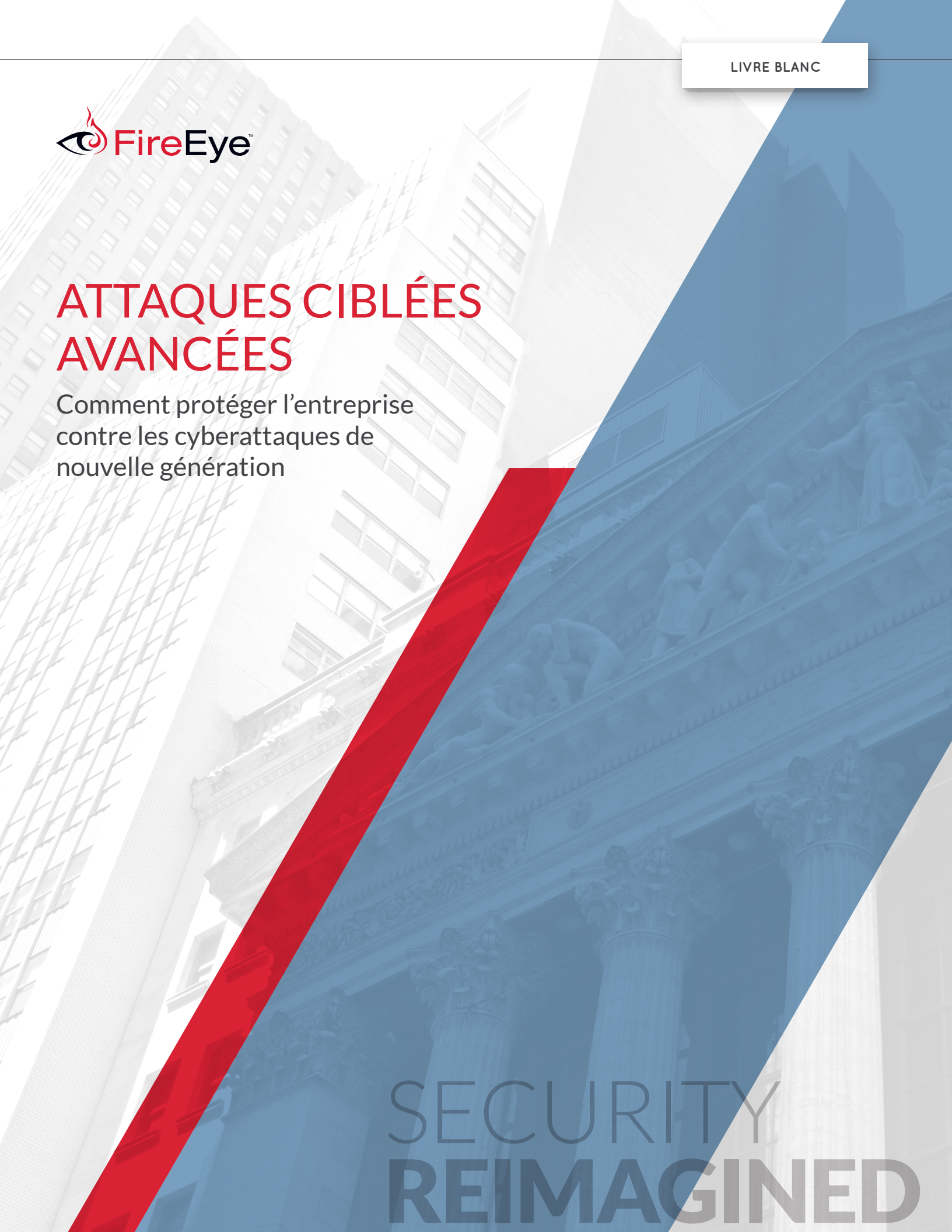
LIVRE BLANC

FireEye

ATTAQUES CIBLÉES AVANCÉES

Comment protéger l'entreprise contre les cyberattaques de nouvelle génération



SOMMAIRE

Résumé 3

Nature des menaces de nouvelle génération 4

Les cinq phases des attaques multivectorielles et multiphases 5

Le prix fort 7

Les mesures de sécurité traditionnelles dépassées 8

Les lacunes des défenses univectorielles traditionnelles 8

Colmater la brèche 10

Une sécurité de nouvelle génération pour bloquer les attaques avancées 11

Résumé

Le paysage des menaces a changé. Les cybercriminels et certains États cherchent par tous les moyens à mettre la main sur des données critiques, telles que des informations sur les transactions financières, des projets de conception, des données d'identification pour la connexion à des systèmes sensibles, ou encore des éléments de propriété intellectuelle. Or, les cyberattaques ont pris une longueur d'avance sur les technologies défensives utilisées de nos jours par la plupart des entreprises.

