécifique. Ils sont généralement utilisés dans des devices portables telles que des smartphones ou des tablettes.
ATP	Advanced Threat Protection	Protection de menaces avancées
AV	Anti Virus	Anti virus
BYOD	Bring Your Own Device	Apportez vos appareils personnels
C&C	Command and Control	Commande et contrôle
CHM	Compiled HTML	Fichier HTML compilé
CLI	Command Line Interface	Interface de ligne de commande : terminal
CPU	Central Process Unit	Processeur

DLL	Dynamic-Link Library	Est une bibliothèque logicielle dont les fonctions sont chargées en mémoire par un programme
ESA	Email Security Appliance	Appareil de sécurité du flux email
EXE	Executable	Est une extension de fichier sur Windows pour les fichiers exécutables
FTP	File Transfer Protocol	Protocole de transfert de fichiers
GCHQ	Government Communications Headquarters	Quartier général des communications du gouvernement Britannique
HTML	Hypertext Markup Language	Est le format de données conçu pour représenter les pages web
HWP	Hangul Word Processor	Traitement de texte ayant la capacité d'enregistrer des documents qui sont rédigés en utilisant l'alphabet hangû (très populaire en Corée)
IDS	Intrusion Detection System	Système de détection d'intrusion
IoC	Indicator of Compromise	Indicateur de compromission
IP	Internet Protocol	Protocole se trouvant niveau 3 dans le modèle OSI. Protocole utilisé par internet
IPS	Intrusion Prevention System	Système de prévention d'intrusion
ISP	Internet Service Provider	Fournisseur d'accès à Internet (FAI)
JAR	Java ARchive	Fichier ZIP utilisé pour distribuer un ensemble de classes Java
MTA	Mail Transfert Agent	Serveur de transfert d'emails permettant le filtrage de ces derniers
NFS	Network File Sharing	Protocole de partage de fichiers
NGES	Next Generation Endpoint Security	Sécurité de nouvelle génération au niveau des points finaux
NGFW	Next Generation FireWall	Pare-feu de nouvelle génération

NGIPS	Next Generation IPS	IPS de nouvelle génération
NSA	National Security Agency	Agence de la Sécurité Nationale Américaine
OS	Operating System	Système d'exploitation
OUI	Organisation Unique Identifier	Identifiant unique d'organisation
PDF	Portable Document Format	Langage de description de pages créé par la société Adobe Systems
PE	Portable Executable	Format des fichiers exécutables et des bibliothèques sur les systèmes d'exploitation Windows 32 bits et 64 bits
PoC	Proof of Concept	Preuve du concept, ou démonstration de faisabilité
RAT	Remote Administration Tool	Outil d'administration à distance
SE	Social Engineering	Ingénierie sociale
SIEM	Security Information and Event Management	Appareil de sécurité collectant les informations et les événements
SOC	Security Operation Center	Centre des opérations de sécurité
SSH	Secure SHell	Programme et protocole de communication sécurisé
SSL	Secure Socket Layer	Protocole de sécurisation permettant l'authentification, la confidentialité et l'intégrité
TAP	Test Access Point	Matériel physique utilisé pour analyser le trafic réseau sans le perturber
TCP RST	TCP Reset	Paquet TCP marqué avec le "reset flag"
URL	Uniform Ressource Locator	Les URL sont une invention du World Wide Web et sont utilisées pour identifier les pages et les sites web
VM	Virtual Machine	Machine Virtuelle
VOD	Video On Demand	Vidéo à la demande

WAF	Web Application Firewall	Firewall d'application web
WSA	Web Security Appliance	Appareil de sécurité du flux web
XPF	XProtector Project File	Extension de fichier utilisée par divers logiciels

1. Introduction

1.1 Introduction aux APTs

L'accroissement de l'utilisation des nouvelles technologies n'est plus à prouver. Si au début de l'informatique, les équipements étaient parfois détournés de leur fonction première (premiers cas de piratage informatique), très vite, l'apparition de virus est venue perturber la bonne marche de certains systèmes.

En effet, depuis les années 90, l'explosion de virus a eu plusieurs effets :
— La paralysie de certains systèmes ;
— La prise de conscience de vulnérabilités software ;
— Et surtout la création du marché des antivirus.

Des virus tels que TEQUILA.GRN, AIDS, MELISSA, ILOVEYOU ont connu leur période de gloire en infectant des dizaines, parfois des milliers d'ordinateurs dans la monde. A titre d'exemple, plus de 300.000 pour ILOVEYOU au début 2000.

Si le marché des antivirus a explosé et que l'offre s'est étoffée, certains cybercriminels ont décidé d'exploiter le filon du "virus qui rapporte".

Si généralement les virus ont pour vocation de toucher le plus large public possible, de commettre des dégâts à l'échelle du globe, d'autres plus perfectionnés, les APTs (Advanced Persistent Threats), sont programmés pour tuer un nombre restreint de cibles.

L'APT est en quelque sorte, l'artisanat des attaques virales.

1.2 Présentation de Nethys

La société Nethys a été fondée en 1923. L'entreprise se situe rue Louvrex à liège. Elle compte 30 sites distants, 3 Data Centers ainsi qu'un SOC [1]. Les principales activités de l'entreprise sont les secteurs de l'énergie, des télécommunications et du développement industriel.

Quelques 2500 personnes travaillent au sein de Nethys.

Le chiffre d'affaires de l'entreprise est supérieur à 700 millions d'euros.

1.2.1 Secteurs d'activité de Nethys

Nethys occupe aujourd'hui, au travers de ses participations, des positions fortes dans quatre segments-clés :
— L'énergie (la distribution ainsi que la production d'énergie renouvelable) ;
— Les médias ;
— Les télécommunications ;
— La prise de participations dans des secteurs à haute valeur ajoutée.

Ces différents secteurs d'activité sont assurés par plusieurs sociétés. Elles sont les suivantes :

1.2.1.1 Le pôle énergie

RESA exerce des fonctions de distributeur d'énergie. Les deux secteurs de distribution sont le gaz et l'électricité. RESA est le principal Gestionnaire de Réseaux de Distribution (GRD) d'électricité et de gaz de la province de Liège.

NETHYS ENERGY est le secteur d'activité de NETHYS en charge du développement de projets de production d'énergie renouvelable (photovoltaïque, hydroélectricité, cogénération...). Ce secteur propose également un panel complet de services énergétiques.

ELICIO, société filiale de NETHYS, regroupe les activités de développement, de construction et d'exploitation de parcs éoliens on-shore en Wallonie, en Flandre mais aussi en France ainsi que plusieurs projets à l'étranger.

1. SOC : Security Operation Center : centre des opérations de sécurité

1.2.1.2 Le pôle télécommunication

WIN est opérateur et intégrateur de services ICT (Information and Communication Technologies) au service des entreprises, des organisations du secteur public et du secteur des soins de santé. Win possède son propre Data Center (Wallonie Data Center).

VOO, secteur d'activité de NETHYS, est né de la collaboration entre l'ALE (Association Liégeoise d'Electricité), Télédis et Brutélé.VOO propose sur l'ensemble de la Wallonie et sur une partie de Bruxelles la télévision analogique et numérique, la VOD, la téléphonie fixe et mobile, des connexions internet à haut et très haut débit.

1.2.1.3 Le pôle média

Les éditions de L'AVENIR et L'AVENIR ADVERTISING, sociétés filiales de NETHYS, sont un pôle multimédia principalement actif dans la presse de proximité.

BE TV, société filiale, est la chaîne à péage disponible en exclusivité sur le réseau de VOO. BE TV exerce ses activités dans deux grands domaines : l'édition de chaînes à péage premium (Be Premium) et la distribution de chaînes thématiques (Be Bouquets et Be Options).

1.2.1.4 Le pôle holding

C'est au sein de NETHYS INVEST que sont logées les participations financières détenues par le groupe. NETHYS INVEST a pour mission de prendre des participations dans des secteurs porteurs, en relation directe ou indirecte avec les activités industrielles du groupe, la distribution et la production d'énergie, son utilisation rationnelle, les télécommunications et multimédias mais aussi plus généralement les utilities.

1.2.2 Les métiers IT chez Nethys

De nombreux métiers existent au sein de Nethys. Au niveau de l'IT, on retrouve notamment les secteurs suivants :

- Réseau ;
- Infratucture ;
- Système ;
- Applicatif télécom ;
- Applicatif média ;
- Applicatif énergie ;
- SAP ;
- Support ;
- Front Office ;
- Workstation ;
- Cellule projet ;
- Architecture.

Quelques 400 personnes sont réparties à travers ces secteurs.

1.2.3 La sécurité chez Nethys

3 métiers existent au sein de la cellule sécurité chez Nethys :

- Opérateur SOC ;
- Conseil interne (pentest, forensic support sur les projets, prospective) ;
- Audit interne (investigations).

La cellule sécurité est chargée de la stratégie. La partie opérationnelle est prise en charge par les équipes IT.

Pour des raisons de sécurité, le nombre de personnes affectées à la cellule sécurité est confidentiel.

1.3 Cahier des charges

La société Nethys dispose de divers systèmes de sécurité. Cependant elle ne savait pas si l'usage de ces appareils suffisait à contrer des attaques de type APT.

Il était donc question d'effectuer les tâches suivantes :

1. Etude et expertise dans le domaine des APTs ;
2. Analyse des besoins de Nethys ;
3. Analyse des risques ;
4. Comparaison des solutions techniques :
   (a) Création d'une grille de qualification ;
   (b) Création des plans de test ;
5. Sélection des fournisseurs ;
6. Mise en place, test et analyse de 3 PoCs ;
7. Rédaction d'un dossier d'architecture technique en vue d'une implémentation ;
8. Bilan et conclusions.

Nethys comme d'autres entreprises, peut se voir ciblée par des attaques APTs. Elle peut par exemple être ciblée afin d'atteindre les nombreux clients dont elle dispose.

Une analyse des solutions existantes au sein de l'entreprise ainsi que celles présentes sur le marché a donc été réalisée. L'entreprise souhaitait également une expérimentation de trois solutions choisies afin de sélectionner celle qui répondait le plus aux attentes de l'entreprise.

L'objectif était donc de se familiariser avec les APTs et de comprendre leur fonctionnement. Une fois cet objectif atteint, une analyse de risque a été réalisée afin de déterminer si le risque devait être traité ou accepté. Le risque devant être traité, la définition des besoins de Nethys a été réalisée.

Sur base de ces critères, ont étés réalisés 3 PoCs afin de tester les dires des fournisseurs. Les solutions ayant été testées sont les suivantes :
— Advanced Malware Protection de Lastline ;
— WildFire de PAlo Alto Networks ;
— FortiSandbox de Fortinet.

Suite aux résultats de ces PoCs, des rapports reprenant les résultats de tests ainsi que les avantages et inconvénients des solutions ont étés réalisés . Des recommandations en cas d'implémentation figuraient également dans ces rapports.

2. Les APTs

2.1 Évolution des attaques dans le temps : du virus aux APTs

La ligne du temps suivante représente l'évolution des malwares dans le temps :

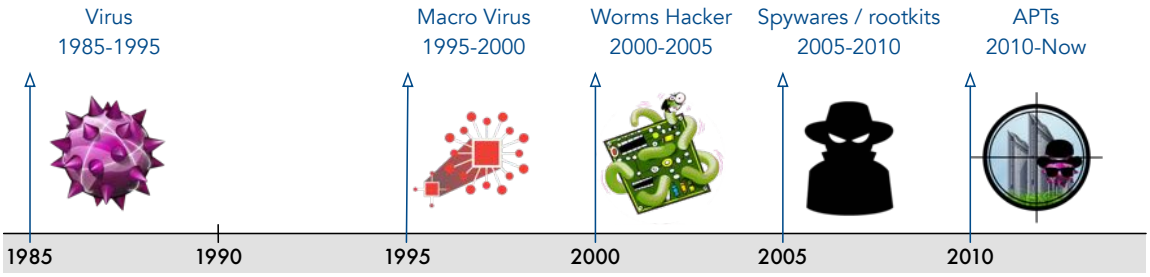


FIGURE 2.1 – Ligne du temps des grands types de malwares

Un *malware* est un logiciel malveillant ayant pour but de nuire à une machine. Un malware est généralement installé sur une machine sans que son utilisateur en ait conscience. Le terme malware englobe des éléments tels que : virus, vers, chevaux de Troie, etc.

Virus

Historiquement, les *virus* sont les premiers malwares à avoir étés créés. Dans leur plus jeune âge, ils n'étaient pas utilisés avec des intentions malveillantes. Leur utilisation a ensuite été détournée pour effectuer des tâches malveillantes. Un virus est un automate autoréplicatif ou du code qui se duplique autonomement . Les virus s'intègrent dans des logiciels légitimes. Ils peuvent être transmis par pièces jointes dans des emails, par le web, ou encore via du matériel corrompu. Le matériel corrompu peut-être des disquettes, des CD ou du stockage USB. Certains virus exécutent directement leur code malveillant. D'autres attendent que certains critères soient respectés pour s'exécuter. Par exemple, un virus peut s'exécuter à une date précise.

Macro virus

Un *macro virus* est un virus écris en langage macro : un langage qui est intégré dans des logiciels tels que Microsoft Word. De tels logiciels permettent d'exécuter automatiquement les macros d'un document lors de son ouverture. Ce qui permet d'effectuer une série d'actions. Les actions réalisées par les macros virus sont malveillantes. Ces malwares sont généralement diffusés par email.

Worms

Un *ver* (worm) est un malware qui se reproduit sur plusieurs machines via le réseau. Il réside dans la mémoire active. Les vers utilisent généralement des parties de système d'exploitation qui sont automatiques et qui ne paraissent pas étranges à l'utilisateur. Ces derniers ne sont généralement détectés que lors de la consommation excessive de ressources. Cette consommation ralentit le système ou arrête des tâches.

Spywares / rootkit

Un *spyware* permet de recueillir des informations sur une entité sans son consentement. Un spyware est un malware permettant de collecter des informations diverses afin d'en tirer profit. Ce malware est installé sans que l'utilisateur en ait conscience. Il est également possible de trouver des spywares dans des shareware. Un shareware est un logiciel pouvant être utilisé pendant une certaine période avec des fonctionnalités réduites.

APTs

Les APTs sont ciblés et furtifs. Ils sont développés au point suivant.

2.2 Advanced Persistent Threat

2.2.1 Définition des APTs

Les APTs sont une catégorie d'attaques informatiques principalement dirigée avec des objectifs commerciaux, politiques, ou encore militaires. Les APTs sont élaborés avec un haut degré de furtivité et s'étendent sur une durée de fonctionnement prolongée. Par exemple, un déclenchement tardif ou après une action spécifique et anodine de prime abord pour l'utilisateur. Les APTs sont parfois tellement complexes et évolués qu'ils peuvent agir non seulement sans être détectés mais en plus sans modifier le comportement initial du système vérolé.

2.2.1.1 Avanced

Un APT est dit avancé, car sa structure est complexe et qu'il utilise tout un arsenal de techniques d'attaques et d'outils pour atteindre son objectif final (phishing, malware, XSS, social engineering ...).

C'est la combinaison de différents composants (codes, programmation, outils perturbants, click-jacking ...) sur ou via différents vecteurs (supports amovibles, réseaux, protocole SMB, HTTP, HTTPS...) qui complexifie l'attaque et la définit comme avancée.

2.2.1.2 Persistent

Les attaques de type APT ciblent des entités particulières et ont un objectif bien défini, même s'il arrive qu'une diffusion de masse soit faite au détriment de l'attaquant (voir point 2.3.1). Les vecteurs d'intrusion sont multiples et n'ont pour limite que l'innovation technologique. Dans certains cas, les attaquants vont jusqu'à laisser traîner une clef USB infectée près de l'entité ciblée. Ils espèrent ensuite que cette dernière finisse par être introduite dans une machine. Comme dit précédemment, les mécanismes utilisés sont souvent complexes et comptent sur le manque de vigilance humain pour s'introduire dans un système d'information. Aucune solution technique ne permet d'ailleurs de complètement gérer le risque humain et les failles y étant liées (social engineering). Contrairement à d'autres attaques, un APT s'étend sur une longue période. L'appât du gain immédiat n'est pas l'objectif principal. Au contraire, il est avant tout dans le but de rester furtif, de ne pas éveiller l'attention. La durée d'un APT est calculée en mois, voire en années, elle dépend du scénario à succès mis en place par l'attaquant. Ce type d'attaque ne s'utilise que sur une technologie bien particulière. Il n'est généralement pas possible d'utiliser tel quel un APT sur une technologie différente, aussi infime soit-elle que celle qui était prévue initialement. Ils sont persistants aussi dans le sens où ils sont capables non seulement de passer inaperçus, mais aussi de passer à travers plusieurs lignes de défense techniquement et technologiquement différentes : firewalls, IDS, IPS … Bien entendu, depuis l'apparition des APTs, des solutions ATP (Advanced Threat Prevention) ont vu le jour. Malgré cela, les APTs existent toujours, et sont toujours utilisés ! Les attaques se complexifient. Réalisées en mode "sur mesure", il est très difficile de lutter efficacement et pro-activement.

2.2.1.3 Threat

Une *menace* (threat) est un ensemble de circonstances pouvant potentiellement causer des préjudices. Une menace est le résultat de l'existence de vulnérabilité et de la potentielle présence d'attaquants. Une vulnérabilité est une faiblesse dans un système qui pourrait être exploitée pour causer préjudice. Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation du système informatique. Il s'agit généralement de l'exploitation de failles logicielles.

On parle de menaces avancées et persistantes car les méthodes généralement utilisées pas les APTs comportent des failles zero-day. Ces failles exploitent des vulnérabilités non découvertes ou non corrigées.

N'importe quelle organisation peut être la cible d'un APT. Dès lors, on suppose la présence potentielle d'attaquants. Un APT ne peut être que peu automatisé. Cela implique une coordination de moyens techniques et humains, et donc la présence d'attaquants.

2.2.2 Risques

Les définitions des APTs données par les entreprises de cyber sécurité sont différentes. Il existe donc déjà un flou au niveau de la littérature spécifique et des experts en la matière. En effet, il peut être difficile de cerner exactement le champ d'action des APTs, d'en connaître toute la mesure. Bien entendu, toutes les entités ne sont pas ciblées directement par les APTs. Une épicerie locale dont la gestion n'est pas informatisée n'aura que peu d'intérêt pour un APT. Il n'en va par contre pas de même pour certaines petites entreprises (PME) sous-traitantes de grands groupes.

Chaque jour, de nouveaux produits connectés sont inventés et mis sur le marché. Néanmoins, ce qui est connecté est par conséquent exposé aux risques de piratage. D'ici peu, il sera certainement possible, si ce n'est pas déjà le cas, de contrôler toute sa maison et ses fonctionnalités numériques via son smartphone. Il est déjà possible de contrôler certaines voitures à distance. Il paraît évident qu'un APT pouvant s'introduire dans tous les systèmes connectés pourrait avoir, en marge de conséquences importantes, deux buts :

— Le premier pourrait être un vol de données à grande échelle. Il peut également s'agir d'espionnage. Regin a espionné un grand nombre d'organisations basées dans divers pays. De plus amples informations sur Regin se trouvent au point 2.3.2 ;
— Le second pourrait être à caractère destructif. Stuxnet, par exemple, a retardé le programme nucléaire iranien. Il a dégradé des centrifugeuses servant à l'enrichissement d'uranium. Des informations complémentaires sur Stuxnet se trouvent au point 2.3.1.

Imaginons qu'un APT puisse détourner des avions, des voitures ou encore des centrales dans un but destructeur. En cas de cyberguerre, un APT de ce genre aurait la capacité de faire d'énormes dégâts.

Une différence peut être faite entre ces deux types d'APTs. Le critère étant l'impact destructeur matériel dont il dispose. Deux grands types d'APTs sont alors distinguables :

— Ceux dont l'impact est physique ;
— Ceux dont l'impact est virtuel.

Dans un cas comme dans l'autre, un APT est dirigé contre une entité en particulier. L'infection de masse n'est pas son objectif principal, bien que ce soit parfois nécessaire dans certains cas.

La création, l'élaboration et l'orchestration d'un APT peut coûter très cher. De plus, cela demande des compétences spécifiques et rares. C'est pourquoi, les ordinateurs "privés" ne sont que peu ciblés par ces attaques, en tout cas pas d'un point de vue d'une attaque de masse.

Les risques qu'une entité soit ciblée par un APT résultent des enjeux stratégiques, parfois de son ampleur et des données qui y sont créées, manipulées et nécessaires à son bon fonctionnement. D'une manière logique, il faut qu'il y ait un intérêt pour les attaquants à prendre une entité pour cible.

2.2.3 Conséquences

Les conséquences d'un APT peuvent être dévastatrices pour l'entité touchée. Il peut s'agir de dégâts matériels ou de dégâts d'une autre nature.

Dégâts matériels

Les dégâts matériels peuvent être divers. Un exemple concret peut être le cas de Stuxnet. La reprogrammation furtive des centrifugeuses d'enrichissement d'uranium a fait perdre du temps aux Iraniens. Les détails concernant les retards ne sont pas importants. Cependant, ce qui a permis de dégrader ces centrifugeuses est leur vitesse de rotation.

Conséquence sur l'entité attaquée

Les conséquences qu'entraînent un ATP qui a atteint ses objectifs sont diverses et varient en fonction des actions réalisées par l'attaque. Plusieurs conséquences sont envisageables dans le cas où l'attaque a été menée à bien et que ses objectifs ont été remplis.
Ces conséquences sont les suivantes :
— La réputation, la mauvaise publicité dégagée par l'attaque ;
— L'impact financier.

La réputation, la mauvaise publicité

Lors d'une attaque, une entreprise peut se voir dérober des informations sur ses clients. Les systèmes pouvant être victimes de ce genre de vols sont des entités telles que les banques, les ISP ou les hôpitaux. Il est certain que se voir dérober son dossier médical, ou ses informations bancaires n'inspire pas forcément confiance. Une entité victime de tels vols pourrait se voir impactée dans ses relations commerciales. La finalité est un impact financier.

Dans le but d'éviter de perdre sa clientèle et donc de subir des pertes financières supplémentaires, les victimes d'attaques persistantes et avancées évitent autant que possible que l'information se répande. Les dépôts de plainte sont rares.

L'impact financier

Lorsqu'un APT arrive à atteindre ses objectifs en étant resté furtif, il est plus que probable qu'un grand nombre de machines présentes sur le réseau soient infectées. Le premier impact financier est le prix que va coûter la décontamination. Non seulement toutes les machines vont devoir être analysées et potentiellement réinstallées, mais, en plus, les machines n'ayant pas étés analysées ne pourront plus être connectées à l'infrastructure. Vient donc s'ajouter à cet impact financier le manque à gagner causé par l'incapacité de travail du personnel et le temps perdu à récupérer les données et/ou le travail effectué.

Dans le cas où l'objectif de l'APT est l'espionnage industriel, la perte des données dérobées vient également s'ajouter au total . Un exemple serait un APT ayant réussi à se glisser dans le réseau d'une compagnie de création de moteurs d'avions pour y voler les plans d'un nouveau moteur électrique. La perte d'un avantage, que ce soit au niveau du coût des recherches et du développement ou tout simplement l'avantage d'utiliser le fruit des recherches, peut se chiffrer en millions, voir plus. Bien entendu, tout dépend de la valeur des informations dérobées.

Tout le monde est exposé à l'espionnage industriel. Il est courant que les PME ou sous-traitants soient indirectement visés dans le but d'impacter de plus grosses entreprises. Pour reprendre l'exemple de la compagnie aérienne, dans le cas où celle-ci sous-traite une partie de la construction de ses avions, la compagnie sous-traitante est autant ciblée, si pas plus que la compagnie aérienne en elle-même. En effet, il suffit de changer suffisamment de données sur les plans de la compagnie sous-traitante pour qu'il y ait un impact sur la qualité des pièces du moteur fabriquées. Lorsque les moteurs se dégraderont, il ne fait aucun doute que cela ne fera ni bonne presse à la compagnie aérienne ni à la société sous-traitante. Elles seront toutes deux impactées même si la cible indirecte était la compagnie aérienne. C'est l'impact de leur clientèle qui sera le premier touché. Celui-ci se répercutera sur leurs revenus et donc leurs finances.

2.2.4 Vecteurs d'infection

Les APTs utilisent des failles et des mécanismes complexes pour s'introduire en toute discrétion dans un système d'information. L'atout principal des attaques avancées et persistantes est l'exploitation de failles zero-day.
Il s'agit de failles n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. Ces failles sont inconnues ou non corrigées par l'éditeur du logiciel concerné par la faille. Leur existence n'est donc généralement connue que de ceux les exploitant. La principale caractéristique de ces failles est qu'aucune protection n'est disponible. Un véritable marché noir existe autour de ces failles prisées pour des attaques silencieuses. Des sociétés telles que Google, Facebook ou encore Microsoft offrent des récompenses aux personnes leur rapportant l'existence d'une faille. La discrétion et la faible diffusion font la force d'une attaque zero-day. Une fois la faille connue et documentée, les logiciels sont patchés et elle ne présente plus aucun intérêt. Les failles zero-day sont le "noyau" d'une attaque furtive. Elles sont essentielles pour un APT. Cependant, ces éléments ne sont qu'un élément exploitable permettant de contourner la sécurité d'un système. Il faut donc un moyen d'exploiter ces failles. Les malwares permettent cette exploitation. On retrouve plusieurs vecteurs d'infection.

Exploit kits

Un *exploit kit* est un logiciel destiné à être déployé sur un serveur. Son but est d'identifier les vulnérabilités logicielles que le client utilise. Une fois les vulnérabilités découvertes, le serveur s'en sert pour envoyer du code malveillant au client. La dangerosité des exploit kits est leur facilité d'utilisation et la facilité de déploiement.
Les logiciels habituellement visés sont les produits Java, Adobe ou encore des navigateurs Internet. Un exploit kit collecte des informations sur le client (au sens client-serveur) trouve la vulnérabilité et l'exploitation associée. L'exploitation est alors faite par drive-by download.
Le drive-by download possède deux formes différentes :

— Soit l'utilisateur effectue le téléchargement sans avoir conscience qu'il s'agit d'un logiciel malveillant ;
— Soit le téléchargement s'effectue à l'insu de l'utilisateur (en tâche de fond par exemple)

Dans les deux cas, la machine est compromise sans que l'utilisateur ne s'en rende compte. Si le malware n'utilise pas de failles zero-day, il peut certainement être détecté et bloqué par un agent antivirus. Si l'antivirus ne reconnaît pas l'exploitation de faille, le malware infecte la machine et exécute son code malveillant.

Social engineering (SE)

Le *social engineering* est une méthode d'attaque qui consiste à tromper, duper l'adversaire. Il s'agit d'attaques généralement "orales" qui consistent à demander les identifiants d'une personne. Il en existe différents types, mais tous se basent sur la capacité à tromper sa victime pour en obtenir des informations. La plupart du temps, la victime ne se rend pas compte qu'elle est abusée, escroquée. Les méthodes utilisées se basent sur l'imposture, le charisme, ou encore le culot afin d'abuser de la confiance, de l'ignorance des personnes ciblées. Les personnes ciblées sont généralement les plus faibles d'une organisation, le personnel non technique (secrétaires, comptables, ...) ou encore le personnel récemment recruté. La paranoïa reste le meilleur moyen de défense face au SE.

Voici différents exemples de SE :

Fishing

Le *fishing* consiste à envoyer un email malveillant déguisé en email légitime. Cet email se fait généralement passer pour entité de confiance. L'email est rédigé de telle sorte à duper le récepteur pour qu'il partage des informations personnelles ou pour qu'il clique sur un lien malveillant.

Spear fishing

Le *spear fishing* est une forme de fishing plus ciblée. En effet, les emails ciblent des entités ou des individus en particulier et sont adaptés en conséquence. Un exemple de spear fishing serait la réception d'un email d'une connaissance ou d'un individu prétextant avoir une connaissance en commun. Le fait d'avoir une relation avec la prétendue connaissance en commun rend moins vigilant. Il peut également s'agir d'un email concernant un achat en ligne récent. Ce qui rend en fait moins vigilant sont les informations plus ou moins "personnelles" contenues dans ces emails.

Pretexting

Le *pretexting* consiste à mentir au destinataire pour accéder à des données à caractère personnel ou confidentiel. Un exemple est de prétexter du besoin de confirmer l'identité de la victime sur base d'informations personnelles déjà collectées.

Scareware

Le *scareware* consiste à faire croire à l'utilisateur que son ordinateur est infecté ou qu'il a téléchargé du contenu illégal. Le scareware propose alors à l'utilisateur de désinfecter sa machine. Néanmoins, ce que l'utilisateur ignore, c'est que le logiciel fait tout le contraire. Le scareware influence l'utilisateur pour qu'il télécharge et installe un logiciel de 'décontamination' qui procède en réalité à l'infection de sa machine.

Baiting

Toutes les entités ne sont pas directement infectables depuis le réseau. En effet, il arrive que des sites soient déconnectés de l'internet global pour éviter les attaques venant de l'extérieur de leur réseau. Ce genre d'entités disposent tout de même d'un intranet, mais il est cloisonné et ne communique pas avec le monde extérieur. Les recours aux méthodes citées précédemment sont alors inefficaces contre ce genre de cibles. Dans ces conditions, le recours à une autre stratégie est alors nécessaire.
Le *baiting* consiste à infecter intentionnellement un espace de stockage amovible tel qu'une clé USB, CD-ROM, HD portables... Il faut ensuite la laisser en évidence dans un endroit où l'attaquant sait qu'une victime potentielle la trouvera. L'utilisateur lambda aura ensuite tendance à insérer ce support amovible dans son ordinateur qui sera ensuite infecté par le malware. Ne fut-ce que pour vérifier l'identité du propriétaire.
Évidemment, les techniques évoquées précédemment ont un beaucoup plus grand potentiel de réussite si le malware est un zero-day. Cependant, que le malware utilisé soit détectable ou non, il est question ici des méthodes d'ingénierie sociale et non de la qualité du malware utilisé.

