FireEye™

Livre blanc

Efficacité zéro :

Étude sur les attaques zero-day de 2013 et ce qu'elles révèlent au sujet du modèle de sécurité traditionnel

Sommaire

Introduction

De toutes les menaces qui pèsent sur les systèmes informatiques d'entreprise, les vulnérabilités zero-day comptent parmi les plus pernicieuses et dangereuses. Inconnues et imprévisibles par nature, elles mettent en péril les systèmes des utilisateurs et des administrateurs les plus diligents.

Les vulnérabilités zero-day sont des failles logicielles qui exposent les utilisateurs à des cyberattaques jusqu'à ce qu'une solution temporaire soit mise en place ou un correctif distribué. Parfois, la vulnérabilité est inconnue de tous — à l'exception d'un cybercriminel (ou d'un éditeur prêt à vendre les découvertes de ce type sur le marché noir). Parfois encore, l'éditeur du logiciel l'a identifiée, mais n'a encore distribué aucun correctif permettant d'y remédier.

Dans un cas comme dans l'autre, les utilisateurs sont totalement vulnérables, et ce quel que soit le budget consacré à leur défense. Des vulnérabilités inconnues sont sans doute présentes dans tous les logiciels. Elles ne constituent un véritable risque qu'une fois lâchées « dans la nature », à la merci de pirates prêts à les exploiter pour lancer leurs cyberattaques.

Comment se protéger ? L'application de correctifs ne suffit pas, pas plus que la mise à jour des définitions de logiciels malveillants (*malware*) des logiciels antivirus. Bien souvent, même les stratégies de défense « en profondeur » multiniveau ne parviennent pas à bloquer une attaque zero-day contre vos actifs informatiques.

« Il n'y a quasi aucun moyen de se protéger contre une attaque zero-day », indiquait un rapport de sécurité publié en 2012. « Tant que la vulnérabilité n'est pas connue, aucun correctif ne peut être appliqué au logiciel concerné et les analyses antivirus basées sur les signatures sont incapables de détecter l'attaque[1]. »

Ce livre blanc explique les dangers des attaques zero-day et démontre l'impuissance des mécanismes de défense traditionnels face à elles. Il décrit également 11 vulnérabilités zero-day mises au jour par FireEye en 2013, ainsi que l'exploitation qui en a été faite dans le cadre d'attaques réelles. Enfin, il recommande 9 mesures concrètes à mettre en œuvre pour réduire les risques liés à de telles menaces.

Banalisation alarmante des attaques zero-day

Les menaces zero-day sont omniprésentes. Chaque jour au cours des trois dernières années, des cybercriminels ont exploité au moins 85 vulnérabilités pour attaquer des logiciels populaires de Microsoft, Apple, Oracle et Adobe[2]. Dans la mesure où cette estimation ne tient compte que des vulnérabilités finalement signalées, il est probable que le nombre réel de vulnérabilités zero-day accessibles aux cybercriminels soit largement supérieur.

Les vulnérabilités découvertes par les cybercriminels restent inconnues du public — éditeurs des logiciels concernés compris — pendant une période moyenne de 310 jours[3].

Il n'est pas surprenant de constater que les attaques ciblées recourent massivement aux exploits zero-day. Ces armes secrètes confèrent aux pirates un avantage décisif sur les entreprises ciblées, combien même investiraient-elles des sommes exorbitantes en produits de sécurité traditionnels.

Qui plus est, l'abondance des vulnérabilités zero-day et la maturité croissante de ce marché noir au niveau mondial contribuent à la prolifération des exploits zero-day. Selon un article récent de Reuters[4], les administrations restent les principaux acheteurs d'exploits zero-day. Toutefois, quiconque est prêt à y mettre le prix — dans certains cas, 5 000 dollars suffisent[5] — peut s'en procurer.