Les pare-feux de nouvelle génération, les systèmes de prévention des intrusions (IPS), les solutions antivirus et les passerelles de sécurité ne protègent pas efficacement contre les menaces de nouvelle génération. Si le montant total des dépenses en sécurité informatique devrait passer de 60 milliards de dollars en 2012 à 86 milliards en 2016[1], la quasi-totalité de ces investissements seront dévolus à des technologies obsolètes, basées sur les signatures. Pourtant, ces dernières bloquent seulement les menaces connues, mais pas les attaques dynamiques inconnues qui font rage de nos jours. C'est pourquoi plus de 95 %[2] des entreprises subissent la présence de logiciels malveillants dans leur réseau, en dépit des nombreuses couches de défenses traditionnelles qu'elles mettent généralement en place.

Les cybercriminels exploitent des vulnérabilités « zero-day », des kits d'outils de niveau professionnel et diverses techniques d'ingénierie sociale pour lancer des attaques ciblées avancées. Ces menaces à progression lente et insidieuse enchaînent plusieurs phases et recourent à divers canaux pour esquiver les défenses traditionnelles, afin d'identifier les systèmes vulnérables et les données sensibles. Une lutte efficace contre ces attaques exige par conséquent une stratégie plus élaborée que des signatures statiques et l'analyse heuristique comportementale rudimentaire.

Les mécanismes de défense traditionnels deviennent de plus en plus des points d'application de stratégie, plutôt que des protections robustes contre les intrusions informatiques. Ainsi, les filtres d'URL restent utiles pour appliquer des stratégies d'utilisation acceptable en termes de navigation Web des employés, mais ils ne sont plus efficaces pour bloquer les téléchargements dynamiques à l'insu de l'utilisateur (drive-by download). De même, les pare-feux de nouvelle génération ne font qu'offrir de nouvelles options de stratégie régissant les utilisateurs et les applications, ou encore consolider les protections traditionnelles basées sur les signatures. Ainsi, si ces nouveaux types de pare-feux peuvent regrouper antivirus et IPS classiques, ces technologies reposent sur les signatures et ne procurent aucune innovation ni aucun renforcement en matière de sécurisation des réseaux. Au bout du compte, l'intégration de ces mesures conventionnelles n'est guère plus efficace face aux menaces de nouvelle génération. En présence de menaces dynamiques, les protections traditionnelles que sont les pare-feux, les systèmes IPS, les solutions antivirus

« Il est généralement admis que les attaques avancées contournent nos contrôles de sécurité traditionnels basés sur les signatures et continuent à sévir sur nos systèmes sans être détectées pendant de longues périodes. La menace est bien réelle. Vos systèmes sont déjà compromis ; c'est juste que vous n'en êtes pas conscient. » ” – *Gartner, Inc., 2012*

[1] Gartner, « Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update », septembre 2012
[2] Données d'utilisateurs finaux de FireEye

FireEye

et antispam ou encore les passerelles de sécurité sont pratiquement impuissantes, laissant une brèche béante dans laquelle les cybercriminels peuvent s'engouffrer.

Les attaques actuelles recourent à des tactiques avancées, par exemple en combinant polymorphisme et personnalisation, afin d'échapper aux outils basés sur les signatures tout en restant pourtant suffisamment authentiques pour contourner les filtres antispam et même tromper les victimes désignées. À titre d'exemple, les attaques par harponnage (spearphishing) tirent parti d'informations glanées sur les sites de réseaux sociaux pour créer des messages électroniques personnalisés contenant des URL dynamiques malveillantes qui passent outre les filtres d'URL.

