SOPHOS
Security made simple.

Rapport Sophos 2014 sur les menaces à la sécurité

Des malwares plus dangereux, plus discrets et plus efficaces

Sommaire

1

Avant-propos

2

Introduction : les malwares évoluent en 2013

4

Les botnets s'étendent et deviennent plus furtifs

- Tendance 2013 : ZeroAccess : impacté par la redirection de son trafic d'attaque (sinkholing) mais rebondit rapidement 5
- Détections ZeroAccess par pays 6
- Les Botnets exploitent Bitcoin 6

7

Malwares Android : transformation et gain d'efficacité

- Détections des malwares Android les plus diffusés, octobre 2013 8
- Anatomie d'un mobile piraté : comment les pirates tirent profit des smartphones 9

10

Linux : une technologie capitale qui attire les criminels

12

Mac OS X : une année marquée par une multitude de petites attaques

- 4 conseils pratiques pour protéger facilement votre Mac 13

14

Malwares de type Web : plus sophistiqués, variés et camouflés

- Kits d'exploits : Blackhole à la traîne derrière des modèles plus évolués 15
- Propagation mondiale de Zbot 16
- Conseils pratiques pour protéger votre serveur Web et vos clients 17

18

Menaces ciblant les comptes financiers

20

Windows : le danger croissant des systèmes sans correctifs

22

Le spam se réinvente

- Juin 2013 : le spam en pièce jointe, ou comment télécharger une montagne d'ennuis 23

24

SophosLabs : comment garder une longueur d'avance sur les attaques les plus complexes de notre époque

26

Tendances à observer en 2014

29

En conclusion

- Sources 30

Pour accéder à des ressources supplémentaires et aux outils référencés dans le rapport, rendez-vous sur

sophos.fr/threatreport


SMS

Avant-propos

La tendance la plus marquante de cette année 2013 fut le recours au camouflage de plus en plus courant des attaques de malwares. Grâce à la distribution massive de botnets sophistiqués et de code source de kits d'exploits, les auteurs de malwares ont été capables de mettre au point des attaques plus évoluées et diversifiées.

Les cybercriminels proposent désormais leurs services sur le marché noir à l'aide de solutions de commercialisation en-ligne. Le kit d'exploit Blackhole, pourtant à la pointe de l'innovation en 2012, s'est vu dépasser cette année par plusieurs autres kits d'exploits basés en partie sur le même code. Les botnets ainsi créés sont responsables de l'augmentation massive des ransomwares, comme Cryptolocker.

Les malwares modernes se caractérisent principalement par leur furtivité. L'une des menaces furtives les plus virulentes actuellement, les APTs (menaces persistantes avancées), cible très précisément les données des individus, des entreprises et des gouvernements. Les APT sont donc des armes ultra sophistiquées pour livrer des attaques ciblées dans le cyber-espace. L'année 2013 a connu un nombre considérable de fuites de données dont l'espionnage industriel et la divulgation de données d'entreprise).

Les APT que nous avons détectées cette année étaient bien organisées, bien financées, et menées par des individus ultra-motivés, compétents, et utilisant des technologies de pointe. Une fois sa mission achevée, l'APT continue à récolter des informations supplémentaires. Pour se défendre contre la nature furtive et persistante des APT, il est nécessaire d'adopter une approche coordonnée à la fois sur les systèmes et au niveau du réseau.

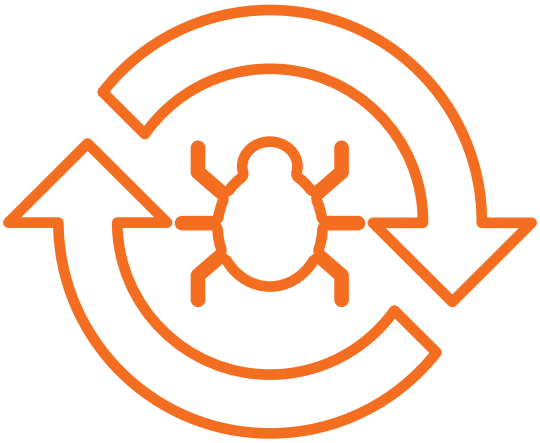
La sécurité n'est plus un luxe mais une nécessité. Les entreprises et les gouvernements concernés à juste titre par la protection des données sensibles et la confidentialité, ont désormais le devoir de connaître la nature des problèmes de sécurité pesant sur les systèmes d'infrastructures critiques. Nous ne pouvons plus considérer la sécurité des guichets automatiques, des systèmes aéronautiques, et des systèmes permettant l'approvisionnement en eau et en électricité, comme acquise et immuable. Ces réseaux vitaux ont fait l'objet d'attaques récentes, ce qui démontre bien la vulnérabilité de l'infrastructure fondamentale sur laquelle nous reposons tous. Ces systèmes, dont ceux des infrastructures de réseu intelligent « smart grid », pourraient bien être visés à nouveau au cours de l'année à venir.

La popularité croissante de l'"Internet des objets" (appareils mobiles, applications, réseaux sociaux, gadgets interconnectés) fait que les menaces sont également en essor constant. De nouvelles menaces font leur apparition à mesure que des technologies émergentes, telles que la communication sans contact (NFC), sont intégrées dans les plates-formes mobiles. Par ailleurs, l'usage de services GPS innovants, pour relier nos vies digitales et physiques fournit encore plus d'opportunités aux cybercriminels de compromettre sécurité et confidentialité.