1 Leyla Bilge et Tudor Dumitras (Conférence ACM sur la sécurité informatique et des communications), *Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World*, octobre 2012

2 Kelly Jackson Higgins (Security Dark Reading), *Hacking The Zero-Day Vulnerability Market*, décembre 2013

3 Andy Greenberg (Forbes), *Hackers Exploit 'Zero-Day' Bugs For 10 Months On Average Before They're Exposed*, octobre 2012

4 Joseph Menn (Reuters), *Special Report: U.S. cyberwar strategy stokes fear of blowback*, mai 2013

5 Andy Greenberg (Forbes), *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits,* mars 2012

Exploitation dans le cadre de campagnes hautement destructrices

Ces dernières années, les exploits zero-day ont permis le déploiement d'attaques particulièrement dévastatrices et par ailleurs très médiatisées.

Opération Aurora

Cette campagne tristement célèbre lancée en 2009 a pris pour cible une bonne vingtaine d'entreprises, dont Google, Adobe Systems, Juniper Networks, Rackspace, Yahoo!, Symantec, Northrop Grumman, Morgan Stanley et Dow Chemical[6].

C'est une vulnérabilité d'Internet Explorer, CVE-2010-0249, qui a servi de point d'entrée à cette attaque de point d'eau (*watering hole*). À l'aide de code JavaScript exploitant la vulnérabilité, les pirates compromettaient un site Web légitime, dont les visiteurs étaient ensuite infectés à leur insu par un logiciel malveillant, qui pouvait alors dérober des éléments de propriété intellectuelle, compromettre les comptes d'utilisateur et espionner les systèmes.

Stuxnet

En 2010, s'appuyant sur au moins trois exploits zero-day distincts — un fait sans précédent —, le ver Stuxnet a endommagé des systèmes de contrôle industriels et saboté l'infrastructure iranienne d'enrichissement d'uranium de Natanz[7].

L'attaque exploitait notamment les vulnérabilités zero-day suivantes :

- **CVE-2010-2568** — Permet l'exécution d'un code arbitraire lorsque l'utilisateur ouvre un dossier contenant un fichier .LNK ou .PIF conçu à des fins malveillantes.
- **CVE-2010-2729** — Permet l'exécution d'un code arbitraire lorsque le pirate envoie un message d'appel de procédure distante (RPC) spécialement conçu.
- **CVE-2010-2772** — Permet aux utilisateurs locaux d'accéder à une base de données principale d'un système SCADA Simatic WinCC ou PCS 7 de Siemens et d'obtenir des privilèges dans celui-ci.

L'attaque exploitait également des vulnérabilités déjà corrigées, ce qui tend à indiquer que les pirates savaient que les systèmes n'auraient probablement pas été mis à jour.

Attaque contre RSA

En 2011, des cybercriminels ont infiltré la division RSA Security d'EMC et dérobé des informations secrètes relatives à son système d'authentification largement répandu. Ce vol de données pouvait avoir de sérieuses conséquences sur l'efficacité des systèmes d'authentification par jeton SecurID et ainsi affaiblir la sécurité d'un nombre incalculable de clients RSA[8].

Les employés de RSA ont reçu des messages d'hameçonnage (*phishing*) auxquels était joint un fichier Excel piégé nommé « 2011 Recruitment Plan ». Celui-ci contenait un objet Adobe Flash malveillant exploitant la vulnérabilité CVE-2011-0609, qui a permis l'installation de l'outil d'accès à distance (RAT) Poison Ivy. Ainsi, les cybercriminels ont pu recueillir les identifiants de connexion de cibles d'importance stratégique disposant d'un accès aux données d'authentification de RSA.