2.2.5 Cycle de vie des APTs

Les menaces avancées et persistantes ont des objectifs différents et utilisent des mécanismes différents en fonction de leur cible. Cependant, il est possible de décerner des étapes communes entre les différentes attaques ayant déjà eu lieu.
À titre d'exemple, le schéma suivant représente le cycle de vie d'une attaque APT :

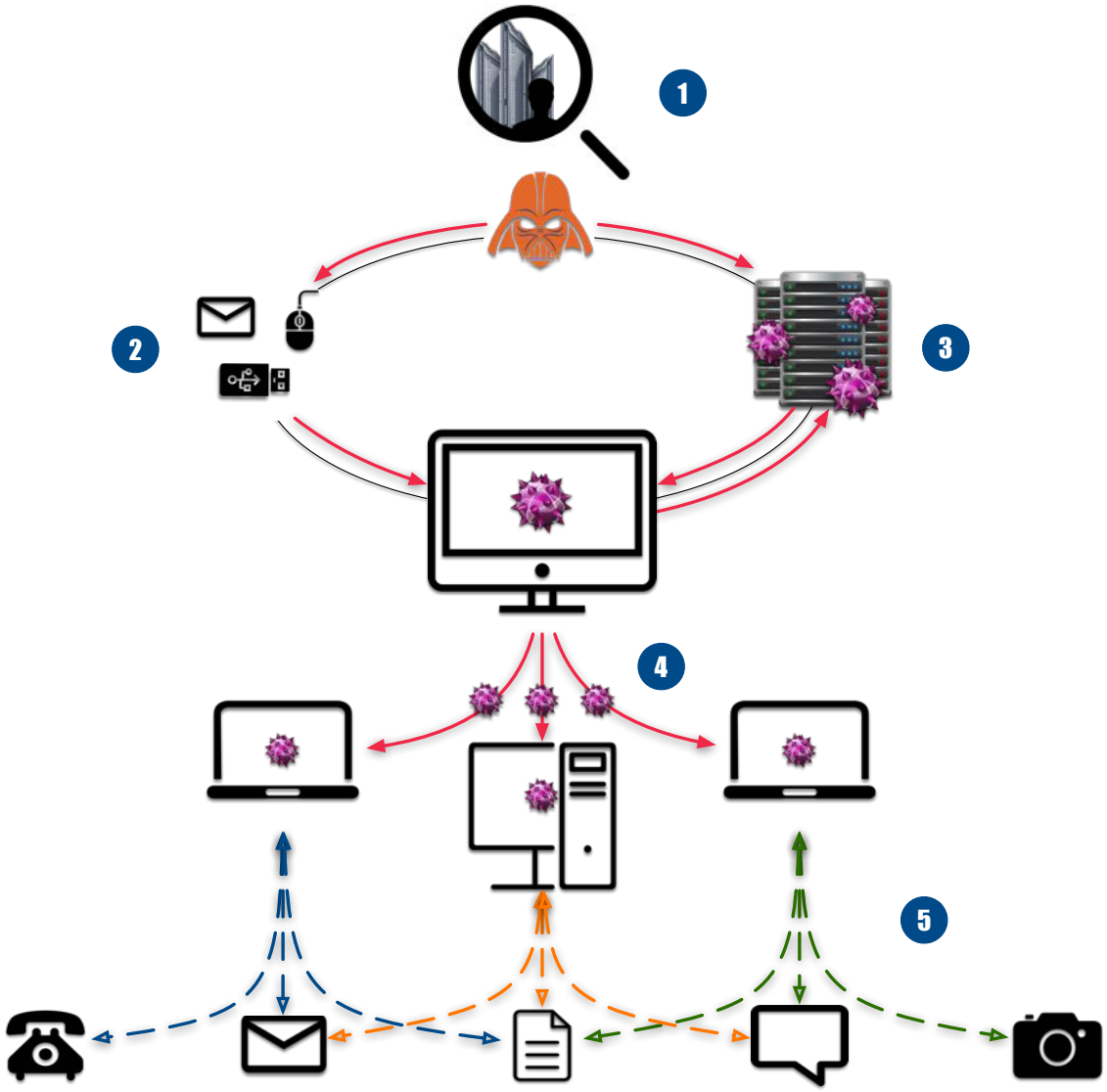


FIGURE 2.2 – Cycle de vie des APTs

Le cycle de vie d'un APT dépend essentiellement du type d'attaque ainsi que de la cible.
Généralement, les grandes étapes par lesquelles les APTs passent, bien qu'elles ne soient pas normalisées, sont les suivantes :

1. Reconnaissance

L'attaquant récolte une variété d'informations sur sa cible afin de comprendre au mieux son fonctionnement et de savoir quelles sont les failles exploitables. Il peut s'agir de repérage physique de l'entité ou de collecte d'informations sur les personnes y travaillant afin de mettre en place une stratégie de social engineering adaptée. Une information utile serait de connaître le modèle de Firewall utilisé. Connaître les systèmes d'exploitation utilisés au sein de l'entité peut également s'avérer utile pour créer un malware adapté.

2. Intrusion

L'attaquant s'introduit dans l'entité cible en utilisant les mécanismes évoqués dans la section 2.2.4. Des backdoors sont généralement utilisées pour cette étape. Ce procédé permet d'accéder à une machine tout en contournant les systèmes de sécurité mis en place. Il n'est donc pas nécessaire de se réintroduire de la même façon que pour la première intrusion.
Bien évidemment, pour garantir la durée de l'attaque, il est crucial que l'infection ne soit pas détectée. Dans le cas contraire, toute l'attaque tombe à l'eau.

3. Command&Control (C&C)

À ce stade, les machines infectées vont prendre contact avec un serveur, à l'extérieur de l'entité. Ce serveur est appelé un serveur C&C. Les machines infectées prennent contact avec ce genre de serveur pour recevoir des instructions. Il peut s'agir de télécharger des données pour l'évolution de l'attaque. L'instruction reçue peut également consister à n'effectuer aucune action pour ne pas être découvert. Il peut s'agir de recevoir des données qui serviront à infecter d'autres machines figurant sur le réseau.

4. Découverte et expansion

Durant cette étape, l'attaque est lente pour éviter d'être repérée. L'attaquant repère les systèmes de sécurité mis en place par l'entité cible, mais cette fois-ci à partir de l'intérieur. Les machines infectées exécutent toujours les ordres reçus des opérateurs (automatiques, virtuels ou humains) C&C tout en restant aussi furtives que possible. Les machines infectées tentent d'infecter d'autres machines pour avoir une meilleure vision logique du réseau et afin de s'assurer de toujours avoir un accès à l'intérieur de l'entreprise. Les attaquants attendent le bon moment pour accomplir l'objectif principal. Les machines infectées sont mises en "veille" (elles ne communiquent plus avec le C&C) jusqu'au moment clé.

5. Accomplissement de l'objectif

À cette étape est accompli l'objectif. Il dépend de la nature de l'APT, mais il peut-être de saboter ou de récupérer des données. Il peut aussi être de rester actif et furtif autant que possible si son but est un espionnage à grande échelle.

2.2.6 Origine des APTs

À cause des ressources non négligeables que sont le temps et l'argent, les APTs ne sont, aujourd'hui en tout cas, pas accessibles aux hackers de base. Non seulement les ressources citées sont un frein pour les hackers débutants, mais les APTs demandent des compétences qui sortent de l'ordinaire.
Les attaques avancées et persistantes sont menées par des hackers travaillant pour le compte d'agences gouvernementales, pour le compte de l'armée ou par le crime organisé.
Les cyberattaques sont classées par l'OTAN dans la déclaration de Lisbonne de 2010 dans la même catégorie que le nucléaire et le terrorisme [1] [2].

2.3 Quelques exemples d'APTs

Dans cette section sont expliqués des exemples d'APTs ayant marqué l'histoire de ces attaques.

2.3.1 Stuxnet

Stuxnet est découvert par Symantec le 13 juillet 2010. Symantec est une des principales sociétés de cybersécurité. Elle fait partie d'une des seules compagnies ayant une vision d'ensemble et en temps réel sur l'internet mondial. Cette opération est possible grâce aux millions de clients dont elle dispose. En effet, les machines de leurs clients leur servent de sonde et permettent d'avoir cette vue d'ensemble. Des milliards de connexions journalières sont effectuées. Un malware y est détecté en moyenne toutes les deux minutes.

Stuxnet apparaît alors à ce moment-là comme un "virus" standard s'attaquant au système d'exploitation Windows. À cet instant, seules 100.000 machines dissimulées à travers le globe sont découvertes comme infectées par le "virus". L'infection est limitée et ciblée. Le malware est baptisé Stuxnet.

Cependant, Stuxnet interpelle, car il paraît tellement difficile à détecter qu'on estime qu'il est présent sur le réseau depuis au moins une année. À partir de ce moment sont lancées les analyses du malware. Les analystes découvrent que quatre failles de type zero-day sont exploitées, ce qui est très peu courant. En temps normal, les malwares se contentent d'exploiter une seule faille.

Début août, les analystes découvrent que Stuxnet cible les machines utilisant un logiciel de gestion d'équipements industriels tel que des chaînes de montage ou des canalisations. Ce logiciel est développé par Siemens. Stuxnet reste jusqu'ici un mystère. Personne ne comprend son utilité. Habituellement, les malwares sont déployés par appât du gain. Dans le cas de Stuxnet, ce n'est pas le cas, ce qui attire l'attention sur les intentions de ses créateurs.

Les analyses et observations continuent lorsque mi-août sont découverts les serveurs permettant au malware de se mettre à jour et se dupliquer. Ces serveurs sont situés au Danemark et en Malaisie. Ces deux serveurs sont alors pris en mains par Symantec pour pouvoir intercepter les communications avec les machines infectées. La source des communications est alors connue. Bien que les machines infectées se situent à travers le globe, 60% des adresses IP se connectant à ces serveurs sont des adresses iraniennes. Les analystes savent alors que Stuxnet cible l'Iran.

1. Source : VITRINE, Antoine, *La guerre inisible*, DOC EN STOCK, 2012, documentaire ARTE, 48 minutes
2. Déclaration de Lisbonne : `http://www.nato.int/cps/fr/natohq/official_texts_68828.htm`

Cependant, peu d'informations sont à leur disposition. Le fait que le malware s'attaque à un logiciel de gestion industriel, que la cible soit l'Iran et que les connexions aboutissent sur des serveurs anonymes sont les seuls éléments de preuve sur l'affaire.

L'enquête Stuxnet atteint le point mort quand le 26 septembre 2010, les autorités nucléaires iraniennes déclarent que leurs installations ont été victimes d'une vaste attaque informatique. Les Iraniens reconnaissent que leur production d'uranium s'est effondrée. C'est le centre nucléaire de Natanz qui a été visé et plus précisément les centrifugeuses qu'il contient. Les centrifugeuses sont des tubes à l'intérieur desquels tournent très rapidement des rotors dont la vitesse doit être contrôlée par ordinateur. La vitesse de rotation doit rester constante. C'est ce procédé qui permet l'enrichissement de l'uranium. Stuxnet s'est donc attaqué aux ordinateurs les contrôlant. La vitesse de rotation a été changée pour qu'elle devienne instable, et fasse exploser les centrifugeuses. L'explosion d'une centrifugeuse a alors déclenché une réaction en chaîne et atteint d'autres centrifugeuses. Des centaines voire un millier de centrifugeuses ont été mises hors d'état de fonctionnement dans une période de temps très brève.

De tels accomplissements ont été possibles, car Stuxnet est resté furtif tout au long de son activité. En effet, il a non seulement endommagé les centrifugeuses, mais a également trafiqué les données que les capteurs envoyaient aux techniciens. Ceux-ci ne se doutaient de rien étant donné que les données qu'ils recevaient étaient supposées être correctes. Rien ne permettait de déterminer l'existence du malware.

Cependant, le plus impressionnant est qu'un malware ait pu s'introduire dans un site déconnecté d'internet tel que la centrale de Natanz. Ce que les attaquants ont fait pour parvenir à infecter cette centrale est qu'ils ont infecté le maximum d'ordinateurs aux alentours de la centrale. Le but était qu'une clé USB infectée se retrouve insérée dans un ordinateur connecté à l'intranet de la centrale. Est-ce que la clé USB ayant servi pour propager le malware a été introduite consciemment dans les systèmes, personne ne le saura jamais. Néanmoins, suite au recours de ce procédé, des entreprises iraniennes n'ayant aucun rapport avec le programme nucléaire ont été touchées. Ces entreprises ont dû, par la suite, dépenser de grandes sommes pour désinfecter leurs infrastructures de Stuxnet.

Selon certaines estimations, Stuxnet aurait fait prendre deux ans de retard à l'Iran dans la fabrication de la bombe.
Les rumeurs et les fuites dans la presse désignent Israël et les États-Unis d'avoir orchestré cette attaque.

2.3.2 Regin

Regin est un outil universel de collecte de données qui est utilisé depuis des années. Ce malware a été observé par Symantec et Kaspersky Lab en automne 2013. Différentes versions du malware ont étés trouvées. La version 1.0 a opéré de 2008 à 2011 et la version 2.0 de 2008 à 2013. Ces dernières avaient pour cible différentes entités.
Regin possède différentes fonctions d'espionnage. Parmi celles-ci, on retrouve l'analyse de trafic et le vol de données. Il est également capable d'effectuer des fonctions particulières sur des cibles précises et d'installer un grand nombre de charges utiles [3] adaptées aux ordinateurs ciblés. Les capacités standard de Regin sont des fonctionnalités communes à un RAT.
On retrouve notamment la capture d'écran ou la prise de contrôle du curseur de souris. Le malware permet également le vol d'information tel que des mots de passe, l'analyse du trafic réseau ou encore la collecte d'information sur l'utilisation du processeur et de la mémoire de la machine infectée. Des charges utiles destinées à des machines ciblées permettent la collecte du trafic de téléphonie mobile ou encore la collecte d'emails.

Regin a infecté différents types d'entités dont les secteurs sont les suivants :
— Hospitalier ;
— Aérien ;
— Énergétique ;
— Recherche ;
— Télécommunications ;
— Internet.

Le graphique suivant représente les infections confirmées de Regin par secteurs :

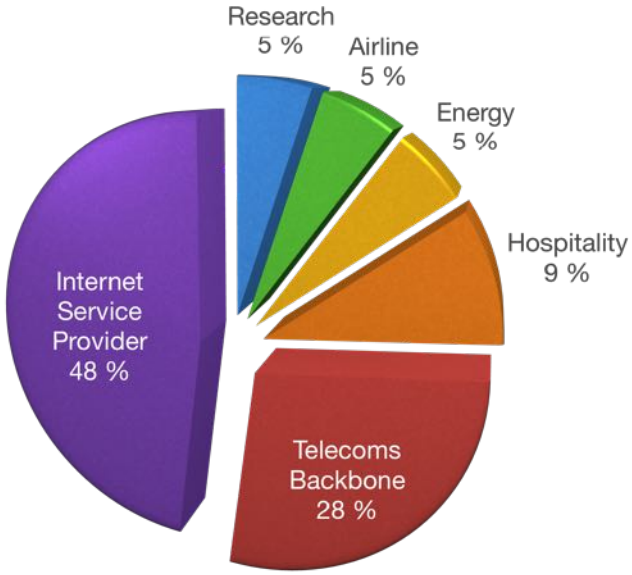


FIGURE 2.3 – Infections confirmées de Regin par secteurs d'après Symantec

3. La charge utile ou payload en anglais, est la partie d'un malware qui contient les fonctions destinées à causer des dommages à l'ordinateur infecté

Regin est une attaque ciblée qui visait différents milieux dans différents pays. L'APT a été jusqu'à infecter la Belgique. Les principaux pays touchés par Regin sont les suivants :
— Le Pakistan ;
— L'Autriche ;
— La Belgique ;
— L'Iran ;
— L'Afghanistan ;
— L'Inde ;
— L'Irlande ;
— Le Mexique ;
— L'Arabie Saoudite ;
— La Russie.

Le graphique suivant représente les infections confirmées de Regin par région :

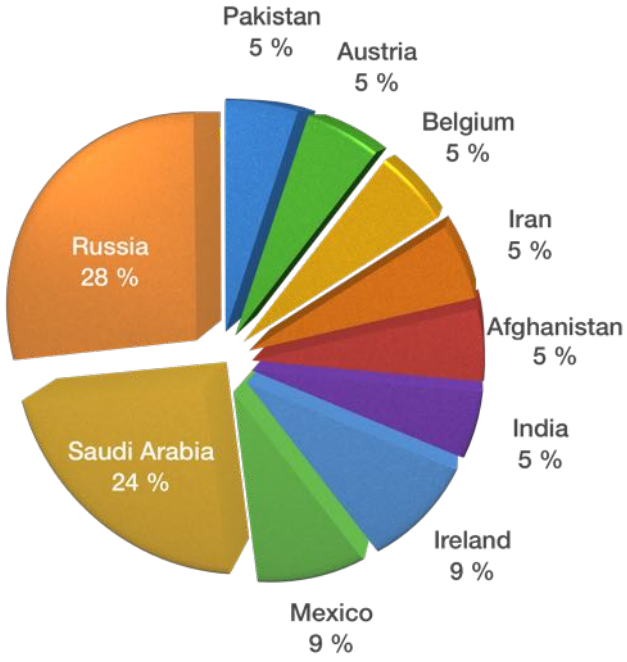


FIGURE 2.4 – Infections confirmées de Regin par région d'après Symantec

En 2013, l'opérateur Belgacom a été détecté comme infecté par Regin. En effet, la société offrant des services de télécommunication ainsi que l'accès à internet s'est vue ciblée par cette attaque. Regin a espionné le trafic des clients de Belgacom. On estime que Regin était capable d'espionner aussi bien le trafic internet que le trafic GSM, que ce soit les appels ou encore les SMS.

Nethys, anciennement Tecteo, semble également avoir été touché par Regin. Certains IoCs fournis par l'institut Belge des services postaux et des télécommunications permettent d'identifier la trace de l'APT. Les IoCs ainsi que l'article de presse se trouvent respectivement en annexe D et E.

D'après les rumeurs, Regin serait l'oeuvre de la NSA et du GCHQ.

3. Les moyens de défense contre les cyber-attaques

3.1 Défense au niveau des endpoints

3.1.1 Les antivirus

Les antivirus sont des logiciels qui permettent d'identifier un malware grâce à des signatures si celui-ci est connu de l'éditeur du logiciel. La plupart des malwares possédant une signature peuvent être stoppés par un logiciel antivirus standard. Cependant pour les malwares inconnus, deux scénarios sont envisageables :

— Le but de l'attaquant est le déploiement de masse de malwares pour toucher le plus de machines possible et ainsi faire le plus de victimes possible. Si aucune signature ne permet de bloquer le malware, toutes les personnes exécutant le malware entre le moment où il est déployé et le moment ou une signature est générée, seront infectées. Les utilisateurs ayant reçu la signature seront avertis par leur antivirus de la nature du fichier. Celui-ci sera alors supprimé ou isolé ;

— Le deuxième scénario est celui d'une attaque ciblée. Le déploiement du malware visera une entité en particulier. Comme le déploiement de masse ne sera pas effectué, il est probable que l'entité cible ne se rende pas compte qu'elle est victime d'une attaque ciblée. Le problème des antivirus est qu'il faut une signature pour détecter les malwares. Pour que cette dernière soit générée, il faut qu'un certain nombre de machines rapportent l'infection. Il est probable que l'infection ne soit détectée que trop tard si la seule sécurité utilisée est l'antivirus. Le malware aura alors eu le temps d'agir avant d'être stoppé par l'antivirus.

Les antivirus sont un bon moyen d'écarter les malwares déjà connus, mais sont inefficaces contre ceux qui n'ont pas de signature.

3.1.2 Next Generation Endpoint Security (NGES)

Un *NGES* est un agent qui assure de manière approfondie la sécurité d'un endpoint. Ce type d'agent est plus complet qu'un antivirus standard. Il n'est en effet pas uniquement défini pour faire de la détection de signature. Cependant, "NGES" est un terme générique et les fonctionnalités apportées sont différentes en fonction des différents agents. Bien qu'un NGES ne doive pas remplir de fonctions particulières pour être considéré comme tel, les fonctions généralement proposées par ce dernier sont les suivantes :

Prévention d'exécutables malveillants

Lors de la découverte d'un malware par un appareil tel qu'une sandbox [1], cette dernière préviendra l'agent afin d'empêcher l'utilisateur d'exécuter le malware. Le poste ne sera alors pas infecté.

Cheminement de fichier (File tracking)

Toutes les actions effectuées sur le système de fichier sont enregistrées. Ce qui permet une résolution d'incident plus rapide lors d'une infection d'un grand nombre de postes. Les machines infectées par le malware seront alors rapidement connues.

Résolution d'incidents plus rapides

En cas d'infection, l'agent permet de mettre le poste en quarantaine. Le but est de l'isoler du réseau pour l'empêcher d'infecter d'autres machines ou des fichiers partagés. La vitesse de résolution d'incident est ici augmentée, car aucune interaction physique n'est requise pour mettre la machine hors du réseau.

3.2 Défense au niveau du réseau

3.2.1 IPS & IDS

3.2.1.1 Les signatures

Les signatures permettent aux systèmes de sécurité les utilisant de savoir si un fichier est considéré comme malveillant. Si la signature se trouve dans le fichier analysé, et que cette dernière réfère un malware, le fichier est considéré comme malveillant. Ce qui est appelé "signature" est une chaîne de caractère unique et incompréhensible par l'homme. Elle peut être reconnue par des logiciels antivirus ou par des IDS/IPS lors de l'analyse d'un fichier. Les systèmes se basant sur la détection par signature sont des systèmes dits "signature-based". La chaîne de caractères suivante est une signature permettant de tester le fonctionnement des antivirus :

X5O !P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE !$H+H*

L'inclusion de cette chaîne de caractères dans n'importe quel fichier le rendra malveillant pour les systèmes de sécurité signature-based.

1. Une sandbox est un appareil effectuant une analyse comportementale. De plus amples informations se trouvent au point 3.4.

Les signatures sont générées à partir du code du malware. Il faut pour cela que le malware ait été découvert. Pour qu'un malware soit découvert, il faut qu'il ait déjà infecté un certain nombre de machines. La problématique des systèmes signature-based est qu'il y a un temps entre lequel le malware est déployé pour infecter des machines, le temps où il est découvert et analysé pour la génération de signature, et le moment où le malware pourra être bloqué par ces systèmes. Une attaque courte et rapide utilisant des malwares auxquels aucune signature n'est attribuée ne peut être stoppée par les systèmes utilisant uniquement les signatures comme source d'information.

3.2.1.2 IDS

Un *IDS* est un composant de la sécurité agissant au niveau du réseau. Il examine le trafic réseau pour détecter l'exploitation d'une faille connue. La détection peut se faire de plusieurs façons, mais les plus répandues sont la détection par signature et la détection d'anomalies. La détection par signature est basée sur un dictionnaire de signature. Ce dictionnaire est mis à jour à chaque découverte de nouveaux malwares. Cet appareil permet uniquement de faire de la détection.

3.2.1.3 IPS

Un *IPS* se trouve généralement derrière un firewall et procure un niveau complémentaire d'analyse du trafic. Contrairement à un IDS, l'IPS permet de bloquer le trafic qu'il détecte comme malveillant. Pour effectuer cette fonction, il est placé en in-line. C'est-à-dire qu'il se trouve directement dans la route entre la source et la destination. L'IPS analyse activement et effectue des actions automatiques sur le trafic réseau. Les principales actions qu'il effectue sont les suivantes :
— Envoi de notification à l'administrateur (tout comme un IDS le fait) ;
— Suppression de données malveillantes ;
— Blocage du trafic malveillant en fonction de l'adresse IP source ou de l'adresse IP destination ;
— Remise à l'état initial de la connexion (TCP RST).

Étant donné son architecture d'implémentation, un appareil de ce genre se doit de travailler efficacement pour ne pas dégrader les performances du réseau.

3.2.2 Firewall & Next Generation Firewall

Un *firewall* est un appareil permettant de contrôler le trafic accepté entre un point d'entrée et un point de sortie d'un réseau. Le trafic est contrôlé en vérifiant que chaque paquet passant par le firewall dispose de l'autorisation pour aller de la source à la destination. Cet appareil agit généralement entre la couche 2 (Data Link) et la couche 4 (Transport) du modèle OSI.
Un Firewall est structuré par règle. Une règle contient plusieurs arguments tels que les suivants :
— Status : exemple : deny ;
— IP source : exemple : 10.0.1.0/24 ;
— PORT source : exemple : 64870 ;
— IP Destination : exemple : 188.213.143.112 ;
— PORT destination : exemple : 22 ;
— PROTOCOL : exemple : TCP.

Cette règle empêche les utilisateurs disposant d'adresses IP entre 10.0.1.1 et 10.0.2.254 d'accéder en SSH (TCP22) à une machine disposant de l'adresse IP 188.213.143.112. La figure 3.1 représente cette règle.

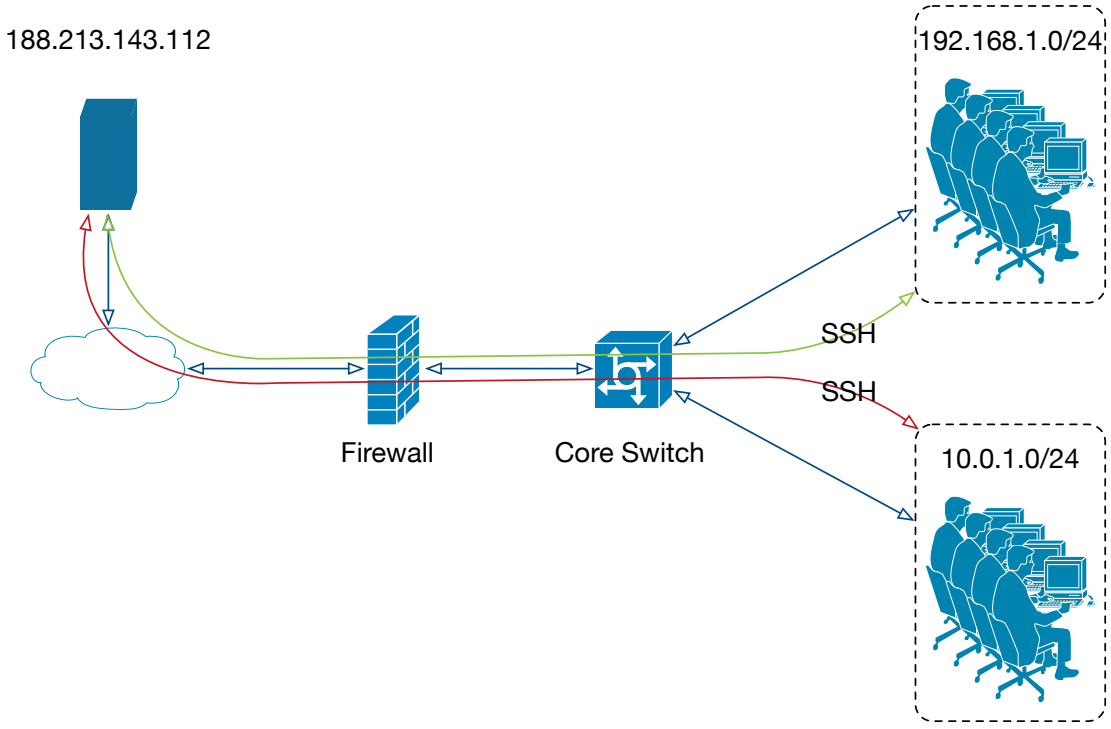


FIGURE 3.1 – Exemple d'utilisation de Firewall

Les seuls utilisateurs concernés par cette règle étant ceux du réseau 10.0.1.0/24, les autres utilisateurs pourront accéder au serveur 188.213.143.112 en SSH(TCP22).
Un firewall permet de remplir d'autres fonctionnalités. Elles sont les suivantes :
— Le NAT (Network Address Translation) ;
— Le PAT (Port Address Translation) ;
— Le VPN (Virtual Private Network).

NGFW

Le terme *NGFW* est générique et est différent pour chaque vendeur. Cependant, généralement, ce qui est décrit comme NGFW permet d'effectuer les opérations suivantes :
— Fonctions d'un firewall standard ;
— IDS/IPS ;
— Decryption SSL/SSH ;
— Inspection approfondie de paquets ;
— Détection de malwares en foncions de leur signature.

3.2.3 Comparaison d'IDS/IPS à un Firewall

Un firewall est un appareil basé sur des règles qu'il applique sur des adresses IPs. Un IDS/IPS est un système basé sur des signatures et/ou sur le comportement. D'une manière logique, on peut dire que ces appareils effectuent un travail à des niveaux différents. Si nous reprenons la figure 3.1, le firewall va se contenter de restreindre l'accès aux machines . Un IPS va inspecter le contenu du trafic entre deux machines. Un IPS permettra donc par exemple d'empêcher le téléchargement d'un malware. Un firewall standard (donc pas un NGFW), ne pourra effectuer ce travail, car il se contente de vérifier que les deux machines ont le droit de communiquer en utilisant certains protocoles.
Les NGFW offrent des fonctions IPS/ IDS. À titre d'exemple, Palo Alto en temps que NGFW, offre des modules IDS/IPS.

3.2.4 Email Security Appliance (ESA) / Email Security Gateway

Un *ESA* ou, email gateway, est un appareil permettant de filtrer le trafic email. Cet appareil effectue généralement les fonctions suivantes :
— Antispam ;
— Antiphishing ;
— Antimalware.
Cet appareil permet également de trier les emails sur les politiques de l'entité qui l'utilise. En d'autres termes, si la politique définit que les mails contenant des fichiers exécutables ne sont pas autorisés, cet appareil permettra de traiter ces emails.
Les emails détectés comme malveillants ou ne respectant pas la politique mise en place sont mis en quarantaine ou bloqués. Ce procédé a pour but de diminuer le nombre d'emails malveillants reçus et donc de diminuer le vol d'informations sensibles dû au phishing ou d'autres méthodes d'ingénierie sociale.

3.2.5 Web Security Appliance (WSA) / Secure Web Gateway

Un Secure Web Gateway protège des machines d'infections en provenance du web. Il permet également d'appliquer les politiques de l'entité l'utilisant. En d'autres termes, un Secure Web Gateway est un appareil qui filtre le trafic web des utilisateurs pour réduire le nombre de malwares téléchargés en provenance du web.
Les fonctions effectuées par cet appareil sont les suivantes :
— Filtrage d'URL ;
— Détection et filtrage de code malveillant ;
— Contrôle d'applications populaires basées web (exemple : la messagerie instantanée ou Skype) (Cette fonction peut également être réalisée par un WAF).

3.3 Supervision de la sécurité

La plupart des appareils de sécurité génèrent des alertes sur une console qui leur est propre. Cependant si l'entreprise dispose d'une dizaine de ces appareils, il n'est pas envisageable que celle-ci dispose d'une dizaine de consoles. En effet, il n'est pas financièrement intéressant de placer un opérateur derrière chaque console à l'affût d'une alerte. Des solutions SIEM (Security Information and Event Management) ont alors étés inventées pour remédier à ce souci.