Ces systèmes pourraient bien engendrer des attaques susceptibles de nous toucher tous très personnellement. En 2014, il sera donc crucial non seulement d'observer l'évolution des attaques existantes, mais aussi l'apparition de nouveaux types inconnus jusque-là.

Bonne lecture,

Gerhard Eschelbeck
Directeur technique, Sophos



Introduction : les malwares évoluent en 2013

Depuis notre précédent rapport de 2012, les malwares et les menaces à la sécurité informatique se sont développés et ont mûri, et leurs auteurs, ainsi que les éditeurs de code et de sites malveillants, sont devenus plus aptes à camoufler leurs attaques.

L'année 2013 a vu proliférer les botnets et les kits d'exploits ultra-sophistiqués, et une nouvelle génération d'auteurs de malwares s'inspirer de l'expérience et du code source de leurs prédécesseurs. Les cyberciminels savent désormais éviter plus facilement la détection en utilisant le chiffrement et s'appuient massivement sur ledarknet, une section anonyme du Web non-surveillée, qui abrite leurs serveurs.

Les périphériques mobiles et certains services Web sont de plus en plus ciblés en raison de leur popularité croissante auprès des utilisateurs. Cette année, les malwares pour Android ont évolué en complexité et en maturité, et des attaques ultra discrètes telles que Darkleech ont pris le contrôle de milliers de serveurs Web. Dans le même temps, les utilisateurs Windows, eux, se préparent à l'arrêt des mises a jour de sécurité pour Windows XP et Office 2003 et se demandent à quelles attaques du “jour zéro perpétuel” ils devront faire face.

Sophos et d'autres éditeurs de sécurité détectent de plus en plus de menaces destinées à des entreprises, des industries ou des organismes gouvernementaux spécifiques. Les attaques sur les transactions et comptes financiers ont commencé à franchir les limites des pays d'Europe de l'Est, où elles s'étaient concentrées jusqu'à présent.

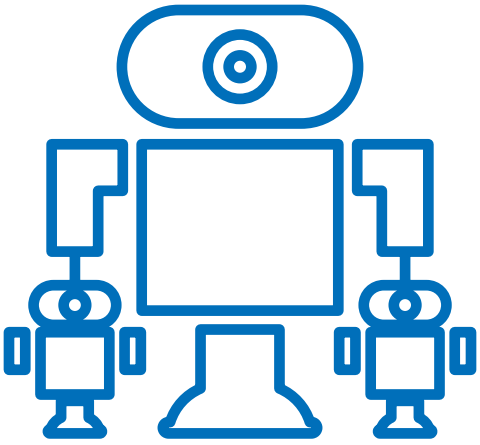
Certaines menaces restent cycliques : elles reviennent plusieurs fois avant de disparaître pendant quelques années. Nous avons par exemple constaté le retour des arnaques de "pump-and-dump" (spam liés à des cours de stock options) que l'on pensait avoir été éradiquées il y a quelques années par la commission américaine des titres et de la Bourse.

Nous avons également rencontré cette année une nouvelle version de ransomware particulièrement virulent connu sous le nom de Cryptolocker. Bien que le ransomware existe depuis presque 25 ans, cette nouvelle version soutire de l'argent à l'utilisateur en lui bloquant l'accès à ses fichiers au moyen d'une technique de chiffrement très robuste.

Heureusement, l'année 2013 a aussi connu des événements positifs, comme l'attestent les informations suivantes. Le créateur présumé de Blackhole, un fléau mondial en 2012, a été arrêté en octobre, preuve d'une réactivité accrue des autorités à l'encontre de la cybercriminalité. Google a fait des progrès techniques dans le domaine de la protection de sa plate-forme Android et a mis en place un règlement plus strict à l'égard des applications malveillantes et potentiellement indésirables.

Les experts des SophosLabs ont découvert des méthodes révolutionnaires pour détecter et désinfecter les menaces, en s'appuyant sur les technologies d''informatique dans le Cloud et les approches « Big Data ».

Que vous soyez une PME, une grande entreprise, une école, un organisme gouvernemental ou encore un particulier, notre lutte commune contre les malwares continue avec vous. Et comme toujours, nous nous engageons à vous fournir les outils indispensables à votre protection.



Les botnets s'étendent et deviennent plus furtifs

Au cours des 12 derniers mois, les botnets se sont propagés tout en devenant plus résistants et discrets. Il semblerait par ailleurs qu'ils s'attaquent à des cibles de plus en plus dangereuses.

Jusqu'à présent, le code source des botnets était toujours gardé secret par ses auteurs. Il arrivait même que ceux-ci vendent leur code à prix d'or lorsqu'ils se retiraient du jeu. Or récemment des fuites de code source ont permis à de nouveaux criminels de créer leurs propres botnets et de les faire évoluer dans des directions jusqu'alors inimaginables.

