Rapport

Prévisions 2014 en matière de menaces – McAfee® Labs

Sommaire

1. Les logiciels malveillants sur mobiles seront des facteurs de croissance, tant en ce qui concerne l'innovation technique que le volume des attaques sur le « marché » global des malware en 2014.

En 2013, le taux de croissance des nouveaux logiciels malveillants sur mobiles détectés (qui ciblent presque exclusivement la plate-forme Android) a été nettement supérieur au taux d'apparition de malware visant des PC. Au cours des deux derniers trimestres, la croissance des nouveaux logiciels malveillants sur PC est demeurée quasiment stationnaire, tandis que les apparitions de nouveaux échantillons visant Android ont enregistré une hausse de 33 %.

McAfee Labs prévoit la poursuite de cette tendance en 2014, mais le taux de croissance des nouvelles attaques sur mobiles ne sera pas le seul fait saillant. Nous nous attendons également à voir apparaître des types d'attaques totalement nouveaux qui cibleront Android. Il est fort probable que nous assisterons aux premières vraies attaques par logiciels de demande de rançon (*ransomware*) visant les terminaux mobiles. Les maîtres chanteurs chiffrent des données critiques sur l'équipement et les gardent en otage, les « libérant » contre paiement d'une rançon en monnaie conventionnelle ou virtuelle (comme Bitcoin). Nous prévoyons l'apparition d'autres nouvelles tactiques dans le domaine des mobiles, notamment des attaques contre les vulnérabilités dans les communications en champ proche (NFC) que l'on trouve maintenant sur un grand nombre de terminaux, et des attaques entraînant la corruption d'applications légitimes dans le but d'exfiltrer des données en échappant à la détection.

Les attaques à l'encontre des terminaux mobiles cibleront également les infrastructures d'entreprise. Elles seront favorisées par le phénomène désormais universel d'utilisation d'équipements personnels sur le lieu de travail, associé à l'immaturité relative de la technologie de sécurisation de l'environnement mobile. Les utilisateurs qui téléchargent involontairement des logiciels malveillants introduiront à leur tour à l'intérieur du périmètre de l'entreprise des logiciels malveillants conçus pour exfiltrer des données confidentielles. L'utilisation des terminaux personnels sur le lieu de travail est vouée à perdurer, de sorte que les entreprises doivent mettre en place des stratégies et des solutions complètes de gestion des équipements si elles ne veulent pas devenir victimes de la cybercriminalité.

2. Les monnaies virtuelles encourageront des attaques par logiciels de demande de rançon de plus en plus virulentes à travers le monde.

Les attaques par ransomware qui chiffrent les données sur les terminaux de leurs victimes ne sont pas une nouveauté, loin de là. Cependant, ces attaques ont toujours été vulnérables aux actions des forces de l'ordre à l'encontre des services de traitement des paiements qu'utilisent les cybercriminels.

Boîte de dialogue CryptoLocker

Bien que l'utilisation croissante des monnaies virtuelles favorise l'activité économique, ces dernières offrent également aux cybercriminels l'infrastructure de paiement idéale, anonyme et dérégulée dont ils ont besoin pour recevoir l'argent de leurs victimes. Nous pensons que des attaques telles que CryptoLocker proliféreront aussi longtemps qu'elles resteront (très) profitables. De même, nous nous attendons à voir apparaître de nouvelles attaques par ransomware visant les entreprises et s'efforçant de chiffrer des données d'entreprise critiques.

La bonne nouvelle, tant pour les particuliers que les entreprises, est que bien que la charge active des logiciels de demande de rançon soit unique, leurs mécanismes de distribution (spam, téléchargements à l'insu de l'utilisateur et applications infectées) ne le sont pas. Ainsi, les particuliers et les entreprises qui conservent leurs systèmes antimalware à jour (tant au niveau des postes clients que du réseau) seront relativement épargnés par cette menace. Un système de sauvegarde performant, qu'il soit personnel ou déployé par l'entreprise, protégera aussi contre la plupart des conséquences du ransomware.

3. Dans le monde sans merci de la cybercriminalité et de la cyberguerre, les gangs de malfaiteurs et les Etats lanceront de nouvelles attaques furtives qui seront plus difficiles que jamais à identifier et à bloquer.