« (...) Les entreprises déploient toutes les combinaisons possibles de contrôles de sécurité de pointe au niveau du périmètre réseau, des serveurs et des postes de travail, et associent ces contrôles à des opérations de sécurité avec tout autant d'ingéniosité », constate Uri Rivner, cadre dirigeant chez RSA à l'époque, dans un article de blog. « Pourtant, un pirate déterminé réussira toujours à passer entre les mailles du filet. Qu'est-ce que cela nous montre[9] ? »

6 Wikipédia, *Operation Aurora*, octobre 2013

7 Gregg Keizer (InfoWorld), *Is Stuxnet the 'best' malware ever?*, septembre 2010

8 John Markoff (The New York Times), *SecurID Company Suffers a Breach of Data Security*, mars 2011

9 Uri Rivner (RSA), *Anatomy of an Attack*, avril 2011

Des mécanismes de défense standard totalement démunis face aux menaces zero-day

Bien qu'il ne réponde pas directement à cette question dans l'article, M. Rivner dresse un constat sans équivoque : les outils de sécurité traditionnels ne font plus le poids face aux exploits zero-day.

Ces outils s'appuient sur les signatures binaires des logiciels malveillants ou sur la réputation de serveurs et d'URL externes. Par définition, ils ne sont en mesure d'identifier que des menaces connues et confirmées. L'auteur d'une attaque peut facilement pirater un site Web légitime dans le but de contourner une liste noire. Les techniques de dissimulation et de mutation de code génèrent de nouvelles variantes de logiciels malveillants plus vite que les éditeurs de solutions de sécurité traditionnelles ne peuvent créer de nouvelles signatures. De plus, les filtres antispam sont impuissants face aux attaques de harponnage (*spear phishing*) ciblées et de faible ampleur.

Parallèlement, les protections du système d'exploitation, comme la distribution aléatoire de l'espace d'adressage (ASLR, Address Space Layout Randomization) et la prévention de l'exécution des données (DEP, Data Execution Prevention), perdent de leur efficacité. Plusieurs exploits zero-day découverts par FireEye au cours des derniers mois utilisent des techniques de contournement des fonctionnalités ASLR qui ont clairement montré les limites de ces protections[10].

Il n'est pas étonnant qu'une attaque zero-day classique dure en moyenne huit mois — et jusqu'à trois ans dans certains cas[11]. Les cybercriminels disposent ainsi de tout le temps nécessaire pour dérober les ressources les plus précieuses des entreprises... et disparaître avant que quiconque ne sache ce qui s'est passé.

Vulnérabilités zero-day découvertes par FireEye en 2013

En 2013, FireEye a mis au jour et signalé 11 vulnérabilités zero-day — bien plus que n'importe quelle autre société du secteur. Ainsi, la même année, seules 2 autres vulnérabilités de ce type ont été révélées par les 10 principales sociétés spécialisées dans la cybersécurité (classées selon les revenus liés à la sécurité). Cette différence souligne la difficulté, pour les solutions de cyberdéfense en particulier, de détecter les attaques zero-day.

Voici les vulnérabilités zero-day signalées par FireEye, et décrites en détail ci-après :

- CVE-2012-4792
- CVE-2013-0422
- CVE-2013-0634
- CVE-2013-0640 / CVE-2013-0641
- CVE-2013-1493
- CVE-2013-1347
- CVE-2013-3893
- CVE-2013-5065
- CVE-2013-3918 / CVE-2014-0266

10 Xiaobo Chen (FireEye), *ASLR Bypass Apocalypse in Recent Zero-Day Exploits*, octobre 2013

11 Leyla Bilge et Tudor Dumitras (Conférence ACM sur la sécurité informatique et des communications), *Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World*, octobre 2012

CVE-2012-4792

Découverte vers le jour de l'An[12], cette vulnérabilité permet à des pirates d'exécuter du code d'exploit sur les ordinateurs d'utilisateurs Internet Explorer qui consultent des sites Web conçus à des fins malveillantes. L'exploit tire parti d'une faille de type utilisation de zone mémoire désallouée (*use-after-free*), où du code défaillant essaie d'accéder de manière incorrecte à de la mémoire « libérée » à d'autres fins. Ainsi, le pirate peut exécuter du code malveillant à distance sur un système ciblé.