C'est le cas notamment de Gameover, créé suite à la fuite du code de Zeus il y a quelques années. Celui-ci a remplacé le lien du centre de commande et de contrôle (C&C) de Zeus par un réseau P2P d'ordinateurs infectés. Gameover est doté de mécanismes de communication de secours; utilise plus de techniques de chiffrement; et peut exécuter des commandes plus variées, comme faire participer la machine à des attaques par déni de service distribué (DDoS) de grande envergure.[1]

Des botnets plus résistants

Les botnets intègrent désormais plusieurs formes différentes de centre de commande et de contrôle de secours. Par exemple, si un client infecté par un botnet tel que Gameover ne réussit pas à se connecter à d'autres machines infectées du réseau, il exécute des algorithmes de "génération de domaine" intégrés. Il lui suffit alors de détecter un seul nouveau serveur de C&C pour permettre au client de restaurer son rôle actif au sein du botnet.[2]

Les opérateurs de botnets sont aussi plus réactifs aux contre-mesures. Un certain éditeur d'antivirus avait réussi à gagner un contrôle partiel du botnet ZeroAccess, en redirigeant le trafic de 500 000 clients infectés vers l'un de ses serveurs (technique dite de "sinkholing").[3] Grâce à des réseaux affiliés, les opérateurs du botnet ont immédiatement réagi en augmentant le nombre de « droppers » qu'ils plaçaient sur les clients. En l'espace de quelques semaines, les clients perdus avaient été remplacés, et les nouvelles versions n'étaient plus vulnérables à cette technique de prise de contrôle (sinkholing).

En savoir plus

- Réseaux zombie : La face cachée du Cloud
- Ransomware: Hijacking Your Data
- Back Channels and Bitcoins: ZeroAccess' Secret C&C Communications
- Watch Cryptolocker in Action

Les botnets distribuent des ransomwares plus dangereux

Plus les utilisateurs sont éduqués à propos des escroqueries en ligne et des « faux antivirus », plus les botnets s'orientent vers les « ransomwares ». Les criminels demandent désormais des sommes exorbitantes aux utilisateurs pour leur rendre l'accès à leurs données.

Cryptolocker est sans aucun doute le ransomware le plus dangereux et le plus répandu actuellement. Celui-ci s'ajoute à la liste de programmes Windows qui s'exécutent au démarrage. Puis il détecte un serveur infecté, envoie un fichier ID de l'ordinateur hôte, cherche une clé publique dans le serveur (qui contient également la clé privée correspondante), et grâce à cela, encode toutes les données et les fichiers image qu'il peut trouver.

Le seul moyen de récupérer les données chiffrées est d'utiliser la clé privée, pour laquelle les criminels demandent une rançon (que nous vous déconseillons de payer).[4]

Bien que Cryptolocker soit parfois diffusé par courriel, il est le plus souvent distribué par des botnets qui ont déjà le contrôle de votre ordinateur. Et pour cela, rien de plus facile : les bots répondent tout simplement à une commande de mise à niveau permettant aux criminels de mettre à jour, de remplacer ou de compléter des malwares déjà présents sur l'ordinateur. Quand l'utilisateur s'en rend compte il est déjà trop tard.[5]

Hausse des botnets distribuant des malwares bancaires

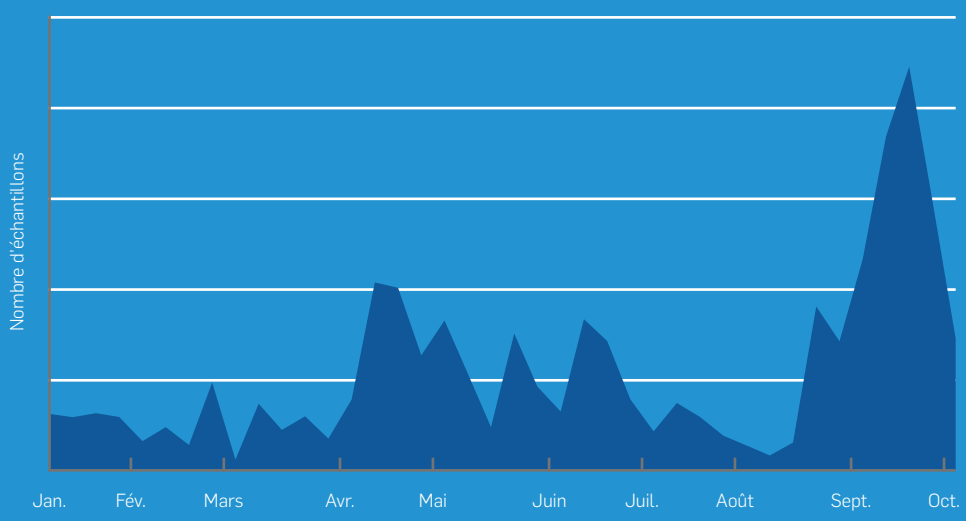
Le code source de Carberp, un kit de détournement d'identifiants bancaires responsable du vol de plus de 250 millions de dollars, a été disséminé mi 2013.[6] Il a depuis franchi les frontières russes, son domaine d'origine, et nous avons reconnu des éléments de son code source dans d'autres botnets Ce code est basé sur le code du kit Power Loader, qui grâce à des techniques d'avant-garde, réussit à livrer les malwares sans être détecté.[7]

En Europe et au Royaume-Uni, de nombreux utilisateurs ont rencontré Shylock/Caphaw, un malware bancaire distribué par botnet qui cible les clients des plus grands organismes financiers tels que Barclays, Bank of America, Capital One, Citi Private Bank, et Wells Fargo.[8]

Tendance 2013 : ZeroAccess est frappé par la redirection du trafic d'attaque (sinkholing), mais rebondit rapidement

Le sinkholing réalisé par les éditeurs de sécurité avait réussi à faire chuter le nombre de systèmes infectés par ZeroAccess détectés par Sophos en juillet et août 2013. Pourtant en septembre, un nombre record d'ordinateurs se trouvaient à nouveau infectés par le botnet, preuve de l'extrême réactivité des opérateurs de ZeroAccess.

Source : SophosLabs



Des botnets plus furtifs

Dans certains botnets, la première adresse de C&C que le client infecté tente de contacter ne fait pas partie d'un botnet. C'est un domaine légitime (mais piraté), difficile à bloquer.