Les solutions de sécurité ont vu leur sophistication croître, à l'instar des efforts consentis par la communauté cybercriminelle pour contourner ces défenses. Les attaques mettant en œuvre des techniques de contournement avancées représentent le nouveau front dans la guerre pour la sécurité des données d'entreprise. L'une des techniques déjà très utilisée, et qui connaîtra une large adoption par les cybercriminels en 2014, est le recours à des attaques reconnaissant les environnements sandbox : celles-ci ne se déploient complètement que lorsqu'elles détectent qu'elles sont exécutées directement sur un terminal non protégé.

D'autres technologies d'attaques courues vont elles aussi être peaufinées et se propager en 2014. C'est notamment le cas des attaques de programmation orientée retour qui provoquent des comportements malveillants de la part d'applications pourtant légitimes ; des logiciels malveillants à suppression automatique qui couvrent leurs traces après avoir compromis une cible ; et des attaques avancées sur des systèmes de contrôle industriel dédiés qui risquent d'endommager des infrastructures publiques et privées.

Les attaques à motif politique vont continuer leur progression, en particulier aux alentours des Jeux olympiques d'hiver 2014 de Sotchi (en février) et de la Coupe du monde de la FIFA au Brésil (en juin-juillet). Les cyberactivistes profiteront eux aussi de ces événements pour promouvoir leurs idées.

Les équipes informatiques des entreprises devront faire face à ce nouveau type de tactiques, et s'assurer que leurs défenses ne dépendent pas complètement de mesures de sécurité facilement contournables par les gangs internationaux de cybercriminels.

4. Les attaques sur médias sociaux vont devenir omniprésentes d'ici la fin de 2014.

Les attaques sur médias sociaux tirent parti des vastes bases d'utilisateurs de Facebook, Twitter, LinkedIn, Instagram, etc. Un grand nombre de ces attaques imiteront les tactiques des logiciels malveillants plus anciens tels que Koobface et utiliseront simplement les plates-formes de médias sociaux comme mécanismes de propagation. En 2014, toutefois, nous nous attendons à observer des attaques qui utilisent les fonctionnalités spécifiques des plates-formes de médias sociaux pour transmettre des données sur les contacts utilisateur, la localisation géographique ou les activités professionnelles qui peuvent ensuite servir à cibler des publicités ou à perpétrer des délits dans le monde réel ou virtuel.

L'une des attaques de ce type les plus courantes consiste simplement à voler les données d'authentification des utilisateurs, pour ensuite les utiliser pour soutirer des données personnelles à des « amis » et collègues qui ne se doutent de rien. Le réseau de robots (*botnet*) Pony[1], qui a volé plus de deux millions de mots de passe d'utilisateurs Facebook, Google, Yahoo et autres, n'est vraisemblablement que le sommet de l'iceberg. Facebook lui-même estime que 50 à 100 millions de ses « utilisateurs actifs mensuels » sont des comptes dupliqués et que jusqu'à 14 millions d'entre eux sont considérés comme « indésirables ». Selon une étude Stratecast récente, 22 % des utilisateurs de médias sociaux ont connu un incident lié à la sécurité[2].

Les entreprises publiques et privées exploiteront aussi les plates-formes de médias sociaux pour mener des « attaques de reconnaissance » contre leurs rivaux et concurrents, soit directement soit par l'intermédiaire de tiers. Des leaders en vue tant du secteur public que du secteur privé ont été ciblés par de telles attaques en 2013. Il faut s'attendre à ce que leur fréquence et leur portée augmentent en 2014.

D'après nos prévisions, une autre forme d'attaques sur médias sociaux sera déployée en masse en 2014 : les attaques recourant à de « fausses enseignes », autrement dit des messages prétextant émaner d'une entreprise réputée et incitant les utilisateurs à révéler des informations personnelles ou des données d'authentification. L'une des attaques les plus courantes prendra la forme d'une demande « urgente » invitant l'utilisateur à réinitialiser son mot de passe. Le pirate détenant désormais le nom d'utilisateur et le mot de passe de la victime, il pourra utiliser le compte de cette dernière à son insu pour rassembler des informations personnelles sur l'utilisateur et ses contacts.