Pour reprendre l'avantage sur les attaques de nouvelle génération, les entreprises doivent se tourner vers des solutions qui sont, elles aussi, de nouvelle génération : proactives, sans signatures, agissant en temps réel. Grâce à une analyse continue du code suspect tout au long du cycle de vie des attaques et grâce au blocage des communications des logiciels malveillants sur les différents vecteurs de menaces, les protections de nouvelle génération sont à même de contrer les logiciels malveillants sophistiqués, les exploits « zero-day » ainsi que les menaces persistantes avancées, les empêchant ainsi de mettre en péril les données sensibles.

Nature des menaces de nouvelle génération

En quelques années à peine, les attaques ont changé de forme et de fonction et gagné en sophistication. Les menaces de nouvelle génération conjuguent des logiciels malveillants de masse, conçus pour infecter un grand nombre de systèmes, et des logiciels malveillants « zero-day » élaborés, destinés à contaminer des systèmes ciblés. Elles associent en outre plusieurs vecteurs d'attaques, dont le Web, la messagerie électronique et les applications. Enfin, les attaques actuelles visent à mettre la main sur des données critiques (informations financières sensibles, éléments de propriété intellectuelle, données d'authentification, informations privilégiées). Bien souvent, elles sont orchestrées en plusieurs phases pour infiltrer les réseaux, se propager et enfin extraire lesdites données.

Des infections courantes par Zeus/Zbot jusqu'aux offensives ciblées de Stuxnet, les cyberattaques ont démontré toute leur efficacité lorsqu'il s'agit de voler des données sensibles, de causer des pertes financières ou de porter atteinte à la réputation des entreprises. Les cybercriminels brassent des milliards de dollars en transactions sur Internet. Les États emploient des logiciels malveillants dans le cadre du cyberespionnage pour surveiller les activistes opposants et perturber le fonctionnement des infrastructures critiques de leurs ennemis. Les enjeux sont importants. C'est pourquoi le développement des exploits « zero-day » et autres activités criminelles sont financés généreusement. Ce soutien financier a permis l'émergence d'un écosystème clandestin actif, pratiquant l'échange et la vente d'accès aux systèmes de certains des réseaux les plus sensibles au monde. Ainsi, des organismes publics et des multinationales ont été mis à mal par des cyberopérations telles que Flame, opération Aurora et Nitro, combinant des tactiques de menaces persistantes avancées, des campagnes de harponnage et des logiciels malveillants sophistiqués.

« Les entreprises sont confrontées à des menaces en perpétuelle évolution, contre lesquelles elles sont mal préparées. » –*Gartner, « Best Practices for Mitigating Advanced Persistent Threats », janvier 2012*

Toutes les organisations de la « chaîne logistique » de l'information sont exposées aux attaques. Le vol d'algorithmes d'authentification à deux niveaux de RSA (une division d'EMC) perpétré en mars 2011, par exemple, illustre bien la nature stratégique de ces attaques. Les éléments de propriété intellectuelle dérobés à RSA étaient « susceptibles d'être utilisés pour réduire l'efficacité d'une implémentation actuelle d'authentification à deux niveaux dans le cadre d'une attaque plus étendue[3] », permettant aux criminels d'infiltrer des entreprises du monde entier.

« Les pirates se servant des menaces persistantes avancées ont des motivations plus fortes. Ils sont plus compétents, mieux financés et plus patients. Ils sont enclins à tenter plusieurs voies d'attaque et leurs chances de réussite sont beaucoup plus grandes[4]. »

En avril 2012, VMware (une filiale d'EMC) a confirmé qu'un pirate informatique avait distribué publiquement une partie du code source de VMware datant de 2003 et 2004. Alors que les centres de données sont toujours plus nombreux à utiliser la virtualisation, « une étude menée par des chercheurs de l'université de Princeton en 2013 a identifié près de 100 vulnérabilités combinées dans des hyperviseurs de virtualisation à code source libre très courants, Xen et KVM. Plus d'un tiers des vulnérabilités de Xen et près de la moitié des vulnérabilités de KVM peuvent permettre aux pirates d'accéder au système hôte[5]. » Ce ne sont là que deux exemples d'attaques ciblées avancées qui convoitent des éléments de propriété intellectuelle pouvant ensuite être exploités dans le cadre d'autres attaques associées aux menaces persistantes avancées.