Souvent, le client botnet contacte un serveur PPP (type de serveur d'accès distant) en mode proxy, qui redirige la connexion. Par conséquent, si l'on cible le premier serveur, un simple proxy, l'on n'atteint pas le vrai centre de commande du botnet.

Les botnets utilisent de plus en plus le "darknet"

Les botnets utilisent de plus en plus souvent les réseaux cachés tels que Tor, qui échappent à la surveillance.[9] Celui-ci a permis notamment à des organismes tels que Wikileaks de protéger leurs sources, et héberge le marché noir Silk Road, connu pour sa facilitation de transactions illicites.

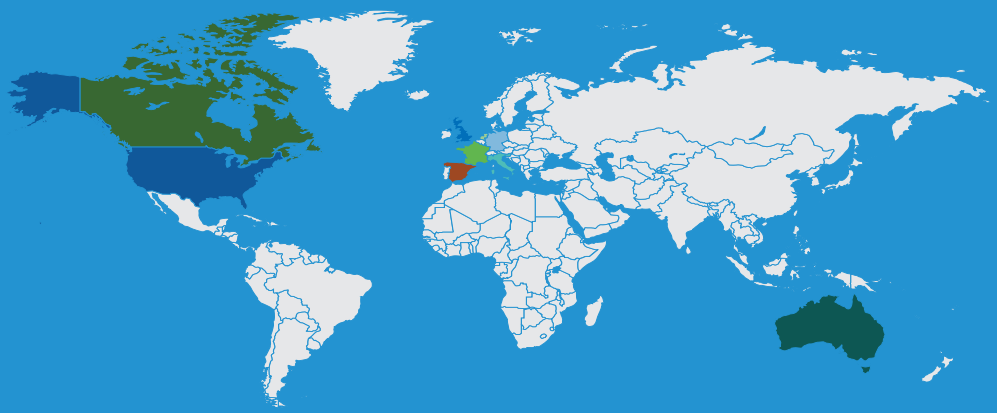
Les botnets peuvent cacher des serveurs de C&C sur le réseau Tor, ce qui les rend infiniment plus difficiles à détecter. Pour se protéger, les entreprises interdisent souvent à leurs employés d'utiliser Tor, et contrôlent les applications pour éviter l'utilisation de logiciel client du navigateur Tor.

Détections ZeroAccess par pays

En octobre 2013, ZeroAccess contrôlait des milliers de systèmes aux Etats-Unis et au Royaume-Uni, et était largement détecté en Allemagne, Australie et Italie.

Systèmes d'extrémité	
Etats-Unis	6,754
Royaume-Uni	1,625
Allemagne	747
Australie	622
Italie	458
Canada	360
France	340
Pays-Bas	170
Espagne	110
Autres	1,014

Source : SophosLabs



La génération de Bitcoins par les botnets : une autre source de revenus permise par les malwares

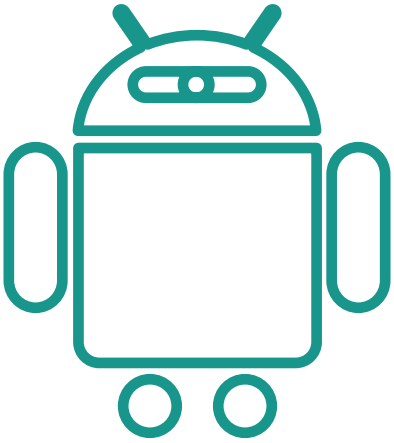
Les opérateurs de botnets sont constamment à la recherche de nouvelles façons de s'enrichir. L'exploitation de Bitcoins, une monnaie électronique totalement indépendante, s'est avéré très lucratif en 2013. La valeur du Bitcoin a fluctué entre $150 et $200 USD au cours des derniers mois.[10]

Les nouveaux Bitcoins sont créés en utilisant des problèmes mathématiques complexes qui demandent une puissance de traitement informatique importante que les plus gros botnets mondiaux sont en mesure de fournir.

Entre mai 2012 et février 2013, et pour trois semaines en avril 2013, les clients du botnet ZeroAccess furent utilisés pour générer des Bitcoins.[11]

Bien que les Bitcoins aient considérablement augmenté durant cette période, ZeroAccess a fini par désactiver la fonctionnalité. Pourquoi ? Nous n'en sommes pas entièrement sûrs, mais peut-être que l'opération attirait trop d'attention ou ne rapportait pas autant que la fraude au clic. Certains parlent d'un nouveau moyen de générer les Bitcoins, bien plus efficace que la distribution par botnet.[12]

Bien que ZeroAccess ne génère plus de Bitcoins, d'autres opérateurs de botnets n'abandonnent pas l'idée pour autant. L'expert en sécurité Brian Krebs a découvert que le botnet russe FeodalCash effectuait de plus en plus d'opérations de génération depuis le mois de mai 2013.[13]



Malwares Android : transformation et gain d'efficacité

Les malwares pour Android continuent à se multiplier et à évoluer dans les pas de Windows. Il y a néanmoins des améliorations en matière de sécurité.

Nous avons enregistré plus de 300 familles de malwares pour Android depuis la première détection en août 2010. Une grande partie de l'écosystème de ces malwares suit le même parcours que les malwares pour Windows ont suivi il y a quelques années.