Dans ce cas précis, il s'agissait de code JavaScript dissimulé sur le site Web du Council on Foreign Relations (CFR), un groupe d'étude et d'analyse de la politique étrangère des États-Unis. Les cibles n'ont pas été identifiées, mais le CFR compte parmi ses membres des personnalités telles que le sénateur et secrétaire d'État John Kerry, la sénatrice et présidente de la Commission du Sénat sur le renseignement Dianne Feinstein (Californie) et l'ancienne secrétaire d'État Hillary Clinton[13].

CVE-2013-0422

Exploitée dès le 2 janvier 2013[14], CVE-2013-0422 est une vulnérabilité de Java 7 qui permet aux pirates de contourner les contrôles de sécurité Java et d'exécuter du code sur un ordinateur cible. Bien que spécifique à Windows, la vulnérabilité a sans doute exposé d'autres systèmes d'exploitation exécutant Java.

Les attaques liées à cette faille téléchargent un logiciel de demande de rançon (*ransomware*) nommé « Tobfy ». Celui-ci verrouille l'ordinateur de l'utilisateur pour empêcher tout accès, affiche en mode plein écran un message censé émaner du FBI qui accuse l'utilisateur d'avoir commis un délit et exige le versement d'une somme d'argent en échange du déblocage de l'ordinateur. Tobfy désactive également le mode sans échec de Windows et met fin à des processus tels que taskmgr.exe, msconfig.exe, regedit.exe et cmd.exe afin de dissuader les utilisateurs de rechercher ou de désactiver le logiciel malveillant.

Par ailleurs, une erreur dans le code empêche le logiciel malveillant de communiquer avec l'auteur de l'attaque, notamment pour lui indiquer que l'utilisateur a versé la rançon et que le logiciel peut être supprimé du système. Les ordinateurs restaient donc inaccessibles, même si les victimes se soumettaient aux conditions du pirate.

CVE-2013-0634

Identifiée le 7 février 2013[15], cette vulnérabilité d'Adobe Flash permet à des pirates d'exécuter certains éléments de code ActionScript malveillants sur les systèmes Windows, Mac et Linux, ainsi que sur les équipements mobiles Android[16].

L'exploit a été utilisé dans le cadre d'une campagne de cyberespionnage baptisée « LadyBoyle ». Les attaques exploitant cette vulnérabilité envoyaient des documents Microsoft Word afin de cibler les utilisateurs Windows. Alors que le contenu des fichiers Word était en anglais, leur page de code était en chinois simplifié (République populaire de Chine, Singapour) Windows. Les fichiers Word contenaient une macro censée charger un objet Shockwave Flash (SWF) incorporé.

Le fichier SWF comportait quant à lui un script d'action nommé « LadyBoyle » qui comprenait le code d'exploit. L'exploit, qui ne prenait en charge que certaines versions de Flash, contrôlait la présence du composant ActiveX, propre à Windows.

Une fois la cible atteinte, le fichier SWF exploitait la vulnérabilité de Flash Player afin d'exécuter la bibliothèque de liaisons dynamiques (DLL) porteuse de la charge active ainsi que les fichiers exécutables imbriqués. La charge active provenait d'une famille connue de logiciels malveillants, utilisés dans des campagnes précédentes. L'un des fichiers exécutables injectés présentait un certificat de signature numérique non valable de MGAME Corporation, une société de jeux établie en Corée. Il se renommait pour tenter de se faire passer pour le processus de mise à jour de Google.

12 Darien Kindlund (FireEye), *CFR Watering Hole Attack Details*, décembre 2012

13 Bill Gertz (The Washington Free Beacon), *Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations*, décembre 2012

14 Yichong Lin (FireEye), *Happy New Year from New Java Zero-Day*, janvier 2013

15 Thoufique Haq et J. Gomez (FireEye), *LadyBoyle Comes to Town with a New Exploit*, février 2013

16 National Vulnerability Database, *Vulnerability Summary for CVE-2013-0422*, février 2013

À partir de ce moment, le logiciel malveillant créait une entrée de démarrage (de façon à se réactiver après un redémarrage du système) et vérifiait la présence de logiciels antivirus. Curieusement, peut-être par négligence, la charge active du logiciel malveillant n'était ni chiffrée ni dissimulée.

