Lettre n°54-Septembre 2016-disponible sur omc.ceis.eu

Brève du mois

« **I do not believe data protection law is standing in the way of your success. It's not privacy or innovation - it's privacy and innovation. [...] The fundamental objective of my five-year term as commissioner is to build a culture of data confidence in the UK.** » Elizabeth Denham, Commissaire à l'Information du Royaume-Uni, au cours de la conférence PIE 2016 (Personal Information Economy).

TABLE DES MATIERES

PANORAMA DES MALWARE CIBLANT LES TÉLÉPHONES MOBILES

Le système d'exploitation Android est une cible privilégiée pour les développeurs de malware. Kaspersky Lab évaluait à plus de 800 000 le nombre de nouveaux programmes malicieux ayant ciblé en 2015 le système d'exploitation pour mobiles développé par Google[1]. Ce phénomène peut s'expliquer par la répartition du parc de téléphones mobiles : selon la dernière estimation de l'entreprise américaine Gartner datant du mois de mai 2016[2], 84.1 % des terminaux vendus durant le premier trimestre 2016 s'appuient sur le système d'exploitation Android, contre 17.4% pour iOS et 0.8 % pour Windows 10 Mobile. Il est naturellement bien plus rentable pour un concepteur de malware de développer un programme destiné à toucher un OS populaire équipant plus d'un milliard d'appareils[3].

À titre de comparaison, le nombre de malware ayant ciblé le système d'exploitation iOS est bien plus faible : treize programmes destinés à un usage cybercriminel ont été recensés depuis 2012 contre six pour les maliciels utilisés par des organismes d'origine étatique[4]. Même si la plupart des décideurs possèdent un terminal de type iPhone, le faible pourcentage de part de marché (environ 15% au premier trimestre 2016) n'incite effectivement pas les cybercriminels à investir du temps et de l'argent dans la création de malware orientés iOS. Cette tendance peut également s'expliquer par le niveau de contrôle exercé sur le développement et la distribution des applications qui leur sont destinées. L'App Store d'Apple dispose effectivement d'un processus de contrôle strict effectué avant la commercialisation des applications, ce qui limite également la marge de manœuvre dans le cadre d'un développement de malware orienté iOS.

Apple a cependant récemment fait la une de l'actualité liée à la cybersécurité. La firme de Cupertino a publié le 26 août dernier une série de correctifs de sécurité (**iOS 9.3.5**)[5] suite à la découverte de trois vulnérabilités critiques zero-day présentes dans les anciennes versions d'iOS. Ces failles touchant le WebKit (**CVE-2016-4657**) et le noyau (**CVE-2016-4655** / **CVE-2016-4656**) ont été identifiées au cours d'une investigation menée conjointement par Citizen Lab[6] et Lookout[7].

Le système d'exploitation iOS cible du malware Pegasus

Ahmed Mansoor est un activiste reconnu d'origine émiratie qui s'est notamment vu remettre en 2015 le prix Martin Ennals pour les défenseurs des droits de l'homme. Il est également, de manière involontaire, la personne à l'origine de la découverte du malware **Pegasus** qui cible entre autres le système d'exploitation iOS. En effet, le 10 et 11 août 2016, Ahmed Mansoor reçut sur son iPhone 6 deux SMS qui promettaient de révéler « de nouveaux secrets » à propos de détenus torturés dans des prisons situées aux Émirats Arabes Unis. Pour cela, il suffisait au destinataire de cliquer sur le lien inséré dans le corps des messages :

[1] https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/
[2] http://www.gartner.com/newsroom/id/3323017
[3] http://www.androidcentral.com/google-says-there-are-now-14-billion-active-android-devices-worldwide
[4] https://www.theiphonewiki.com/wiki/Malware_for_iOS
[5] https://support.apple.com/fr-fr/HT207107
[6] https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[7] http://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

SMS reçus par Ahmed Mansoor – Source : Citizen Lab

Au lieu d'ouvrir les pages dans le navigateur web de son terminal, Ahmed Mansoor transmit ces SMS à des chercheurs de Citizen Lab afin de faire analyser leur contenu. Il s'est avéré que les URLs étaient liés à une infrastructure connectée à la société **NSO Group**. Cette dernière basée en Israël est spécialisée dans la vente de logiciels de surveillance à destination de sa clientèle d'origine étatique.

L'objectif de cette attaque ciblée était très clairement de mettre le téléphone mobile d'Ahmed Mansoor sous surveillance. En effet, dans un premier temps la société Lookout Security – qui collabora avec Citizen Lab sur cette investigation – mit en avant le fait que les liens contenus dans les SMS menaient à la chaîne d'exploits zero-day baptisée **Trident**. Cette dernière aurait permis la compromission de l'iPhone ciblé via **un jailbreak à distance**. La première vulnérabilité **CVE-2016-4657** se situe dans la bibliothèque WebKit utilisée par le navigateur Safari. Elle permet via le chargement une page web d'exécuter du code arbitraire. La seconde faille **CVE-2016-4655** est utilisée pour localiser les zones mémoire du Kernel et la troisième **CVE-2016-4656** pour les modifier. Ce processus permet d'obtenir un accès complet pour déverrouiller toutes les fonctionnalités du système d'exploitation iOS, éliminant ainsi les restrictions et sécurités posées par Apple.