Experts en camouflage

Nous avons remarqué récemment que les malwares pour Android emploient des techniques de plus en plus ingénieuses pour contourner et contrer les méthodes de détection. Prenons l'exemple de Ginmaster. Détecté pour la première fois en Chine en août 2011, ce programme de type cheval de Troie est injecté dans de nombreuses applications distribuées sur des marchés tiers.

En 2012, Ginmaster commençait à déjouer les techniques de détection en camouflant les noms de classe, en chiffrant les URL et les instructions de C&C, et en adoptant des techniques de polymorphisme propres aux malwares pour Windows. Et en 2013, les développeurs de Ginmaster mettaient en œuvre des techniques de camouflage et de chiffrement bien plus complexes, les rendant beaucoup plus difficiles à détecter et à rétroanalyserr.[14] Ginmaster n'a pas cessé de se propager depuis début 2012, jusqu'à enregistrer plus de 4 700 échantillons entre février et avril 2013.

Nouveaux botnets pour Android

Des rapports récents font état d'un botnet de grande envergure contrôlaant des périphériques Android, tout comme d'autres dans le domaine du PC. Ce botnet, que Sophos détecte sous le code Andr/GGSmart-A, semble jusqu'à présent se limiter à la Chine. Il utilise la technologie de centre de commande et de contrôle pour communiquer avec les appareils mobiles infectés, provoquant par exemple l'envoi de SMS surtaxés qui sont facturés au propriétaire du périphérique. Contrairement aux attaques Android typiques, il a la capacité de modifier et de contrôler les numéros de SMS surtaxés, le contenu, et même les programmes d'affiliés sur l'ensemble de son vaste réseau. C'est le malware pour Android le plus efficace et le plus dangereux de sa génération.[15]

Les ransomwares s'attaquent à Android

Le concept du ransomware est relativement ancien, les premiers cas datant d'il y a 25 ans. Celui-ci opère en prenant vos fichiers ou votre périphérique en otage, et en vous demandant une rançon afin d'en regagner l'accès. En juin 2013, Rowland Yu, chercheur à Sophos, a découvert le premier cas de ransomware sur Android. Android Defender, un malware hybride entre faux antivirus et application ransomware, exige un paiement de $99.99 pour rendre l'accès au périphérique retenu.

Au démarrage, l'apparence professionnelle d'Android Defender lui permet de rechercher, sans éveiller les soupçons, les droits d'administrateur grâce à une multitude de techniques d'ingénierie sociale. S'il les obtient, il peut limiter l'accès à toutes les autres applications, bloquant ainsi les fonctions d'appel, de paramétrage, d'arrêt des tâches, de désinstallation des applications, ou même de réinitialisation. Il affiche un message d'avertissement visible à l'écran, quoi que fasse l'utilisateur. Il est même capable de désactiver les touches Retour/Home puis de s'exécuter lors du prochain démarrage pour éviter d'être supprimé. L'une des seules choses qu'il n'est pas capable de faire pour l'instant, c'est de chiffrer votre contenu ou vos données personnelles.[16] Nous nous attendons néanmoins à vous l'annoncer dans le prochain rapport.

Le détournement de fonds via smartphone

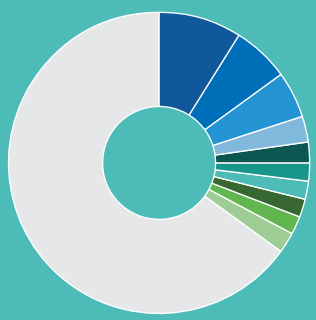
En septembre 2013, nous avons détecté une nouvelle forme de malware bancaire destiné à détourner des fonds via Android grâce à une combinaison de techniques d'ingénierie sociale et d'attaques de type "man-in-the-browser" contre Windows. Parfois appelé Qadars, les SophosLabs le détecte sous le code Andr/Spy-ABN. Bien que le taux de détection soit relativement faible en ce moment, il a déjà frappé des organismes financiers français, néerlandais et indiens.

Détections de malwares Android les plus vastes, octobre 2013

Bien qu'aucune famille de malwares pour Android ne prédomine actuellement, la plus détectée est Andr/BBridge-A. Ce cheval de Troie installe des applications malveillantes sur le périphérique à l'aide d'un exploit qui exécute une escalade de privilèges. Andr/BBridge-A s'est montré très persistant : il occupait déjà la seconde place de notre liste d'infections en juin 2012.[17]

Andr/BBridge-A	9%	Andr/Adop-A	2%	Andr/SmsSend-BE	2%
Andr/Fakeins-V	6%	Andr/Boxer-D	2%	Andr/MTK-B	2%
Andr/Generic-S	5%	Andr/SmsSend-BY	2%	Autres	65%
Andr/Qdplugin-A	3%	Andr/DroidRt-A	2%		

NB : les pourcentages sont arrondis à la hausse
Source : SophosLabs



En savoir plus

- GinMaster: A Case Study in Android Malware
- iPhone vs. Android vs. Windows Phone 8
- Rise of Mobile Malware

Outil gratuit

- Sophos Mobile Security pour Android

Tout comme son prédécesseur Zeus, Andr/Spy-ABN commence par agir du côté de Windows où il injecte du code dans Internet Explorer pour intercepter les données de l'utilisateur avant qu'elles ne soient chiffrées et envoyées vers l'organisme financier. Il capture également les certificats personnels du navigateur et les cookies.