3.3.1 Le SIEM (Security Information and Event Management)

Un *SIEM* est un système qui permet de récolter et de corréler des logs. En effet, il permet, grâce à son moteur de corrélation, de relier plusieurs éléments à une même cause.
Les SIEMs effectuent les fonctions suivantes :
— La collecte ;
— L'agrégation ;
— La normalisation ;
— La corrélation ;
— Le reporting ;
— L'archivage ;
— Le rejeu des événements.
Ce système permet à une entité de centraliser ses logs. Les logs sont des messages d'informations qui sont générés lors d'un comportement inhabituel ou lors d'erreur système. Les logs viennent de beaucoup de différentes sources. Il peut s'agir d'appareils réseau, de serveurs, de postes de travail, etc. La collecte des logs permet à un ou plusieurs opérateurs d'avoir une vue d'ensemble et centralisée des activités du réseau. Le fait de les centraliser permet une gestion des événements plus rapide et centralisée. Cela permet aussi de se conformer aux exigences légales pour la rétention des logs (à titre d'exemple, un an pour le secteur des télécommunications).

3.3.2 Le SOC

Le *SOC* a pour mission de traiter les alertes générées par des solutions SIEM mais également de gérer des alertes qui seraient données par des utilisateurs, par des équipes techniques, etc. Les opérateurs ont un profil correspondant à celui d'un analyste en cybersécurité. Ils comprennent différentes technologies et sont au courant des actualités. L'opérateur doit être capable de déterminer quelles sont les alertes critiques et quelles sont les alertes mineures. Il doit surtout pouvoir résoudre les incidents le plus rapidement possible en concert avec les équipes techniques.

3.4 Le principe de sandboxing

Les systèmes évoqués précédemment permettent de bloquer des adresses IP ou encore des malwares connus. Cependant, aucun système ne permet, à proprement dit, de détecter un nouveau malware. Dans le cas d'une attaque ciblée et persistante, l'utilisation de vulnérabilités inconnues et/ou non corrigées est courante. L'utilisation de ces vulnérabilités permet de contourner la plupart des systèmes de sécurité.

Le mécanise de sandboxing permet d'apporter cette fonction manquante. Une *sandbox* est en fait un environnement cloisonné et surveillé. Dans cet environnement sont envoyés les fichiers suspects pour une analyse dynamique. Cette analyse rapporte les actions effectuées par le fichier.
Dans un environnement Windows, une sandbox relativement complète permet d'analyser les facteurs suivants :

Les librairies

L'analyse des librairies a pour but de faire la corrélation entre les librairies utilisées. Dans le cas d'un ransonware, des librairies de chiffrement doivent être utilisées. Ce qui peut éveiller un soupçon de la part de la sandbox.

Le système de fichier

Toute l'activité du système de fichier c'est-à-dire les créations, modifications ou encore suppressions de fichiers sont enregistrées. Le but de cette analyse est de pouvoir détecter différents aspects. Le premier est la modification ou suppression de fichiers appartenant au système, ce qui est considéré comme suspect. Le second est de pouvoir détecter la duplication du fichier. Les malwares se dupliquent afin de garantir la persistance. Un autre intérêt est de pouvoir détecter si le fichier essaye d'accéder à certains types de fichiers. Ces fichiers dont l'accès permet d'avoir des soupçons sont les suivants :

— L'accès à des fichiers contenant des informations bancaires indique s'il s'agit d'un vol d'information, le fichier est donc malveillant ;
— La vérification de l'existence de fichier se trouvant uniquement sur des environnements virtualisés. Ces fichiers sont soit des fichiers de configuration, soit des drivers. Ce procédé permet aux malwares testant leur existence de savoir s'ils sont dans un environnement virtualisé. Cette détection peut permettre aux malwares de ne s'exécuter que s'ils se trouvent uniquement sur des machines physiques. Le procédé a pour but de "s'évader" de la sandbox.

La registry

Les opérations effectuées sur la registry, la création, modification et suppression de clés de registre sont enregistrées. L'intérêt est de pouvoir détecter deux actions différentes. La première est de détecter la modification de la registry pour établir la persistance et éviter la détection. La seconde est de pouvoir détecter la modification de clé de registre pour que le malware se lance automatiquement au démarrage de la machine ou sous certains critères.

Les processus

L'observation des processus permet d'avoir une vue d'ensemble sur tous les processus lancés par le fichier ainsi que sur l'interaction des processus lancés par le fichier avec ceux existants sur la machine. Un fichier sera considéré comme malveillant s'il injecte du code dans un autre processus. L'API Windows fournit certaines fonctions pour injecter du code telles que CreateRemoteThread(), WriteProcessMemory(), LoadLibrary(), et SetWindowsHookEx(). Malgré le fait que ces fonctions peuvent être utilisées par des applications légitimes, ce procédé est généralement utilisé par les malwares pour exécuter une attaque à travers un processus de confiance afin d'éviter la détection de l'attaque. L'observation des processus permet également de détecter un processus se plongeant dans un sleep d'une longue période. Ce qui est une action suspecte, car elle constitue un mécanisme d'évasion.

Les mutex

Les *mutex* (MUTual EXclusion) sont des objets de programmation qui permettent à plusieurs threads d'accéder à une ressource partagée sans risques. Les noms des mutex légitimes sont longs et incluent un identificateur unique tels qu'un GUID (Global Unique IDentifier) ou un URI (Uniform Ressource Identifier). Souvent les noms de mutex utilisés par les malwares sont plus courts et dans certains cas ils sont réutilisés à travers différents spécimens de la même famille de malware. Ces informations permettent de soupçonner un fichier d'être un malware.

Le réseau

Le réseau est analysé, car un malware peut faire des requêtes vers un serveur distant pour télécharger du code ou des fichiers malveillants. De plus, les requêtes DNS, ou HTTP vers des domaines réputés comme malveillants rendent le fichier suspect. Le but d'un APT étant de s'infiltrer et de persister, l'infection d'autres machines se trouvant sur le réseau peut garantir la persistance de l'attaque. Évidemment, ce procédé ne marche que si la propagation de l'infection n'est pas découverte.

Dans le cycle de vie des APTs on retrouve la découverte du réseau. L'étape après l'infection est la découverte, c'est donc à ce moment que le malware essayera de scanner le réseau pour découvrir les machines qui s'y trouvent. Un fichier essayant de réaliser ce procédé est bien sûr considéré comme malveillant.

Les signatures

Des règles Yara permettent de matcher des patterns textuels ou binaires. Ces règles permettent en d'autres termes d'identifier des signatures ou du texte généralement malveillant et utilisé par les malwares. Ces règles permettent d'identifier des malwares.

Sur base des éléments précédents et sur les actions qui sont réalisées lors de l'analyse du fichier, ce dernier est considéré comme malveillant, suspect, ou sans risque. Bien évidemment, certains critères ont plus d'importance que d'autres, mais cela dépend de la sandbox et de l'interprétation qu'elle en fait. Pour récapituler, la sandbox est un environnement permettant de catégoriser un fichier qui y est envoyé en fonction des actions qu'il y réalise.

3.4.1 Différents types de sandbox

Il existe différents types de sandbox. Elles ont toutes un objectif de sécurité, mais elles effectuent des tâches différentes. On retrouve les sandbox suivantes :
— La sandbox de cloisonnement de ressources ;
— La sandbox de détection et d'analyse.
Bien que les deux types de sandbox évoqués précédemment soient utilisés dans le domaine de la sécurité, ces environnements n'effectuent en rien les mêmes actions.

De manière plus détaillée, voici les fonctions remplies par ses sandbox :

La sandbox de cloisonnement de ressources

Ces sandbox se trouvent généralement dans certains systèmes d'exploitation tels qu'OS X (MacOS) ou à l'exécution de code Java. Ce genre de sandbox, permet de cloisonner un logiciel et ainsi donc lui restreindre l'accès aux ressources dont il a uniquement besoin. Par exemple, une calculatrice légitime ne devrait pas avoir besoin d'accéder au réseau, à une liste de contact ou encore moins au système de fichier.

La sandbox de détection et d'analyse

Cet environnement permet de faire de l'analyse dynamique. L'analyse dynamique consiste à exécuter un élément dans un environnement cloisonné et à observer ses actions sur différents éléments du système d'exploitation. On retrouve cependant plusieurs concepts de sandbox différents. Certaines sandbox sont basées sur de la virtualisation tandis que d'autres se basent sur de l'émulation.

Emulation

Un émulateur est un logiciel permettant de simuler la fonctionnalité d'un autre programme ou la présence de matériel physique. Par exemple, considérons un programme exécuté dans un environnement dont l'hardware est émulé. Quand ce programme sera exécuté, l'émulateur pourra collecter des informations très détaillées sur l'exécution du programme en question. Le programme pourrait ne pas être écrit pour pouvoir s'exécuter sur le CPU sur lequel tourne l'émulateur, mais il pourra être exécuté dans l'environnement émulé. Un exemple serait une application Android écrite pour un processeur ARM. Un émulateur s'exécutant dans un environnement x86 n'empêcherait pas l'application d'être exécutée dans l'émulateur. L'inconvénient d'un émulateur est qu'il est plus facilement reconnaissable qu'une machine virtuelle. Les malwares ont donc plus de facilités à détecter qu'ils sont exécutés dans une sandbox.

Virtualisation

Avec la virtualisation, un programme tourne sur des ressources réellement allouées. L'hyperviseur, le programme de virtualisation, permet juste de contrôler les machines virtuelles et leurs accès au hardware. Dans cet environnement, les machines virtuelles sont indépendantes et isolées les unes des autres. Cependant, quand un programme est exécuté, les ressources sont réellement attribuées. Ce procédé empêche l'hyperviseur et le système d'analyse de malware de fonctionner simultanément. Ce qui rend par conséquent complexe la collecte de données précises. De plus, il est difficile de cacher entièrement la présence d'un environnement virtualisé aux malwares. L'avantage est que les exécutions de programmes dans les machines virtuelles peuvent se faire à vitesse native.

3.4.2 Mécanismes d'évasion de sandbox

Les malwares avancés utilisent des techniques pour éviter de se faire repérer par les sandbox. Ces techniques sont appelées des mécanismes d'évasion. La partie malveillante du malware reste identique aux malwares standards. La différence se trouve au moment de l'exécution. Un malware standard va s'exécuter sans aucune condition, tandis qu'un malware évasif ne va s'exécuter que sous certaines conditions. Ces conditions permettent à un malware de se faufiler à travers les sandbox.

À titre d'exemple, considérons la figure 3.2 :

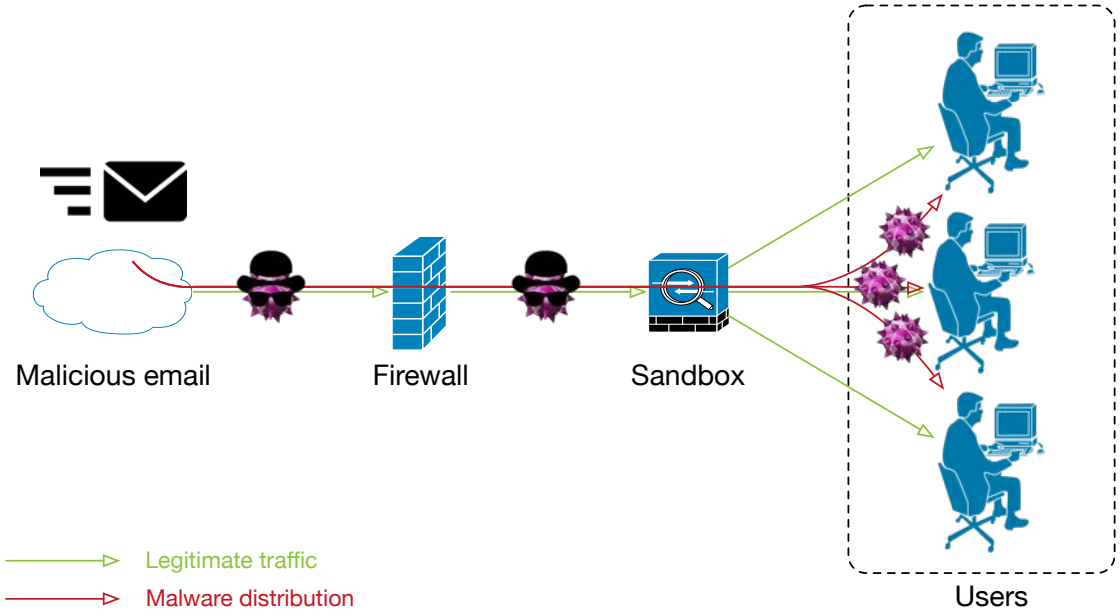


FIGURE 3.2 – Schéma logique de la réception d'un email malveillant

Dans la figure 3.2, un email malveillant est envoyé à tous les utilisateurs de l'entité ciblée. Cet email contient un malware exploitant une faille de type zero-day. Il ne possède pas de signature et ne peut être bloqué par un firewall ou un IPS.

Le malware est donc analysé par la sandbox. Dans la sandbox sont analysées les actions du malware. Cependant, si ce dernier contient un mécanisme d'évasion de sandbox et qu'il parvient à détecter qu'il s'exécute dans une sandbox, le malware ne déclenchera pas l'exécution du code malveillant. Une fois évadé de la sandbox, le malware se retrouve sur les postes utilisateurs. Si les utilisateurs ayant reçu l'email exécutent le malware, celui-ci ne sera pas stoppé.

L'évasion de sandbox peut se faire de façons différentes. Parmi les mécanismes utilisés on retrouve les suivants :

— Comportement humain (déplacement de curseur, scroll, frappe au clavier) ;
— Endormissement (Sleep) (exemple : sleep d'une longue période, ou sleep jusqu'au 25 avril 2017) ;
— Déclenchement uniquement en présence d'un programme ou d'un fichier spécifique (exemple : déclenchement uniquement si la machine dispose du programme de gestion de centrifugeuses dans le cadre de l'attaque Stuxnet) ;
— Détection des drivers des cartes réseau ainsi que leur nom (exemple : vmnet0, vboxnet0) ;
— Détection du nombre de cœurs dont dispose le processeur de la machine infectée (exemple : si la machine ne dispose que d'un seul cœur, ce qui est rare sauf en cas de virtualisation, donc d'éventuel sandboxing).

Comportement humain

Un malware peut se baser sur les interactions qu'effectue généralement un humain pour détecter une sandbox. Le comportement sur lequel un malware se base est le comportement normal d'un utilisateur lorsqu'il utilise sa machine. Les actions effectuées par un comportement traditionnel sont les suivantes :

— L'utilisation de la souris ;
— Le scroll de souris ;
— L'utilisation du clavier ;
— Le lancement, fermeture de programmes ;
— La suppression de fichiers ;
— Interaction avec les alertes reçues ;
— etc.

Endormissement (Sleep)

Le but du malware étant de ne pas se faire repérer par la sandbox, il va "s'endormir" le temps de l'analyse. Si le sleep est plus long que le temps d'analyse, la sandbox pourrait ne pas détecter le malware.

Présence de fichier ou de programme

Un malware peut rechercher l'existence d'un fichier ou d'un programme en particulier avant de lancer son exécution malveillante. L'intérêt est de cibler des machines en particulier. De plus, si la sandbox n'est pas customisable, c'est-à-dire que l'entité qui s'en équipe ne peut y installer de logiciels, un malware pourrait contourner la détection.

Dans le cadre d'une attaque ciblée, une sandbox n'étant pas customisable ne permettrait pas de savoir exactement le contenu d'un fichier vérifiant l'existence d'un programme. La seule déduction que la sandbox pourrait être que le fichier analysé vérifie l'existence d'une application.

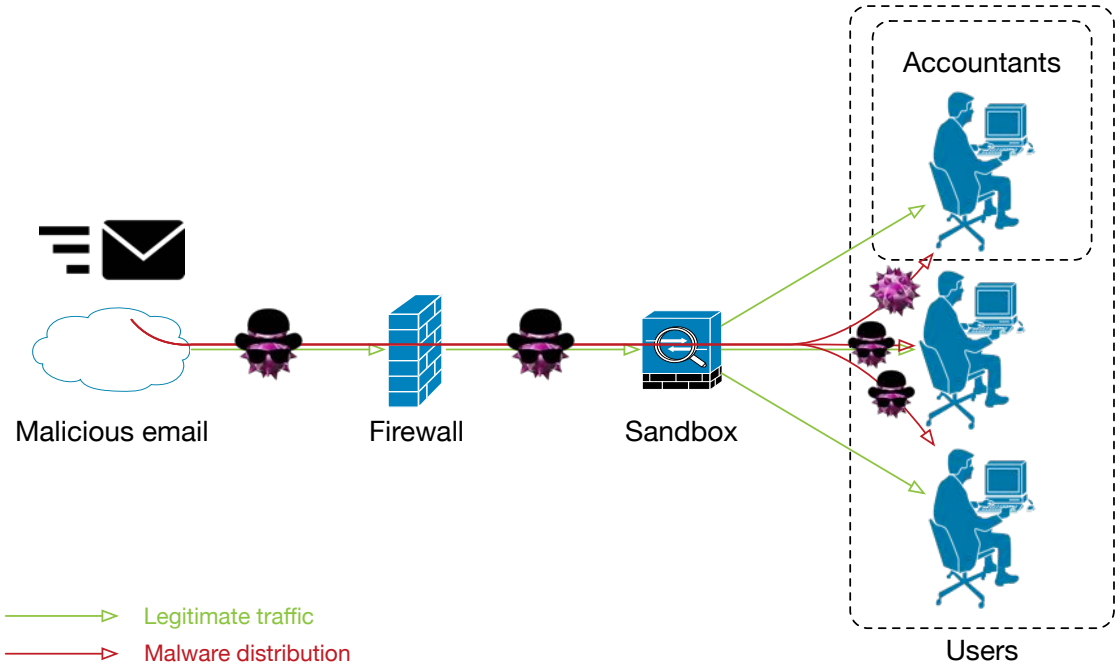


FIGURE 3.3 – Schéma logique de la réception d'un email contenant un malware ciblant les programmes utilisés par les comptables

À titre d'exemple, considérons la figure 3.3. Le contexte est le suivant : dans cette figure est représentée une zone "comptables". Les comptables de la société utilisent un logiciel comptable tel que BOB ou Winbooks. La sandbox quant à elle dispose de Windows7 avec uniquement quelques programmes de base installés tels que Microsoft Office, Adobe Acrobat Reader et Flash.

Dans cet exemple, le verdict du fichier analysé (ici notre malware déguisé) par la sandbox sera qu'il vérifie l'existence d'une application. Cette action sera peut-être considérée comme suspecte, mais le malware ne sera pas découvert.

Ensuite, le malware ne se "réveillera" que sur les postes dont BOB ou Winbooks sont installés. Les utilisateurs n'étant pas comptables seront infectés, mais le malware ne fera ni de dégâts ni de vol de données, ni quoi que ce soit étant donné que BOB ou Winbooks ne sont pas installés.

L'infection étant faite, le malware peut continuer son cycle de vie. Dans le cas d'un APT, le malware va rester tant indétecté que possible pendant une certaine période. Il passera ensuite à l'étape suivante du cycle de vie d'un APT, à savoir le C&C.

Dans cet exemple, l'infection n'a pu être empêchée.

Détection des drivers

Un malware peut également se baser sur le matériel dont dispose la machine sur laquelle il est exécuté. Il peut par exemple se baser sur l'adresse physique(MAC) de la carte réseau de la machine. Une adresse ayant comme OUI $08-00-27$ est une adresse physique donnée par VirtualBox. Ceci indique au malware qu'il se trouve sur une machine virtuelle et non sur une machine physique. Il peut alors supposer être exécuté dans une sandbox. Il n'exécutera donc pas la partie malveillante de son code.

Détection du processeur

Dans la même optique que le point dernier, un malware peut vérifier le nombre de cœurs dont dispose la machine sur laquelle il s'exécute. Les machines virtuelles ont rarement autant de cœurs attribués que des machines physiques. Une machine ne disposant que d'un seul cœur pourrait indiquer au malware qu'il s'exécute dans une machine virtuelle et éventuellement dans une sandbox.

Données existantes sur la machine

On pourrait facilement imaginer un malware faisant une observation des dossiers utilisateur sur la machine sur laquelle il tourne. N'importe quel utilisateur dispose de fichiers sur sa machine, ce qui paraît logique. Une machine ne disposant que d'un OS fraîchement installé ainsi que de deux ou trois programmes supplémentaires, pourrait être considérée comme une sandbox par le malware. La taille du disque, la résolution d'écran, les icônes présent sur le bureau ainsi que les fichiers récemment ouverts permettent également de deviner que l'environnement est une sandbox. Le malware n'exécutera donc pas la partie malveillante de son code sur cette machine.

Bien entendu, la combinaison de ces techniques rend la détection de malwares encore plus complexe pour les sandboxs. Il est certain qu'une attaque ciblée et persistante utilisant un malware comme facteur d'infection utilisera ces mécanismes d'évasion.

Il existe certainement beaucoup d'autres mécanismes d'évasion que ceux évoqués précédemment. L'utilisation de ces mécanismes complique la construction d'une sandbox. Bien entendu, une sandbox, comme aucun autre système de sécurité ne permet pas de garantir à 100% la sécurité d'une entité. Malgré cela, les sandbox de nouvelle génération permettent de lutter au mieux contre des mécanismes d'évasion. Ces dernières réalisent des interactions avec l'OS et se rapprochent tant que possible d'une machine existante pour lutter contre l'évasion de sandboxs.

3.5 Les différentes architectures du sandboxing

Il existe différentes solutions pour implémenter le sandboxing. Les solutions suivantes sont des solutions déployées sur le site de l'entité s'équipant de sandbox. Il existe cependant des solutions basées Cloud. Ce type de déploiement se fait de manière identique à l'exception que la sandbox ne se trouve pas sur site, mais chez le fabricant.
Ci-dessous sont schématisées des solutions utilisant le sandboxing dans le but de se protéger, et de remédier autant que possible aux APTs. Les schémas représentent des déploiements idéaux. Étant idéaux, le sandboxing est "couplé" à d'autres appareils de sécurité tels que des Firewalls ou des NGES.

3.5.1 Blocage via Firewall + endpoints

Cette première architecture représentée dans la figure 3.4 consiste à déployer le sandboxing au niveau du TAP de l'entité. Évidemment, tout le trafic entrant ou sortant de l'entreprise doit passer par la sandbox. Il est primordial, dans l'usage de sandbox contre les APTs, que cette dernière soit en capacité d'analyser tout le trafic de l'entité. Sinon un APT n'aura qu'à utiliser le chemin non analysé par la sandbox pour s'infiltrer dans une entité.
L'architecture représentée dans la figure 3.4 ne perturbe pas le flux réseau étant donné qu'elle n'est pas implémentée en mode in-line. Elle ne rajoute donc pas un élément un flux réseau. Ce que la solution reçoit comme données est en fait une copie des données directement reçues par le client.

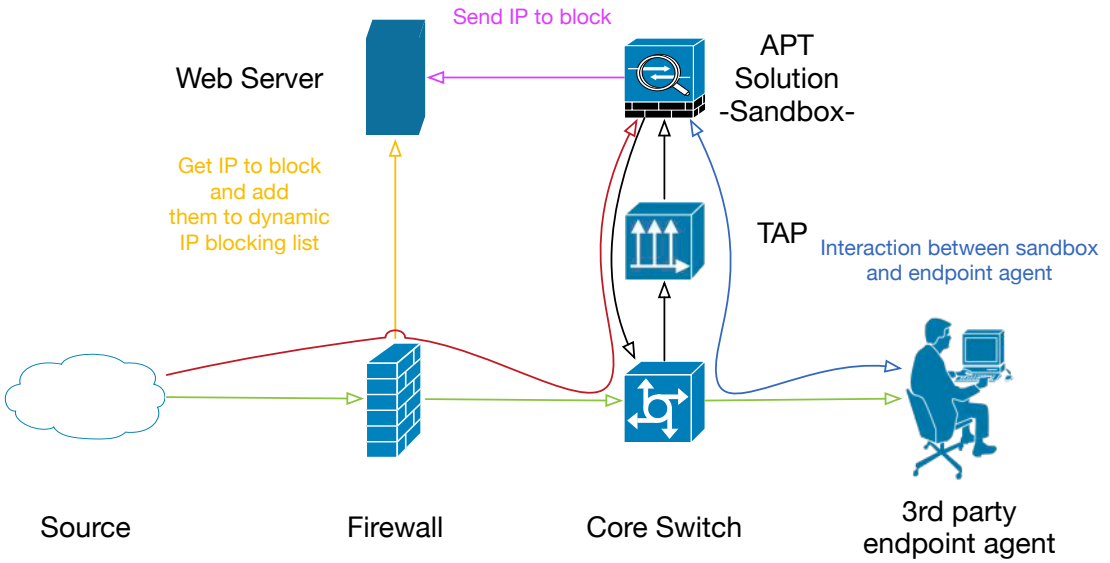


FIGURE 3.4 – Architecture d'une solution in-line distribuée

Blocage

Le blocage de ce genre d'implémentation de sandbox est assez limité. En effet généralement ces solutions sont configuration en MTA pour le traitement du trafic email et permettent de faire un TCP RST pour l'analyse du flux réseau global. Le TCP RST est un moyen de blocage assez limité. Il permet d'envoyer un paquet IP marqué comme TCP RST, ce qui a pour effet de réinitialiser la connexion entre le client et le serveur. Dans ce cas, le téléchargement du malware est interrompu.

MTA

En configurant la solution comme *MTA*, les mails seront filtrés. L'avantage est qu'un retard de quelques minutes sur un email ne perturbe pas le business. Les quelques minutes de retard sont dues au temps de l'analyse de la sandbox. Sur base du résultat de l'analyse, le mail sera soit transféré soit supprimé. Ce procédé permet de traiter le vecteur email séparément du reste du trafic. D'une manière logique, on peut considérer la solution comme étant in-line au niveau du flux email. Cependant, le reste du trafic ne peut subir une latence de plusieurs minutes. C'est pourquoi il doit être bloqué différemment. Plusieurs solutions sont possibles. Elles sont les suivantes :

TCP RST

Étant connecté au TAP et n'étant pas en in-line, la sandbox ne reçoit que des copies de données qui sont envoyées aux utilisateurs. Deux scénarios sont dès lors possibles :

— Soit le fichier envoyé est connu de la sandbox. Elle ne doit pas alors l'analyser et peut envoyer un paquet TCP RST pour bloquer la connexion, ce qui est correct au niveau du délai de bocage ;
— Soit le fichier est inconnu de la sandbox. Le fichier est alors analysé en quelques minutes. Cependant, quelques secondes suffisent pour que l'utilisateur exécute le malware qu'il vient de télécharger. Le paquet TCP RST pourrait alors arriver bien trop tard. Dans ce cas, le blocage ne serait pas possible.

Endpoints

Dans le cas où l'analyse révèle que le fichier est un malware, la sandbox n'a plus la possibilité de le bloquer. C'est ici qu'est l'importance des agents. Les agents vont pouvoir empêcher tous les postes d'exécuter le malware. Évidemment les postes en question sont ceux qui exécutent l'agent. Deux solutions sont possibles pour le blocage grâce à l'agent. Elles sont les suivantes :

— Soit le mécanisme est fait automatiquement grâce à la communication entre la sandbox et les agents ;
— Soit la sandbox va se contenter de générer une alerte qui nécessitera une action humaine pour isoler et désinfecter le patient zéro [2].

Firewall

L'utilisation du firewall permettra de bloquer la source d'infection venant de l'extérieur du réseau. Si nous reprenons exemple sur la figure 3.4, la sandbox va pusher une liste d'IP à bloquer sur un serveur web. Ce serveur web ne sert que de rebond entre la sandbox et le firewall. Le firewall va ensuite créer une liste dynamique d'adresses IP à bloquer. La source de cette liste sera récupérée sur le serveur web servant de rebond.

De manière plus globale, l'implémentation d'une solution avec cette architecture dispose des avantages et des inconvénients suivants :

Avantages

— Blocage des emails via fonction MTA qui est un moyen de filtrage email correct ;
— Ne demande pas l'arrêt du réseau de production pour être déployé ;
— N'ajoute pas de temps de latence au trafic réseau ;
— Facilement intégrable à un environnement disposant déjà d'appareils de sécurité.

2. Le patient zéro est la première machine à être infectée par le malware.

Inconvénients

— La solution réseau, c'est-à-dire la sandbox, ne peut faire de blocage correct sans agent endpoint, car la fonctionnalité de blocage en temps réel (TCP RST) dépend de l'analyse qui peut prendre jusqu'à plusieurs minutes. Le TCP RST ne peut se faire que pendant la durée de la connexion TCP. Une fois ce délai dépassé, le TCP RST est inutilisable. Si le temps d'analyse est supérieur au temps de la connexion TCP, le blocage ne peut plus se faire via TCP RST ;
— Nécessite l'intégration à un firewall compatible pour le blocage d'adresses IPs.

3.5.2 Blocage via solution en mode in-line

Il peut s'agir d'un appareil rajouté dans le trafic réseau ou tout simplement d'une licence activée sur un appareil possédant la fonction de sandboxing ou l'équivalent.
Deux possibilités sont envisageables avec cette architecture. Elles sont les suivantes :
— Soit l'appareil effectue lui même le sandboxing ;
— Soit l'appareil a une fonction qui ressemble plus à celle d'une sonde.

Dans le cas d'une "sonde"

Les sondes permettent d'envoyer les fichiers à analyser à des sandbox situées soit sur site, soit dans le cloud du fournisseur. En ce qui concerne l'analyse, le scénario est comparable à celui d'une architecture TAP. Généralement, les NGFW et les NGIPS/NGIDS permettent de remplir cette fonction.

Blocage

Les méthodes de blocage sont assez similaires que pour l'architecture TAP. On retrouve le blocage par TCP RST, Firewall, Endpoints. En ce qui concerne le blocage par firewall, un serveur web de rebond tel que dans la figure 3.4 n'est plus nécessaire étant donné que la sandbox communique directement avec le NGFW.

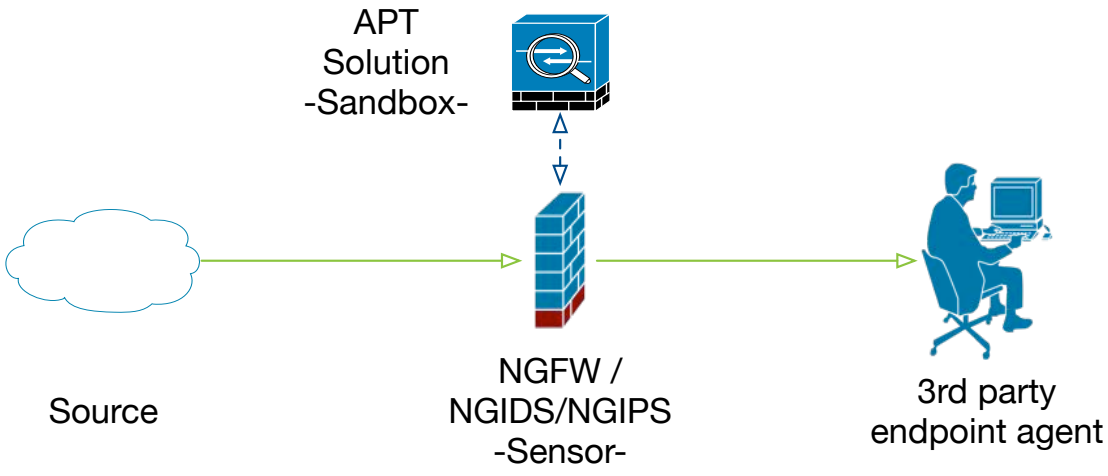


FIGURE 3.5 – Architecture d'une solution in-line - Sensor

Les avantages et inconvénients d'une telle architecture sont semblables à une architecture TAP.