CVE-2013-0640 / CVE-2013-0641

Des pirates ont exploité ces deux vulnérabilités utilisant des fichiers PDF pour installer un outil d'administration à distance doté d'une architecture flexible et extensible. Ils pouvaient ajouter facilement de nouvelles fonctionnalités à l'aide de DLL de type plug-in. Le code shell du logiciel malveillant était capable de contourner les fonctionnalités de protection ASLR et DEP, plaçant ainsi la barre encore plus haut en matière de compromission.

Le code JavaScript incorporé dans le fichier PDF spécialement conçu était extrêmement bien dissimulé à l'aide de techniques de manipulation de chaînes. La plupart des variables JavaScript étaient en italien. Le code JavaScript recherchait diverses versions d'Adobe Reader et créait le code shell approprié en fonction de la version trouvée.

Les pirates injectaient ensuite dans le système trois DLL qui œuvraient de concert pour subtiliser des informations. Le composant principal (LangBar) s'insérait dans les processus Windows et contribuait à coordonner les autres DLL utilisées dans le cadre de l'attaque. La deuxième DLL (Ibarhlp) effectuait la plupart des opérations de vol de données. Enfin, la troisième (Ibarext) était chargée de compresser et de chiffrer les données dérobées.

Le logiciel malveillant, nommé « 666 », a été utilisé dans une campagne de messages de harponnage contre des cibles japonaises. Ces e-mails contenaient une pièce jointe piégée au format PDF, présentée comme un rapport de sécurité.

CVE-2013-1493

Cette vulnérabilité affectant Java Runtime Environment permet aux pirates de compromettre l'intégrité de la machine virtuelle HotSpot et de contourner le gestionnaire de sécurité Java afin de manipuler la mémoire du tas et d'exécuter des éléments de code malveillants[17].

Les attaques exploitant cette vulnérabilité téléchargeaient le cheval de Troie McRAT pour permettre la prise de contrôle des systèmes ciblés. L'exploit avait ceci d'inhabituel qu'il permettait aux pirates d'accéder à la mémoire en lecture et en écriture directement dans le processus Java Virtual Machine. Il confirmait également la tendance du recours à des attaques ciblées contournant les fonctionnalités ASLR, qui avaient formé jusque-là un rempart extrêmement efficace pour la protection des systèmes d'exploitation.

Cet exploit zero-day compte parmi les trois exploits (avec la vulnérabilité zero-day affectant Internet Explorer CVE-2013-1347 et l'exploit Java CVE-2013-2423) utilisés par la campagne Sunshop pendant l'été 2013[18].

Sunshop a compromis plusieurs sites Web stratégiques, notamment :

- Les sites de nombreux groupes de réflexion sur les opérations stratégiques et militaires coréennes
- Un forum de discussion et d'informations ouïghour
- Le site d'une revue sur les orientations scientifiques et technologiques
- Le site d'étudiants évangélistes

17 National Vulnerability Database, *Vulnerability Summary for CVE-2013-1493*, mars 2013

18 Ned Moran (FireEye), *Ready for Summer: The Sunshop Campaign*, mai 2013

CVE-2013-1347

Tout comme CVE-2013-1493, cette vulnérabilité d'Internet Explorer a été utilisée dans le cadre de la campagne Sunshop[19]. Il s'agit plus précisément d'une vulnérabilité de type utilisation de zone désallouée, présente dans les versions 6 à 8 d'Internet Explorer sous Windows XP, qui a été exploitée grâce à une technique de contournement des fonctions de protection ASLR.