Une fois authentifié, l'utilisateur est informé que par mesure de sécurité (quelle ironie!) sa banque exige maintenant une nouvelle application pour smartphones. Sur saisie de son numéro et du modèle du téléphone, il reçoit un SMS contenant un lien vers l'application malveillante. Comme si cela ne suffisait pas, le code injecté empêche l'utilisateur d'accéder à ses comptes jusqu'à ce que le malware soit installé et lui fournisse un code d'activation.[18]

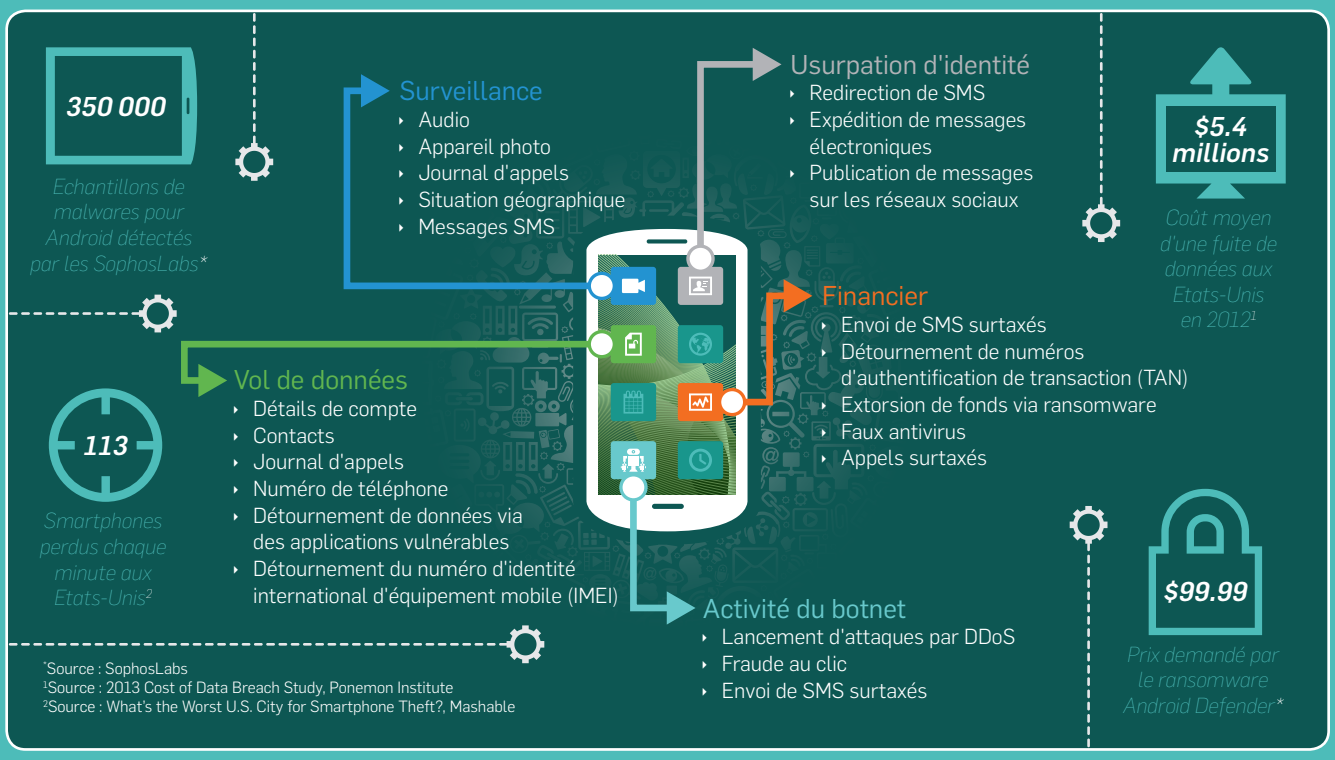
Sécurisez votre Android

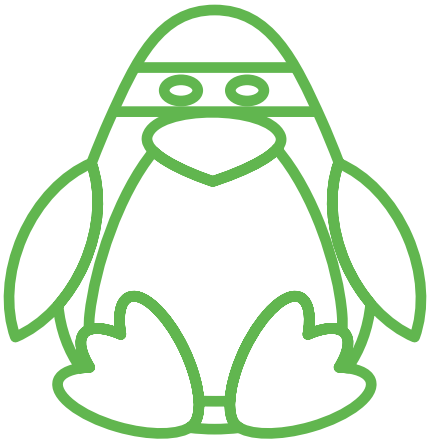
La plate-forme Android a récemment fait l'objet d'améliorations de sécurité. Contrairement aux versions précédentes, Android 4.3 n'autorise plus le téléchargement automatique des applications. Google est également plus strict envers les développeurs, surtout dans le cas des applications potentiellement indésirables, qui ne sont pas des malwares à proprement parler, mais qui sont souvent trop intrusives.

Google interdira désormais certains formats d'applications et d'annonces, notamment l'insertion d'annonces tierces ou de liens sur la page d'accueil, le changement de la page d'accueil du navigateur, ou l'utilisation de la zone de notification du système à des fins différentes.[19]

Anatomie d'un mobile piraté : comment les pirates tirent profit des smartphones

Votre appareil Android vous paraît peut-être inoffensif, mais une fois piraté, il peut surveiller vos moindres faits et gestes et usurper votre identité, participer aux activités dangereuses d'un botnet, dérober vos données personnelles et même votre argent.[20]





Linux : une technologie capitale qui attire les criminels

La plate-forme Linux attire les criminels du fait de la popularité de ses serveurs en tant que plateforme de site et contenu Web.