Dans le cas d'une sandbox

Cette architecture semble comporter des inconvénients que d'autres architectures n'ont pas. À commencer par le fait que dans ce type d'architecture, la sandbox est un single point of failure. C'est-à-dire que si la sandbox venait à ne plus être opérationnelle, tout le réseau serait arrêté. Pour y remédier :

— Soit la solution doit intégrer de la redondance, c'est-à-dire plusieurs systèmes de sandboxing ;
— Soit la solution doit être intégrée à un réseau de haute disponibilité.

De plus, le mode in-line demande une capacité de traiter un débit plus important que celui du TAP. En effet, la sandbox doit être capable de traiter un débit égal à celui du firewall.

Blocage

Dans le cas d'une implémentation de ce type, le blocage de malwares connus peut se faire directement au niveau de la sandbox. Cependant au niveau des malwares inconnus, le problème reste le même que celui d'une architecture TAP.
Contrairement au flux mail, le flux web ne peut être ralenti. Le risque d'infection entre le début de l'analyse du fichier et celui où la sandbox rend son verdict reste le même que pour une architecture TAP. La solution nécessite toujours des agents pour remédier à ce délai pendant lequel un utilisateur peut exécuter un fichier malveillant dont le résultat de l'analyse n'est pas encore connu.

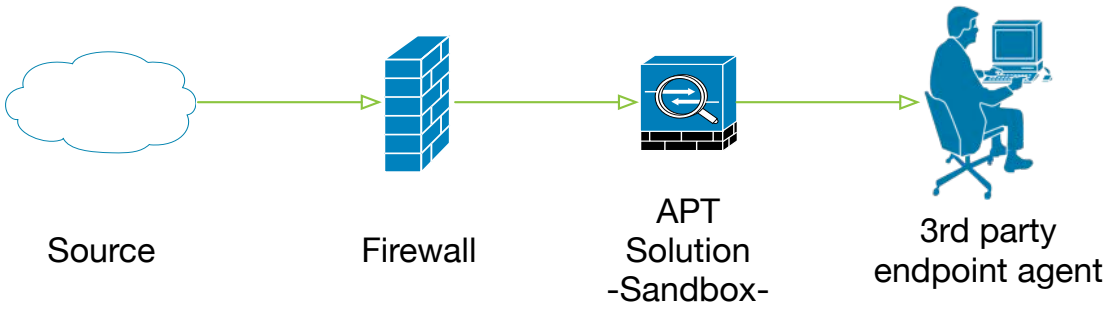


FIGURE 3.6 – Architecture d'une solution in-line - Sandbox

De manière plus globale, l'implémentation d'une solution avec cette architecture dispose des avantages et des inconvénients suivants :

Avantages

— Blocage de malwares connus sans TCP RST.

Inconvénients

— Si cette architecture nécessite le déploiement d'un nouvel appareil monté en in-line sur le flux réseau, la solution ajoute un temps de latence ;
— Cette architecture constitue un single point of failure si la sandbox n'est pas redondante. Si la sandbox est redondante, l'architecture est encore plus coûteuse qu'une architecture TAP ;
— Demande un appareil avec des performances plus grandes que celui d'une architecture TAP.

3.5.3 Blocage via solution distribuée en mode in-line

Le but d'une solution distribuée est que tous les composants de la solution puissent communiquer ensemble pour se protéger et pour remédier au mieux aux attaques avancées. Ce genre de solution permet généralement de tracer le parcours d'un malware à travers toute l'infrastructure de l'entité. Cette fonctionnalité peut s'avérer très utile lors de la remédiation à une infection. Cette architecture est semblable à une architecture TAP à l'exception que les sensors sont des appareils n'ayant pas uniquement la fonction de sonde et qu'ils sont placés en in-line. Les sondes n'effectuent généralement pas le sandboxing.

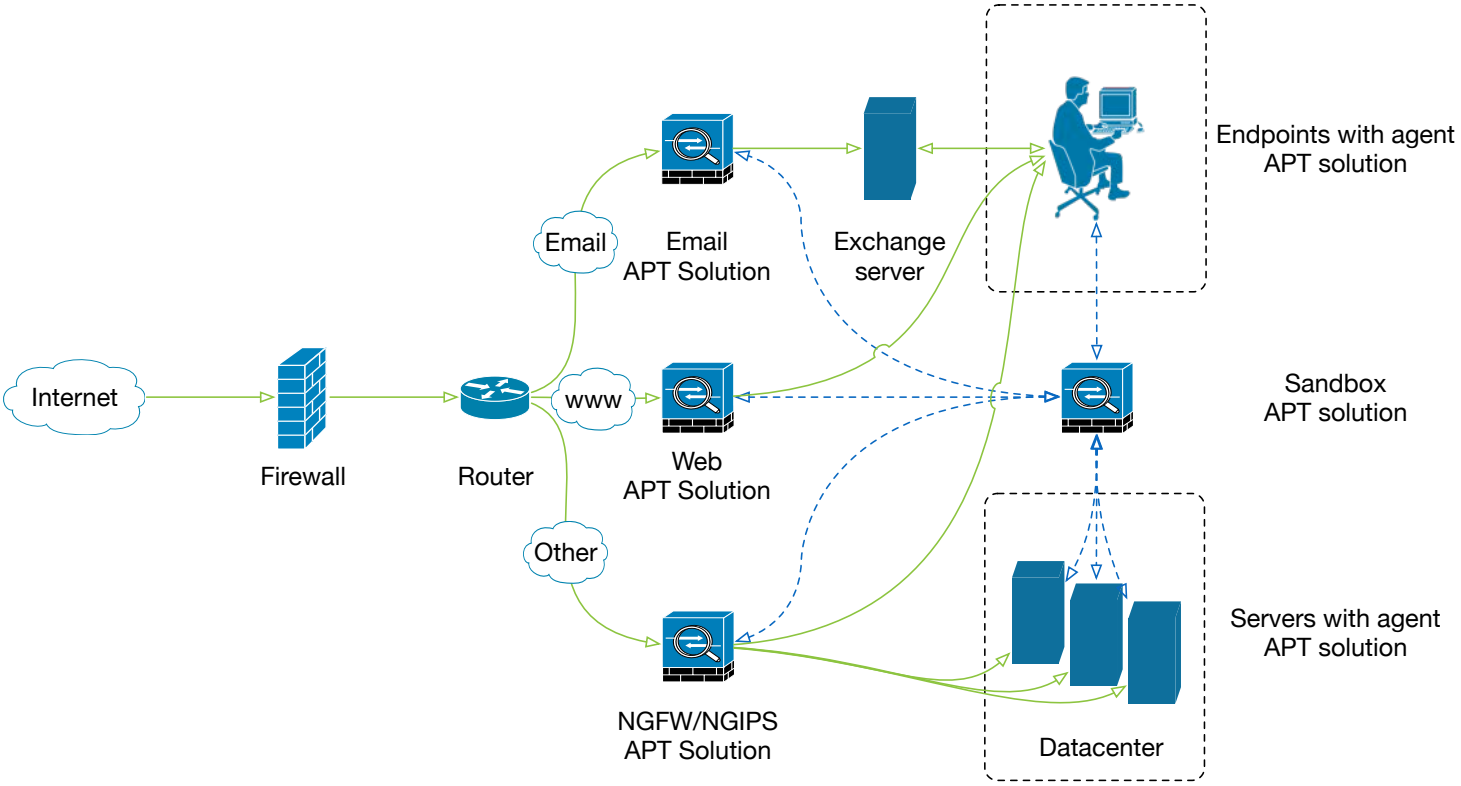


FIGURE 3.7 – Architecture d'une solution in-line distribuée

Intégration

Une solution de type distribué est une solution est une solution qui est divisée dans différents secteurs. C'est-à-dire qu'il y a un appareil effectuant une analyse sur des domaines ou sur des protocoles particuliers. Dans ce genre de solution, les appareils n'ont généralement pas une fonction unique de sandboxing. Un appareil de filtrage mail effectue généralement des autres fonctions que celle de sonde pour le sandboxing. L'intérêt d'une solution telle que celle-ci est de pouvoir se déployer facilement dans des entités possédant déjà les appareils compatibles avec la solution et nécessitant uniquement l'activation de la fonction.

L'intégration d'une solution de ce type n'est pas toujours envisageable. En effet, la solution ne convient pas si elle requiert d'être la seule solution de défense et qu'elle ne peut être intégrée au système de sécurité d'une autre marque que la sienne déjà mis en place. Néanmoins, il est possible d'implémenter cette solution si les systèmes de sécurité sont remplacés par la nouvelle solution. Évidemment, ce remplacement nécessite que la nouvelle solution soit capable, au niveau de ses fonctionnalités, de remplacer l'ancien système.

Avantages

— Si la solution anti APT n'est qu'une activation de licence sur les appareils de sécurité déjà mis en place, la solution est facilement déployable ;
— La répartition du trafic sur des appareils dédiés permet la gestion d'un trafic ciblé.

Inconvénients

— S'il ne s'agit pas d'activation de license, il est possible qu'il y ait des conflits entre la nouvelle solution et les appareils déjà mis mis en place.

4. Fonctionnalités attendues d'une solution ATP

4.1 Les nécessités générales

Dans ce chapitre sont expliquées les fonctionnalités qu'un système se prétendant comme solution ATP (Advanced Threat Protection) doit comporter. Un système ATP doit théoriquement pouvoir prévenir, détecter et idéalement bloquer les attaques avancées et persistantes. Ces fonctions sont les suivantes :

4.1.1 Alerting

L'alerting est une fonctionnalité indispensable dans la remédiation d'un incident. En effet, pour pouvoir réagir le plus rapidement possible, il est important d'avoir un système d'alerting. Les APTs ne s'effectuent pas sur de courtes périodes. Cependant, il est nécessaire de pouvoir être alerté si une machine est infectée et effectue du C&C. Il est également nécessaire de pouvoir être alerté si un fichier a été détecté comme malveillant par une sandbox. Un malware découvert par la sandbox ne peut pas toujours être traité automatiquement et nécessite des alertes pour gérer ce dernier.
Comme expliqué précédemment, et suivant l'architecture implémentée, les moyens de blocage de malwares découverts grâce au sandboxing ne sont pas toujours optimaux. En effet, le TCP RST possède des capacités assez limitées. Ce mécanisme ne sera utile que dans le cas d'un malware déjà connu du système. Le temps d'analyse du malware est la cause principale de l'incapacité du TCP RST à bloquer un malware inconnu. Comme dit au point 3.5.1, ce mécanisme ne permet que de réinitialiser la connexion entre le client et le serveur. Cependant, imaginons que le client en question télécharge un malware depuis le web. La taille de ce malware est par exemple de 5 megabytes. Le temps de téléchargement du malware avec un débit correct sera quasi-instantané. Le temps de l'analyse sera lui de 3 minutes. Dans notre exemple il s'est écoulé au moins 2 minutes et 55 secondes de trop pour que le système de sandboxing puisse réinitialiser la connexion.
Dans ce cas, le système doit pouvoir alerter le personnel de sécurité. En effet, le malware a été détecté, mais trop tard pour qu'une intervention de la sandbox puisse être réalisée.

Si aucune intervention automatique du système n'est possible et qu'aucune alerte n'est générée, la découverte du malware ne sera pas reportée et aucune remédiation ne sera effectuée. Les conséquences d'un système sans alerting seront les mêmes que de ne pas avoir de système du tout.
Il est donc primordial qu'une solution ATP puisse alerter l'entité dans laquelle elle est installée. L'intégration au SIEM de l'entité, si elle en dispose, est la principale fonction dont la solution doit disposer. Sinon les alertes doivent pouvoir être envoyées par email à la sécurité.

4.1.2 Analyse du trafic

L'analyse du trafic doit permettre de déterminer s'il est légitime ou non. Cette analyse doit s'effectuer sur différents protocoles et doit pouvoir déterminer plusieurs facteurs différents. Ils sont les suivants :

Command and Control (C&C)

Tel qu'expliqué au point 2.2.5, les APTs utilisent des serveurs de C&C pour communiquer avec les machines infectées par les malwares déployés. Ces communications sont effectuées avec de protocoles fréquemment utilisés afin de dissimuler les communications dans le flux réseau. Les protocoles les plus utilisés sont les protocoles web (80, 443). Une solution correcte doit être en mesure de détecter ce phénomène afin d'y remédier.

Exfiltration de données

L'exfiltration consiste à récupérer les informations volées. Un exemple d'une exfiltration flagrante serait l'exfiltration de données vers un serveur dans un pays éloigné en dehors des horaires de travail. Les informations volées sont généralement envoyées à un serveur anonyme.
Néanmoins, l'exemple fourni ci-dessus serait éventuellement utilisé par une attaque n'ayant pas pour but de rester furtive. Ce scénario semble peu probable car l'objectif des APTs est de ne pas être détectés. L'exfiltration se fera de façon à évier tout soupçon. On peut imaginer une exfiltration de données faite avec des comptes utilisateur légitimes à des heures de travail. L'exfiltration se fait généralement petit à petit pour ne pas éveiller de soupçons sur l'upload d'un fichier d'une taille considérable vers un serveur externe.

4.1.3 Blocage

Une fonctionnalité attendue d'une solution ATP est qu'elle puisse protéger une entité des attaques effectuées contre cette dernière. Afin de remplir cet objectif, une fonctionnalité de blocage de l'attaque reçue est nécessaire. Le blocage d'une attaque est crucial pour que les machines du réseau ne soient pas infectées.

Le blocage d'attaques standards est généralement effectué par des appareils tels que des NGIPS ou des NGFW. Cependant, ces appareils ne sont pas capables de bloquer les vecteurs d'infection d'une attaque ciblée et persistante. En effet, un firewall n'aura aucune emprise sur un malware zero-day reçu par email. C'est d'ailleurs pour des raisons telles que celles-ci que des sandbox sont utilisées. Cependant plusieurs scénarios dans lesquels l'usage d'une sandbox seule (donc sans agents endpoint ou autre) serait inefficace pour bloquer une attaque. En voici des exemples :

Scénario patient zéro [1]

Le schéma suivant représente un scénario dans lequel un malware zero-day est téléchargé depuis le web :

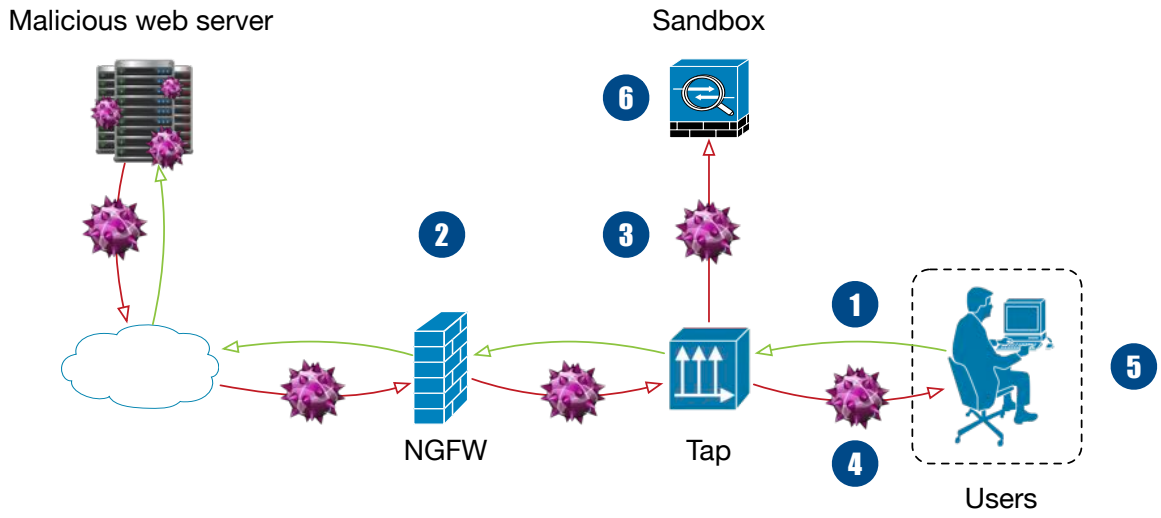


FIGURE 4.1 – Scénario d'un téléchargement de malware depuis le web

Dans cet exemple, le firewall effectue également les fonctions d'un IPS et les utilisateurs ne disposent pas d'agent endpoint sur leurs machines. L'architecture représentée est une architecture TAP mais le résultat serait le même avec une solution in-line.

Six phases sont numérotées dans le schéma, leur interprétation est la suivante :

1. En premier lieu, le client se rend sur un site web infecté [2] ou malveillant et y initie le téléchargement d'un malware de type zero-day ;
2. Le moteur IDS du NGWF ne détecte pas qu'il s'agit d'un fichier malveillant et laisse passer le téléchargement ;
3. Le malware arrive au niveau du TAP. Celui-ci duplique le trafic en direction de la sandbox. L'analyse du malware commence donc immédiatement en supposant qu'aucune "file d'attente" ne soit présente dans la sandbox ;
4. Le client revoit le malware en même temps que la sandbox ;
5. L'utilisateur exécute le malware sans avoir connaissance de la nature du fichier. L'antivirus de la machine ne détecte pas qu'il s'agit d'un malware et laisse le fichier s'exécuter. Le malware infecte alors la machine et effectue différentes tâches malveillantes ;
6. Une fois l'analyse de la sandbox terminée, le verdict est que le fichier est malveillant. Il aura fallu le temps de l'analyse pour connaître la nature du fichier. La durée de l'analyse peut être entre 3 et 15 minutes en fonction des solutions de sandboxing.

1. Le patient zéro est la première machine à être infectée par le malware.
2. Un serveur infecté est un serveur ayant été détourné de sa fonction principale et effectuant des tâches malveillantes

Cet exemple a pour but de démontrer que le blocage en temps réel de menace inconnue n'est pas possible. Il y aura toujours une période de temps pendant laquelle la nature du fichier sera inconnue. Si pendant ce moment, le fichier en question est exécuté, la machine sera infectée. Les solutions endpoint permettent de remédier à l'infection dans les plus brefs délais. En effet, il est possible d'isoler le poste du réseau l'empêchant ainsi de contaminer d'autres machines, si tel était le but du malware. Il est également possible, lors de l'obtention du verdict de la sandbox, d'empêcher l'exécution d'un fichier sur tous les postes disposant de l'agent.

Scénario USB

Dans le scénario suivant la même architecture que celle de la figure 4.1 est utilisée. Les machines des utilisateurs ne disposent donc toujours pas d'agents endpoint.

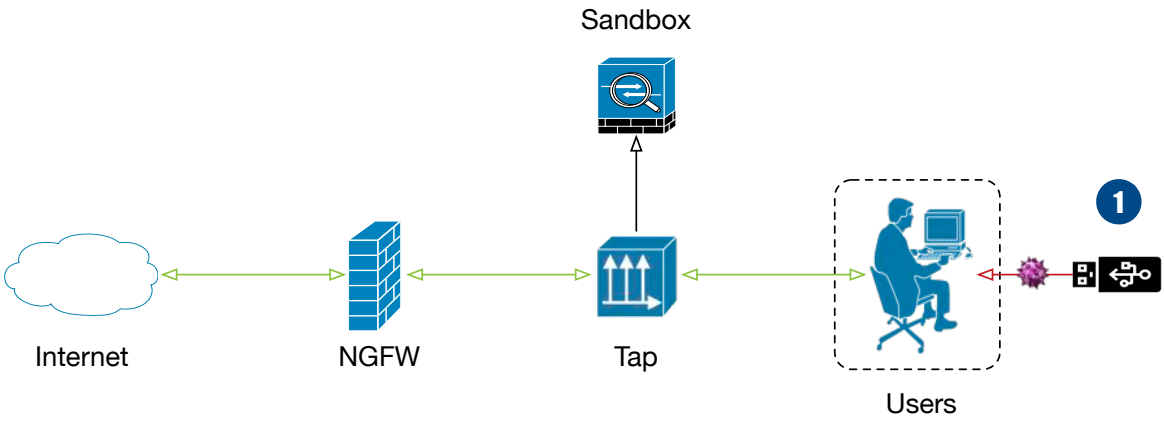


FIGURE 4.2 – Scénario d'un malware importe depuis une clé USB

Dans cet exemple, le scénario est simple. L'utilisateur introduit dans la machine une clé USB infectée qu'il a précédemment trouvée. Le malware s'exécute automatiquement et s'il s'agit d'un malware zero-day rien ne permet de détecter ce dernier.
Le recours à un agent endpoint permettrait d'analyser le contenu de la clé USB directement dans la sandbox. Les agents sont tous différents, mais effectuent généralement ce genre de fonction. Envoyer les fichiers se trouvant sur le support à la sandbox pour analyse permettrait d'empêcher une infection. Évidemment, pour éviter l'infection, les fichiers doivent être mis en quarantaine jusqu'à la réception du verdict de la sandbox.

Il est impossible de bloquer tous les vecteurs en temps réel sans dégrader la productivité de l'entreprise. Cependant, les agents endpoint permettent de bloquer une propagation de l'infection. Ils permettent également de bloquer l'exécution d'un fichier sur toutes les machines après obtention du verdict de la sandbox. Les machines ayant reçu ou téléchargé le fichier, mais l'exécutant après le temps d'analyse de la sandbox pourraient ainsi ne pas subir l'infection.

Afin de rencontrer la fonctionnalité de blocage attendue, la solution doit être intégrable avec un agent pouvant communiquer avec cette dernière.

4.1.4 Emails

D'après une étude réalisée par Trend Micro [3], 91% des attaques ciblées commencent avec des emails de spearfishing. Soit les emails contiennent directement un fichier malveillant soit un lien malveillant vers un serveur malveillant. Il est moins complexe pour les attaquants d'utiliser le spearfishing à d'autres techniques telles que l'infection depuis le web. En effet, pour une infection à partir du web, il faut encore que la cible se rende sur le site en question. Contrairement à cela, un email est destiné à la cible. Il y a plus de chance pour qu'un utilisateur clique sur un lien dans un email que pour qu'un utilisateur se rende sur le serveur web malveillant.

La solution doit donc évidemment pouvoir analyser les emails à la recherche de lien hypertexte malveillant mais également pour analyser les pièces jointes.

4.1.5 Flux chiffrés

De nos jours, la plupart des serveurs web manipulant des informations sensibles telles que des informations bancaires chiffrent leurs communications. Le but de ce chiffrement est d'assurer la confidentialité des données. La confidentialité a été définie par l'Organisation internationale de normalisation (ISO) comme "le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé" [4]. En effet, les données sensibles échangées entre un client et un serveur doivent être uniquement compréhensibles par ces deux acteurs. Le protocole SSL (Secure Socket Layer) est utilisé pour chiffrer les données échangées entre un client et un serveur.
Le schéma suivant représente la création d'une session sécurisée entre un client et un serveur utilisant le protocole SSL :

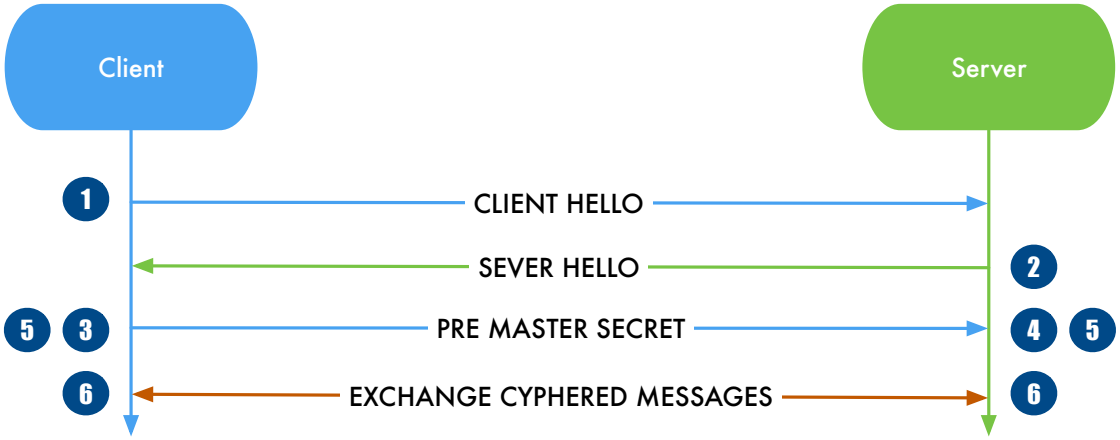


FIGURE 4.3 – Schéma SSL Handshake [5]

3. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
4. https://fr.wikipedia.org/wiki/Confidentialité
5. http://www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake

Les explications correspondantes à la numérotation du schéma sont les suivantes :

1. Client Hello : le client envoie les informations dont le serveur a besoin pour pouvoir communiquer en utilisant SSL. Ces informations sont le numéro de version d'SSL, les paramètres de chiffrement, et les données spécifiques à la session SSL ;
2. Server Hello : le serveur envoie les informations dont le client a besoin pour pouvoir communiquer en utilisant SSL. Ces informations sont le numéro de version d'SSL, les paramètres de chiffrement, et les données spécifiques à la session SSL. Le serveur envoie également son certificat dans lequel est contenue sa clé publique ;
3. Authentication and Pre-Master Secret : le client authentifie le certificat du serveur. Il crée ensuite un pre-master secret pour la session. Une fois généré, le pre-master secret est encrypté avec la clé publique du serveur contenue dans son certificat, puis il lui est envoyé ;
4. Decryption and Master Secret : le serveur reçoit le pre-master secret et le décrypte grâce à sa clé privée. Ensuite, le client et le serveur génèrent le master secret avec les arguments convenus ;
5. Generate Session Keys : le client et le serveur se servent du master secret pour générer la clé de session. Cette clé de session permet de chiffrer symétriquement les communications entre le client et le serveur ;
6. Encryption with Session Key : le client et le serveur peuvent maintenant échanger des données en toute confidentialité.

D'une manière logique, le schéma suivant représente une communication SSL :

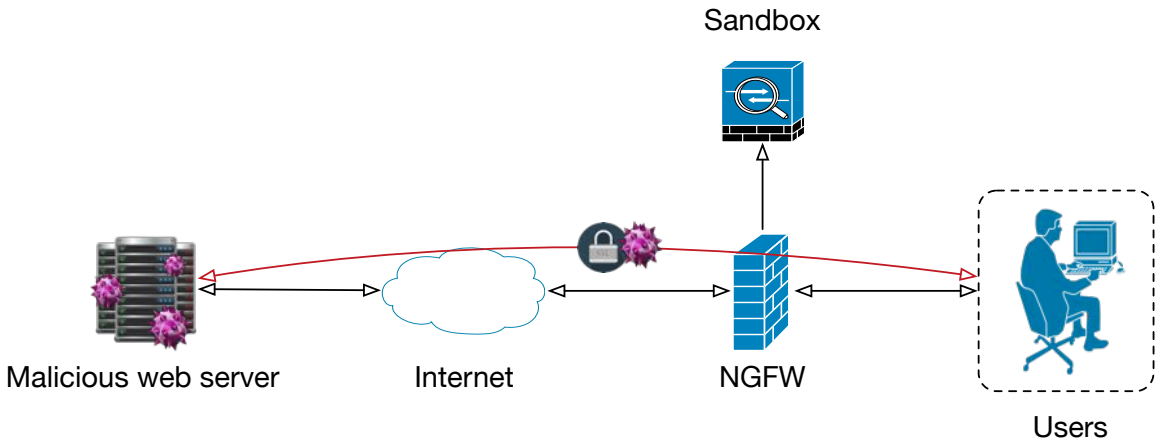


FIGURE 4.4 – Schéma d'une communication utilisant le protocole SSL

Aucun appareil ne peut alors interpréter les données interceptées entre le client et le serveur. Cependant, le protocole SSL peut aussi être utilisé entre un client et un serveur malveillant. Si le client venait à télécharger un malware en utilisant SSL, le trafic serait chiffré et le malware ne serait donc pas analysé par la sandbox. Ce scénario pose problème, car une très grande partie du trafic web est maintenant sécurisée par l'usage du protocole SSL. Pour remédier à cette solution, les NGFW proposent une fonction de décryption SSL. Ce mécanisme consiste à établir une connexion SSL entre le client et le firewall ainsi qu'une autre connexion entre le firewall et le serveur. Les données sont alors compréhensibles par le firewall. Ce procédé "déchiffre" les données uniquement pour le firewall. Les autres appareils entre le client et le serveur seront incapables d'analyser les données.

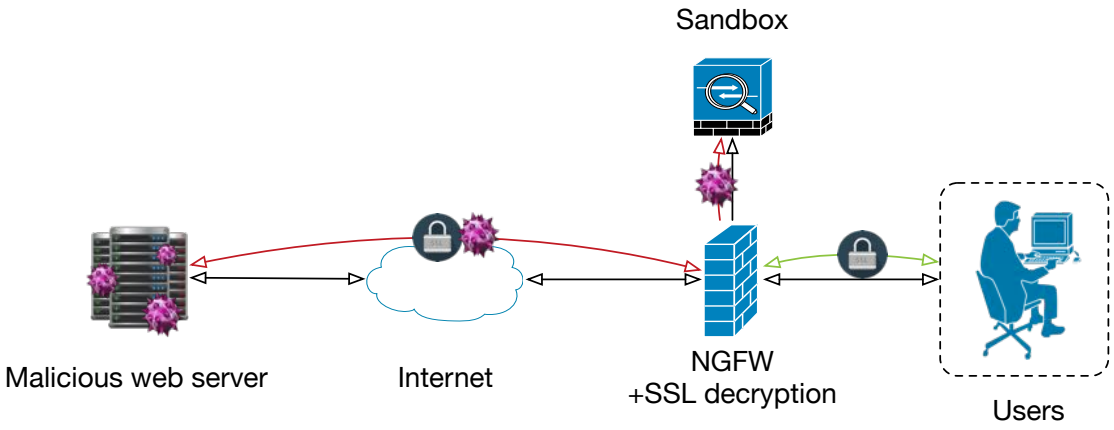


FIGURE 4.5 – Schéma d'une communication SSL "décryptée"

Ce procédé est également utilisé par les hackers et est appelé l'attaque "Man In The Middle", l'homme au milieu. Le mécanisme mis en place sur le firewall consiste à établir la confection sécurisée entre le serveur et le firewall. Le firewall décrypte les données reçues depuis le serveur et les réencrypte pour les envoyer au client. Il y a ici deux sessions SSL sur le schéma 4.5. En rouge la session originale, c'est-à-dire la session établie à partir du certificat du serveur, et en vert, la session établie à partir du certificat de l'entreprise possédant firewall.