En cas de succès, le piratage se serait soldé par le déploiement du malware dédié de la solution Pegasus. À partir d'un échantillon de ce dernier, Lookout Security a pu mettre en avant un ensemble de fonctionnalités destinées à l'espionnage de l'appareil infecté (fonctionnalités qui se déroulent toutes en arrière-plan) :

- Interception des communications texte, audio ou vidéo d'une large série d'applications, notamment : Gmail, Facetime, Facebook, Line, Mail.Ru, Calendar, WeChat, Surespot, Tango, WhatsApp, Viber, Skype, Telegram, KakaoTalk (liste non exhaustive).
  Le malware ne se contente pas de télécharger des versions malicieuses des applications, mais il compromet directement les originales qui sont préalablement installées sur l'iPhone.
- Vol des données de paramétrage réseau, du calendrier, du carnet d'adresse et de la base de mots de passe KeyChain.
- Enregistrement (audio et vidéo) de la victime en temps réel via le microphone et la caméra.

Une fois déployé, le malware demeure sur l'appareil même si le détenteur met à jour le système d'exploitation iOS. Par ailleurs, Pegasus est capable de **s'autodétruire s'il détecte que sa furtivité est compromise**. Ainsi, la victime ne pourra jamais s'apercevoir qu'elle a été espionnée. Le seul élément permettant d'alerter l'utilisateur de l'infection de son appareil est le **crash du navigateur Safari**. Or cet événement n'est pas rare et survient occasionnellement lors d'une utilisation normale de l'iPhone.

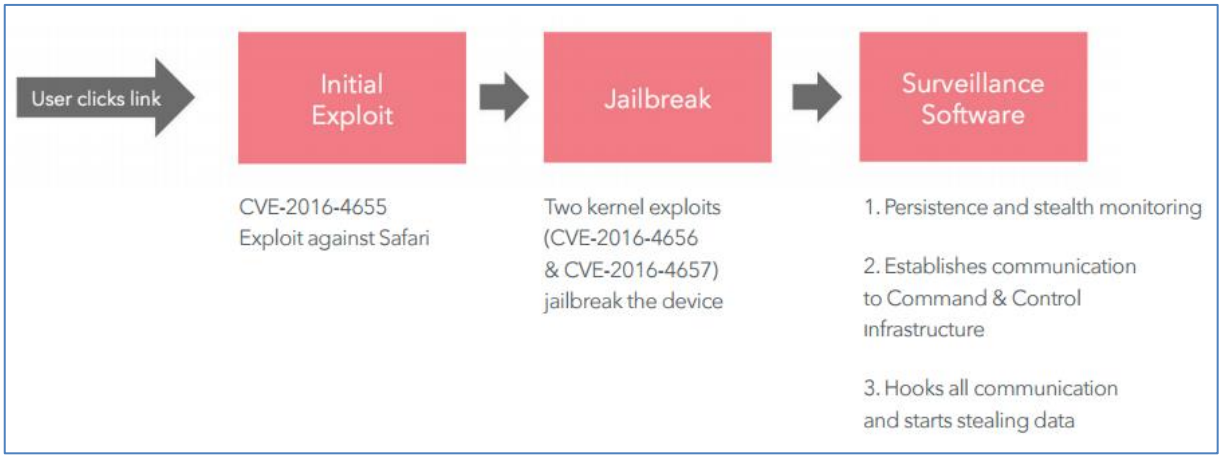
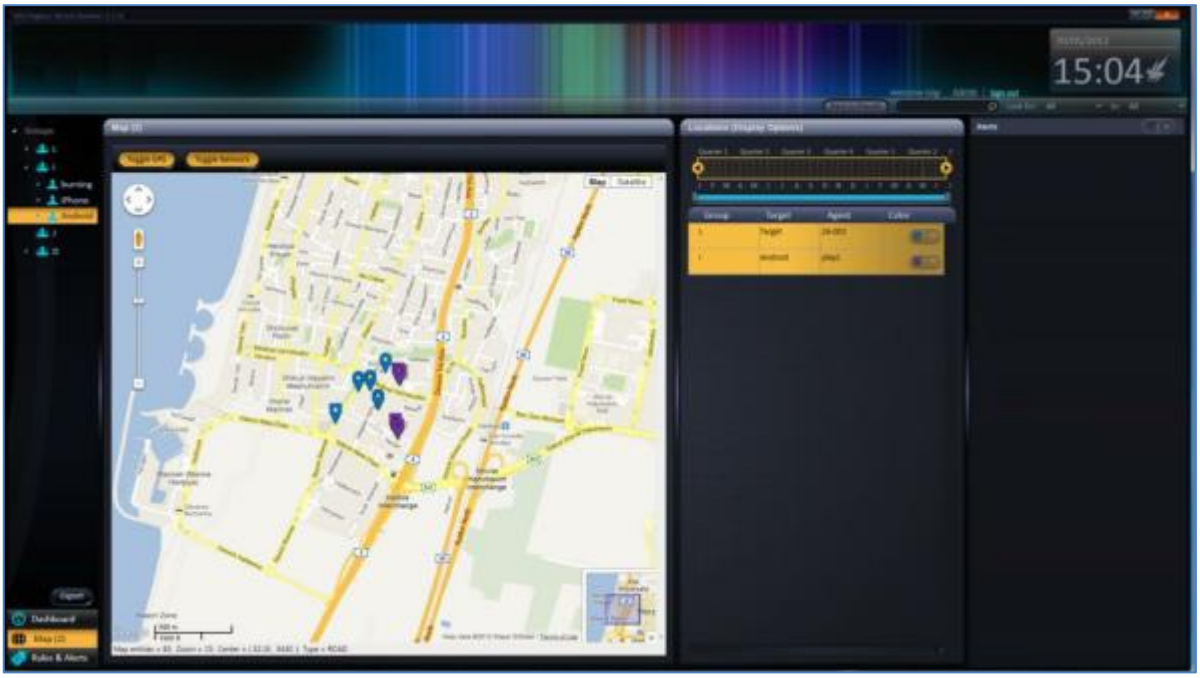