Bien que Linux ne fasse l'objet que de très peu d'attaques par rapport à Windows et Android, le flux modeste de scripts et d'exécutables qui l'attaquent est constant. Nous détectons également de nombreux malwares qui ciblent des services conçus indépendamment de la plate-forme qui les héberge, souvent exécutés sur des serveurs Linux.

Plusieurs raisons expliquent pourquoi les serveurs Linux sont devenus plébiscités par les criminels cherchant à rediriger du trafic vers leurs logiciels malveillants. Premièrement, de nombreux serveurs Web sont exécutés sous Linux, y compris certains des sites Web les plus importants du monde entier. Deuxièmement, comme Linux est considéré plus sûr que les autres systèmes d'exploitation, il est rarement soumis au même degré de surveillance. De ce fait, un serveur Linux peut rester infecté pendant des mois ou même des années, constituant un retour sur investissement exceptionnel pour les criminels.

Nos recherches nous ont montré qu'une grande majorité des serveurs impliqués dans la redirection de trafic vers des pages malveillantes sont des serveurs Linux. Par conséquent, bien que le volume de malwares s'exécutant sur Linux soit plus limité, il est important de rester vigilant à l'égard des infections.

Nous détectons tous les mois des dizaines de milliers d'échantillons de code malveillant exécuté sur des serveurs Linux, et ce malgré les mesures extrêmes prises par les auteurs de malwares pour camoufler leurs scripts PHP (un langage côté serveur fréquemment utilisé pour la programmation des sites Web).

En savoir plus

Naked Security : Linux

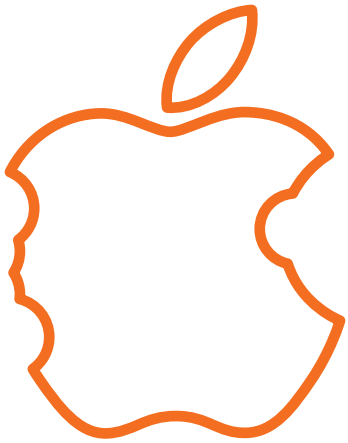
Nous voyons un grand nombre de scripts PHP malicieux qui jouent le rôle de "nœuds" dans un système de distribution plus large affilié à un botnet, qui permet au système d'exécuter des charges virales malveillantes telles que les attaques par déni de service. (pour plus d'informations sur les attaques de serveurs Web telles que Darkleech et Redkit, voir page 16.)

Les scripts PHP piratés s'exécutent souvent sur des plates-formes vulnérables telles que les versions non corrigées de WordPress.[21] Par exemple, en 2013, nous avons détecté un exploit dans le moteur PHP exécutant le système de gestion de contenu Plesk. Une certaine commande permettait aux criminels de gagner l'accès au moteur et d'exécuter le script PHP de leur choix.[22]

Plus les administrateurs ajoutent de scripts et de services tiers, plus ils élargissent la surface d'attaque de leurs systèmes Linux. Ceci souligne l'importance d'installer les correctifs rapidement et d'adopter une approche multi-niveaux de la protection du système d'exploitation Linux et des services qu'il exécute.

Souvent, les serveurs de fichiers Linux traditionnels hébergent des malwares ciblant Windows et d'autres systèmes d'exploitation. Par conséquent, même si un serveur Linux n'est pas lui-même directement visé, il peut infecter les périphériques auquel il est relié.

En 2013, nous avons réalisé nos premières détections de gros volumes de malwares pour Android sur les systèmes Linux. Bien sûr, si un serveur Linux, un hébergeur de script, ou un serveur Web *est* infecté par du malware, celui-ci peut facilement détecter les requêtes HTTP provenant d'appareils Android, et distribuer les malwares en fonction. Il est donc important que tout système Linux qui fournit des services à Windows ou à d'autres clients soit équipé d'un logiciel antimalware.



Mac OS X : une année marquée par une multitude de petites attaques

Bien que cette année, Mac OS X n'a pas fait l'objet d'attaques marquantes, nous avons tout de même détecté une flux constant de petites attaques créatives et diverses. Restez vigilant.

Bien que cette année la plate-forme Mac OS X n'ait pas subi d'attaque égalant l'étendue mondiale de Flashback en 2012, les attaques ont continué à évoluer en 2013, sous des formes diverses : chevaux de Troie, attaques contre les vulnérabilités de Java et les formats des documents Word, plug-ins agressifs, JavaScript malveillant et malwares conçus pour passer outre la protection Apple Gatekeeper grâce à une fausse identité Apple Developer.

En février 2013, l'agence Reuters publiait la nouvelle que les Macs des employés Apple avaient été piratés par une nouvelle vulnérabilité dans Java, la même qui avait touché Facebook la semaine précédente[23] et qui a attaqué l'unité Mac de Microsoft quelque temps après.[24] Distribuée via un site pour développeurs de logiciels, cette campagne “watering hole” est sans doute un signe que les pirates savent qu'il est parfois plus facile de s'infiltrer dans une entreprise via des petits sites fréquentés par leurs employés plutôt que d'attaquer directement leur infrastructure principale, généralement bien protégée.

Chevaux de Troie pour Mac

En 2012, AlienVault et Sophos découvraient des chevaux de Troie type porte dérobée qui infectaient des ordinateurs Mac par le biais de documents Word piégés. Ces attaques étaient intégrées dans des documents qui prétendaient aborder le thème de la violation des droits de l'homme au Tibet, portant à croire que l'attaque avait été organisée par des sources proche du gouvernement chinois.[25]

En février 2013, des documents portant sur des abus perpétrés à l'encontre de minorité ouïghoure du Turkestan oriental hébergeaient le même type de malware. Toutes ces attaques exploitent une vulnérabilité de Word 2004/2008 depuis longtemps corrigée par Microsoft (MS09-027).[26] Que vous vous trouviez ou non dans cette partie du monde, pensez donc à installer le correctif en question si vous utilisiez cette version du logiciel.