Pour avoir une visibilité sur l'ensemble du trafic réseau de l'entité, il est primordial que la solution ATP mise en place puisse traiter le flux SSL. Il a y dès lors deux possibilités pour une solution analysant le flux SSL. Il faut que la solution possède une solution de décryption SSL intégrée ou qu'elle puisse être intégrée à un appareil effectuant cette décryption. Dans le cas d'une décryption faite par un appareil tiers, le trafic décrypté doit évidemment être envoyé à la sandbox pour y être analysé.

4.1.6 HA

Le HA, *Hight Availability*, haute disponibilité, réfère un système ou un composant qui est continuellement opérationnel pour une longue période de temps. Il est indispensable pour une solution ATP d'être opérationnel à tout moment. Il ne serait pas tolérable que l'appareil n'ait été en exploitation durant plusieurs heures. L'entité serait alors exposée aux attaques ce qui ne peut être tolérable.

4.1.7 Mobile

Les infections en provenance des mobiles ne sont pas à exclure dans le cas d'une infiltration d'une attaque avancée et persistante. Les mobiles sont de nos jours, des machines capables, ou presque, d'effectuer les mêmes tâches que nos postes de travail. Ils sont également exposés à toute source d'infections. Les applications qui y sont installables depuis les stores officiels sont généralement contrôlées. Cependant, dans le cas des mobiles utilisant l'OS Android, il est possible d'installer des applications en provenance d'autres stores. Ces stores ne sont pas forcément contrôlés ou directement infectés. Les applications téléchargées en provenance de ces endroits ne sont en rien sûres. Il est tout à fait possible qu'une application ait été remplacée ou modifiée pour y ajouter du contenu malveillant. Il est nécessaire, à partir du moment où les mobiles sont connectés sur le même réseau que celui de l'entreprise, que la solution ATP puisse générer les menaces en provenance de ces mobiles.

BYOD

Le *Bring Your Own Devide* consiste à utiliser du matériel personnel dans le cadre professionnel. Ce procédé pose plusieurs problèmes liés à la sécurité des données. Il n'est pas possible pour les entreprises d'avoir autant de contrôle sur des appareils privés que sur des appareils professionnels. Par exemple, un appareil personnel peut ne pas disposer de logiciel antivirus. Il est alors possible que cette machine soit connectée au réseau de l'entreprise et infecte d'autres machines. Elle peut également récupérer des données sensibles et les envoyer aux pirates. Un autre exemple est la sécurité pour accéder au contenu des appareils personnels. Ils peuvent ne pas posséder de mot de passe. En cas de vol du dispositif, les données sensibles présentes sur ces appareils sont directement exploitables.

Pour garantir la sécurité de l'entreprise et tout comme pour les mobiles, les appareils personnels, doivent être utilisés suivant les politiques de l'entreprise ou être bannis du réseau de cette dernière.

4.1.8 Sandboxing

Le *sandboxing* est la pièce maîtresse d'une solution ATP. C'est cette fonction qui permet de détecter des malwares zero-day tels qu'expliqués dans la section 3.4. L'analyse dynamique est un monitoring de l'exécution d'un fichier dans un environnement. Dans un environnement d'entreprise, sans sandbox, il n'est pas possible d'effectuer d'analyse dynamique, de déterminer les actions d'un fichier et d'en déduire ses intentions.

Personnalisation

Comme évoqué dans la section 3.4.2, les malwares avancés et persistants utilisent des mécanismes d'évasion de sandbox. Il peut s'agir d'une vérification de l'existence d'un programme sur la machine ou encore d'un type de processeur. Les possibilités sont nombreuses, combinables entre elles et sans réelles limites. Pour tromper au maximum les malwares, les environnements virtualisés ou émulés, doivent être une copie des machines existantes au sein du système d'information de l'entreprise. Cette particularité et très complexe, car il n'est pas envisageable d'avoir un environnement dédié à chaque machine existante. Il faut savoir que la plupart des solutions de sandboxing comprennent rarement plus d'une centaine d'environnements virtualisés ou émulés. Ce besoin de dupliquer chaque machine pour s'en servir dans une sandbox serait trop coûteux.
Néanmoins, afin de se rapprocher au plus de cette fonctionnalité idéale, il doit être possible pour la sandbox de personnaliser les environnements qu'elle utilise.

OS émulés/virtualisés

Dans la plus grande majorité des entreprises, Windows est l'Operating System utilisé. Néanmoins, il arrive que l'usage d'autre OS soit nécessaire. De plus, comme évoqué dans la section 4.1.7, il est possible dans certains cas que les mobiles soient connectés au réseau de l'entreprise. Il serait donc théoriquement possible pour une attaque APT d'utiliser ce vecteur d'infection.
Les sandbox doivent être capables d'analyser des malwares sur d'autres systèmes d'exploitation que Windows. Dans le cas contraire, tout malware n'étant pas supporté par Windows ne sera pas analysé et donc pas détecté par la sandbox.

4.1.9 Support des protocoles

Une solution ATP se doit de supporter les protocoles utilisés par l'entreprise. Dans les protocoles devant être analysé on retrouve par exemple des protocoles email (POP, SMTP, IMAP), des protocoles de partage de fichier (SMB, NFS) ainsi que des protocoles web(HTTP).
Dans le cas d'extraction de données, la solution doit être capable de détecter l'usage d'un protocole inhabituellement utilisé.

4.1.10 Support des fichiers

Les malwares utilisés pour l'infection utilisent des formats anodins pour ne pas éveiller de soupçons à l'utilisateur. Il est courant que les malwares utilisent des noms et des extensions n'attirant pas l'attention. Un exemple pourrait être "invoice_723961.doc". Dans le cas d'un tel fichier reçu au service comptabilité, il ne fait aucun doute que ce dernier sera ouvert. Ce genre de malware utilise des macros pour automatiser des téléchargements d'autres malwares inconnus de l'utilisateur. En plus d'effectuer des actions inconnues de l'utilisateur, le malware peut aussi bien afficher le contenu du document. Ce procédé rend la découverte de l'infection encore plus difficile si aucun appareil n'a détecté la nature du fichier. Les documents Microsoft Office permettent ce genre de manipulation. Il existe également des PDF (Portable Document Format) contenant du code JavaScript malveillant effectuant des actions similaires. Il est également possible d'effectuer d'autres actions telles que de lancer des exécutables avec les fichiers PDF.

Évidemment, il est également possible que les malwares se trouvent sous la forme d'exécutable. Le procédé est néanmoins moins discret qu'un document infecté. En effet, un fichier exécutable au nom d'une facture sera moins crédible pour une personne ayant un minimum de connaissance en informatique. Les formes sous lesquelles se trouvent les malwares sont nombreuses. L'idéal est de pouvoir analyser le plus de fichiers possible indépendamment de l'extension qu'ils possèdent.

Les archives sont également utilisées pas les malwares. En effet, certains malwares sont compressés et recompressés successivement pour éviter d'être détectés. Il est également possible d'utiliser des formats d'archivage peu communs.

Il faut donc qu'une solution ATP puisse analyser différents types de fichiers, mais qu'elle puisse également désarchiver toute une panoplie d'archive, pour avoir la meilleure vue possible sur les potentiels malwares.

4.1.11 Threat intelligence

Le *Threat Intelligence* est ce qui permet à des appareils de sécurité de communiquer avec le cloud du constructeur pour recevoir des informations sur des malwares. Cette fonction permet de mettre à jour les hashs des malwares connus entre les appareils de différentes entités. Le fait d'avoir connaissance du hash d'un malware permet d'éviter d'avoir à refaire l'analyse dynamique si le fichier est réputé comme malveillant. Le fait de posséder cette fonctionnalité est un plus pour une solution ATP. Elle permet essentiellement d'être informé et de pouvoir se protéger des malwares rencontrés dans d'autres entités. Le seul réel apport de cette fonctionnalité est l'économie d'une analyse dynamique. Sans cette fonctionnalité, le malware pourra tout de même être détecté par la sandbox.

4.1.12 Web

Le *web* est une des secondes sources d'infection les plus importantes. Il est également utilisé pour l'extraction de données. Le web peut permettre le téléchargement d'un malware ou des communications de commande et de contrôle. De plus il est primordial pour avoir une visibilité correcte, d'avoir la décryption SSL comme expliqué à la section 4.1.5.

4.2 Les nécessités pour Nethys

Les critères auxquels doit répondre la solution sont adaptés à l'entreprise qui veut s'en équiper. Cela varie en fonction des technologies utilisées au sein de cette dernière. Certains protocoles de partage de fichier peuvent ne pas être utilisés, ou certaines extensions de fichier bannies du SI. Dans ce cas, il n'est pas nécessaire que la solution ATP puisse les traiter.

D'autres contraintes telles que l'intégration, le débit ou la scalability peuvent être intégrées dans les besoins de la solution.

Les abréviations suivantes permettent une meilleure compréhension de la matrice :
— M : Must ;
— S : Should ;
— O : Optionnal ;
— AC : Accepted.

La matrice des besoins de Nethys est la suivante :

ID	Domaine	Requirement description	Source	Priorité	Statut
B-SAPT-001	Alerting	Système de log et d'alerte au niveau du SIEM et/ou par mail, SMS	Cellule sécurité	M	AC
B-SAPT-002	Analyse du trafic	Analyse du trafic à travers le réseau afin de repérer le trafic malveillant tel que le C&C et de pouvoir le bloquer par la suite	Cellule sécurité	M	AC
B-SAPT-003	Blocage	Blocage du trafic malveillant	Cellule sécurité	M	AC
B-SAPT-004	Debit	[illegible]	Cellule sécurité	M	AC
B-SAPT-005	Email	Analyse des emails, des pièces jointes et des URLs se trouvant dans les mails	Cellule sécurité	M	AC
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	AC
B-SAPT-007	High Availability	L'architecture de la solution doit être de type 'High Availability'	Cellule sécurité	M	AC
B-SAPT-008	Integration	La solution APT doit s'intégrer dans le réseau actuel sans impact majeur sur l'architecture	Cellule sécurité	M	AC
B-SAPT-009	Latence réseau	La solution APT ne doit pas apporter de latence significative qui puisse perturber les flux applicatifs et business	Cellule sécurité	M	AC
B-SAPT-010	Mobile	Application des mesures de sécurité au niveau des devices mobiles	Cellule sécurité	O	AC
B-SAPT-011	Object	Analyse d'objet en temps réel	Cellule sécurité	M	AC
B-SAPT-012	Sandboxing	Pour un objet malveillant, la sandbox doit émuler un comportement utilisateur classique de façon à ce que l'objet malveillant ne suspecte pas qu'il s'agit d'une sandbox.	Cellule sécurité	M	AC
B-SAPT-013	Scalability	Possibilité d'évolution du système au point de vue volumétrique et au point de vue fonctionnel (par exemple, analyse d'autres protocoles, etc.)	Cellule sécurité	M	AC
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	AC
B-SAPT-015	Traitement des fichiers	La solution doit analyser et détecter des menaces venant de fichiers d'au moins le types suivants :	Cellule sécurité		
B-SAPT-015-1	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-015-2	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-015-3	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-015-4	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-015-5	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-015-6	Traitement des fichiers	[illegible]	Cellule sécurité	M	AC
B-SAPT-016	Traitement des protocoles	Les protocoles à supporter sont les suivants :	Cellule sécurité		
B-SAPT-016-1	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-2	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-3	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-4	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-5	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-6	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-7	Traitement des protocoles	[illegible]	Cellule sécurité	M	AC
B-SAPT-016-8	Traitement des protocoles	[illegible]	Cellule sécurité	S	AC
B-SAPT-017	Web	Solution contre les ExploitKits	Cellule sécurité	O	AC
B-SAPT-018	Web	Solution contre les malwares téléchargés sur le web et exploitant une faille de type Zero-day	Cellule sécurité	M	AC

5. Solutions aux APTs

5.1 Advanced Malware Protection de Cisco

La solution AMP de Cisco est une solution qui permet facilement de s'intégrer dans une infrastructure Cisco. En effet, AMP est présent dans une grande partie des produits Cisco. AMP opère à plusieurs niveaux et sur différents appareils. On retrouve notamment AMP au niveau des appareils de filtrage mail et web, mais également sur les IPS Sourcefire. Cisco a acquis Sourcefire le 7 octobre 2013. La solution AMP de Cisco, anciennement FireAMP est une solution distribuée.

La solution Cisco AMP n'a pas été testée, mais des recherches ainsi que des meetings on étés effectués afin d'obtenir de plus amples informations sur le produit. Les informations suivantes en sont donc issues.

5.1.1 Vision de la solution

Selon Cisco, lutter contre les cyberattaques se fait à plusieurs points dans le temps :
— Avant, en sécurisant le réseau ;
— Durant, en détectant et bloquant les attaques ;
— Après, en remédiant aux dommages de l'attaque.

Le schéma suivant représente cette vision de la sécurité informatique :

FIGURE 5.1 – Vision de Cisco pour contrer les attaques informatiques

Afin de pouvoir lutter à différents points dans le temps, différentes technologies sont mises en place. On retrouve notamment le “file retrospective”. Cette technologie permet d’alerter qu’un fichier ayant été “trusté” à un moment t1 est devenu malveillant à un moment t2. La solution Cisco traque tous les fichiers du réseau dans le cas où un fichier s’avérerait finalement malveillant. L’objectif est de connaître quelles sont les machines ayant reçu le fichier et de savoir quelles actions ont été effectuées. À savoir, des actions telles que l’exécution du fichier, le transfert du fichier à une autre machine, ou dans le cas de la résolution de l’infection, la mise en quarantaine. Cette action est possible grâce à la fonction “Network File Trajectory” de Cisco qui conserve toute trace des fichiers.

Cisco AMP opère à différents niveaux pour avoir une vue aussi complète que possible. Ceux-ci sont les suivants :

5.1.2 Threat Grid

Cisco a acquis Threat Grid le 14 juin 2014. Threat Grid est la solution qui effectue le sandboxing de Cisco AMP. Threat Grid est déployable sur site ou dans le cloud du constructeur. L’intérêt d’une solution déployée sur site est de garder les données confidentielles au sein de l’entreprise.

OS disponibles

Threat Grid effectue les analyses dynamiques dans des environnements Windows. On retrouve notamment des Windows XP ainsi que des Windows Seven 32 et 64 bits. Les malwares à destination de machines Unix ne sont pas analysables dynamiquement par cette solution.

Types de fichiers analysés

Les fichiers pouvant être analysés par Threat Grid sont les suivants :
— Portable Executable 32-bit (PE32) files : executable (EXE), dynamic-link library (DLL) ;
— Java Archives (JAR) ;
— Adobe Portable Document format (PDF) ;
— Documents Microsoft Office ;
— ZIP ;
— URLs ;
— Documents HTML.

Comportement anti-évasion de sandbox

Aucun comportement utilisateur n’est émulé tel que recommandé au point 3.4.2. L’opérateur peut toutefois prendre la main sur la sandbox grâce à une fonction appelée “GloveBox”. Il est alors possible d’interagir avec la sandbox.

Capacité de personnalisation de sandbox

Rien n’indique dans la documentation de Threat Grid que la sandbox est personnalisable suivant les souhaits du client. Il n’est donc pas possible de personnaliser cet environnement pour qu’il se rapproche au plus possible des machines présentes au sein de l’entreprise. Tel qu’expliqué au point 3.4.2, il est bénéfique qu’une sandbox puisse être aussi similaire que possible aux machines utilisées par l’entreprise.

Appareils utilisés par Cisco AMP

Threat Grid est utilisé pour faire le sandboxing de la solution Cisco AMP. Cependant, elle nécessite d'autres appareils pour recevoir les données à analyser. Ces appareils ne sont pas exclusivement des sondes et effectuent bien d'autres tâches en parallèle. Ces différents appareils permettent également de faire le "Network File Trajectory" de Cisco. Les principaux sont les suivants :

ESA

ESA est l'appareil de filtrage mail de Cisco. Il permet d'analyser le trafic email et d'envoyer les pièces jointes à la sandbox. D'autres fonctions sont réalisées par cet appareil, mais sortent du carde de ce travail.

WSA

WSA est l'appareil de filtrage web de Cisco. Cet appareil filtre le flux web et permet d'envoyer différents fichiers à la sandbox. Tel que l'ESA, cet appareil effectue d'autres fonctions. Cependant, ces dernières sortent du cadre de ce travail.

NGIPS

Les NGIPS Sourcefire permettent d'analyser le reste du trafic. Il peut s'agir du trafic de partage de fichier tel que Samba (SMB), NFS, FTP. Le NGIPS, tel que les autres appareils, permet d'envoyer des fichiers à la sandbox.

Anyconnect

Anyconnect est l'agent endpoint multifonctions de Cisco. Cet agent intègre la fonction AMP. Il est possible grâce à cet agent d'effectuer les tâches suivantes :
— Mettre en quarantaine un poste infecté ;
— Empêcher l'exécution d'un fichier découvert comme malveillant par la sandbox ;
— Envoyer des fichiers à analyser à la sandbox.

Anyconnect est disponible pour les distributions suivantes :
— Microsoft Windows XP avec Service Pack 3 ou plus récent ;
— Microsoft Windows Vista avec Service Pack 2 ou plus récent ;
— Microsoft Windows 7 ;
— Microsoft Windows 8 et 8.1 ;
— Microsoft Windows 10 ;
— Microsoft Windows Server 2003 ;
— Microsoft Windows Server 2008 ;
— Microsoft Windows Server 2012 ;
— Mac OS X 10.7 ou plus récent ;
— Linux Red Hat 6.5 et 6.6 ;
— Linux CentOS 6.4, 6.5, et 6.6 ;
— Android version 2.1 ou plus récent.

5.1.3 TALOS

Talos est le Cloud Threat Intelligence de Cisco. Il permet notamment de prévenir une attaque qui a été détectée sur une autre organisation équipée de la solution Cisco AMP.

5.1.4 Protocoles supportés

Cisco AMP ne supporte que quelque protocoles [1]. Les voici :
— HTTP ;
— SMTP ;
— IMAP ;
— POP3 ;
— FTP ;
— SMB.
Ces protocoles sont supportés et analysés par les NGIPS ou par les appareils AMP dédiés.

5.1.5 Blocage

Cisco AMP est une solution distribuée et qui permet de bloquer tel qu'expliqué au point 3.5.3. Chaque appareil possède différentes manières pour bloquer. Les malwares téléchargés depuis le web ne sont pas bloqués de la même manière que ceux reçus par email. En effet, les emails peuvent subir une latence égale au temps de l'analyse de la sandbox. Le web ne peut être ralenti à tel point.

5.1.6 Avantages de la solution

— Couvre toutes les sources d'infection, d'infiltration possible : couverture email, web, endpoints et autres ;
— Permet de traiter le flux SSL(crypté) ;
— La solution est distribuée, ce qui permet de traiter un trafic sans en impacter un autre ;
— La solution a obtenu un score de 99,2% aux tests réalisés par NSS Lab.

5.1.7 Inconvénients de la solution

— La solution nécessite des appareils séparés pour traiter le flux mail et le flux web, ce qui peut créer de potentiels conflits entre AMP et les solutions déjà en place dans le cas ou une intégration ou une collaboration des solutions n'est pas possible ;
— Threat Grid ne simule pas de comportement utilisateur dans les sandbox, ce qui pose problème si les malwares utilisent des mécanismes d'évasion ;
— Il y a une latence ajoutée au parcours des flux, car des appareils sont rajoutés en in-line.

1. http://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html

5.1.8 Conformité de Cisco AMP aux nécessités générales d'une solution ATP

Le tableau suivant résume les conformités théoriques aux besoins généraux établis au point 4.1 :

Agent endpoint	Anyconnect est l'agent qui intègre AMP for endpoint
Alerting	AMP offre cette fonction
Analyse du trafic	L'analyse du trafic est faite par différents appareils en fonction du trafic en question
Blocage	Le blocage des menaces connues peut se faire sur les machines appropriées au type de trafic. Les menaces inconnues dépendent du temps d'analyse de la sandbox. En cas d'infection, il est tout de même possible d'y remédier rapidement grâce aux agents endpoint
Emails	L'ESA effectue tout ce qui est analyse d'emails
Flux chiffrés	Le NGIPS est capable d'effectuer de la décryption SSL
HA	AMP dispose de cette fonction
Mobile	AMP dispose de client Android. Néeanmoins, Threat Grid ne possède pas de sandbox pour cet OS. Les malwares capables d'être détectés sont sûrement des malwares connus
Sandboxing	Les fonctionnalités des sandboxing, que ça soit au niveau de la personnalisation, des mécanismes d'évasion ou encore des OS supportés, sont faibles
Support des fichiers	Cisco AMP supporte les principaux types de fichiers
Support des protocoles	Supporte les protocoles basiques d'emails, de partage de fichiers et de web
Threat Intelligence	Talos effectue la fonction de Threat intelligence
Web	Les WSA couvrent la partie web

5.2 WildFire de Palo Alto Networks

Un PoC WildFire a été réalisé. La solution a été testée dans sa version cloud et sans agent endpoint. Les fonctionnalités de l'agent correspondant sont donc purement théoriques car elles n'ont pas étés testées.

5.2.1 Fonctionnement général

La solution de Palo Alto est une solution utilisant les NGFW comme sonde. Deux types de déploiement sont possibles.

5.2.2 Sandboxing WildFire

Le trafic est analysé par une sandbox sur site ou dans le cloud du constructeur. L'usage d'un appareil sur site permet de ne pas exposer les données analysées au cloud public. Il est possible d'avoir une architecture hybride. C'est à dire d'utiliser un appareil sur site pour analyser certaines données sensibles et d'utiliser le cloud pour les autres données.

Os disponibles

WildFire possède des sandbox Windows XP, Windows Seven, Android et Mac OS X. Il est donc possible avec cette solution de détecter les malwares à destination de ces OS.

Types de fichiers analysés

Seuls les fichiers suivants sont analysables par WildFire :
— Portable Executable (PE) ;
— Java Archives (JAR) ;
— Adobe Portable Document format (PDF) ;
— Android Package (APK) ;
— Documents Microsoft Office ;
— ZIP ;
— GZIP.

Les tests effectués sur la solution ont permis de prouver que les malwares sous forme de PE, documents office, ZIP et GZIP sont bien détectés par la sandbox. Néanmoins, la sandbox semble avoir un problème pour la détection d'APKs malveillants.

Comportement anti-évasion de sandbox

WildFire implémente différents mécanismes anti-évasion de sandbox.
Afin de vérifier les dires de Palo Alto, différents "malwares" de test ont étés implémentés. Ceux-ci, effectuent diverses actions sur la registry. Ces malwares comportement des mécanismes d'évasion de sandbox. Le but de ces tests était de déterminer la capacité de WildFire à détecter des malwares évasifs.

Les malwares ne déclenchent les actions sur la registry que lorsque certains critères sont remplis. On retrouve notamment le déplacement du curseur, la frappe au clavier, etc.

Les rapports de la sandbox permettent de savoir si les malwares se sont activés. Ils permettent de savoir si la sandbox a correctement interagi avec le malware pour que celui-ci se déclenche.

Le tableau suivant résume les mécanismes d'évasion implémentés ainsi que le verdict de la sandbox :

Pas de mécanisme d'évasion	Le malware se déclenche lors de son exécution, aucun mécanisme n'est implémenté. Il permet de connaître les résultats lors de l'activation du malware
Déplacement du curseur	Le malware ne se déclenche que lorsque le curseur de la souris se déplace
Double click	Le malware ne se déclenche que lors d'un double click
Frappe au clavier	Le malware ne se déclenche que lorsqu'une frappe au clavier est détectée
Déplacement du curseur + double click + frappe au clavier	Le malware ne se déclenche que lorsque les trois critères précédents sont détectés
Déplacement du curseur + double click + frappe au clavier + boîte de dialogue	Le malware ne se déclenche que lorsqu'est détecté le déplacement de curseur, le double click, la frappe au clavier et l'acceptation des alertes que génère le malware

En vert sont représentés les malwares ayant été détectés par WildFire. En rouge sont ceux qui ne l'ont pas été.

Capacité de personnalisation de sandbox

La Sandbox de WildFire n'est pas personnalisable. Cet aspect est assez fermé chez cette solution. En effet, il n'est ni possible de customiser la sandbox ni de prendre la main sur l'exécution d'un malware tout comme le propose la solution Cisco.

5.2.3 Protocoles supportés

La plupart du trafic analysé par WildFire est envoyé depuis le NGFW. Celui-ci est basé sur des règles comme expliqué au point 3.2.2. WildFire est un module d'analyse qui est rajouté aux règles. Celui-ci s'active de la même manière que l'on active l'analyse de signature sur une règle. Il est alors possible d'analyser toute une panoplie de protocoles différents.

Les tests effectués ont révélé des anomalies pour les protocoles de partage de fichiers. Ces protocoles sont SMB, NFS, FTP. Les malwares échangés avec ces protocoles n'ont pas été détectés.

5.2.4 Traps for endpoint

Traps est l'agent endpoint de Palo Alto Networks qui permet de communiquer avec WildFire et les NGFW de Palo Alto. Les fonctions sont assez similaires avec l'agent Anyconnect de Cisco. Traps est essentiellement disponible pour Windows. Les versions compatibles sont les suivantes :

— Windows XP avec SP3 ;
— Windows Vista ;
— Windows 7 ;
— Windows 8/8.1 ;
— Windows 10 ;
— Windows Serveur 2003 ;
— Windows Serveur 2008 ;
— Windows Serveur 2012.

5.2.5 Blocage

WildFire est une solution qui utilise les NGFW Palo Alto comme sonde. Les moyens de blocage correspondant à ce type d'architecture se trouvent au point 3.5.2. Le blocage est basé sur les règles des NGFW.

5.2.6 Résultats de tests

L'entièreté des tests effectués ainsi que les résultats obtenus sont les suivants (l'annexe A est une version agrandie de ces tests) :
(Suite à la demande de Nethys, une grande partie des tests ont étés camouflés.)

ID	Domaine	Description	Scénario	Priorité	C-PAN	R-PAN
Q-SAPT-001				M	OK	
Q-SAPT-002				M	OK	
Q-SAPT-003				M	OK	
Q-SAPT-004				M	OK	
Q-SAPT-005	Flux chiffrés	Est-ce que la solution sait analyser les flux chiffrés	Téléchargement depuis un serveur HTTPS comme "MEGA", d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement du filtrage avec des flux chiffrés	M	KO(MAJ)	La fonction de décryption a été testée mais les flux déchiffrés n'étaient pas envoyés au WildFire. La fonction d'envoi au WildFire n'a pas été trouvée
Q-SAPT-006				M	OK	
Q-SAPT-007				M	OK	
Q-SAPT-008				M	OK	
Q-SAPT-009	Mobile	Est-ce que le système détecte les menaces venant de mobiles	Depuis un mobile : téléchargement web ou réception d'un email contenant d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement de l'alerting	O	KO(MIN)	Aucun APK n'est envoyé à WildFire alors que ce type de fichier est configuré dans la policy
Q-SAPT-010				M	OK	
Q-SAPT-011	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-011-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-012				M	OK	
Q-SAPT-013				S	OK	
Q-SAPT-014						
B-SAPT-014-1				M	OK	
B-SAPT-014-2				M	OK	
B-SAPT-014-3				M	OK	
B-SAPT-014-4	Traitement des fichiers	Rar	Téléchargement d'un malware sous la forme de fichier Rar	M	KO(MAJ)	Le malware diffusé sous forme Rar n'a pas été détecté par WildFire
B-SAPT-014-5	Traitement des fichiers	Tar	Téléchargement d'un malware sous la forme de fichier Tar	M	KO(MAJ)	Le malware diffusé sous forme Tar n'a pas été détecté par WildFire
B-SAPT-014-6				M	OK	
Q-SAPT-015						
B-SAPT-015-1				M	OK	
B-SAPT-015-2				M	OK	
B-SAPT-015-3				M	OK	
B-SAPT-015-4	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MIN)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté, cependant durant le POC, du trafic FTP a été détecté par WildFire
B-SAPT-015-5				M	OK	
B-SAPT-015-6	Traitement des protocoles	NFSv4	Envoi d'un malware tel que les cryptolockers déjà reçus via NFSv4	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFSv4 n'a pas été détecté
B-SAPT-015-7	Traitement des protocoles	SMB	Envoi d'un malware tel que les cryptolockers déjà reçus via SMB	M	KO(MAJ)	Le malware diffusé au moyen du protocole SMB n'a pas été détecté
Q-SAPT-016	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						3 critères mineurs non conformes
						6 critères majeurs non conformes

5.2.7 Avantages de la solution

— L'intégration de WildFire est très simple dans une entreprise possédant un NGFW Palo Alto ;
— Il n'y a pas de latence ajoutée au flux réseau analysé ;
— WildFire peut traiter les flux chiffrés grâce à la décryption SSL du NGFW Palo Alto.

5.2.8 Inconvénients de la solution

— WildFire est une solution basée réseau. Elle nécessite l'agent Traps pour couvrir toutes les sources d'infection d'un APT ;
— Le web portal est très basique, très peu de fonctionnalités sont disponibles. Elle ne permet pas d'effectuer un grand nombre d'actions ni d'appliquer un grand nombre de filtres sur les recherches.

5.2.9 Conformité de WildFire aux nécessités générales d'une solution ATP

Le tableau suivant résume les conformités ainsi que les résultats des tests effectués concernant les besoins généraux établis au point 4.1 :

Agent endpoint	Traps est l'agent permettant d'effectuer cette fonctionnalité
Alerting	Le NGFW Palo Alto est capable d'envoyer des logs sur un serveur syslog ou au SIEM
Analyse du trafic	Le trafic est analysé sur base des règles du NGFW
Blocage	Le blocage des malwares connus peut être effectué par le NGFW. Les malwares inconnus ne sont pas blocables par le NGFW. Le blocage se fait au niveau des endpoints si l'analyse de la sandbox révèle un malware
Emails	Les mails sont correctement analysés et les fichiers malveillants sont correctement détectés
Flux chiffrés	Le NGFW Palo Alto est capable d'effectuer la décryption SSL
HA	Le HA est possible avec plusieurs NGFW Palo Alto
Mobile	Des anomalies concernant l'analyse de fichiers APKs ont étés relevées durant les tests. Le WildFire n'était pas capable d'exécuter le fichier dans une sandbox Android
Sandboxing	Le sandboxing a permis de contrer 4/5 des mécanismes d'évasion testés
Support des fichiers	Les malwares archivés sous format TAR et RAR n'ont pas été détectés lors des tests. Les autres fichiers annoncés comme supportés par la solution ont étés testés et bien détectés par la sandbox.
Support des protocoles	Des anomalies ont étés détectées concernant les protocoles de transfert de fichiers. Les malwares échangés avec des protocoles mails et web ont correctement étés détectés par la sandbox
Threat Intelligence	WildFire intègre une fonction de Threat Intelligence
Web	Les malwares en provenance du web ont étés correctement détectés

5.3 Advanced Malware Protection de Lastline

5.3.1 Fonctionnement général

Lastline est une solution basée uniquement au niveau réseau. Elle ne dispose donc pas d'agent endpoint. Différentes architectures sont envisageables. En plus du sandboxing, Lastline est capable de détecter le C&C.
La solution Lastline comporte 3 boîtiers :
— Le sensor qui capture le trafic et l'envoie à l'engine ;
— L'engine qui effectue le sandboxing,,
— Le manager qui corrèle les alertes entre les engines et les sensors.