Les cinq phases des attaques multivectorielles et multiphases

Les menaces de nouvelle génération sont complexes : elles exploitent plusieurs vecteurs d'attaques pour maximiser leurs chances de franchir les protections réseau. Les attaques multivectorielles sont généralement perpétrées via le Web ou la messagerie électronique. Elles exploitent les vulnérabilités des applications ou des systèmes d'exploitation, et l'incapacité des mécanismes conventionnels de protection du réseau à offrir une défense unifiée.

En plus d'utiliser différents vecteurs, les attaques ciblées avancées opèrent en plusieurs phases pour s'infiltrer dans un réseau et en extraire les informations de valeur. Les risques de détection s'en trouvent dès lors nettement réduits. Les cinq phases du cycle de vie d'une attaque sont les suivantes :

Phase 1: **exploitation du système.** Lors de la première phase, le système est infecté à l'insu de l'utilisateur alors que celui-ci visite un site (drive-by attack). Il s'agit souvent d'une attaque combinée transmise via le Web ou un message électronique contenant une URL malveillante.

Phase 2: **téléchargement de charges actives exécutables malveillantes et établissement d'un contrôle à long terme.** Un exploit unique engendre des dizaines d'infections sur un même système. Une fois l'exploitation réussie, d'autres exécutables malveillants (enregistreurs de frappe, chevaux de Troie de type porte dérobée (backdoor), craqueurs de mots de passe et extracteurs de fichiers) sont ensuite téléchargés. Les criminels disposent ainsi de mécanismes de contrôle à long terme sur le système.

Phase 3: **rappel effectué par le logiciel malveillant.** Dès que le logiciel malveillant est installé, l'auteur d'attaque a passé la première étape de l'établissement d'un point de contrôle à l'intérieur des dispositifs de défense de l'entreprise. Une fois en place, le logiciel malveillant rappelle les serveurs du cybercriminel

[3] PC World, « RSA Warns SecureID Customers After Company is Hacked », mars 2011
[4] Bruce Schneier, « Advanced Persistent Threat (APT) », novembre 2011
[5] Diego Perez-Botero et al., « Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers », mai 2013

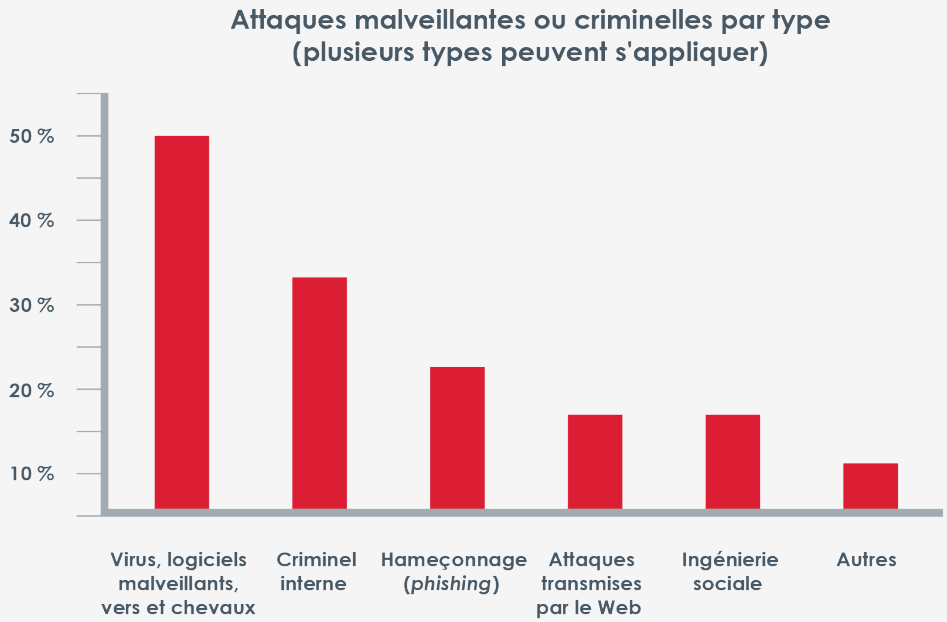
« Un auteur d'attaque qui est parvenu à compromettre l'ordinateur d'un titulaire de compte peut contrôler tous les aspects de l'environnement que voit la victime, car cet escroc peut ensuite intercepter, supprimer, modifier ou réacheminer toutes les communications à destination et en provenance de la machine infe ctée[6]. »

afin d'obtenir des instructions complémentaires. Il peut également se répliquer et se dissimuler de façon à échapper aux analyses, désactiver les analyseurs antivirus, réinstaller certains de ses composants manquants après un nettoyage ou encore rester inactif pendant des jours voire des semaines. Dans la mesure où le logiciel malveillant utilise des rappels émanant du réseau approuvé, ses communications sont autorisées à traverser le pare-feu et à pénétrer toutes les couches du réseau.