L'exploit n'a pas été utilisé uniquement par des attaqués liées à Sunshop. En effet, il a été identifié dans une attaque de point d'eau qui a compromis le site Web du ministère américain du Travail[20]. Le code JavaScript intégré dans le site redirigeait ses visiteurs (des fonctionnaires fédéraux pour la plupart) vers un autre site hébergeant l'outil d'accès à distance Poison Ivy, qui permettait aux pirates de prendre le contrôle des systèmes ciblés.

CVE-2013-3893

Cette vulnérabilité affectant Internet Explorer permet aux pirates d'exécuter du code sur les ordinateurs d'utilisateurs visitant des sites Web conçus à des fins malveillantes. Elle a notamment été exploitée par la campagne « DeputyDog ».

Cette campagne a débuté en août 2013 et ciblé des entreprises situées au Japon. Au moins trois autres campagnes basées sur des menaces persistantes avancées — Web2Crew, Taidoor et th3bug — ont eu recours à ce même exploit.

CVE-2013-3918 / CVE-2014-0266

Ces vulnérabilités ActiveX, présentes dans presque toutes les versions de Windows à partir de Windows XP Service Pack 2, permettent l'exécution de code malveillant sur les ordinateurs d'utilisateurs d'Internet Explorer visitant des sites Web conçus à des fins malveillantes.

Des pirates ont exploité cette vulnérabilité dans le cadre d'une attaque de point d'eau exceptionnellement aboutie et difficile à repérer, nommée « Opération Ephemeral Hydra ». Cette attaque a pris pour cible un site Web d'une grande importance stratégique, connu pour attirer des visiteurs intéressés par la politique de sécurité nationale et internationale des États-Unis[21]. Elle présentait la même infrastructure que la campagne DeputyDog (voir le point consacré à la vulnérabilité CVE-2013-3893). En outre, le cheval de Troie utilisé pour mener ces deux attaques comprenait une chaîne de texte également identifiée dans les attaques de la tristement célèbre Opération Aurora.

Bien décidés à compliquer encore les activités de détection, d'analyse et de correction, les pirates injectaient la charge active de cette attaque directement dans la mémoire de l'ordinateur, sans aucune écriture sur le disque. Ainsi, au redémarrage de l'ordinateur infecté, la quasi-totalité des traces de l'attaque disparaissaient[22].

CVE-2013-5065

Identifiée le 27 novembre 2013, cette vulnérabilité affectant Windows XP et Windows Server 2003 permet une élévation des privilèges de l'utilisateur local, de sorte qu'un compte d'utilisateur standard est en mesure d'exécuter du code dans le noyau[23]. Elle ne permet pas d'exécuter le code à distance, mais pour ce faire, il suffit aux pirates distants de l'associer à d'autres exploits.

Des pirates ont exploité la vulnérabilité CVE-2013-5065 en même temps que la vulnérabilité CVE-2013-3346, propre à Adobe Reader et corrigée en mai. Ces attaques ciblées utilisaient comme arme un fichier PDF pour injecter la charge active du logiciel malveillant dans un dossier temporaire dans Windows et l'exécuter.

19 Yichong Lin (FireEye), *IE Zero-Day is Used in DoL Watering Hole Attack*, mai 2013

20 Michael Mimoso (Threat Post), *Watering Hole Attack Claims US Department of Labor Website*, mai 2013

21 Ned Moran, et al. (FireEye), *Operation Ephemeral Hydra: IE Zero-Day Linked to DeputyDog Uses Diskless Method*, novembre 2013

22 M. Smith (NetworkWorld), *IE zero-day attack delivers malware into memory then poofs on reboot*, novembre 2013

23 Xiaobo Chen et Dan Caselden (FireEye), *MS Windows Local Privilege Escalation Zero-Day in The Wild*, novembre 2013

Conclusion

Les vulnérabilités zero-day mises au jour en 2013 révèlent plusieurs tendances qui devraient inciter les entreprises à réévaluer leur niveau de protection :