Lastline a été testé avec un boîtier de PoC en mode de détection uniquement. Ce boîtier effectue les tâches des trois appareils cités précédemment.

5.3.2 Sandboxing Lastline

Le sandboxing de Lastline diffère des autres solutions. Lastline utilise des sandbox de nouvelle génération dotée d'un Full System Emulation. Ce système combine les avantages de la virtualisation et de l'émulation. La virtualisation est moins facilement détectable que l'émulation. Cependant, l'émulation permet d'avoir une meilleure vue sur le comportement d'un malware. Le Full System Emulation combine la visibilité de l'émulation ainsi que la quasi-furtivité de la virtualisation.

OS disponibles

Lastline émule des environnements Microsoft Windows XP, Windows Seven 32 et 64 bits, Mac OS X et Android.

Types de fichiers analysés

Lastline est capable d'analyser les fichiers suivants :
— Portable Executable (PE) ;
— Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .docm, .xlsm, .pptm, .rtf) ;
— Java Archives (JAR) ;
— Adobe Portable Document format (PDF) ;
— Android Package (APK) ;
— De nombreux formats d'archive (ZIP, BZIP, GZIP, RAR, TAR, LHA / LZH, XZ) ;
— HWP ;
— XPF ;
— CHM ;
— URLs.

Comportement anti-évasion de sandbox

Tel qu'expliqué au point 5.2.2, des malwares de test ont étés créés pour tester l'efficacité des sandbox. Le tableau suivant résume les mécanismes d'évasion implémentés ainsi que le verdict de la sandbox :

Pas de mécanisme d'évasion	Le malware se déclenche lors de son exécution, aucun mécanisme n'est implémenté. Il permet de connaître les résultats lors de l'activation du malware
Déplacement du curseur	Le malware ne se déclenche que lorsque le curseur de la souris se déplace
Double click	Le malware ne se déclenche que lors d'un double click
Frappe au clavier	Le malware ne se déclenche que lorsqu'une frappe au clavier est détectée
Déplacement du curseur + double click + frappe au clavier	Le malware ne se déclenche que lorsque les trois critères précédents sont détectés
Déplacement du curseur + double click + frappe au clavier + boîte de dialogue	Le malware ne se déclenche que lorsqu'est détecté le déplacement de curseur, le double click, la frappe au clavier, et l'acceptation des alertes que génère le malware

En vert sont représentés les malwares ayant été détectés par Lastline. En rouge sont ceux qui ne l'ont pas été.

Capacité de personnalisation de sandbox

Lastline n'offre pas la possibilité de personnaliser les environnements émulés.

5.3.3 Protocoles supportés

Lastline analyse tout le trafic pour détecter le phénomène de C&C. En ce qui concerne l'analyse à destination de la sandbox, Lastline analyse différents protocoles, dont les suivants :

— HTTP ;
— FTP ;
— SMB ;
— SMTP ;
— IMAP ;
— POP.

5.3.4 Endpoints

Lastline ne possède pas de solution endpoint. Il est cependant possible d'utiliser des agents NGES compatibles avec Lastline. Parmi les agents compatibles, on retrouve notamment l'agent Carbon Black ou encore l'agent ECAT de RSA. Ces agents ne possèdent pas seulement la capacité de communiquer avec Lastline. Ils sont équipés de bien d'autres fonctions.

5.3.5 Décryption SSL

Lastline ne possède à ce jour pas la fonctionnalité de décryption SSL. Il est au programme du constructeur d'ajouter cette fonctionnalité à son produit. Il est possible de recevoir le trafic déchiffré depuis un NGFW effectuant cette tâche.

5.3.6 Blocage

Lastline peut être implémenté avec une architecture TAP ou in-line. Les moyens de blocage de ce genre d'architecture se trouvent au point 3.5.1.

5.3.7 Résultats de tests

L'entièreté des tests effectués ainsi que les résultats obtenus sont les suivants (l'annexe B est une version agrandie de ces tests) :
(Suite à la demande de Nethys, une grande partie des tests ont étés camouflés.)

ID	Domaine	Description	Scénario	Priorité	C-LL	R-LL
Q-SAPT-001				M	OK	
Q-SAPT-002	Débit	Mesure et analyse du débit, est-ce que le débit annoncé correspond bien au débit mesuré	Utilisation d'un client et d'un serveur "iperf" pour mesurer le débit entre deux machines en passant par la solution	M	KO(MIN)	Sans LastLine : AVG : 940 Mbit/s Avec LastLine : Résultat 1 : 798 Mbit/s Résultat 2 : 855 Mbit/s Résultat 3 : 800 Mbit/s Résultat 4 : 827 Mbit/s AVG : 820 Mbit/s : 87% de moins que les 940Mbit/s de départ
Q-SAPT-003				M	OK	
Q-SAPT-004	Flux chiffrés	Est-ce que la solution sait analyser les flux chiffrés	Téléchargement depuis un serveur HTTPS comme "MEGA", d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement du filtrage avec des flux chiffrés	M	KO(MAJ)	La solution a été testée sans l'intégration nécessaire d'appareils permettant le déchiffrement SSL
Q-SAPT-005				M	OK	
Q-SAPT-006				M	OK	
Q-SAPT-007				O	OK	
Q-SAPT-008			correctement	M	OK	
Q-SAPT-009	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-09-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-010				M	OK	
Q-SAPT-011				S	OK	
Q-SAPT-012						
B-SAPT-012-1				M	OK	
B-SAPT-012-2				M	OK	
B-SAPT-012-3				M	OK	
B-SAPT-012-4				M	OK	
B-SAPT-012-5	Traitement des fichiers	Tar	Téléchargement d'un malware sous la forme de fichier Tar	M	KO(MAJ)	Le malware diffusé sous forme Tar n'a pas été détecté par LastLine
B-SAPT-012-6				M	OK	
Q-SAPT-013						
B-SAPT-013-1				M	OK	
B-SAPT-013-2				M	OK	
B-SAPT-013-3				M	OK	
B-SAPT-013-4	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MIN)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté par LastLine
B-SAPT-013-5				M	OK	
B-SAPT-013-6	Traitement des protocoles	NFS	Envoi d'un malware tel que les cryptolockers déjà reçus via NFS	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFS n'a pas été détecté par LastLine
B-SAPT-013-7				M	OK	
Q-SAPT-014	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						3 critères mineurs non conformes
						4 critères majeurs non conformes

5.3.8 Avantages de la solution

— La solution ne nécessite pas d'appareils séparés pour traiter le flux mail et le flux web, ce qui permet d'éviter de potentiels conflits entre Lastline et les solutions déjà en place dans le cas ou une intégration ou une collaboration des solutions n'est possible ;
— La solution possède un système de sandboxing innovant ayant pour but d'obtenir le plus de détail sur l'exécution des malwares tout en étant quasi-furtif ;
— Il n'y a pas de latence ajoutée au flux réseau analysé pour l'architecture TAP ;
— La solution a obtenu un score de 95,9% aux tests réalisés par NSS Lab.

5.3.9 Inconvénients de la solution

— La solution ne peut être utilisée seule, car elle ne couvre pas tous les points d'infection d'un APT. L'intégration d'un NGES est alors indispensable en cas d'implémentation.

5.3.10 Conformité de Lastline aux nécessités générales d'une solution ATP

Le tableau suivant résume les conformités ainsi que les résultats des tests effectués concernant les besoins généraux établis au point 4.1 :

Agent endpoint	Lastline ne possède pas d'agent endpoint. Cependant, il est possible d'intégrer des agents d'autres constructeurs
Alerting	Lastline permet d'envoyer des logs à un serveur syslog ou au SIEM
Analyse du trafic	Lastline analyse le trafic y compris pour détecter le C&C
Blocage	Le blocage peut se faire à plusieurs niveaux. Cependant, si un agent n'est pas utilisé, il n'est pas toujours possible de bloquer
Emails	Les emails sont analysés par la solution
Flux chiffrés	Les flux chiffrés doivent être déchiffrés par un tiers appareil puis envoyés à Lastline car la solution ne possède pas la fonction de décryption SSL
HA	Les managers et les engines sont capables de faire du HA. Pour les sensors, cela dépend de l'architecture et de la topologie du réseau
Mobile	La solution permet de détecter des APKs malveillants
Sandboxing	Le système de sandboxing de Lastline est un système performant et innovant qui permet une détection approfondie du comportement des malwares. Le PoC a permis de le démontrer
Support des fichiers	Les malwares archivés sous format TAR n'ont pas été détectés lors des tests. Les autres fichiers correctement analysés par Lastline correspondent aux fichiers susceptibles de contenir du contenu malveillant
Support des protocoles	Les protocoles mail, web et de partage de fichiers sont supportés
Threat Intelligence	Lastline possède la fonction de Threat Intelligence
Web	Les menaces en provenance du web sont détectables

5.4 FortiSandbox de Fortinet

FortiSandbox est la Sandbox de Fortinet. Celle-ci peut interagir avec les autres éléments de la marque. Il peut s'agir de FortiWeb, FortiMail, FortiClient ou encore FortiGate.

5.4.1 Fonctionnement général

Cette solution peut fonctionner avec une architecture TAP. L'idéal est de pouvoir l'intégrer dans un environnement où se trouvent d'autres produits Fortinet tels que cités dans le point précédent. Cette intégration permet de remédier aux attaques ainsi que de s'en protéger.

La solution a été testée en mode TAP et sans intégration à d'autres produits Fortinet. La version testée était la 2.2 et semblait avoir différents soucis. La solution n'a été testée qu'en présence de VM Windows XP et Windows Seven (32/64 bits)

5.4.2 Sandboxing FortiSandbox

Le système de sandboxing est la virtualisation. Il a été observé lors de tests que la sandbox ne détectait pas toutes les actions effectuées par le malware. Dans le cas des malwares de tests, les actions sur la registry n'étaient que partiellement détectées.

OS disponibles

Il est possible de configurer des environnements Windows XP, Windows 7 (32/64 bits), Windows 8.1, Windows 10 et Android.

Types de fichiers analysés

Seuls les fichiers suivants sont analysables par FortiSandbox :
— Portable Executable (PE) ;
— Microsoft Office ;
— Adobe Flash ;
— Java Archives (JAR) ;
— Adobe Portable Document format (PDF) ;
— Android Package (APK) ;
— Scripts (.js,.bat,.vbs,.ps1,.cmd) ;
— Media (.avi, .mpeg, .mp3, .mp4) ;
— Archives (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z,.cab, .rar, .arj).

Comportement anti-évasion de sandbox

Le tableau suivant résume les mécanismes d'évasion implémentés ainsi que le verdict de la sandbox :

Pas de mécanisme d'évasion	Le malware se déclenche lors de son exécution, aucun mécanisme n'est implémenté. Il permet de connaître les résultats lors de l'activation du malware
Déplacement du curseur	Le malware ne se déclenche que lorsque le curseur de la souris se déplace
Double click	Le malware ne se déclenche que lors d'un double click
Frappe au clavier	Le malware ne se déclenche que lorsqu'une frappe au clavier est détectée
Déplacement du curseur + double click + frappe au clavier	Le malware ne se déclenche que lorsque les trois critères précédents sont détectés
Déplacement du curseur + double click + frappe au clavier + boîte de dialogue	Le malware ne se déclenche que lorsqu'est détecté le déplacement de curseur, le double click, la frappe au clavier, et l'acceptation des alertes que génère le malware

En vert sont représentés les malwares ayant été détectés par FortiSandbox. En rouge sont ceux qui ne l'ont pas été.

Capacité de personnalisation de sandbox

Une fonctionnalité très intéressante et retrouvée uniquement chez cette solution est la capacité de personnalisation de sandbox. Il est possible de choisir quels fichiers seront analysés dans quel sandbox. Il est également possible de changer le nombre de VM pour chaque OS disponible. Le nombre de VM est limité au hardware. Il s'agit plus ici de gestion de VM que de personnalisation

Cependant, il est prévu dans les prochaines versions de la sandbox de pouvoir installer des logiciels sur les VM utilisées par la FortiSandbox.

5.4.3 Protocoles supportés

En étant en mode sniffer sur le TAP, la solution peut analyser les protocoles suivants :
— HTTP ;
— FTP ;
— POP3 ;
— IMAP ;
— SMTP ;
— SMB.

Les appareils Fortinet peuvent envoyer des fichiers à la FortiSandbox pour qu'elle les analyse. Ils sont les suivants :
— FortiGate : HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM ainsi que leurs équivalents encryptés avec SSL ;
— FortiMail : SMTP, POP3, IMAP ;
— FortiWeb : HTTP.

5.4.4 FortiClient

FortiClient est l'agent Fortinet permettant d'interagir avec la FortiSandbox et d'effectuer les fonctions attendues d'un agent endpoint.

5.4.5 Résultats de tests

L'entièreté des tests effectués ainsi que les résultats obtenus sont les suivants (l'annexe C est une version agrandie de ces tests) :
(Suite à la demande de Nethys, une grande partie des tests ont étés camouflés.)

ID	Domaine	Description	Scénario	Priorité	C-FN	R-FN
Q-SAPT-001	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-002	Débit	Mesure et analyse du débit, est-ce que le débit annoncé correspond bien au débit mesuré	Envoi de fichiers exécutables ou de scripts avec des hashs différents afin de confirmer le débit de fichiers analysés	M	KO(MIN)	Le capacité à analyser le débit d'élément n'est pas toujours suffisante
Q-SAPT-003	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-004	Mobile	Est-ce que le système détecte les menaces venant de mobiles	Téléchargement d'un APK malveillant	O	KO(MIN)	APK non détecté par signature mais pas de VM Android pour le test
Q-SAPT-005	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-006	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-06-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	KO(MIN)	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware" mais les actions effectuées sur la registry ne sont pas toutes détectées
Q-SAPT-06-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-07	Sandboxing	Est-ce que le sandbox détecte bien la création, suppression, modification de clés de registre	Écriture d'un programme de test en C# qui modifie, crée ou supprime des clés de registre	M	KO(MAJ)	La sandbox n'a pas correctement repéré les actions effectuées sur la regirstry. Toutes las cations ne sont pas détectées. Ceratins oui, et d'autres non
Q-SAPT-08	[illegible]	[illegible]	[illegible]	S	OK	[illegible]
Q-SAPT-09	[illegible]	[illegible]	[illegible]			
B-SAPT-09-1	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-2	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-3	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-4	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-5	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-010	[illegible]	[illegible]	[illegible]			
B-SAPT-010-1	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-010-2	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MAJ)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté par la FortiSandbox
B-SAPT-010-3	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-010-4	Traitement des protocoles	NFS	Envoi d'un malware tel que les cryptolockers déjà reçus via NFS	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFS n'a pas été détecté par la FortiSandbox
B-SAPT-010-5	Traitement des protocoles	SMB	Envoi d'un malware tel que les cryptolockers déjà reçus via SMB	M	KO(MAJ)	Le malware diffusé au moyen du protocole SMB n'a pas été détecté par la FortiSandbox
Q-SAPT-011	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						4 critères mineurs non conformes
						8 critères majeurs non conformes

5.4.6 Avantages de la solution

— L'interface de management est très complète et permet de gérer les VM ;
— Intégration de différentes étapes avant de passer au sandboxing (AV scan, code emulation, ...) ;
— Elle permet de traiter le flux SSL ;
— Elle n'ajoute pas de latence réseau ;
— La solution a obtenu un score de 87,6% aux tests réalisés par NSS Lab.

5.4.7 Inconvénients de la solution

— Le produit semble subir de nombreux bugs. En voici quelques exemples :
  — Bug d'affichage des statistiques de processing ;
  — Bug d'affichage des analyses des VMs ;
  — Bug, ou manque de précision sur la détection des actions des malwares ;
  — Les liens vers les encyclopédies de malwares sont introuvables ;
  — Malfonctionnement des commandes du CLI servant à purger la file d'attente des analyses ;
  — Les fichiers PDFs font augmenter la taille de la file d'attente de manière improbable ;
— Suite aux tests effectués, le produit semble avoir quelques lacunes notamment au niveau du sandboxing ;
— L'accumulation de fichiers à analyser dans la file d'attente ajoute une latence au temps de détection d'un malware.

5.4.8 Conformité de FortiSandbox aux nécessités générales d'une solution ATP

Le tableau suivant résume les conformités ainsi que les résultats des tests effectués concernant les besoins généraux établis au point 4.1 :

Agent endpoint	FortiClient remplit cette fonction
Alerting	La FortiSandbox envoie des logs
Analyse du trafic	La solution reçoit et analyse le trafic de différentes sources
Blocage	Le blocage peut se faire de manières différentes en fonction des appareils Fortinet présents dans l'infrastructure
Emails	La FortiSandbox est capable d'analyser les emails
Flux chiffrés	Le FortiGate permet d'effectuer la décryption SSL et d'envoyer le trafic déchiffré à la FortiSandbox
HA	Le HA est possible entre les FortiSandbox
Mobile	Les APKs malveillants n'ont pas été détectés durant les tests effectués
Sandboxing	Dans l'environnement de test utilisé, le sandboxing n'a pas permis d'avoir une détection correcte des actions effectuées par les malwares. Elle n'a pas non plus permis de contrer de simples mécanismes d'évasion
Support des fichiers	Un grand nombre de fichiers sont analysables
Support des protocoles	La FortiSanbox n'a détecté aucun malware échangé via les protocoles de partage de fichier standards (SMB, NFS, FTP) dans l'environnement de test utilisé
Threat Intelligence	La solution de Fortinet intègre une fonction de Threat Intelligence
Web	Les menaces en provenance du web sont détectées

Bien entendu, les tests ont étés effectués dans un environnement bien précis. Le changement de l'architecture peut influencer les résultats. Le couplage de la FortiSandbox au FortiGate permet d'utiliser les moteurs de capture du firewall. Ces derniers sont plus puissants que ceux de la FortiSandbox et permettent d'avoir une solution plus optimisée.

5.5 Deep Discovery de Trend Micro

Deep Discovery est une solution qui n'a pas été testée. Les annonces faites ne sont que théoriques, car elles n'ont pas étés vérifiées.

5.5.1 Fonctionnement général

La gamme Deep Discovery comporte plusieurs appareils :
— Deep Discovery Inspector : analyse le flux réseau, il permet d'effectuer du sandboxing ;
— Deep Discovery Email Inspector : analyse le flux email, il permet d'effectuer du sandboxing ;
— Deep Discovery Endpoint Sensor : est l'agent endpoint ;
— Deep Discovery Analyser : est un appareil consacré au sandboxing. Il peut être utilisé pour centraliser le sandboxing des produits Deep Discovery.

5.5.2 Sandboxing Deep Discovery

OS disponibles

Trend Micro indique pouvoir détecter des menaces à destination de Windows, Android, Mac, Linux et d'autres.

Types de fichiers analysés

Seuls les fichiers suivants sont analysables par Deep Discovery :
— Portable Executable (PE) ;
— Microsoft Office ;
— Adobe Portable Document format (PDF) ;
— Java Archives (JAR) ;
— Archives ;
— SWF ;
— Ink ;
— HWP ;
— CELL ;
— JTD ;
— GUL ;
— CHM.

Comportement anti-évasion de sandbox

Deep Discovery est continuellement mis à jour contre les techniques d'évasion.

Capacité de personnalisation de sandbox

Il est possible avec cette solution d'utiliser des images custom pour les VMs.

5.5.3 Protocoles supportés

Deep Discovery supporte plus de 80 protocoles, dont les protocoles web (HTTP), mail (IMAP, POP, SMTP), et de transfert de fichiers (SMB, FTP , NFS).

5.5.4 Deep Discovery endpoint sensor

Deep Discovery endpoint sensor est l'agent de Trend Micro permettant d'interagir avec le reste de la solution Deep Discovery et d'effectuer les fonctions attendues d'un agent endpoint.

5.5.5 Décryption SLL

Deep Discovery n'est pas capable d'effectuer la décryption SSL. Tout comme Lastline, il peut recevoir le trafic déchiffré depuis un appareil ayant cette fonction.

5.5.6 Avantages de la solution

— Couvre toutes les sources d'infection (web, mail, endpoint, autre) ;
— Possibilité de personnalisation des images utilisées par les VMs ;
— La solution a obtenu un score de 96,6% aux tests réalisés par NSS Lab.

5.5.7 Inconvénients de la solution

— Ne permet pas d'effectuer la décryption SSL. Nécessite l'usage d'un appareil ayant cette fonction.

5.5.8 Conformité de Deep Discovery aux nécessités générales d'une solution ATP

Le tableau suivant résume les conformités théoriques concernant les besoins généraux établis au point 4.1 :

Agent endpoint	Deep Discovery endpoint sensor remplit cette fonctionnalité
Alerting	Deep discovery peut envoyer des logs et s'intégrer dans un SIEM
Analyse du trafic	Deep Discovery est capable de détecter le C&C
Blocage	La capacité de blocage est identique aux autres solutions, il n'est possible de bloquer un élément que lorsque sa nature est connue
Emails	Deep Discovery est capable d'analyser les emails ainsi que leur contenu
Flux chiffrés	La solution n'est pas capable de décrypter le flux SSL. Elle nécessite qu'un autre appareil lui envoie le trafic déchiffré
HA	Plusieurs appareils effectuant les mêmes fonctions peuvent être connectés au TAP
Mobile	Trend Micro dit pouvoir détecter des menaces à l'intention d'Andoird, cependant il n'est pas dit que les fichiers APK peuvent être analysés
Sandboxing	Il est possible de personnaliser les images utilisées par la sandbox. Des mécanismes anti-évasion sont implémentés
Support des fichiers	Les fichiers supportés répondent aux attentes
Support des protocoles	Deep Discovery supporte plus de 80 protocoles
Threat Intelligence	Trend Micro Smart Protection Network est la solution de Threat Intelligence de Trend Micro
Web	La solution est capable de détecter les menaces en provenance du web

5.6 Comparaison des différentes solutions

Il est possible de comparer les solutions sur de nombreux critères. La comparaison faite ici est une comparaison des éléments nécessaires pour une solution ATP. Les conformités sont basées sur les réponses obtenues de la part des fournisseurs, sur la documentation, sur les meeting organisés ainsi que sur les résultats des tests effectués. Seules trois solutions ont étés testées. Il est possible d'avoir un meilleur jugement sur ces solutions que sur des faits théoriques. Les Solutions testées sont Lastline AMP, WildFire et FortiSandbox. Les solutions non-testées sont Cisco AMP et Deep Discovery.

Le tableau suivant reprend les différentes solutions ainsi que leurs conformités aux besoins établis au point 4.1.

	LL	PA	FN	CC	TM
Agent endpoint	NC	C	C	C	C
Alerting	C	C	C	C	C
Analyse du trafic	C	C	C	C	C
Blocage	PC	PC	PC	PC	PC
Emails	C	C	C	C	C
Flux chiffrés	PC	C	C	C	PC
HA	PC	C	C	C	C
Mobile	C	NC	NC	PC	PC
Personnalisation de sandbox	NC	NC	PC	NC	C
Sandboxing	C	PC	NC	PC	C
Support des fichiers	PC	PC	C	C	C
Support des protocoles	C	PC	NC	C	C
Threat Intelligence	C	C	C	C	C
Web	C	C	C	C	C

Les solutions reprises dans le tableau sont respectivement les solutions des constructeurs suivants : Lastline (Advanced Malware protection), Palo Alto (WildFire), Fortinet (FortiSandbox), Cisco (Advanced Malware Protection), Trend Micro (Deep Discovery).

Les éléments de conformité repris dans le tableau sont C (conforme), PC (Partiellement conforme), NC (non conforme).

Il est à prendre en compte que les tests ont étés réalisés dans un environnement bien spécifique. Il est possible que certaines solutions requièrent une architecture différente afin d'être optimales.

6. Solution open source

6.1 Cuckoo sandbox

6.1.1 Qu'est ce que Cuckoo

Cuckoo Sandbox est un système d'analyse de malware. C'est une solution Open Source qui exécute toute une série de script Python. Cuckoo possède plein d'avantages dûs à l'ouverte du code. Il est possible de modifier un grand nombre de choses.

Il s'agit d'une solution de sandboxing moins complète que les solutions évaluées précédemment. Cette solution de sandboxing demande plus de configuration et de connaissance sur le sandboxing que pour l'installation d'une solution payante. Il est nécessaire de savoir quels sont les modules nécessaires et comment les configurer.

6.1.2 Environnement virtualisé ou émulé ?

Cuckoo utilise des hyperviseurs ou des émulateurs pour effectuer le sandboxing. On retrouve notamment VirtualBox ou encore VMWare. Il est également possible d'utiliser QEMU qui est un émulateur. Il est alors possible de fabriquer une solution qui se rapproche plus au sandboxing de Lastline. Cuckoo se charge d'interagir de manière automatique avec l'émulateur ou l'hyperviseur choisi.

Les environnements virtuels ou émulés sont en fait de simples machines dans lesquelles un agent permettant de communiquer avec Cuckoo est exécuté.

Schématiquement, le résultat est le suivant :

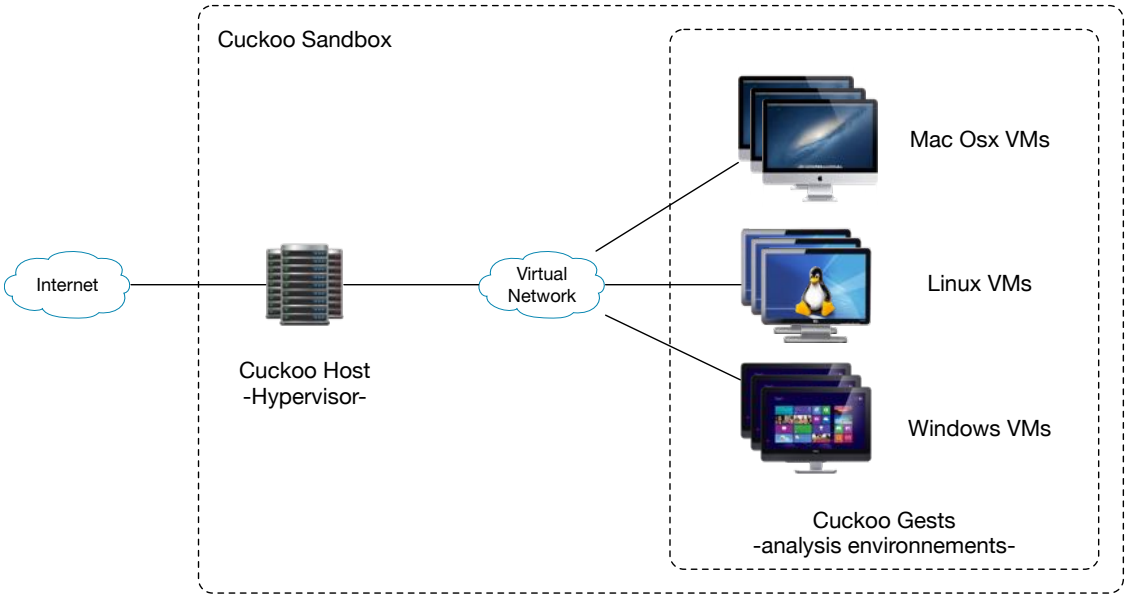


FIGURE 6.1 – Architecture d'une solution Cuckoo

6.1.3 Quels OS sont supportés

Il est possible de faire des analyses de grand nombre d'OS. On retrouve Windows, Mac OS X, Android et Linux. Il est possible de personnaliser les sandboxs autant que souhaité. Il suffit de prendre le contrôle des environnements avant de les mettre en production pour y apporter les modifications voulues.
De nombreux modules existent pour effectuer différents types d'analyses.

6.1.4 Mécanismes d'évasion

Un niveau des interactions humaines, Cuckoo effectue des déplacements de curseurs, des frappes au clavier, etc. Et ce qui concerne la détection de sandbox via des éléments de virtualisation, rien n'est fait étant donné que la sandbox doit être construite par celui voulant s'en équiper. Libre à qui veut d'ajouter ou de supprimer des éléments dans ces environnements pour éviter la détection de sandbox. De plus, étant personnalisable à 100%, il est possible d'importer le clone d'une machine utilisée sur le réseau. La sandbox sera alors identique au niveau du contenu à cette machine. Les malwares ne se déclenchant qu'en présence d'un logiciel seront alors détectés.

6.1.5 Configuration avancée

Dans un premier temps, Cuckoo permet uniquement de soumettre des fichiers à analyser de manière manuelle. Il est ensuite possible de configurer et d'implémenter des APIs pour effectuer un envoi automatique de contenu à analyser.
Cuckoo a été testé avec des compétences de débutant en la matière. Il est certainement possible d'arriver à un résultat identique, si pas meilleur, que celui obtenu par les solutions vendues du chapitre 5 avec des compétences d'expert en la matière.

6.1.6 Inconvénients de Cuckoo

— L'avantage de l'open source est également le plus gros inconvénient de Cuckoo. N'importe qui peut se procurer le code de Cuckoo et implémenter différents types de sandbox. Il peut s'agir de personnes qui utilisent Cuckoo pour se protéger, mais il peut aussi s'agir d'hackers testant leurs malwares évasifs afin de les rendre furtifs.

6.1.7 Avantages de Cuckoo

— Cuckoo est une solution open source qui peut être modifiée si nécessaire, elle demande cependant plus de travail de mise en place qu'une solution telle que celles examinées au chapitre 5 ;
— Des solutions telles que celles du chapitre 5 ont un coût non négligeable. Une solution de type de celle de Cuckoo peut être une bonne première ligne de défense dans des entreprises n'ayant pas de grand budgets dédiés à la sécurité informatique.

6.1.8 Analyse d'un malware

Ci-dessous se trouve un aperçu du résultat d'une analyse faite par une sandbox Cuckoo dont la configuration est relativement basique. Un rapport dans son entièreté est plus détaillé. Il comporte également de nombreux points d'analyse. Tel qu'on le devine sur les screenshots, le malware analysé est un ransonware.