La prévention de ces deux types particuliers d'attaques exigera une vigilance accrue de la part des utilisateurs, des stratégies d'entreprise rigoureuses et des solutions efficaces pour s'assurer que l'utilisation des médias sociaux par les employés n'entraîne pas des compromissions de données importantes.

5. Les nouvelles attaques de PC et de serveurs cibleront des vulnérabilités de niveaux supérieurs et inférieurs au système d'exploitation.

Alors que de nombreuses organisations cybercriminelles se focalisent sur les terminaux mobiles, d'autres vont continuer à cibler les plates-formes PC et serveurs. Les nouvelles attaques que nous connaîtrons en 2014, cependant, ne viseront pas seulement le système d'exploitation mais également des vulnérabilités situées aux niveaux inférieurs et supérieurs à celui-ci.

En 2014, un grand nombre des attaques sur PC exploiteront des vulnérabilités du HTML5, qui assure aux sites web un grand dynamisme grâce à des interactions, à des possibilités de personnalisation et à des fonctions riches pour les programmeurs. Toutefois, le HTML5 expose malheureusement un certain nombre de nouvelles surfaces d'attaque. A l'aide de ce langage, les chercheurs ont déjà montré comment utiliser l'historique de navigation d'un utilisateur pour mieux cibler les publicités. De plus, comme de nombreuses applications HTML5 sont conçues pour les terminaux mobiles, tout porte à croire que des attaques contourneront le sandbox de navigateur et donneront aux pirates un accès direct au terminal et à ses services. De nombreuses entreprises vont également développer des applications d'entreprise au moyen du langage HTML5. Pour prévenir l'exfiltration des données utilisées par ces applications, ces nouveaux systèmes devront intégrer des fonctions de sécurité dès la conception.

Les cybercriminels cibleront de plus en plus des vulnérabilités dans les niveaux inférieurs au système d'exploitation, dans la pile de stockage et même le BIOS. Dans l'environnement d'entreprise, contrer ces attaques de bas niveau nécessitera de déployer des mesures de sécurité assistées par le matériel, qui fonctionnent elles aussi au-delà du système d'exploitation.

6. Le paysage des menaces en perpétuelle évolution imposera l'adoption d'instruments d'analyse de données de sécurité de masse afin de répondre aux exigences en matière de détection et de performance.

Historiquement, la plupart des solutions de sécurisation des informations dépendaient de l'identification des charges actives malveillantes (listes de blocage/noires) ou du suivi des applications valides connues (listes d'autorisation/blanches). Le défi actuel auquel sont confrontés les responsables de la sécurité des informations concerne l'identification et le traitement approprié des charges actives dites « grises ». Pour ce faire, ils doivent appliquer plusieurs technologies de sécurité fonctionnant de concert avec des services robustes d'évaluation de la réputation/des menaces.

Les services d'évaluation de la réputation/des menaces ont déjà prouvé leur valeur en termes de détection de logiciels malveillants, de sites web malveillants, de spam et d'attaques réseau. En 2014, les fournisseurs de solutions de sécurité ajouteront de nouveaux services de réputation et outils d'analyse qui leur permettront, à eux et à leurs utilisateurs, d'identifier les menaces furtives et persistantes avancées plus rapidement et plus précisément qu'à l'heure actuelle. Les outils d'analyse des grands volumes de données permettront aux responsables de la sécurité informatique d'identifier les attaques sophistiquées mettant en œuvre des techniques de contournement avancées ainsi que les menaces persistantes avancées qui peuvent perturber les processus d'entreprise stratégiques.

7. Le déploiement d'applications d'entreprise dans le cloud créera de nouvelles surfaces d'attaque qui seront exploitées par des cybercriminels.

Willie Sutton, à qui l'on attribue une centaine de braquages au début du XX^{e} siècle, aurait répondu à la question de savoir pourquoi il cambriolait des banques : « parce que c'est là que se trouve l'argent[3] ». Il en va de même pour les gangs de cybercriminels du XXI^{e} siècle : ils s'en prennent aux applications de cloud et aux magasins de données parce que c'est là que se trouvent les données, ou qu'elles se trouveront bientôt. Ces attaques pourraient exploiter des applications d'entreprise qui n'ont pas encore été évaluées par l'équipe informatique pour s'assurer de leur conformité aux stratégies de sécurité de l'entreprise. Selon un rapport récent, plus de 80 % des utilisateurs en entreprise emploient des applications de cloud à l'insu ou sans le support de l'équipe informatique de l'entreprise[4].