- Les protections du système d'exploitation deviennent moins efficaces contre les attaques zero-day. Si les fonctionnalités ASLR et DEP ont constitué de grandes avancées, les pirates parviennent désormais à les contourner.
- Les attaques de point d'eau (*watering hole*) sont de plus en plus courantes. Les pirates commencent par compromettre un site Web de confiance qui rassemble un public très précis — ce qui permet de cibler des segments industriels ou gouvernementaux spécifiques —, puis attendent patiemment que les proies se présentent à eux, sans même devoir se frayer un chemin dans les systèmes visés.
- Le degré de sophistication des attaques augmente. Si l'on rencontre toujours des logiciels criminels frappant au hasard et des attaques de masse peu ingénieuses, la tendance est à la prolifération des attaques qui visent un objectif précis auprès de cibles de grande valeur. Et ces dernières trompent de plus en plus efficacement les lignes de défense des entreprises.

Recommandations

Seule l'adoption d'une approche fondamentalement nouvelle de la cybersécurité peut protéger vos ressources informatiques contre les menaces zero-day. Les mécanismes de défense basés sur les signatures recommandés hier ne font plus le poids face à l'avalanche d'exploits subie aujourd'hui. Les techniques de protection basées sur la réputation ne sont pas conçues pour détecter les attaques les plus récentes ou qui prennent le contrôle de serveurs et de sites Web de confiance à des fins malveillantes. Enfin, les environnements sandbox d'exécution de fichiers se laissent facilement berner par les logiciels malveillants de nouvelle génération et sont souvent incapables de détecter les attaques zero-day.

De nos jours, les professionnels de la sécurité doivent se préparer à affronter des menaces connues mais aussi une nouvelle dimension de menaces inconnues. Comme l'a dit le philosophe grec Héraclite, il faut s'attendre à l'inattendu[24].

À cette fin, FireEye formule les recommandations suivantes :

- **Segmenter les réseaux.** Limitez l'accès entre segments de réseau en leur attribuant des profils de risque différents. Cette mesure consiste à limiter l'accès à la zone démilitarisée depuis Internet, au réseau interne depuis la zone démilitarisée, et ainsi de suite. Elle prévoit également d'empêcher les systèmes d'une unité fonctionnelle d'accéder à ceux d'une autre unité si l'accès n'est pas absolument requis. Par exemple : empêcher l'accès aux systèmes du service d'ingénierie par ceux du service financier. Une telle initiative peut bloquer la tentative d'un pirate d'accéder à une vulnérabilité non corrigée.
- **Limiter les privilèges réseau.** Les utilisateurs et les applications ne doivent accéder qu'aux informations et ressources nécessaires pour le bon déroulement des activités. Cette mesure de précaution permet de réduire la surface d'attaque étant donné que certaines attaques nécessitent une élévation des privilèges pour être menées à bien. Elle diminue également le risque posé à l'environnement dans le cas d'une attaque fructueuse, puisqu'elle restreint l'accès aux systèmes et informations.
- **Utiliser des listes blanches d'applications.** Le fait d'autoriser les utilisateurs à installer uniquement des applications préapprouvées permet d'empêcher l'exécution de fichiers non autorisés, notamment des exploits sous la forme d'exécutables et des charges actives de logiciels malveillants.