Dashboard | Recent | Pending | Search | Submit

cuckoo

Compare this analysis to... | Resubmit this sample

Quick Overview | Static Analysis | Behavioral Analysis (2) | Network Analysis (59) | Dropped Files (1) | Dropped Buffers (1) | Process Memory (1) | Memory Analysis | Admin

This file is definitely malicious with a score of **6.8 out of 10!** You should **NOT** open this file on a production system.

Note that the scoring system is still in alpha state and should not yet be considered as a definitive outcome. Please at all times check the analysis yourself - especially when the scoring says it's benign.

Analysis

Category	Started	Completed	Duration	Log
FILE	2016-05-15 12:05:21	2016-05-15 12:09:25	244 seconds	Show Log

Machine

Name	Label	Manager	Started On	Shutdown On
cuckoo1	Seven	VirtualBox	2016-05-15 12:05:21	2016-05-15 12:09:25

File Details

File Name	avis n.000113385653.zip.exe
File Size	754690 bytes
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	d490333b5aad22880b4f582655205305
SHA1	96fee0b37835a4e98cca125976290ce7828b7a52
SHA256	05981146fe3c52c09ccba0c3ac001262d2918c6b87368c88222b4c660cf65455
SHA512	9cc279933adbb62cbbfaea8ce67f0665aa186c349146c38e4a874fea96e7e6b050f861b19692018ae47ccfb103e7f7b27628e38f4dc9dae3978b9e88498595f6
CRC32	EEF15A73
Ssdeep	None
Yara	None matched

Download

Signatures

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)

The executable has PE anomalies (could be a false positive) (1 event)

One or more potentially interesting buffers were extracted, these generally contain injected code, configuration data, etc.

Allocates read-write-execute memory (usually to unpack itself) (6 events)

A process attempted to delay the analysis task. (1 event)

Creates executable files on the filesystem (1 event)

File has been identified by at least one AntiVirus on VirusTotal as malicious (1 event)

One or more thread handles in other processes (1 event)

Raised Snort alerts (2 events)

PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (50 events)

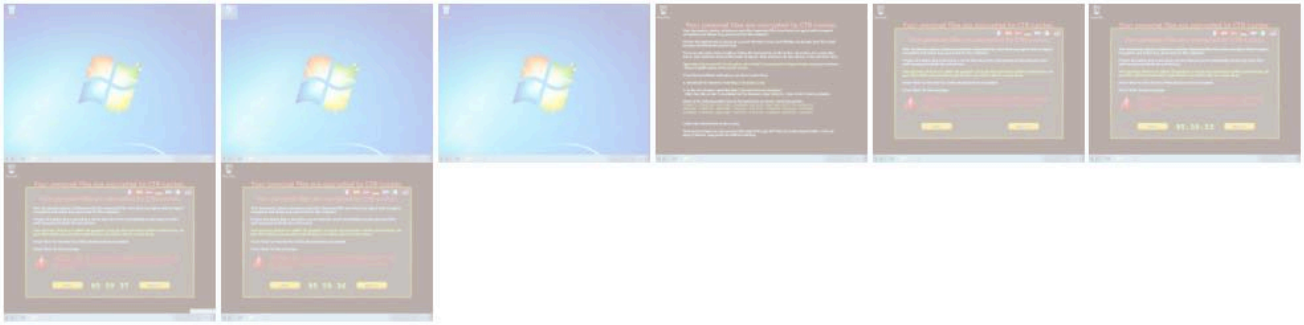
Malfind detects one or more injected processes (1 event)

Stopped Firewall service (1 event)

Stopped Application Layer Gateway service (1 event)

Executed a process and injected code into it, probably while unpacking (16 events)

Screenshots



Hosts

No hosts contacted.

DNS

Name	Response	Post-Analysis Lookup
time.windows.com		
www.msftncsi.com		212.68.207.153
teredo.ipv6.microsoft.com		

Summary

Files | Registry | Mutexes | Directories | Processes

Process avis n.000113385653.zip.exe (3376)

Opened files

- C:\ProgramData\Microsoft\dplxuib
- C:\Users\Johnson\AppData\Local\Temp\avis n.000113385653.zip.exe
- C:\Users\Johnson\AppData\Local\Temp\hmujuwf.exe

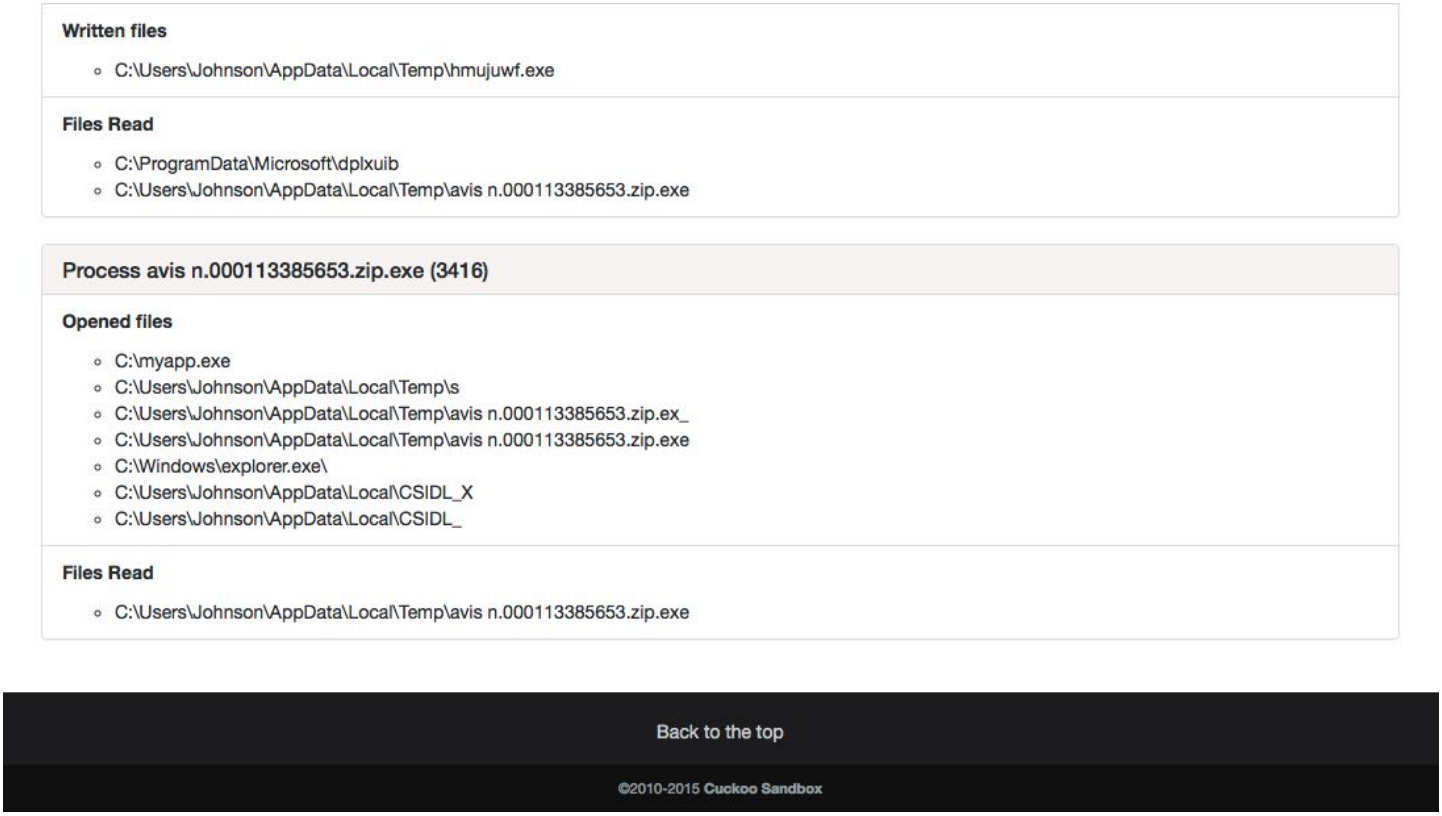


FIGURE 6.2 – Rapport d'analyse d'une Cuckoo sandbox

6.2 Autres solutions

Cuckoo n'est pas la seule solution Open Source du marché. Il existe une variété de sandbox effectuant des tâches plus ou moins similaires. Limon sandbox permet d'analyser le comportement de malwares à destination de systèmes Linux.

Les créateurs d'Anubis et de Wepawet (qui permettent respectivement de recevoir le rapport des actions d'un exécutable Windows ou Android, et de recevoir le rapport concernant un site web) sont les créateurs de Lastline. Les solutions open source sont parfois le début d'un projet d'une grande envergure telles que Lastline.

Conclusion

Après 14 semaines passées à me documenter sur le sujet de diverses façons dans un domaine qui m'était jusque là inconnu, les APTs m'ont beaucoup intrigué. J'ai beaucoup appris sur la sécurité informatique, qui est une bataille infinie opposant attaquants et défenseurs. Ce que j'en ai retenu est que les solutions utilisées au cours de temps pour contrer les attaques finissent toujours par être dépassées et/ou contournées. En effet, rien n'arrête l'évolution technologique, qu'elle soit à caractère bienveillant ou non.

J'avais pour objectif, au cours de mon stage, d'effectuer une étude des différentes solutions luttant contre les APT existantes sur le marché. Le véritable objectif qui m'a été proposé était de débuter le projet anti-APTs au sein de Nethys. Pour ce faire, j'ai dû réaliser une analyse des risques ainsi que des scénarios pour lesquels Nethys serait prise comme cible par un APT.

Issue de cette analyse, a été réalisé, une matrice des besoins auxquels devait répondre la solution anti-APTs. Cette matrice a été partagée avec différents fournisseurs de solutions. Trois solutions ont étés choisies sur base des respects théoriques des besoins établis afin d'effectuer des PoCs.

Le but de ces PoCs était de tester les performances des solutions face aux besoins établis. Les rapports effectués par mes soins sur ces solutions permettront à l'entreprise de prendre une décision sur la solution choisie pour assurer sa protection contre les APTs. À l'heure actuelle, le comité de direction de Nethys n'a pas encore été informé des résultats de mon stage au sein de l'entreprise. Lorsque la cellule sécurité leur en informera, une décision concernant la sécurité au niveau des APTs sera prise sur base de mon travail.

Mon efficacité de travail a été remerciée par le comité de direction, car elle a permis d'éviter un incident lié à mon projet. La cellule sécurité m'a également félicité pour le travail que j'ai accompli en leur présence.

Ce qui suit est ce que j'ai tiré de ces 14 semaines d'apprentissage en entreprise sur les APTs.

Les APTs sont les attaques de nouvelle génération auxquelles tout le monde est exposé de près où de loin. Les cibles peuvent être l'entreprise dans laquelle nous travaillons, nos données personnelles stockées par une organisation tierce, les secteurs énergétiques et bien d'autres. Il s'agit ici d'attaques ayant de telles répercussions qu'elles peuvent être utilisées pour la cyber-guerre. Les vecteurs vitaux tels que l'eau ou l'électricité sont gérés informatiquement et peuvent être détournés. Que faire sans électricité au 21^{e} siècle ? Les APTs sont des attaques qui peuvent être effrayantes et dévastatrices.

En ce temps, les APTs basent leurs intrusions sur 2 grands facteurs :
— Duper l'humain avec le social engineering ;
— Duper la machine avec des mécanismes d'évasion de sandbox.

Dès lorsque ces deux tromperies sont réussies, il n'est pas possible dans un premier temps de détecter une attaque et par conséquent de la stopper.

Le social engineering utilisé par les APTs est si poussé que même les meilleurs chercheurs/experts en sécurité peuvent être dupés et se voir victime de ce genre d'attaque. S'il n'est pas possible, en tant qu'homme, tout en restant productif, de détecter un APT, c'est aux machines que revient cette tâche.

Les sandbox sont à ce jour les solutions les plus utilisées et certainement les plus appropriées pour contrer les APTs. Cependant, comme toutes les technologies précédentes, elles possèdent des limites. Le système parfait n'existe pas (encore). Il n'existe pas de sandbox miracle ayant une détection incontournable. Il existe des différences entre les solutions ATP. La solution choisie par une entreprise ne dépend pas uniquement de la qualité de sandboxing de cette dernière. D'autres critères tels que l'architecture, l'intégration, ou encore le prix font partie de l'équation. Il se peut qu'une entreprise opte pour une solution n'étant pas la meilleure du marché, mais qui soit plus adaptée à ses critères de sélection.

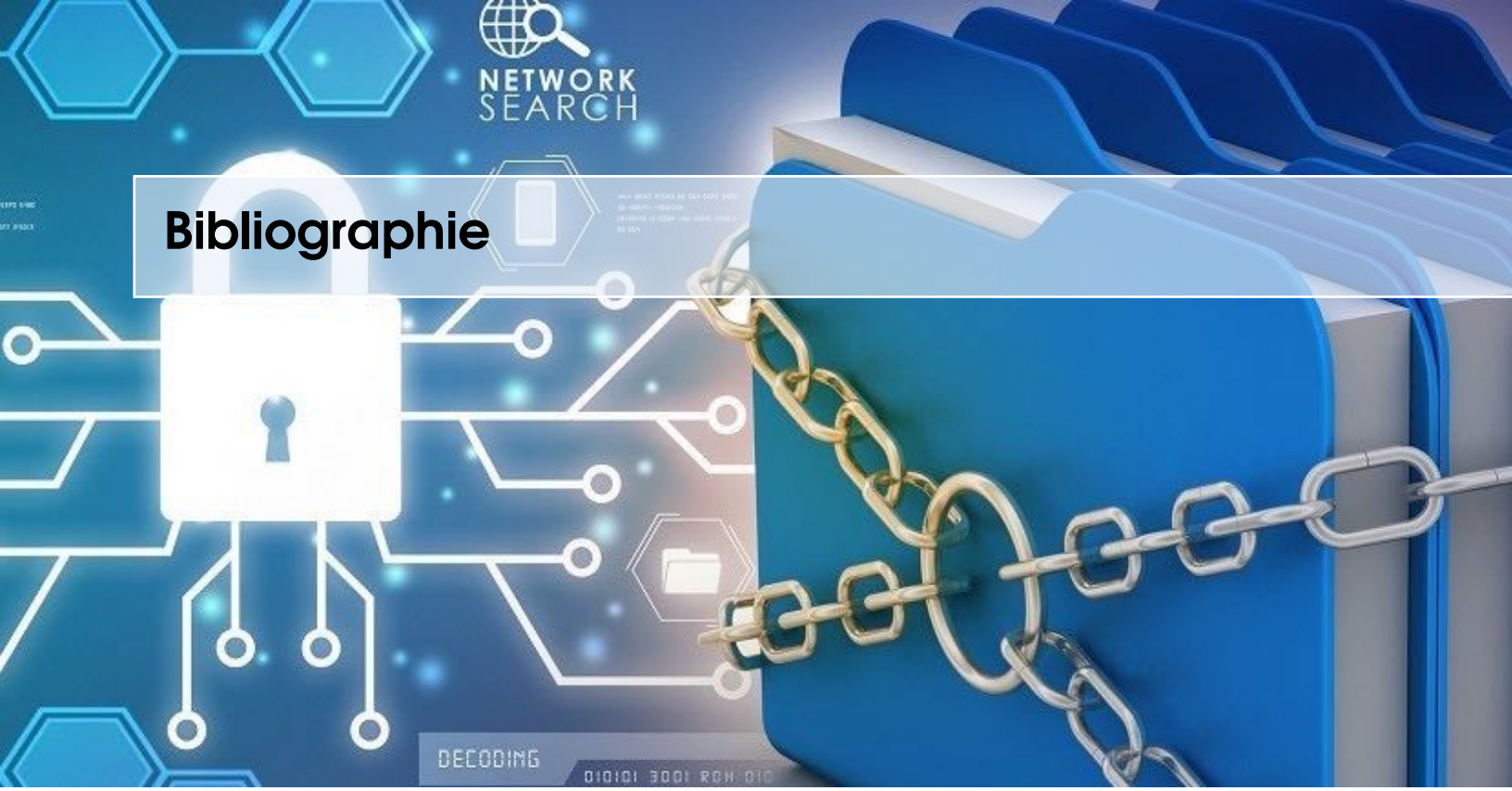
En sachant que les APTs sont généralement construits par des organisations puissantes et disposant de nombreuses ressources, qu'est-ce qui empêcherait ces mêmes organisations de s'équiper de solutions ATPs pour essayer de les contourner ? Les solutions ATPs open source sont disponibles pour tous et peuvent permettre d'élaborer des malwares évasifs. La fonction première d'un sandbox est de déterminer la nature d'un fichier grâce à une analyse comportementale. En d'autres termes, une sandbox permet principalement de détecter des malwares avancés qui sont généralement utilisés par les APTs.

La sécurité est l'ennemie directe de la productivité. La sécurité informatique est comparable à un frein de voiture de course. En ligne droite, il est inefficace, ralentit la voiture et est inutile. À l'abord d'un virage, il est cependant plus que nécessaire. Il permet d'éviter de finir dans le décor, et par conséquent de ne pas crasher la voiture. Il en est de même pour la sécurité informatique. Lorsqu'aucune attaque n'est subie par une entreprise, celle-ci se porte à merveille. Dès lors qu'elle en subit une sans avoir pu s'en protéger, celle-ci éponge des pertes, qui peuvent entraîner jusqu'à la fermeture voire la faillite de l'entreprise. Il faut trouver la parfaite harmonie entre la sécurité et la productivité.

La finalité est que sécuriser un organisme des APTs n'est pas possible à 100%. Dans le meilleur des

cas, une solution ATP permet de détecter un APT et d'y remédier. Cependant, dans le pire des cas, elle ne fait que ralentir le procédé d'intrusion de l'APT. Dans la majorité des APTs découverts, ces derniers n'ont étés identifiés que des années après leur intrusion lors d'analyses statiques réalisées par des hommes.

La véritable question concernant les APTs est la suivante : peut-on réellement stopper une attaque de type APT avec les solutions ATPs présentes sur le marché actuel ?



Bibliographie

Documentaires

[19] BOUNHIR ANASS. *La guerre invisible Docs ARTE*. URL : https://www.youtube.com/watch?v=FOH4gwF4ukk (visité le 05/04/2016).

Vidéos

[41] IBM SECURITY. *What are Advanced Persistent Threats ?* URL : https://www.youtube.com/watch?v=1qFga_DJs0c (visité le 05/04/2016).

Livres

[110] Tyler WRIGHTSON. *Advanced Persistent Threat Hacking*. Mc Graw Hill Education, 2015.

Pages Web

[1] *0day*. Korben. 15 déc. 2015. URL : http://korben.info/n-0day.html (visité le 25/04/2016).

[2] *70 ans de menaces informatiques | Dell France*. URL : http://www.dell.com/learn/fr/fr/frbsdt1/campaigns/revueit-securite-historique-menaces-informatiques (visité le 09/02/2016).

[3] *A Guide to Choosing a Next-Generation Firewall - Next Generation Firewall vs. Traditional Firewall*. Tom's IT Pro. 23 déc. 2014. URL : http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html (visité le 20/04/2016).

[4] ADMIN. *Detecting Malware With ThreatGRID Overview...* TheSecurityBlogger ... URL : http://www.thesecurityblogger.com/detecting-malware-with-threatgrid-overview/ (visité le 10/05/2016).

[5] *Advanced persistent threat*. 10 jan. 2016. URL : https://en.wikipedia.org/w/index.php?title=Advanced_persistent_threat&oldid=699079005.

[6] *Advanced Persistent Threat (APT)*. Damballa. 1er fév. 2016. URL : https://www.damballa.com/paper/advanced-persistent-threats-a-brief-description/.

[7] *Advanced Persistent Threats (APT) 101 - Advanced Persistent Threats (APT) 101*. Tom's IT Pro. 21 oct. 2015. URL : http://www.tomsitpro.com/articles/advanced-persistent-threats-apt-101,2-526.html.

[8] *Advanced Persistent Threats : How They Work | Symantec*. URL : http://www.symantec.com/theme.jsp?themeid=apt-infographic-1 (visité le 06/04/2016).

[9] *Aperçu sur la sécurité*. 8 fév. 2016. URL : http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/ch-sgs-ov.html (visité le 08/02/2016).

[10] *APT : des attaques quasi indétectables*. URL : http://www.indexel.net/securite/les-apt-des-attaques-furtives-quasi-indetectables-3627.html (visité le 15/02/2016).

[11] *APT, la menace du 3ème type | Orange Business Services*. URL : http://www.orange-business.com/fr/blogs/securite/securite-du-poste-de-travail/apt-la-menace-du-3eme-type (visité le 11/04/2016).

[12] *APT Prevention*. URL : https://www.paloaltonetworks.com/features/apt-prevention (visité le 23/04/2016).

[13] *Automated Malware Analysis - Cuckoo Sandbox*. URL : https://www.cuckoosandbox.org/ (visité le 14/05/2016).

[14] AVASTCH. *antivirus historique et fonctionnement | avast ! Antivirus gratuitavast ! Antivirus gratuit*. 8 fév. 2016. URL : http://www.avast-free-antivirus.ch/antivirus-historique-fonctionnement-test/ (visité le 08/02/2016).

[15] *Backdoor (computing)*. 21 jan. 2016. URL : https://en.wikipedia.org/w/index.php?title=Backdoor_(computing)&oldid=701007389.

[16] *Belgacom piratée par le spyware américain Regin*. 25 nov. 2014. URL : http://datanews.levif.be/ict/actualite/belgacom-piratee-par-le-spyware-americain-regin/article-normal-354843.html.

[17] *Belgacom says alleged GCHQ APT attack cost firm £12 million - SC Magazine UK*. URL : http://www.scmagazineuk.com/belgacom-says-alleged-gchq-apt-attack-cost-firm-12-million/article/378870/ (visité le 11/02/2016).

[18] Kristin BENT. *Cisco To Acquire ThreatGRID For Malware Analysis, Threat Intelligence*. CRN. URL : http://www.crn.com/news/security/300072900/cisco-to-acquire-threatgrid-for-malware-analysis-threat-intelligence.htm (visité le 06/05/2016).

[20] *Cheval de Troie (informatique)*. 19 jan. 2016. URL : https://fr.wikipedia.org/w/index.php?title=Cheval_de_Troie_(informatique)&oldid=122496952.

[21] Histoire CIGREF. *Sécurité informatique | Histoire CIGREF*. URL : http://www.histoire-cigref.org/blog/tag/securite-informatique/ (visité le 09/02/2016).

[22] *Cisco Advanced Malware Protection for Endpoints Data Sheet*. Cisco. URL : http://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html (visité le 06/05/2016).

[23] *Cisco Advanced Malware Protection for Networks Data Sheet*. Cisco. URL : http://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html (visité le 10/05/2016).

[24] *Combating Advanced Persistent Threats - Trend Micro USA*. URL : http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/ (visité le 06/04/2016).

[25] *Comment fonctionne un antivirus ?* URL : http://www.symantec.com/region/fr/resources/antivirus.html (visité le 08/04/2016).

[26] *Comprendre le programme "Prism"*. URL : http://www.lemonde.fr/international/infographie/2013/06/11/le-programme-prism-en-une-infographie_3427774_3210.html (visité le 18/02/2016).

[27] *Cryptolocker*. Page Version ID : 121189421. 9 déc. 2015. URL : https://fr.wikipedia.org/w/index.php?title=Cryptolocker&oldid=121189421 (visité le 18/02/2016).

[28] *Data Exfiltration Techniques - InfoSec Resources*. URL : http://resources.infosecinstitute.com/data-exfiltration-techniques-2/ (visité le 23/04/2016).

[29] *Description of an APT Attack - IT Security, Inc.* URL : http://www.it-security-inc.com/home/blog/security-hacking-stories/description-of-an-apt-attack3 (visité le 04/04/2016).

[30] *Détection et classification de malwares par Yara / MISC-065 / MISC / Connect - Edition Diamond*. URL : http://connect.ed-diamond.com/MISC/MISC-065/Detection-et-classification-de-malwares-par-Yara (visité le 16/02/2016).

[31] *Drive-by download*. Page Version ID : 705621937. 18 fév. 2016. URL : https://en.wikipedia.org/w/index.php?title=Drive-by_download&oldid=705621937 (visité le 09/03/2016).

[32] *Exploit kit*. Page Version ID : 714290886. 8 avr. 2016. URL : https://en.wikipedia.org/w/index.php?title=Exploit_kit&oldid=714290886 (visité le 25/04/2016).

[33] *File Types That are Scanned by FireAMP Connector - Cisco*. URL : http://www.cisco.com/c/en/us/support/docs/security/advanced-malware-protection-endpoints/118711-technote-fireamp-00.html (visité le 03/03/2016).

[34] Tim GREENE. *Next-generation endpoint protection not as easy as it sounds*. Network World. 20 juil. 2015. URL : http://www.networkworld.com/article/2949863/security/next-generation-endpoint-protection-not-as-easy-as-it-sounds.html (visité le 08/04/2016).

[35] Roger A. GRIMES. *5 signs you've been hit with an advanced persistent threat*. InfoWorld. 16 oct. 2012. URL : http://www.infoworld.com/article/2615666/security/5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html.

[36] *Histoire des virus, cauchemars de l'informatique | Histoire CIGREF*. 8 fév. 2016. URL : http://www.histoire-cigref.org/blog/histoire-des-virus-cauchemars-de-l-informatique/ (visité le 08/02/2016).

[37] *How antivirus software works : Virus detection techniques*. SearchSecurity. URL : http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques (visité le 08/04/2016).

[38] *How does SSL work ? What is an SSL handshake ?* URL : http://www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake (visité le 29/04/2016).

[39] *How the NSA became an advanced persistent threat to global cybersecurity*. URL : http://warincontext.org/2013/12/24/how-the-nsa-became-an-advanced-persistent-threat-to-global-cybersecurity/ (visité le 18/02/2016).

[40] *How To Deploy the Most Effective Advanced Persistent Threat Solutions*. 3 fév. 2016. URL : http://www.gartner.com/newsroom/id/2595015.

[42] Lastline INC. *Compare Trend Micro Deep Discovery to Lastline*. 2 fév. 2016. URL : http://landing.lastline.com/compare-trend-micro-deep-discovery-to-lastline-alternative.

[43] Lastline INC. *NSS*. 3 fév. 2016. URL : http://landing.lastline.com/nss-2015.

[44] *Introduction to email security gateways in the enterprise*. SearchSecurity. URL : http://searchsecurity.techtarget.com/feature/Introduction-to-email-security-gateways-in-the-enterprise (visité le 21/04/2016).

[45] *Intrusion Prevention System (IPS)Fortinet | Network Security, Enterprise and Data-Center Firewall*. URL : http://www.fortinet.com/solutions/ips.html (visité le 08/04/2016).

[46] Dr Christopher KRUEGEL. *How To Build An Effective Malware Analysis Sandbox*. 2 fév. 2016. URL : http://labs.lastline.com/different-sandboxing-techniques-to-detect-advanced-malware.

[47] *La NSA peut surveiller les smartphones Android, BlackBerry et iOS*. URL : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-583062-nsa-surveillance-smartphones.html (visité le 17/02/2016).

[48] *Le Social Engineering : un espionnage sans compétences techniques*. SecuriteInfo.com. URL : https://www.securiteinfo.com/attaques/divers/social.shtml (visité le 05/05/2016).

[49] Michaël Szadkowski et Damien LELOUP. *Prism, Snowden, surveillance de la NSA : 7 questions pour tout comprendre*. 2 juil. 2013. URL : http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html (visité le 18/02/2016).

[50] *Les différents types de malware - Kaspersky Daily*. Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français. URL : https://blog.kaspersky.fr/les-differents-types-de-malwares/1898/ (visité le 09/02/2016).

[51] *Les menaces persistantes avancées décryptées par les experts : Les menaces persitantes avancées décryptées par les experts - JDN*. URL : http://www.journaldunet.com/solutions/securite/les-menaces-persitantes-avancees-apt-definition-et-moyens-de-protection/ (visité le 15/02/2016).

[52] *Logfile*. Page Version ID : 700391632. 18 jan. 2016. URL : https://en.wikipedia.org/w/index.php?title=Logfile&oldid=700391632 (visité le 23/04/2016).

[53] *Logiciel malveillant*. 18 déc. 2015. URL : https://fr.wikipedia.org/w/index.php?title=Logiciel_malveillant&oldid=121423954.

[54] *Macro malware help*. URL : https://www.microsoft.com/security/portal/threat/macromalware.aspx (visité le 01/05/2016).

[55] Freddy MANGUM. *Next-Generation Sandbox Offers Comprehensive Detection of Advanced Malware*. 2 fév. 2016. URL : http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware.

[56] Freddy MANGUM. *Web Security For Advanced Malware And Persistent Threats*. 4 fév. 2016. URL : http://info.lastline.com/blog/web-security-for-advanced-persistent-threats.

[57] Ellen MESSMER. *Gartner : 'Five Styles of Advanced Threat Defense' can protect enterprise from targeted attacks*. Network World. 30 oct. 2013. URL : http://www.networkworld.com/article/2171375/network-security/gartner---five-styles-of-advanced-threat-defense--can-protect-enterprise-from-targe.html.

[58] NATO. *Déclaration du sommet de Lisbonne publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Lisbonne le 20 novembre 2010*. NATO. URL : http://www.nato.int/cps/fr/natohq/official_texts_68828.htm (visité le 24/04/2016).

[59] NEWSOFTPCLAB. *C'est quoi une faille Zero Day ? | Panoptinet*. URL : http://www.panoptinet.com/cybersecurite-decryptee/cest-quoi-une-faille-zero-day/ (visité le 25/04/2016).

[60] *Next-gen firewall reviews : Palo Alto Networks PA-5060*. 8 fév. 2016. URL : http://searchnetworking.techtarget.com/tip/Next-gen-firewall-reviews-Palo-Alto-Networks-PA-5060 (visité le 08/02/2016).

[61] *Nouvelle découverte : le spyware sophistiqué 'Regin' collecte depuis des années déjà des données en Belgique*. 24 nov. 2014. URL : http://datanews.levif.be/ict/actualite/nouvelle-decouverte-le-spyware-sophistique-regin-collecte-depuis-des-annees-deja-des-donnees-en-belgique/article-normal-354625.html.

[62] *Que sont les attaques APT ? - Kaspersky Daily*. Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français. URL : https://blog.kaspersky.fr/que-sont-les-attaques-apt/1089/ (visité le 25/04/2016).

[63] *Rootkit*. 27 août 2015. URL : https://fr.wikipedia.org/w/index.php?title=Rootkit&oldid=118115228.

[64] *Sandbox (sécurité informatique) — Wikipédia*. 8 fév. 2016. URL : https://fr.wikipedia.org/wiki/Sandbox_(s%C3%83%C2%A9curit%C3%83%C2%A9_informatique) (visité le 08/02/2016).