Phase 4: **exfiltration des données.** Les données collectées sur les serveurs infectés sont transférées secrètement via des fichiers chiffrés sur un protocole couramment autorisé, comme FTP ou HTTP, à un serveur externe compromis contrôlé par le criminel.

Phase 5: **propagation transversale du logiciel malveillant** Le criminel s'efforce de dépasser le stade du seul système compromis et de s'assurer un contrôle à long terme au sein du réseau. Le logiciel malveillant avancé recherche les lecteurs mappés sur les ordinateurs de bureau et ordinateurs portables infectés, pour ensuite se propager de manière transversale et plus en profondeur dans les partages de fichiers réseau. Il effectue une reconnaissance : il cartographie l'infrastructure réseau, détermine les principales ressources et fait une percée dans le réseau en s'infiltrant sur les serveurs cibles.

Figure 1— Les attaques malveillantes sont la principale cause de la hausse du pourcentage des compromissions de données[7].



[6] Krebs on Security, « Sold a Lemon in Online Banking », février 2011
[7] Ponemon Institute, « 2011 Cost of Data Breach Study », mars 2012

« RSA a été piraté durant la première quinzaine de mars lorsqu'un employé s'est laissé piéger par unmessage de harponnage et a ouvert une feuille de calcul infectée. Dès l'ouverture de la pièce jointe, une menace persistante avancée nommée Poison Ivy (un cheval de Troie de type « porte dérobée ») a été installé. À partir de là, les auteurs de l'attaque ont eu les coudées franches dans le réseau interne de RSA, ce qui a abouti à la divulgation des données associées aux authentificateurs à deux niveaux de la société[8]. »

Le prix fort

Les menaces informatiques occasionnent aux entreprises des coûts opérationnels élevés. Une étude menée en 2012 par InformationWeek a révélé qu'en 2011, plus d'un quart des entreprises interrogées ont consacré au moins 10 % et jusqu'à plus de 25 % de leur budget informatique annuel à la sécurité[9]. « L'hameçonnage (phishing) et les logiciels malveillants forment une équipe de choc. D'après notre étude [InformationWeek], les logiciels malveillants restent la première cause des compromissions subies par nos répondants[10]. »

Außerdem handeln Cyberkriminelle nach dem Grundsatz „teile und herrsche", da auch herkömmliche Sicherheitsmechanismen und IT-Abteilungen stark unterteilt sind. Traditionelle Abwehrmaßnahmen sind meist so konzipiert, dass jeder Angriffsvektor als separater Pfad und jede Phase als unabhängiges Ereignis betrachtet wird. Sinnvoller ist es jedoch, die verschiedenen Phasen und Vektoren als zusammenhängende Serie von Cybervorfällen zu analysieren. Eine Drive-by-Webinfektion, die Technologie- und Anwendungssilos in IT-Abteilungen ausnutzt, wird häufig als Zufallsereignis abgetan – verursacht durch einen unvorsichtigen Anwender, der eine dubiose Website besucht hat. Sie kann nicht zur ursprünglichen Spear-Phishing-Mail zurückverfolgt werden, die Ausgangspunkt eines mehrstufigen, weitaus verheerenderen Angriffs ist. So gelingt es Cyberkriminellen schließlich, über das Web und E-Mails an die gewünschten Daten zu gelangen und so lange unbemerkt zu bleiben, bis für das Opfer jede Hilfe zu spät kommt.