24 Heraclitus (publié par Charles H. Kahn), *The Art and Thought of Heraclitus: An Edition of the Fragments*, 1979

- **Mettre en place un plan de réponse aux incidents.** Une attaque zero-day est imprévisible par définition. C'est pourquoi la mise en place d'un plan de réponse aux incidents robuste et résilient est d'autant plus essentielle. Les professionnels de la sécurité peuvent limiter les dommages causés par une attaque s'ils sont à même de la détecter rapidement et disposent d'une stratégie de réponse aux incidents définie, éprouvée et prête à l'emploi.
- **Connaître l'environnement.** Une équipe de sécurité ne peut pas espérer limiter le risque associé à une application présentant une vulnérabilité non corrigée si elle n'est pas au courant de l'existence de cette application et ne connaît pas suffisamment le réseau pour élaborer un plan de réduction des risques digne de ce nom.
- **Déployer une plate-forme de sécurité capable d'identifier les menaces connues et inconnues.** Les experts en sécurité s'accordent à dire que les mécanismes de protection basés sur les signatures sont inefficaces face aux menaces dynamiques en perpétuelle évolution d'aujourd'hui[25]. De tels mécanismes ne fonctionnent que contre les menaces découvertes et documentées.

  De même, les techniques de protection basées sur la réputation sont conçues pour intercepter des menaces connues. Même la technologie de sandbox d'exécution de fichiers, pourtant présentée comme une approche innovante de la sécurité, ne fournit pas les informations détaillées requises pour bloquer les attaques zero-day. Repousser les menaces avancées actuelles exige de nouvelles technologies entièrement conçues pour faire front à ce nouveau paysage.
- **Veiller à ce que les systèmes disposent des derniers correctifs.** L'équipe responsable de la sécurité doit appliquer les correctifs les plus récents et vérifier qu'il n'en manque aucun au sein de l'environnement. Il est évident que cette mesure ne protège pas en soi vos systèmes contre les attaques zero-day, mais il faut savoir que de nombreuses entreprises restent exposées à des vulnérabilités zero-day déjà corrigées par le simple fait qu'elles n'ont pas appliqué l'ensemble des correctifs à leurs systèmes.
- **Utiliser des systèmes d'exploitation et des applications qui prennent en charge les fonctionnalités de protection DEP et ASLR.** Comme expliqué précédemment, de plus en plus d'attaques zero-day contournent les fonctionnalités de distribution aléatoire de l'espace d'adressage (ASLR) et de prévention de l'exécution des données (DEP). Cette mesure ne règle donc pas tous les problèmes, mais le fait que vos systèmes d'exploitation et applications prennent en charge de telles fonctionnalités peut rendre bien plus complexe l'exploitation des vulnérabilités. Dans la mesure du possible, les entreprises doivent utiliser les dernières versions des systèmes d'exploitation, lesquelles intègrent habituellement les techniques les plus récentes de blocage des menaces.
- **Favoriser la coopération entre les acteurs du secteur de la sécurité.** Les attaques zero-day sont rapides. Ceux qui les traquent doivent l'être plus encore. Si le secteur de la sécurité veut identifier et contrer les exploits zero-day plus rapidement, il doit encourager une collaboration plus fréquente et plus transparente. C'est en partagent les informations et en sonnant rapidement l'alarme que la communauté de la sécurité parviendra à maîtriser les dommages — et participera à la sécurité de chacun par les efforts de tous.

25 Gartner, *Best Practices for Mitigating Advanced Persistent Threats*, janvier 2012

À propos de FireEye, Inc.

FireEye a développé une plate-forme de sécurité virtualisée et spécialisée qui offre aux entreprises privées et aux organismes publics du monde entier une protection en temps réel contre les cyberattaques de nouvelle génération. Plus sophistiquées que jamais, ces cyberattaques contournent sans aucune difficulté les défenses traditionnelles basées sur les signatures, telles que les pare-feux de nouvelle génération, les solutions IPS, les logiciels antivirus et les passerelles. La plate-forme FireEye assure une protection dynamique en temps réel contre les menaces sans utiliser de signatures et met ainsi les organisations à l'abri des attaques sur les principaux vecteurs à toutes les phases de leur cycle de vie. La plate-forme FireEye repose sur un moteur d'exécution virtuel et sur des informations dynamiques sur les menaces pour identifier et bloquer les cyberattaques en temps réel. FireEye compte plus de 1 900 clients dans plus de 60 pays, dont plus de 130 figurent au classement Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | france@FireEye.com | www.FireEye.com