Schéma de l'attaque – Source : Lookout

Par ailleurs, la fuite de données qui a suivi le piratage de la société Hacking Team en 2015 a permis de mettre en avant un ensemble de documents apparemment relatifs au fonctionnement de la solution Pegasus. Cette dernière repose sur trois modules : **une station de travail, un serveur d'infection et une infrastructure Cloud**. Les données exfiltrées lors de l'attaque peuvent être visualisées via une interface graphique dédiée qui géo-localise également les victimes :



Capture d'écran de la supposée station de travail de Pegasus – Source : WikiLeaks[8]

L'attaque dont a été victime Ahmed Mansoor n'a pu être orchestrée que par une entité disposant de ressources importantes en raison des moyens déployés. À titre d'exemple, l'achat d'une faille zero-day ciblant iOS représente un coût d'acquisition très élevé : la société Zerodium a déboursé 1 million de dollars en 2015 pour obtenir ce type de faille[9].

L'espionnage d'un appareil reposant sur iOS demande donc des moyens conséquents pour l'attaquant dont l'origine est souvent étatique. Le système d'exploitation développé par Apple ne représente effectivement pas une opportunité pour le cybercriminel classique développant des malware : en raison des différents facteurs préalablement évoqués, cette communauté préfère se tourner vers l'OS Android qui représente une bien meilleure opportunité.

Les malware Android provenant des plateformes cybercriminellles underground

Les téléphones mobiles stockent un grand nombre de données personnelles et professionnelles qui sont très prisées par les cybercriminels. Lorsque ces derniers parviennent à voler ces informations, ils monétisent leur butin en les revendant sur les plateformes cybercriminelles underground où des acteurs malveillants proposent les malware à l'origine des attaques. Ainsi, les vendeurs présents sur les forums ou marchés noirs cherchent à développer leur portefeuille clients et commercialisent de manière quasi-exclusive des produits ou services qui ciblent les terminaux reposant sur le système d'exploitation Android. La part de marché relativement basse des terminaux reposant sur iOS n'incite pas non plus les cybercriminels à consacrer des ressources au développement de malware et préfèrent se tourner vers le système d'exploitation plus populaire qu'est Android. Ainsi, quatre malware Android de haute qualité sont actuellement proposés sur les plateformes cybercriminelles underground :