D'après l'étude 2013 Cost of a Data Breach réalisée par le Ponemon Institute, le coût des compromissions de données résultant d'attaques malveillantes ou criminelles est invariablement supérieur au coût résultant de problèmes de fonctionnement des systèmes ou d'erreurs humaines[11]. En fait, l'étude révèle que les attaques malveillantes ou criminelles constituent les compromissions de données les plus coûteuses dans les neuf pays auxquels elle s'est intéressée[12]. Les attaques malveillantes engendrent des coûts plus importants parce qu'elles sont plus difficiles à

« Les mécanismes de défense actuels sont dépassés [...] Les initiatives menées contre les logicielsmalveillants son t devenues insuffisantes. » – *Forrester Research, « Malware and Trojans and Bots, Oh My! », février 2011*

[8] Sebastian Anthony, « Security firm RSA attacked using Excel-Flash one-two sucker punch », avril 2011
[9] InformationWeek, « 2012 Strategic Security Survey », mai 2012
[10] Ibid.
[11] Ponemon Institute, « 2013 Cost of Data Breach Study - United States, Global Analysis », mai 2013
[12] Ibid.

détecter et nécessitent une procédure d'enquête plus approfondie, sans compter qu'il est plus compliqué de les maîtriser et de corriger leurs effets[13].

Les mesures de sécurité traditionnelles dépassées

Pour s'infiltrer dans un réseau et en extraire des informations de valeur, les menaces de nouvelle génération mettent en œuvre une succession de phases et plusieurs vecteurs d'attaques. En effet, en combinant des vecteurs tels que le Web, les messages électroniques et les fichiers, organisés dans une attaque articulée en plusieurs étapes, les cybercriminels échappent beaucoup plus facilement à la détection. Les pare-feux, systèmes IPS, antivirus et passerelles Web actuels ont peu de chances d'arrêter les pirates qui recourent à des logiciels « zero-day » à usage unique et à des tactiques associées aux menaces persistantes avancées.

Au-delà de tous les avantages technologiques des exploits, les cybercriminels savent également qu'ils doivent diviser pour régner. En d'autres mots, ils doivent tirer parti des faiblesses inhérentes des mesures de sécurité traditionnelles et des départements informatiques en matière d'organisation. Les outils de sécurisation conventionnels sont généralement conçus pour inspecter chaque vecteur d'attaque en tant que point d'entrée distinct, et chaque phase comme un événement indépendant, plutôt que d'observer et d'analyser ces phases et vecteurs comme une série orchestrée d'incidents informatiques. Par ailleurs, profitant du cloisonnement entre fonctions technologiques et fonctions métiers au sein des départements informatiques, une infection contractée lors de la consultation d'un site Web (drive-by) ressemble à un événement fortuit, imputé à la visite irréfléchie d'un site douteux par un utilisateur. Il est impossible de remonter au message de harponnage initial qui a servi à duper l'utilisateur et à lancer l'attaque ciblée avancée articulée en plusieurs phases. Dès lors, après plusieurs étapes d'attaques via le Web et la messagerie électronique, les cybercriminels sont en mesure d'exfiltrer des données à l'insu des responsables de la sécurité, qui ne se rendent compte de la compromission que bien trop tard.

Les lacunes des défenses univectorielles traditionnelles

- **Pare-feux —** Les pare-feux autorisent le trafic Web HTTP. Les pare-feux de nouvelle génération ajoutent de nouvelles couches de règles de stratégie, basées sur les utilisateurs et les applications. Ils consolident les protections traditionnelles, telles que les antivirus et les systèmes IPS, sans toutefois ajouter de protection dynamique capable de détecter le comportement ou le contenu des menaces de nouvelle génération..

- **Systèmes de prévention des intrusions (IPS) —** Les signatures, l'inspection des paquets, l'analyse DNS et l'analyse heuristique ne détectent aucun élément inhabituel dans un exploit « zero-day », en particulier si le code est soigneusement camouflé ou distribué par phases.

- **Protection antivirus et filtrage Web des logiciels malveillants —** Les filtres Web et antivirus laissent passer les logiciels malveillants, dans la mesure où tant ceux-ci que les vulnérabilités qu'ils exploitent sont inconnus (« zero-day ») et où le site Web a bonne réputation. Si l'on considère le très grand nombre de vulnérabilités des plug-ins de navigateur et les combinaisons exponentielles entre ces navigateurs et les systèmes d'exploitation, il n'est pas étonnant que les éditeurs d'antivirus éprouvent beaucoup de difficultés à tenir le cap.

[13] Ponemon Institute, « The Post Breach Boom », février 2013

- **Filtrage du spam —** Les sites de hameçonnage falsifiés utilisent des URL et des domaines dynamiques, si bien que les listes noires sont à la traîne par rapport aux activités criminelles. Il faut plus de 26 heures pour fermer un site de phishing ordinaire[14].