[65] *secure Web gateway*. Gartner IT Glossary. 10 fév. 2012. URL : http://www.gartner.com/it-glossary/secure-web-gateway/ (visité le 22/04/2016).

[66] *Security information management system*. Page Version ID : 121071034. 5 déc. 2015. URL : https://fr.wikipedia.org/w/index.php?title=Security_information_management_system&oldid=121071034 (visité le 22/04/2016).

[67] *Seriously ? - NSS Labs, Inc. - The Security Insight Company*. 8 fév. 2016. URL : https://www.nsslabs.com/blog/seriously/ (visité le 08/02/2016).

[68] *Shopping For Zero-Days : A Price List For Hackers' Secret Software Exploits*. Forbes. URL : http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (visité le 25/04/2016).

[69] Comm SOLUTIONS. *The Evolution of Malware and Security Compromise | Comm Solutions*. 8 fév. 2016. URL : http://www.commsolutions.com/2014/04/evolution-malware-security-compromise/ (visité le 08/02/2016).

[70] *Symantec Advanced Threat Protection Outperforms Competitors in Independent Third-Party Tests | Symantec Connect Community*. URL : http://www.symantec.com/connect/blogs/symantec-advanced-threat-protection-outperforms-competitors-independent-third-party-tests (visité le 29/02/2016).

[71] *Take Digital to the Core — Remaster Your Leadership Using Six Personas to Win in Digital Business*. 4 fév. 2016. URL : https://www.gartner.com/doc/3143317/digital-core--remaster-leadership.

[72] *TAP réseau — Wikipédia*. URL : https://fr.wikipedia.org/wiki/TAP_r%C3%83%C2%A9seau (visité le 10/02/2016).

[73] *Tecteo aussi victime d'espionnage informatique*. 7s7. 23 oct. 2013. URL : http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/1728185/2013/10/23/Tecteo-aussi-victime-d-espionnage-informatique.dhtml (visité le 08/05/2016).

[74] *Test a Sample Malware File*. URL : https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin/submit-files-for-wildfire-analysis/test-a-sample-malware-file.html (visité le 19/02/2016).

[75] *Test Malware ! - WICAR.org - Test Your Anti-Malware Solution !* URL : http://www.wicar.org/test-malware.html (visité le 02/03/2016).

[76] *Testez votre antivirus avec EICAR file - Sécurité Informatique Eur'Net, est un "architecte" d'Internet.* URL : http://securite-informatique.info/virus/eicar/ (visité le 02/03/2016).

[77] *The 5 cyber attacks you're most likely to face | InfoWorld*. URL : http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html (visité le 10/03/2016).

[78] *The evolution of self-defense technologies in malware - Securelist*. 8 fév. 2016. URL : https://securelist.com/analysis/publications/36156/the-evolution-of-self-defense-technologies-in-malware/ (visité le 08/02/2016).

[79] *The Regin Platform | What is Regin ? | Virus Definition*. URL : http://www.kaspersky.com/internet-security-center/threats/regin-platform-malware (visité le 24/04/2016).

[80] *Turing Test in Reverse : New Sandbox-Evasion Techniques Seek Human Interaction « Threat Research*. FireEye. 8 fév. 2016. URL : https://www.fireeye.com/blog/threat-research/2014/06/turing-test-in-reverse-new-sandbox-evasion-techniques-seek-human-interaction.html.

[81] *Ver informatique*. 15 jan. 2016. URL : https://fr.wikipedia.org/w/index.php?title=Ver_informatique&oldid=122347216.

[82] *Virus et Antivirus | Informations | Histoire | Évolution - Informations sur la sécurité informatique - Panda Security*. 8 fév. 2016. URL : http://www.pandasecurity.com/france/homeusers/security-info/classic-malware/ (visité le 08/02/2016).

[83] *Vulnérabilité Zero day*. Page Version ID : 123908375. 2 mar. 2016. URL : https://fr.wikipedia.org/w/index.php?title=Vuln%C3%83%C2%A9rabilit%C3%83%C2%A9_Zero_day&oldid=123908375 (visité le 25/04/2016).

[84] *Welcome to YARA's documentation ! — yara 3.4.0 documentation*. URL : http://yara.readthedocs.org/en/v3.4.0/ (visité le 16/02/2016).

[85] *What is a firewall ?* URL : https://www.paloaltonetworks.com/documentation/glossary/what-is-a-firewall (visité le 09/04/2016).

[86] *What is a Secure Web Gateway ? - Definition from Techopedia*. Techopedia.com. URL : https://www.techopedia.com/definition/29303/secure-web-gateway (visité le 21/04/2016).

[87] *What Is a Virtual Sandbox - Sandboxing Applications - Tom's Guide*. 8 fév. 2016. URL : http://www.tomsguide.com/us/sandbox,news-17762.html (visité le 08/02/2016).

[88] *What is a White Hat Hacker ? - Definition from Techopedia*. Techopedia.com. URL : https://www.techopedia.com/definition/10349/white-hat-hacker (visité le 02/05/2016).

[89] *What is advanced persistent threat (APT) ? - Definition from WhatIs.com*. SearchSecurity. 1er fév. 2016. URL : http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

[90] *what is advanced persistent threat kaspersky - Recherche Google*. URL : https://www.google.be/search?client=safari&rls=en&q=what+is+advanced+persistent+threat+kaspersky&ie=UTF-8&oe=UTF-8&gfe_rd=cr&ei=VbYEV6eeKaLP8AfSj72QAQ (visité le 06/04/2016).

[91] *What is an intrusion prevention system ?* URL : https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips (visité le 08/04/2016).

[92] *What is ARM processor ? - Definition from WhatIs.com*. URL : http://whatis.techtarget.com/definition/ARM-processor (visité le 08/05/2016).

[93] *What is back door ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/back-door (visité le 25/04/2016).

[94] *What is high availability (HA) ? - Definition from WhatIs.com*. SearchDataCenter. URL : http://searchdatacenter.techtarget.com/definition/high-availability (visité le 30/04/2016).

[95] *What is intrusion detection (ID) ? - Definition from WhatIs.com*. SearchMidmarketSecurity. URL : http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection (visité le 08/04/2016).

[96] *What is intrusion prevention ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/intrusion-prevention (visité le 08/04/2016).

[97] *What is macro virus ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/macro-virus (visité le 26/04/2016).

[98] *What is malware and how can we prevent it ? | Security News*. 1er fév. 2016. URL : http://www.pctools.com/security-news/what-is-malware/.

[99] *What is network tap ? - Definition from WhatIs.com*. SearchNetworking. URL : http://searchnetworking.techtarget.com/definition/Network-tap (visité le 02/05/2016).

[100] *What is security information and event management (SIEM) ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM (visité le 22/04/2016).

[101] *What is social engineering ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/social-engineering (visité le 25/04/2016).

[102] *What is spear phishing ? - Definition from WhatIs.com*. SearchSecurity. 2 fév. 2016. URL : http://searchsecurity.techtarget.com/definition/spear-phishing.

[103] *What is spyware ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/spyware (visité le 26/04/2016).

[104] *What is Trojan horse ? - Definition from WhatIs.com*. SearchSecurity. 1er fév. 2016. URL : http://searchsecurity.techtarget.com/definition/Trojan-horse.

[105] *What is virus ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/virus (visité le 26/04/2016).

[106] *What is white hat ? - Definition from WhatIs.com*. SearchSecurity. URL : http://searchsecurity.techtarget.com/definition/white-hat (visité le 02/05/2016).

[107] *Why Next-Gen Firewalls & Sandboxes Are Not Enough | OpenDNS*. 8 fév. 2016. URL : https://www.opendns.com/enterprise-security/resources/webcasts/next-gen-firewalls-sandboxes-not-enough/ (visité le 08/02/2016).

[108] *WildFire - Palo Alto Networks*. URL : http://www.networkequipment.net/products/palo-alto-networks/wildfire/ (visité le 19/02/2016).

[109] *WildFire - Protection from Targeted and Unknown Malware*. 8 fév. 2016. URL : https://www.paloaltonetworks.com/products/technologies/wildfire.html (visité le 08/02/2016).

[111] *YARA - The pattern matching swiss knife for malware researchers*. URL : https://plusvic.github.io/yara/ (visité le 16/02/2016).

[112] *Zero-day (computing)*. 1er fév. 2016. URL : https://en.wikipedia.org/w/index.php?title=Zero-day_(computing)&oldid=702686769.

Lexique

AIDS	Virus DOS du début des années 90 qui prenait le contrôle de l'écran de l'utilisateur.
APT	Selon Wikipédia, une Advanced Persistent Threat (traduction littérale, menace persistante avancée ; en anglais, souvent abrégé APT) est un type de piratage informatique furtif et continu, souvent orchestré par des humains ciblant une entité spécifique.
ILOVEYOU	Virus apparu début des années 2000. Selon Wikipédia, il cachait un script VBS malicieux derrière une fausse lettre d'amour. Ce script permettait la propagation de ce ver à travers une diffusion massive grâce à Outlook. 10% des ordinateurs connectés à internet ont étés touchés.
In-line	Un appareil réseau dit in-line est un appareil recevant des paquets et qui les transferts à leur destination. Voici quelques appareils généralement placés en in-line : router, switch, firewall, IDS/IPS, WAF, TAP, etc.
Macro Virus	Selon Wikipédia, les macrovirus utilisent le langage de programmation d'un logiciel pour en altérer le fonctionnement. Ils s'attaquent principalement aux fichiers des utilisateurs. Leur expansion est due au fait qu'ils s'intègrent à des fichiers très échangés et que leur programmation est plus facile que celle des virus.
MELISSA	Virus datant de la fin du 20e siècle. Il saturait les systèmes de messagerie et envoyait les fichiers (confidentiels ou non) à de multiples adresses.

NSS Lab	NSS Lab est une société effectuant des benchmarks sur des produits de différents constructeurs afin de comparer le marché.
Open Source	Selon Wikipédia, la désignation open source, ou “code source ouvert”, s’applique aux logiciels dont la licence respecte des critères précisément établis par l’Open Source Initiative, c’est-à-dire les possibilités de libre redistribution, d’accès au code source et de création de travaux dérivés. Mis à la disposition du grand public, ce code source est généralement le résultat d’une collaboration entre programmeurs.
ShareWare	Selon Wikipédia, un shareware, partagiciel ou contribuciel, est un logiciel qui peut être utilisé gratuitement généralement durant une certaine période ou avec des fonctionnalités limitées. Après cette période d’essai, l’utilisateur doit rétribuer l’auteur s’il veut continuer à utiliser le logiciel ou avoir accès à la version complète.
Spywares	Selon Wikipédia, un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais spyware) est un logiciel malveillant qui s’installe dans un ordinateur dans le but de collecter et transférer des informations sur l’environnement dans lequel il s’est installé, très souvent sans que l’utilisateur en ait connaissance. L’essor de ce type de logiciel est associé à celui d’Internet qui lui sert de moyen de transmission de données.
TEQUILA.GRN	Virus datant des années 90. Tequila infectait les fichiers DOS .exe.
Virus	Selon Wikipédia, un virus informatique est un automate autoréplicatif à la base non malveillant, mais aujourd’hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d’autres ordinateurs en s’insérant dans des logiciels légitimes, appelés “hôtes”
Worms	Selon Wikipédia, un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Annexes

A. Grille de test WildFire

Explications

Ci-dessous se trouvent en version agrandie, les tests ainsi que leurs résultats effectués sur la solution WildFire.

ID	Domaine	Description	Scénario	Priorité	C-PAN	R-PAN
Q-SAPT-001	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-002	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-003	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-004	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-005	Flux chiffrés	Est-ce que la solution sait analyser les flux chiffrés	Téléchargement depuis un serveur HTTPS comme "MEGA", d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement du filtrage avec des flux chiffrés	M	KO(MAJ)	La fonction de décryption a été testée mais les flux déchiffrés n'étaient pas envoyés au WildFire. La fonction d'envoi au WildFire n'a pas été trouvée
Q-SAPT-006	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-007	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-008	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-009	Mobile	Est-ce que le système détecte les menaces venant de mobiles	Depuis un mobile : téléchargement web ou réception d'un email contenant d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement de l'alerting	O	KO(MIN)	Aucun APK n'est envoyé à WildFire alors que ce type de fichier est configuré dans la policy
Q-SAPT-010	[illegible]	[illegible]	[illegible]	M	OK	[illegible]

Q-SAPT-011	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-011-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-011-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-012				M	OK	
Q-SAPT-013				S	OK	
Q-SAPT-014						
B-SAPT-014-1				M	OK	
B-SAPT-014-2				M	OK	
B-SAPT-014-3				M	OK	
B-SAPT-014-4	Traitement des fichiers	Rar	Téléchargement d'un malware sous la forme de fichier Rar	M	KO(MAJ)	Le malware diffusé sous forme Rar n'a pas été détecté par WildFire
B-SAPT-014-5	Traitement des fichiers	Tar	Téléchargement d'un malware sous la forme de fichier Tar	M	KO(MAJ)	Le malware diffusé sous forme Tar n'a pas été détecté par WildFire
B-SAPT-014-6				M	OK	

Q-SAPT-015						
B-SAPT-015-1				M	OK	
B-SAPT-015-2				M	OK	
B-SAPT-015-3				M	OK	
B-SAPT-015-4	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MIN)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté, cependant durant le POC, du trafic FTP a été détecté par WildFire
B-SAPT-015-5				M	OK	
B-SAPT-015-6	Traitement des protocoles	NFSv4	Envoi d'un malware tel que les cryptolockers déjà reçus via NFSv4	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFSv4 n'a pas été détecté
B-SAPT-015-7	Traitement des protocoles	SMB	Envoi d'un malware tel que les cryptolockers déjà reçus via SMB	M	KO(MAJ)	Le malware diffusé au moyen du protocole SMB n'a pas été détecté
Q-SAPT-016	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						3 critères mineurs non conformes
						6 critères majeurs non conformes

B. Grille de test Lastline

Explications

Explications

Ci-dessous se trouvent en version agrandie, les tests ainsi que leurs résultats effectués sur la solution Lastline.

ID	Domaine	Description	Scénario	Priorité	C-LL	R-LL
Q-SAPT-001	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-002	Débit	Mesure et analyse du débit, est-ce que le débit annoncé correspond bien au débit mesuré	Utilisation d'un client et d'un serveur "iperf" pour mesurer le débit entre deux machines en passant par la solution	M	KO(MIN)	Sans LastLine : AVG : 940 Mbit/s Avec LastLine : Résultat 1 : 798 Mbit/s Résultat 2 : 855 Mbit/s Résultat 3 : 800 Mbit/s Résultat 4 : 827 Mbit/s AVG : 820 Mbit/s : 87% de moins que les 940Mbit/s de départ
Q-SAPT-003	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-004	Flux chiffrés	Est-ce que la solution sait analyser les flux chiffrés	Téléchargement depuis un serveur HTTPS comme "MEGA", d'un malware tel que les cryptolockers déjà reçus afin de vérifier le bon fonctionnement du filtrage avec des flux chiffrés	M	KO(MAJ)	La solution a été testée sans l'intégration nécessaire d'appareils permettant le déchiffrement SSL
Q-SAPT-005	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-006	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-007	[illegible]	[illegible]	[illegible]	O	OK	[illegible]
Q-SAPT-008	[illegible]	[illegible]	[illegible] correctement	M	OK	[illegible]

Q-SAPT-009	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-09-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	OK	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-09-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-010				M	OK	
Q-SAPT-011				S	OK	
Q-SAPT-012						
B-SAPT-012-1				M	OK	
B-SAPT-012-2				M	OK	
B-SAPT-012-3				M	OK	
B-SAPT-012-4				M	OK	
B-SAPT-012-5	Traitement des fichiers	Tar	Téléchargement d'un malware sous la forme de fichier Tar	M	KO(MAJ)	Le malware diffusé sous forme Tar n'a pas été détecté par LastLine
B-SAPT-012-6				M	OK	

Q-SAPT-013						
B-SAPT-013-1				M	OK	
B-SAPT-013-2				M	OK	
B-SAPT-013-3				M	OK	
B-SAPT-013-4	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MIN)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté par LastLine
B-SAPT-013-5				M	OK	
B-SAPT-013-6	Traitement des protocoles	NFS	Envoi d'un malware tel que les cryptolockers déjà reçus via NFS	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFS n'a pas été détecté par LastLine
B-SAPT-013-7				M	OK	
Q-SAPT-014	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						3 critères mineurs non conformes
						4 critères majeurs non conformes

C. Grille de test FortiSandbox

Explications

Ci-dessous se trouvent en version agrandie, les tests ainsi que leurs résultats effectués sur la solution FortiSandbox.

ID	Domaine	Description	Scénario	Priorité	C-FN	R-FN
Q-SAPT-001	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-002	Débit	Mesure et analyse du débit, est-ce que le débit annoncé correspond bien au débit mesuré	Envoi de fichiers exécutables ou de scripts avec des hashs différents afin de confirmer le débit de fichiers analysés	M	KO(MIN)	Le capacité à analyser le débit d'élément n'est pas toujours suffisante
Q-SAPT-003	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-004	Mobile	Est-ce que le système détecte les menaces venant de mobiles	Téléchargement d'un APK malveillant	O	KO(MIN)	APK non détecté par signature mais pas de VM Android pour le test
Q-SAPT-005	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-006	Sandboxing	Est ce que la sandbox détecte bien des malwares qui utilisent le comportement utilisateur pour se déclencher. Les comportements sont les suivants :	Écriture d'un programme qui agit seulement quand il détecte une séquence que seul un comportement utilisateur peut déclencher			
Q-SAPT-06-1	Sandboxing	Déplacement de souris	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris	M	KO(MIN)	La sandbox a permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware" mais les actions effectuées sur la registry ne sont pas toutes détectées
Q-SAPT-06-2	Sandboxing	Double click	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Double click	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-3	Sandboxing	Utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue une Utilisation du clavier	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-4	Sandboxing	Déplacement de souris + double click + utilisation du clavier	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier	M	KO(MAJ)	La sandbox n'a pas permis de contourner le mécanisme utilisateur et donc de détecter les actions effectuées pas le "Malware"
Q-SAPT-06-5	Sandboxing	Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	Le 'Malware' ne se déclenche que si l'utilisateur effectue un Déplacement de souris + double click + utilisation du clavier + acceptation boîtes de dialogues modales	M	KO(MAJ)	La sandbox n'a pas su éviter les boîtes de dialogue. Il y avait en fait 3 boîtes différentes, suite à chaque acceptation de boîte se faisait une action sur la registry, aucune action n'a été détectée
Q-SAPT-07	Sandboxing	Est-ce que le sandbox détecte bien la création, suppression, modification de clés de registre	Écriture d'un programme de test en C# qui modifie, crée ou supprime des clés de registre	M	KO(MAJ)	La sandbox n'a pas correctement repéré les actions effectuées sur la regirstry. Toutes las cations ne sont pas détectées. Ceratins oui, et d'autres non

Q-SAPT-08	[illegible]	[illegible]	[illegible]	S	OK	[illegible]
Q-SAPT-09	[illegible]	[illegible]	[illegible]			
B-SAPT-09-1	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-2	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-3	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-4	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-09-5	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
Q-SAPT-010	[illegible]	[illegible]	[illegible]			
B-SAPT-010-1	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-010-2	Traitement des protocoles	FTP	Envoi d'un malware tel que les cryptolockers déjà reçus via FTP	M	KO(MAJ)	Le malware diffusé au moyen du protocole FTP n'a pas été détecté par la FortiSandbox
B-SAPT-010-3	[illegible]	[illegible]	[illegible]	M	OK	[illegible]
B-SAPT-010-4	Traitement des protocoles	NFS	Envoi d'un malware tel que les cryptolockers déjà reçus via NFS	M	KO(MAJ)	Le malware diffusé au moyen du protocole NFS n'a pas été détecté par la FortiSandbox
B-SAPT-010-5	Traitement des protocoles	SMB	Envoi d'un malware tel que les cryptolockers déjà reçus via SMB	M	KO(MAJ)	Le malware diffusé au moyen du protocole SMB n'a pas été détecté par la FortiSandbox
Q-SAPT-011	Web	Est-ce que tout ce qui est URL malveillant, ou Malware téléchargé est bien détecté par le système mis en place	Téléchargement d'un malware de test depuis le web, si détecté et bloqué, la solution marche	M	KO(MIN)	Malware détecté, mais la solution ne permet pas dans son installation actuelle de bloquer
						4 critères mineurs non conformes
						8 critères majeurs non conformes

D. IoC de Regin

Explications

Explications

Ci-dessous se trouvent les IoCs de Regin. Ces derniers permettent de repérer les postes susceptibles infectés par Regin.

Indicators of compromise

Inhoud / Sommaire

Algemene beschrijving / Description générale

Systemen die potentiëel het doelwit zijn van de malware zijn zowel servers als werkstations die werken op de hieronder vermelde besturingssystemen.

Les cibles potentielles du malware sont aussi bien des serveurs que des postes de travail qui tournent sous les systèmes d'exploitation répertoriés ci-dessous.

Windows 32 bits

%SystemRoot%\Security\logs\scecomp.dat	File
%SystemRoot%\System32\iapfltr.dat	File
%SystemRoot%\Security\logs\sceRoot.dat	File
%SystemRoot%\Security\logs\sceback.old	File
%SystemRoot%\Security\logs\scesetup.dat	File
%SystemRoot%\System32\ntsec.dat	File
%SystemRoot%\System32\drivers\adpu160.sys	3500d38ebb80709f6bb1b95636c1c5e1 / 8c3fa693558eb3138f2c3f92d420813e
\\pipe\{E582DF91-4D8F-959D-9F33-8A7A2E1B9C8D}	named pipe (may change)
BROWSERPC<random string>	SMB named pipe (network communication) port 445
HKLM\SYSTEM\ControlSet001\services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
HKLM\SYSTEM\ControlSet002\services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
software\Microsoft\SystemCertificates\ROOT\Certificates\9399E79CE9417B34707B2B51EEA2F829A7A3A172	Rogue Microsoft root CA

Windows 64 bits

%SystemRoot%\IME\IMESC5\DICTS\PINTLGBS.IMD	File
%SystemRoot%\Security\logs\sceback.old	File
%SystemRoot%\system32\desk.cfg	File
%SystemRoot%\IME\IMESC5\DICTS\PINTLGBP.IMD	File
%SystemRoot%\system32\svcsstat.exe	66afaa303e13faa4913eaad50f7237ea / 9da7ae7d9967a61fd90ff06bb078c9dd
%SystemRoot%\system32\winhttpc.dll	File
%SystemRoot%\system32\wshnetc.dll	44be80340bdaa0f4c1f9f071280e5ca3
%SystemRoot%\SysWow64\wshnetc.dll	File
\\pipe\{22CA803F-C4CF-21BE-D9F0-6AEFF27188A1}	System or network
\\pipe\{EA3AA1F2-B2E9-00A7-559C-21D0101E8095}	System or network
BROWSERPC<random string>	SMB named pipe (network communication) port 445
HKLM\SYSTEM\ControlSet001\services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
HKLM\SYSTEM\ControlSet002\services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes\BROWSERPC<randomstring>	Registry key
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Winsock\HelperDllName	Value : %SystemRoot%\system32\wshnetc.dll
HKLM\SYSTEM\ControlSet002\Services\Tcpip\Parameters\Winsock\HelperDllName	Value :%SystemRoot%\system32\wshnetc.dll

Solaris

Op een werkend, operationeel systeem ("live system") : niet trachten de bestanden waarvan de namen in **vet** zijn weergegeven, te localiseren, te openen of op een beeldscherm weer te geven (« ls », « openfile », etc.). Dit soort handelingen wordt door de malware gedetecteerd en leidt tot de verwijdering van de betreffende bestanden.

Sur un système opérationnel (« live system ») : ne pas tenter de scanner, d'ouvrir ou d'afficher les fichiers indiqués **en gras** (« ls », « openfile », etc.)**.** Cette opération est détectée par le malware et mène à la suppression desdits fichiers.

/etc/rcS.d/S85bootclient	reference to /usr/bin/bootclient
/etc/rcS.d/S85ntpstatd	reference to /usr/bin/ntpstatd
/usr/bin/bootclient	File
/usr/bin/ntpstatd	File
/lib/.tmp<random>	Directory
/lib/.tmp<random>/<random>	File

Linux 32 bits

Op een werkend, operationeel systeem (“live system”) : niet trachten de bestanden waarvan de namen in **vet** zijn weergegeven, te localiseren, te openen of op een beeldscherm weer te geven (« ls », « openfile », etc.). Dit soort handelingen wordt door de malware gedetecteerd en leidt tot de verwijdering van de betreffende bestanden.

Sur un système opérationnel (« live system ») : ne pas tenter de scanner, d’ouvrir ou d’afficher les fichiers indiqués **en gras** (« ls », « openfile », etc.)**.** Cette opération est détectée par le malware et mène à la suppression desdits fichiers.

/etc/rc.modules	reference to /bin/modload
/bin/modload	File
/lib/.tmp<random>	Directory
/lib/.tmp<random>/<random>	File

Linux 64 bits

Op een werkend, operationeel systeem ("live system") : niet trachten de bestanden waarvan de namen in **vet** zijn weergegeven, te localiseren, te openen of op een beeldscherm weer te geven (« ls », « openfile », etc.). Dit soort handelingen wordt door de malware gedetecteerd en leidt tot de verwijdering van de betreffende bestanden.

Sur un système opérationnel (« live system ») : ne pas tenter de scanner, d'ouvrir ou d'afficher les fichiers indiqués **en gras** (« ls », « openfile », etc.)**.** Cette opération est détectée par le malware et mène à la suppression desdits fichiers.

/etc/rc.serial	reference to /bin/initserial
/bin/initserial	File
/lib/.tmp<random>	Directory
/lib/.tmp<random>/<random>	File

Indicators of compromise (Part 2)
Network Analysis

Inhoud / Sommaire

External IP addresses

IP Address	Netname	Description	Country
113.20.29.245	ARDH-ID	PT. ARDH GLOBAL INDONESIA	Indonesia
113.20.29.246	ARDH-ID	PT. ARDH GLOBAL INDONESIA	Indonesia
119.235.248.140	RAJASA-ID	PT. Raja Sepadan Abadi Indonesia	Indonesia
180.149.240.162	WEBWERKS1-AP	Web Werks India Pvt. Ltd	India
180.149.240.96	WEBWERKS1-AP	Web Werks India Pvt. Ltd	India
180.149.240.249	WEBWERKS1-AP	Web Werks India Pvt. Ltd	India
180.149.240.161	WEBWERKS1-AP	Web Werks India Pvt. Ltd	India

SNORT Rules

alert tcp any any -> any 445 (msg:"named pipe BROWSERPC"; content:"|420052004f00570053004500520050004300 00|"; nocase; classtype:protocol-command-decode; sid:21000584; rev:4;)

alert tcp any any -> any 445 (msg:"PIPE Possible malicious named pipe (SMB2)"; flow: established; content: "|fe 53 4d 42 40 00 01 00 00 00 00 00 0b 00|"; offset:4; depth:14; content: "|00 00 00 0c 40 11 00|"; offset:65; threshold: type both, track by_src, count 1, seconds 60; classtype:protocol-command-decode; sid:21000673; rev:1;)

alert tcp any any -> any 139 (msg:"Named pipe 139"; content:"|FF 53 4D 42 A2|"; depth:5; offset:4; pcre:"/\\(\x00[0-9a-f]){32}\x00\x00/i"; classtype:trojan-activity; sid:21000708; rev:2;)

alert tcp any any -> any 139 (msg:"Named pipe wz 139"; content:"|FF 53 4D 42 A2|"; depth:5; offset:4; pcre:"/\\\x00w\x00z(\x00[0-9a-fA-F]){2}\x00\x00/i"; classtype:trojan-activity; sid:21000710; rev:2;)

alert tcp any any -> any 445 (msg:"Named pipe wz 445"; content:"|FF 53 4D 42 A2|"; depth:5; offset:4; pcre:"/\\\x00w\x00z(\x00[0-9a-fA-F]){2}\x00\x00/i"; classtype:trojan-activity; sid:21000711; rev:2;)

E. Article de presse concernant Regin chez Tecteo

Explications

L'article suivant résume l'activité de Regin chez Nethys.

Dimanche 8 mai 2016 - 14h24:55
Se connecter | 0 article sauvegardé

i7SUR7 INTERNET & JEUX EN LIGNE
BELGIQUE MONDE SPORTS SHOWBIZ PLUS 7S7
i7SUR7 INTERNET PIRATAGE INFORMATIQUE

Tecteo aussi victime d'espionnage informatique

Tweet

Par: rédaction
23/10/13 - 19h28 Source: Belga

SAUVEGARDER

© thinkstock.

Tecteo a été victime d'une attaque informatique similaire à celle perpétrée contre d'autres opérateurs télécoms européens comme Belgacom, France-Telecom ou Wanadoo, indique-t-elle mercredi. Il est toutefois trop tôt à l'heure actuelle pour établir si des informations ont pu être dérobées sur les infrastructures du groupe, ou de ses filiales telecom VOO ou d'énergie RESA.

Sur base de divers éléments techniques précis fournis par l'IBPT, Tecteo a mené une vérification approfondie de ses systèmes informatiques et a identifié les indices concordants d'une attaque. Le modus operandi semble identique aux intrusions dont les autres opérateurs telecoms européens ont été victimes, explique le groupe.

Le service informatique travaille en étroite collaboration avec l'IBPT et les autorités compétentes pour établir si les tentatives d'intrusion ont abouti, notamment par le biais d'une attaque virale permettant la captation de signaux téléphoniques ou le vol de données informatiques, poursuit Tecteo.

Le groupe déposera plainte sous peu contre "cette attaque d'une portée internationale".

© belga.

LIRE AUSSI


Les SPF, paradis pour les pirates informatiques


Down-Sec révèle l'identité des harceleurs de Madison


Down-Sec: nouvelle offensive dès lundi?

Plus d'infos sur Piratage Informatique , Internet

A VOIR AUSSI


Foot européen: ce qu'il faut absolument savoir avant ce week-end


Hiddink: "L'avenir de John Terry est encore incertain"


Transfert surprise d'El Chapo dans une autre prison du Mexique


Le secret des pyramides percé par une nouvelle technologie

Recommandé par Outbrain

7SUR7 NOUVEAU

14h11 Il faudra aller sonner au ...
14h02 EN DIRECT: Tottenham pour ...
14h00 EN DIRECT: Heylen titulaire à ...
13h51 Elle reçoit trois millions par ...
13h49 Plus de 70 personnes tuées dans ...


ACDC - Black In Black (Axl Rose) Lisbon


Jennifer Lopez - Ain't Your Mama


EN IMAGES
Charleroi en finale des PO2


EN IMAGES
Nos cadeaux pour la fête des mères

7SUR7 LE PLUS POPULAIRE