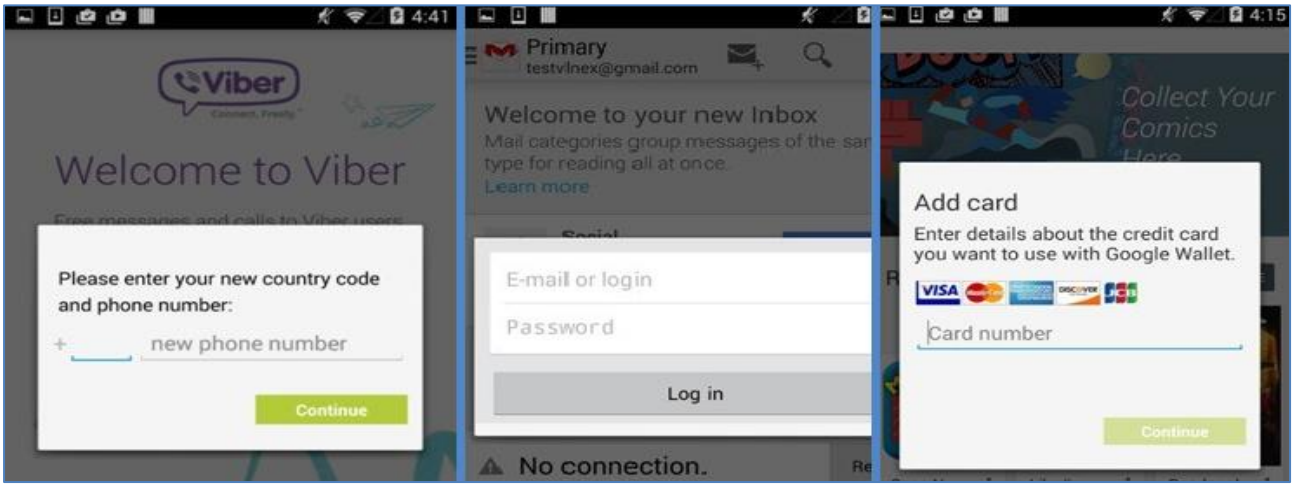
- **Exo** est aujourd'hui considéré comme le malware Android le plus puissant et le plus complet : contrôle total de l'appareil infecté, vol des informations bancaires, interception des messages et appels, mise hors service du terminal, coupure du son et de la vibration, blocage des anti-virus, etc.

[8] https://wikileaks.org/hackingteam/emails/emailid/5391

[9] https://www.zerodium.com/ios9.html

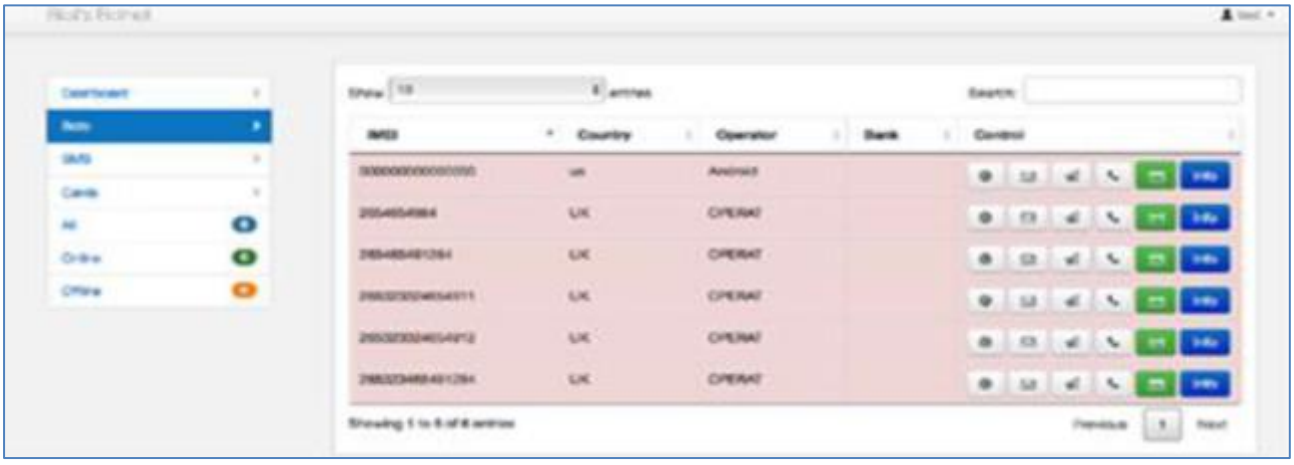
Panel d'administration du malware Exo – Source : CEIS

Exo est en mesure de **superposer des injections par-dessus un grand nombre d'applications** comme Gmail, Facebook, Skype, WhatsApp, Instagram, Paypal, Twitter, Google Play, Google Musique, ou encore les applications bancaires. En d'autres termes, lorsque l'utilisateur du terminal Android souhaite accéder à l'une de ses applications, une fausse fenêtre apparait et lui demande ses identifiants ou coordonnées bancaires qui sont récupérés par la suite par l'attaquant :



Exemple d'injections par-dessus des applications – Source : Kaspersky Lab

- **Bilal** se démarque des autres malware par **des mises à jour régulières** (deux fois par semaine), **un nombre de fonctionnalités limitées mais très élaborées** et **une furtivité quasi-totale face aux anti-virus.** Le développeur de Bilal s'est également démarqué en s'associant à **Kaktys**, un spécialiste de la conception **d'injections ciblant les applications**. De la même manière qu'Exo, ces dernières sont des surcouches qui se mettent sur les applications et volent les données renseignées par la victime.



Panel d'administration du malware Bilal – Source : CEIS

- La particularité du malware **Cron bot** est **sa double version Android (apk) et Windows (exe)** qui dispose de nombreuses caractéristiques dédiées. Ce produit est considéré comme l'un des plus

dangereux. Son créateur a récemment mis à disposition le loader **C2H5OH** pour Android (malware permettant d'installer des malware complémentaires) et le stealer **Fox v1.0** (malware dédié au vol d'informations du type mots de passe ou frappes exécutées sur un clavier).