Bien que les applications de cloud présentent clairement des avantages fonctionnels et économiques importants, elles exposent cependant une série inédite de surfaces d'attaque — par exemple, les hyperviseurs omniprésents dans tous les centres de données, l'infrastructure de communication multilocataire implicite dans les services de cloud et l'infrastructure de gestion utilisée pour activer et surveiller des services de cloud à grande échelle. Pour les responsables de la sécurité en entreprise, le problème qui se pose est que, lorsqu'une application d'entreprise migre vers le cloud, l'entreprise perd la visibilité et le contrôle sur le profil de sécurité.

Cette perte de contrôle direct sur le périmètre de sécurité de l'entreprise fait peser une pression terrible sur les administrateurs et les responsables de la sécurité. Ils doivent en effet veiller à ce que l'accord conclu avec le fournisseur des services de cloud, ainsi que les procédures de fonctionnement connexes garantissent que des mesures de sécurité sont en place et constamment actualisées, pour répondre aux exigences d'un paysage des menaces en perpétuelle évolution. Les grandes entreprises ont sans doute suffisamment de poids pour imposer aux fournisseurs de services de cloud de mettre en place des mesures de sécurité en accord avec le profil de sécurité de l'entreprise. Les petits consommateurs de services de cloud, cependant, n'ont pas une telle influence. Ils doivent donc étudier très attentivement le contrat du fournisseur, souvent ambigu, en matière de sécurité et de propriété des données. Les nouveaux services de cloud pourraient par ailleurs exposer de nouvelles surfaces d'attaque le temps d'atteindre le niveau de maturité requis, incluant l'instrumentation et les contre-mesures, pour assurer la sécurité des données qu'ils doivent protéger.

Les auteurs

Ce rapport a été préparé et rédigé par Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky et Chong Xu.

A propos de McAfee Labs

McAfee Labs est la principale source d'informations au monde en matière de recherche sur les menaces, de renseignements détaillés sur les menaces et de réflexion innovante sur la cybersécurité. Forte de 500 chercheurs, son équipe rassemble des données provenant de millions de sondes et des principaux vecteurs de menaces : fichiers, Web, messagerie et réseau. Elle exécute ensuite des analyses de corrélation des menaces entre vecteurs et procure, via son service de cloud McAfee Global Threat Intelligence, des renseignements en temps réel sur les menaces aux produits de sécurité McAfee hautement intégrés pour la protection des postes clients et du réseau. McAfee Labs met aussi au point des technologies de base pour la détection des menaces (DeepSAFE, profilage des applications, gestion des listes grises, etc.) qui sont incorporées dans la gamme de produits de sécurité la plus large sur le marché.

A propos de McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC), met ses compétences au service des entreprises, du secteur public et des particuliers pour les aider à profiter en toute sécurité des avantages d'Internet. McAfee propose des solutions et des services proactifs réputés, qui assurent la sécurisation des systèmes, des réseaux et des terminaux mobiles dans le monde entier. Avec sa stratégie Security Connected, une approche innovante de la sécurité optimisée par le matériel, et son réseau mondial de renseignements sur les menaces Global Threat Intelligence, McAfee consacre tous ses efforts à garantir à ses clients une sécurité sans faille. www.mcafee.com/fr

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, *The Hidden Truth Behind Shadow IT* (La vérité cachée derrière l'informatique de l'ombre), novembre 2013. http://www.mcafee.com/fr/resources/reports/rp-six-trends-security.pdf

[3] Sutton a affirmé qu'il n'avait jamais prononcé cette phrase célèbre dont il est crédité, expliquant par contre qu'il cambriolait des banques parce qu'il « aimait ça ».

[4] Stratecast, *The Hidden Truth Behind Shadow IT* (La vérité cachée derrière l'informatique de l'ombre), novembre 2013. http://www.mcafee.com/fr/resources/reports/rp-six-trends-security.pdf

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

60756rpt_threats-predictions_1213_fnl_ETMG