Le code malveillant peut également être diffusé au travers d'ordinateurs portables, de périphériques USB ou de services de partage de fichiers dans le cloud, afin d'infecter un ordinateur et de se propager de manière transversale dans le réseau lorsque celui-ci s'y connecte. Il arrive fréquemment que des systèmes mobiles manquent des correctifs et des mises à jour de fichiers DAT (signatures), demeurant vulnérables aux exploits connus et inconnus. En général, même les ordinateurs correctement mis à jour peuvent être infectés à l'aide d'exploits « zero-day » et de techniques d'ingénierie sociale, particulièrement lorsque le système n'est pas connecté au réseau de l'entreprise.

Une fois en place, les logiciels malveillants peuvent se répliquer, chaque instance bénéficiant de modifications subtiles qui la font apparaître comme unique, puis se dissimuler pour éviter les analyses. Certains désactivent les analyseurs antivirus, d'autres se réinstallent après un nettoyage, et d'autres encore restent inactifs pendant des jours voire des semaines.

Finalement, le code recontacte le site d'origine du criminel pour obtenir des instructions supplémentaires ou une nouvelle charge active, ou pour lui transmettre des informations de connexion, des données financières et d'autres données précieuses. Un grand nombre d'hôtes compromis offrent au criminel une base privilégiée pour de nouvelles explorations ou l'enrôlement de nouvelles cibles dans son réseau de robots (botnet).

La majorité des entreprises n'analysent pas le trafic sortant pour tenter d'identifier ces transmissions et destinations malveillantes. Et

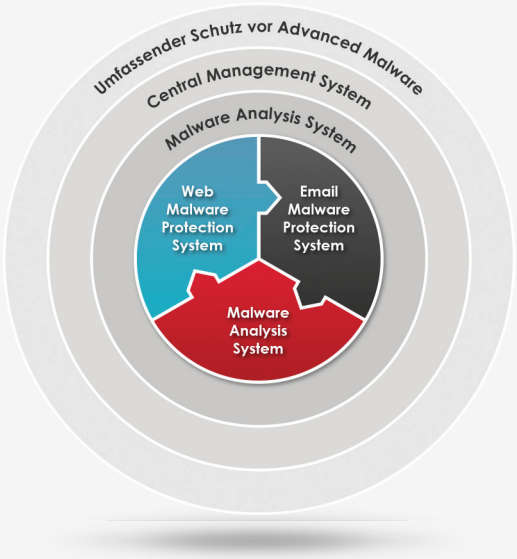


Figure 2: — Protection complète contre les attaques ciblées avancées

[14] Anti-Phishing Working Group, « Global Phishing Survey 2H2012: Trends and Domain Name Use », avril 2013.

celles qui surveillent les transmissions sortantes recourent à des outils qui recherchent les données réglementées et les adresses reconnues comme dangereuses.

- **Filtrage de contenu Web** — La plupart des mécanismes de filtrage en sortie bloquent le contenu pour adultes ou les sites de divertissement qui nuisent à la productivité. Moins d'un quart des entreprises empêchent l'accès aux sites de réseaux sociaux[15]. Qui plus est, les URL dynamiques, le piratage de sites Web légitimes et les adresses temporaires, actives pendant de brèves périodes seulement, rendent obsolètes les listes noires d'URL statiques.

- **Prévention des fuites de données** — Les outils de prévention des fuites de données (DLP, Data Loss Prevention) ont été principalement conçus pour contrôler les informations d'identification personnelle — des chaînes telles que les numéros de sécurité sociale, les numéros de licence ou les données médicales. Leur efficacité dépend étroitement de celle de leurs règles. La plupart d'entre eux n'offrent pas la souplesse et la granularité nécessaires pour détecter l'exfiltration d'informations d'identification ou d'éléments de propriété intellectuelle. Le chiffrement des canaux de rappel permet par ailleurs aux données de s'échapper en toute discrétion. Cette approche statique ne cadre pas avec la nature dynamique des menaces de nouvelle génération.