- **GM_Projects's VBV Grabber** est un malware Android très épuré dont la caractéristique est de voler exclusivement des informations bancaires, donnés très recherchées par les cybercriminels. Son code source s'appuie en partie sur celui du malware **Mazar** dont les vagues d'attaques ont largement été relayées par d'importants site web comme celui de la BBC[10] ou Forbes[11] durant le mois de février 2016.

Ainsi, le recours aux malware ciblant les téléphones mobiles témoigne d'une réelle tendance en termes de cyber-attaques. Ces programmes informatiques restent cependant utilisés de manières très différentes selon l'OS ciblé. Les moyens demandés pour s'attaquer à iOS sont considérables comme en témoigne l'exploitation de trois failles zero-day lors du déploiement de la solution Pegasus. En raison d'un marché bien plus important comparé au système d'exploitation d'Apple, les cybercriminels optent pour le développement de malware Android : Cron bot, Bilal, Exo et GM_Project's VBV Grabber se démarquent ainsi des autres malware. La concurrence est féroce entre les développeurs de ces programmes. Ces derniers cherchent à se mettre en avant en assurant un support constant, en proposant des mises à jour régulières, mais également des fonctionnalités avancées.

Le malware Android Twitoor s'est récemment démarqué en recevant ses instructions via le réseau social Twitter plutôt qu'un serveur C&C classique[12]. Twitoor est une backdoor permettant l'installation d'autres malware. Il ne se propage pas via Google Play mais par des SMS/MMS contenant les liens malveillants. Ce sont les messages privés de Twitter qui permettent au programme malveillant de prendre ses instructions. Cette capacité lui permet d'être plus furtif et résistant. Dans le cas classique du C&C, lorsque le serveur est saisi, c'est l'ensemble du botnet qui tombe, or un compte Twitter est facilement remplaçable et permet de maintenir en vie le parc d'appareils zombies. Les attaquants ont de plus en plus recours à ce type de technique pour contrôler leur botnet, avec l'utilisation du chat Google ou Facebook, ou encore des statuts sur des comptes fantômes LinkedIn, Facebook, Twitter, Pastebin.

[10] http://www.bbc.com/news/technology-35586446

[11] http://www.forbes.com/sites/ewanspence/2015/02/04/android-malware-apps-deleted/#5bac29191d55

[12] http://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/

AUTOMATISATION DE PROCESSUS DECISIONNEL EN CYBERDEFENSE

Les départements IT des grandes entreprises sont confrontés aux mêmes impératifs de rendement et de rentabilité que les autres. Ses responsables ont besoin de justifier, contrôler, voire de limiter leurs coûts de fonctionnement ainsi que la croissance de leurs effectifs sur l'ensemble de leur périmètre, qu'il s'agisse de la gestion et maintenance informatiques ou de la sécurité.

L'univers de la Cybersécurité défensive, structuré autour des trois grandes postures que sont la prévention, la détection et les activités d'investigation/réaction, n'échappe pas à la règle. Principaux défis : la croissance exponentielle des événements sécurité, l'impossibilité de les traiter manuellement et la rareté des profils compétents.

Il appartient donc désormais aux DSI et RSSI de jongler avec ces différents besoins et contraintes, notamment en cherchant à automatiser certaines tâches de gestion, de supervision ou de traitement (remédiation).

Historique de l'automatisation de la cybersécurité et bilan

Ces quinze dernières années, les outils de détection et les approches retenues ont subi de multiples métamorphoses en fonction des évolutions technologiques des systèmes et des réseaux (augmentation des débits et capacités de traitement (cloud et logique Big Data par exemple). Ils offrent de nouvelles possibilités d'automatisation ainsi qu'un panel de mesures et de capacités d'observation et de surveillance sans cesse étendu : détection de code malveillant, détection des attaques dans les réseaux de capteurs, détection des attaques par déni de service, détection d'attaques contre des applications spécifiques, etc.

Historiquement, on observe que les moyens de détection, domaine de recherche actif depuis le début des années 1980 et déployé opérationnellement depuis les années 1990, ont ouvert la voie au domaine de l'automatisation des réponses à incident cyber. Ils ont été parmi les premiers systèmes à proposer des capacités de remédiation systématique à certaines familles d'attaques (DoS ou DDoS principalement). Ce type de technologies et de sondes (NIDS ou HIDS) font aujourd'hui partie de la panoplie des outils des professionnels de la sécurité.

Sur le plan technique, la genèse de l'automatisation dans la gestion des équipements et logiciels de Cybersécurité a débuté dans les années 2001-2002. Un éditeur français, Solsoft, tentait de remédier aux lacunes de gestion semi-automatique d'un parc hétérogène d'équipements. Son logiciel *Net Partitionner (NP)* ciblait plus d'une dizaine de marques de pare-feu et de réseaux privés virtuels (VPN) distincts. Pour chacune de ces applications, il créait des règles de sécurité et les traduisait dans des fichiers de configuration spécifiques. Il ne s'agissait plus d'avoir une vue d'ensemble de son réseau, mais plutôt et surtout d'administrer simplement des équipements souvent distants et hétérogènes. Toutefois, ce logiciel ne gérait pas les remontées d'informations et celui-ci était limité en action pour chaque éditeur de plate-forme. De son côté, l'éditeur de sécurité McAfee est le premier à parler d'orchestration avec un outil centralisé destiné à

orchestrer les différents composants et à remonter les principaux incidents (ePolicy Orchestrator).

En parallèle sont apparues au début des années 2000 les sondes de détection d'intrusion, les plates-formes de gestion de la sécurité, puis les centres opérationnels de sécurité (SOC[13]). Objectif : externaliser, pour des raisons à la fois technologiques et économiques, la gestion des événements et des alertes issues des sondes de détection, des pare-feu et des serveurs ainsi que leur analyse et les éventuelles réactions associées. Ces fonctions permettent de traiter des volumes de logs et d'alertes toujours plus importants pour connaitre l'état du système. Les moyens de détection et de surveillance émettent en effet des alertes qui, individuellement, sont souvent peu explicites. La mise en évidence de la difficulté à opérer, surveiller et superviser un à un ces éléments, a conduit à la conception de centres de sécurité spécialisés dans le traitement des alertes. Au niveau système, les premiers besoins en automatisation des contre-mesures apparaissent au cours de cette même période.

Retours d'expériences

Aujourd'hui, les moyens mis-en-œuvre dans les SOC permettent le traitement d'incidents et d'alertes de complexité variable (via des fonctions de normalisation, d'agrégation, de corrélation puis de remontée des incidents pertinents). Le SOC a pour objectif en particulier d'afficher des indicateurs cybersécurité sur les biens essentiels à protéger pour l'entreprise. Cependant, à l'exception de la lutte contre les attaques par déni de service à grande échelle, les outils de gestion et de supervision des incidents de sécurité ne disposent pas encore de capacités de déploiement optimal des mesures de réaction automatique.

Cette expérience opérationnelle permet de dresser le panorama suivant :

1. En complément de l'activité de Maintien en Condition de Sécurité classique (MCS), une veille ciblée permet une meilleure évaluation du risque. Les activités de prévention et d'anticipation de la menace sont ainsi en ébullition ces dernières années avec la montée en puissance de la *Threat Intelligence* (TI). En fournissant des données statistiques pertinentes, des tendances et des potentialités d'agressions, cette veille vient enrichir et compléter les activités de supervision classiques. Elle améliore la réactivité d'un centre opérationnel de sécurité et participe à la compréhension d'alerte ou d'activités douteuses. La TI met aussi en avant certaines menaces ou vulnérabilités détectées dans les signaux faibles. Ce type de veille, manuelle ou partiellement automatisée, permet ainsi d'orienter et d'augmenter la sensibilité et l'acuité d'un ensemble de capteurs et de sondes afin d'anticiper certaines attaques en concentrant les ressources sur les activités prédictives.

2. L'automatisation des mesures de détection et de contrôle de conformité ont déjà passé un certain niveau d'automatisation (dans le domaine de la gestion des règles par exemple). Si le développement des approches statistiques et heuristiques permet de dépasser les limites de la détection par signature, il faut en effet être conscient que les attaques non détectées sont souvent les plus dangereuses (ces attaques ne correspondent généralement à aucune signature présente dans la sonde ou à aucun comportement anormal). Il est ainsi vraisemblable que de nombreuses attaques non détectées subsistent toujours dans les réseaux et systèmes

[13] Security Operation Center

actuels et que d'autres ne sont que très partiellement détectées et traitées par des processus et règles automatiques des SIEM (Security Information and Event Management). Lorsqu'elles sont détectées par les sondes, certaines ne sont ainsi pas déjouées car les alertes ne sont pas transmises au bon niveau opérationnel ou ne sont pas correctement traitées par les opérateurs. Il s'agit donc plutôt d'une faiblesse de diagnostic et d'intelligence collective dans un système d'information complexe, voire d'une insuffisance dans la chaîne de pilotage et de décision, quand bien même celle-ci est équipée d'outils de corrélation de type SIEM, que d'un défaut de détection de la sonde.

3. Aujourd'hui, les responsables cybersécurité demeurent très réticents par rapport au concept de réaction automatisée. En effet, le nombre et la faible qualité des alertes à traiter, même en présence d'un Centre Opérationnel de Sécurité (SOC) bien équipé et constitué de profils compétents, pose toujours un problème d'interprétation. Les outils de prévention d'intrusion et de réaction automatique présents sont ainsi souvent désactivés en raison du risque non négligeable de perdre un service opérationnel sur une action mal maitrisée. Peut-il exister une réponse systématique à un problème de sécurité qui est protéiforme et de nature et d'origine multiples, alors qu'une même conséquence peut avoir des origines différentes ou être générée par l'exploitation de chemins d'attaques divers/distincts ? La mise en œuvre d'indicateurs opérationnels Cyber est ainsi loin d'être automatisée.