Colmater la brèche

Les failles dans la protection et la sophistication accrue des cybercriminels exigent une nouvelle catégorie d'outils de protection adaptés à la résilience, à la capacité de dissimulation et à la complexité des menaces de nouvelle génération. C'est pour cette raison que les entreprises exigeantes en matière de sécurité choisissent FireEye® pour son offre de protection de pointe, contre les menaces actuelles qui associent plusieurs vecteurs et plusieurs phases de mise en œuvre pour contourner de façon systématique les défenses traditionnelles. La plate-forme FireEye complète les pare-feux traditionnels et de nouvelle génération, les systèmes IPS, les antivirus et les passerelles, dont les signatures et l'analyse heuristique ne sont pas en mesure de refouler ces menaces d'un nouveau genre.

La plate-forme FireEye a été conçue pour assurer une protection contre les menaces véhiculées par le Web et la messagerie électronique ainsi que contre les logiciels malveillants résidant sur les partages de fichiers. Chacune des appliances de sécurité de FireEye inclut le moteur FireEye Multi-Vector Virtual Execution™ (MVX), qui exécute une analyse de pointe sans signatures au moyen de machines virtuelles spécialisées brevetées. La plate-forme FireEye effectue une analyse intégrale des attaques avancées, phase par phase, depuis l'exploitation du système jusqu'à l'exfiltration des données, afin d'arrêter net les menaces persistantes avancées.

Fonctionnant en mode en ligne ou hors bande, la plate-forme FireEye exécute une analyse en temps réel automatisée du trafic Web suspect, des pièces jointes aux messages électroniques et des fichiers sur les serveurs de partage de fichiers réseau. Tout élément douteux est traité par le moteur FireEye MVX où les environnements propriétaires entièrement consacrés aux tests confirment de façon irréfutable le caractère malveillant et les activités de l'auteur d'attaque, en se concentrant sur les menaces réelles tout en évitant les faux positifs et les faux négatifs.

[15] Sophos, « Security threat report 2011 », janvier 2011

Dès lors qu'un code au comportement anormal est marqué, ses ports de communication, ses adresses IP et ses protocoles sont bloqués de façon à empêcher les transmissions sortantes. Les analystes peuvent utiliser l'empreinte numérique du code malveillant pour identifier les systèmes compromis, leur appliquer les mesures correctives nécessaires et empêcher la propagation de l'infection. Les experts en investigations numériques peuvent étudier les fichiers un à un au moyen de tests hors ligne automatisés afin de vérifier la nature malveillante du code et de disséquer celui-ci. Le cloud FireEye Dynamic Threat Intelligence™ permet de tenir tous les intervenants informés des dernières innovations du cybercrime ainsi que des destinations de rappel identifiées par FireEye Labs et d'autres sites de nos clients.

Ces appliances prêtes à l'emploi pour la sécurisation de l'environnement Web, de la messagerie électronique et des partages de fichiers sont déployées en moins de 60 minutes, sans qu'il soit nécessaire d'écrire ou d'optimiser des règles. Et comparé au coût d'une compromission de données, le prix d'achat de départ est plus que modéré.

Une sécurité de nouvelle génération pour bloquer les attaques avancées

La plate-forme FireEye colmate les brèches dans la sécurité des réseaux qui existent dans pratiquement toutes les entreprises. Avec son moteur FireEye MVX spécialisé, la plate-forme FireEye assure une sécurisation dynamique qui met en échec les attaques auparavant inconnues, tout en exécutant un code spécifique conçu pour détecter les menaces « zero- day ». Les entreprises peuvent désormais disposer de véritables protections en temps réel, à l'entrée et en sortie, contre les attaques ciblées avancées.

Quelle que soit leur taille, les entreprises peuvent renforcer leurs mécanismes de défense traditionnels à l'aide d'un système de prévention des menaces de nouvelle génération qui reconnaît la nature et l'intention de ces attaques ciblées sophistiquées, en particulier celles qui possèdent les caractéristiques des menaces persistantes avancées. Demandez sans tarder une évaluation de la sécurité de votre réseau par FireEye : vous constaterez par vous-même que de nombreuses menaces passent outre les mesures de protection en place.

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 (environnement Web, messagerie électronique et fichiers) à tous 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 1 000 clients dans plus de 40 pays, dont plus d'un tiers figure au classement Fortune 100.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | france@fireeye.com | **www.fireeye.com**

FireEye