Des processus semi-automatiques

Pour aborder sereinement la problématique de l'automatisation, il convient tout d'abord d'identifier les technologies de sécurité existantes ou en développement et d'en déterminer le niveau possible d'automatisation. Dans le domaine de la réaction/remédiation, de nombreuses évolutions sont en effet susceptible de faciliter l'automatisation de certains traitements dans une chaine opérationnelle et technique composées d'outils classiques indispensable (fig.1) :

- Des outils de gestion d'incidents, notamment de *ticketing* et de gestion centralisée de fiches de réactions. Ils facilitent la réaction et la remédiation et ainsi un retour du système à la normal sur des alertes simples généralement ;
- Une base d'inventaires alimentée quotidiennement et automatiquement, intégrant par exemple la liste des COTS, des versions logicielles et les adresses IP associées. Celle-ci permet de se concentrer sur les principaux éléments dont une vulnérabilité reste facilement exploitable (on parle plutôt de biens support). Cette base est reliée à l'activité de veille (MCS) et fournit un niveau de vulnérabilité du système ;
- Une base d'incidents ou d'évènements enrichie (PlayBook) alimentant utilement la connaissance du SI supervisé. Elle permet une intervention efficace en réaction face à certains types d'attaques déjà rencontrées. Celle-ci contient le savoir-faire d'une équipe au sein d'un SOC sur la réponse à incident ;
- Les résultats remontés par des outils de vérification et d'audit de conformité automatique sur les principaux constituants du système. Les organisations doivent surveiller en permanence les systèmes informatiques et les applications déployées (intégrité des configuration), incorporer les mises à niveau de sécurité pour les logiciels et déployer des mises à jour des configurations à l'aide de protocoles d'automatisation comme SCAP, OPENIOC, etc.
- Une plate-forme de pré-production représentative permet de dérouler des scénarii de mises à jour et de tester des mesures de contournement. Des outils automatiques de distribution et de tests sont essentiels dans le processus de remédiation ;
- Une analyse de risque dynamique, l'objectif étant de réévaluer le niveau de risque à chaque modification du système ou découverte de nouvelles vulnérabilité ;

- Des outils d'orchestration facilitant la démarche de réaction en cas de crise ou de remédiation. Ce *cockpit de sécurité* visualise les niveaux de menaces, les alertes et propose des mesures de réaction et de remédiation semi-automatiques.

Les liens entre ces différents outils devront être à terme automatisés, la difficulté résidant aujourd'hui dans la diversité des solutions choisies.

Fig.1. Principales briques d'un SOC

Orchestration et automatisation : où se trouvent les limites ?

La différence entre la simple réponse automatique à incident et l'orchestration de réponses unitaires réside dans l'automatisation avancée des traitements dans le SOC. L'orchestration permet de contrôler l'ensemble de l'environnement de sécurité et les nombreuses briques technologiques qui le composent (la remontée de faux-positifs est encore trop importante sur les outils classiques de SIEM). L'orchestration permet de se protéger plus efficacement dans une approche par étape successives pour remédier aux problèmes. L'intérêt suscité par ces nouveaux outils s'explique de façon simple : les grandes entreprises ont besoin de réduire leurs coûts et d'optimiser leurs ressources humaines. Le premier enjeu de l'automatisation est donc bien de réduire le nombre d'événements traités manuellement chaque jour, ce qui suppose déjà que les éditeurs de logiciels développent des solutions interopérables avec les outils d'orchestration.

Au-delà de cet enjeu, c'est en réalité l'action humaine qui arrive à ses limites. Face à un incident, la réaction passe par un circuit de décision relativement lent, surtout en cas de crise cybernétique. Les meilleures intelligences humaines ne peuvent donc répondre assez vite et interagir ensuite avec des dizaines de mesures

de sécurité isolées pour protéger l'environnement, constituant ainsi un goulot d'étranglement.

L'orchestration permet aussi d'interagir sur les éléments du cycle de gestion des vulnérabilités (en particulier sur les risques identifiés), de suivre le cycle de vie des systèmes de cyber-protection et d'assurer une mise à jour continue des politiques de sécurité. Il n'est donc plus question de se limiter à la supervision et à l'hypervision d'alertes de sécurité sur des indicateurs prédéfinis et alimentés automatiquement par des règles de corrélation. Ces nouveaux outils permettent la priorisation de la gestion des alertes, la réduction du nombre d'actions simples à mener pour focaliser les ressources sur des évènements et des actions de réaction plus complexes. Il ne semble cependant pas évident d'automatiser ce type de réaction sur toute la chaine de décision, chaque incident devant entraîner une démarche ou une action spécifique.

La prise en main des outils d'orchestration nécessite ainsi un temps d'apprentissage certain, même si celui-ci peut être réduit avec l'emploi des technologies de virtualisation.

Les technologies et le concept même d'automatisation possèdent cependant quelques limites. La première réside dans la complexité des architectures de sécurité, la variété des types de mesures de sécurité à mettre à jour ou à activer et la complexité de la chaine de réaction qui en résulte.

Si la démarche d'automatisation se montre ainsi particulièrement efficace sur des cas concrets et simples (modification d'une règle de filtrage, cloisonnement d'applications infectées dans un cloud par exemple), celle-ci peut avoir des effets non désirés :

- Un ensemble d'actions peut augmenter la surface d'attaque ou créer de nouvelles portes d'entrées ;
- Le blocage d'adresse IP, la mise en quarantaine non voulue et trop systématique d'une application dans un système de virtualisation de type Cloud Computing peut avoir pour conséquence une perte de service.

De plus, le risque de propagation d'une attaque et son adaptation repose sur la capacité d'un attaquant à anticiper ces processus automatisés et répétitifs, tel un virus en mutation capable de résister à un antidote. Le détournement de réactions automatiques à des fins d'attaques pourrait ainsi se traduire par un déni de service généralisé. L'outil lui-même (en particulier les bus de données et d'échanges), faisant le lien avec l'ensemble des mesures de sécurité, constitue une cible de prédilection pour un attaquant souhaitant affaiblir les réactions.

L'automatisation peut également engendrer la déresponsabilisation des intervenants humains : la machine propose, grâce au *machine learning*, une analyse prédictive pour réagir face à une attaque, ce qui est intéressant mais peut introduire certains biais et rend difficile tout retour au mode dégradé, voire décide toute seul, avec un risque de potentielles dérives.

Les technologies d'automatisation et d'orchestration doivent cependant faire leurs preuves sur les architectures de sécurité plus complexes. Cependant, elles restent néanmoins indispensables pour assister les équipes d'un centre de supervision. Reste à savoir s'il doit s'agir de solutions autonomes ou si celles-ci doivent être intégrées avec les autres outils du SOC. A côté des fonctions automatisées d'outils de sécurité généralistes, l'orchestration reste aujourd'hui l'apanage de solutions dédiées compte tenu de la complexité inhérente de ce type de solution. La question est donc de savoir si ces technologies seront efficaces combinées à des produits existants comme des SIEM. Pour être utiles, celles-ci ne doivent en effet pas se

contenter de fournir des réactions types mais des réponses contextualisées, adaptées aux spécificités du SI considéré. Tout dépendra ensuite de la bonne volonté des éditeurs de se rendre pleinement compatible avec ce type de solution et de la capacité de certains gros éditeurs de forcer le marché…

Solutions logicielles d'orchestration : un secteur en pleine effervescence

Phantom Cyber[1] entend accélérer la remédiation d'incidents. C'est le vainqueur de l'Innovation Sandbox de l'édition 2016 de RSA Conference. L'entreprise se présente comme l'éditeur d'une plateforme d'orchestration et d'automatisation dédiée à la réponse aux incidents de sécurité. Autres acteurs clés : Resilient Systems, racheté par IBM, ou Invotas, acquis par FireEye. Ces opérations témoignent de l'ambition des grands éditeurs d'être au cœur du SOC pour contrôler toute la chaine de sécurité.

Le Cyber Grand Challenge de la DARPA dédié à l'automatisation

Pour toute vulnérabilité logicielle, il existe un décalage important entre la fourniture du rapport de vulnérabilité initial et le déploiement généralisé des correctifs. Les analystes de la cybersécurité ont de ce point de vue un désavantage important sur l'attaquant. Dans de nombreux cas, une course contre la montre s'ensuit entre les attaquants qui ont l'intention d'exploiter la vulnérabilité et les analystes qui doivent évaluer, remettre en état, tester et déployer un patch avant que des dommages importants puissent être causés. Les experts suivent un processus qui implique un raisonnement sophistiqué suivi par la création manuelle de chaque signature de sécurité et la fourniture de mesures de contournement ou correctifs logiciels. Une approche artisanale qui peut nécessiter de longs mois et des ressources financières importantes et contribue largement à l'insécurité informatique ambiante.

Pour contribuer à la résolution de ces défis, la DARPA a lancé en 2013 le Cyber Grand Challenge, un concours visant à créer des systèmes de défense automatique capables de comprendre les vulnérabilités, de fournir des patchs et de les déployer sur un réseau en « temps réel ». En agissant à l'échelle de la vitesse de la machine, ces technologies pourraient, dans la vision technologique américaine, renverser la situation actuelle.

A l'issue d'une compétition de deux ans, c'est la startup ForAllSecure[1] qui a remporté il y a quelques semaines le challenge avec un système baptisé Mayhem.

Sources :

http://www.darpa.mil/program/cyber-grand-challenge

https://humanoides.fr/mayhem-cyberdefense-automatisee/

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com