S'il s'agit d'attaques ciblées, elles sont loin d'être les seules. Le mois de septembre 2013 a vu l'apparition de OSX/Bckdr-RQV, une nouvelle attaque de porte dérobée qui, une fois

Outil gratuit
Sophos Antivirus pour Mac édition familiale

installée, divulgue un ensemble d'informations concernant la machine infectée. Selon Intego, certaines versions tentent de télécharger une image de la Syrian Electronic Army, un groupe de pirates qui se vantait d'être à l'origine d'une cyberguerre en faveur du gouvernement syrien de Bashar al-Assad.[27]

Attaques par Apple Developer ID

Dans les versions les plus récentes d'OS X, l'outil Gatekeeper permet l'installation par défaut de logiciels obtenus via la boutique Apple, ou signé viaune signature Apple Developer ID. Mais que se passe-t-il si un logiciel malveillant réussit à s'approprier la signature? C'est ce qui est arrivé entre décembre 2012 et février 2013, quand des applications "Christmas Card" malveillantes, signées par le développeur Apple “Rajinder Kumar”, furent distribuées par courriel. Avant que son identité ne soit révoquée par Apple, plusieurs utilisateurs avaient lancé la charge virale OSX/HackBack-A : un malware qui téléchargeait des versions compressées de leurs documents sur un serveur distant.[28]

Mais Christmas Card n'a pas été le seul malware pour Mac de l'année. Cet été, le cheval de Troie Janicab, basé sur Python, utilisait la même technique.[29] Il est possible que d'autres attaques du même genre aient échappé à la détection, et dans le cas contraire, il est probable que d'autres fassent leur apparition à l'avenir.

Adwares et ransomwares

2013 a vu l'essor des adwares agressifs, entre logiciels potentiellement indésirables et malwares, non seulement dans Android mais aussi dans les navigateurs. Souvent, ces plug-ins utilisent un installateur agressif (qui ignore même parfois les préférences de l'utilisateur), se font passer pour des codecs vidéo exigés par l'utilisateur (OSX/FkCodec-A),[30] ou convainc l'utilisateur d'accepter l'installation.

En parlant de navigateurs, certains utilisateurs de Mac Safari ont fait les frais d'une version inférieure de ransomware en 2013. Tout comme les autres ransomwares, il affichait de faux messages provenant prétendument des autorités, demandant à l'utilisateur de payer une amende pour avoir visionné ou téléchargé du contenu illicite. Contrairement au ransomware le plus dangereux de l'année (Cryptolocker, qui ne touche que Windows), ce malware Mac ne chiffre pas les fichiers. Il exécute simplement un code JavaScript qui capture le navigateur, et qui réapparaît après une « sortie forcée ». Heureusement, ce JavaScript peut être supprimé sans subir de coûts ni de dégâts, en sélectionnant Réinitialiser Safari dans le menu Safari.[31]

Pour terminer, comme dans le cas des serveurs Linux, les serveurs (et parfois les clients) Mac OS X hébergent souvent des malwares inactifs jusqu'à être transférés vers un système Windows. De nombreux utilisateurs exécutent des machines virtuelles Windows sous OS X à l'aide de logiciels tels que Parallels Desktop. Ces machines virtuelles sont tout aussi exposées aux malwares que les systèmes Windows classiques. Les utilisateurs Mac qui utilisent rarement Windows ne devraient pas pour autant négliger leur protection.

4 conseils pratiques pour protéger votre Mac

Les malwares sont moins fréquents sur Mac que sur Windows ou Android, mais ils ne sont pas inexistants, et il est important de s'en défendre. Heureusement, vous pouvez réduire les risques en suivant ces quelques conseils.

Supprimez Java à moins d'en avoir réellement besoin.

Si vous ne pouvez pas le supprimer complètement, retirez-le au moins de votre navigateur, où se trouvent les pires menaces Java. Il est de plus en plus facile d'éviter Java dans Mac. OS X Lion et les versions supérieures ne l'installent plus par défaut, et si vous l'installez quand même, le système d'exploitation le supprime automatiquement après 5 semaines d'inactivité.[32]

Installez régulièrement les correctifs. De nombreuses attaques pourraient être évitées si l'utilisateur installait les correctifs dès leur sortie. Il y a bien sûr toujours des nouvelles vulnérabilités à corriger : la mise à jour OS X 10.8.5 de septembre 2013 a corrigé des failles d'exécution à distance dans plusieurs parties du système, de CoreGraphics à ImageIO en passant par PHP et QuickTime.[33]

Si votre version de OS X le permet, téléchargez uniquement les applications de l'App Store Mac. Vous pourrez toujours occasionnellement contourner la restriction pour télécharger une application légitime, mais tout en sachant que vous êtes bien protégé le reste du temps.

Équipez votre Mac d'un antivirus, si ce n'est pas déjà fait. Si vous êtes un particulier qui utilise actuellement un Mac sans antivirus, nous vous offrons l'opportunité de protéger votre ordinateur avec une solution gratuite de niveau professionnel : téléchargez Sophos Antivirus pour Mac édition familiale, qui bloque même les menaces de type Web nouvelle génération.

Malwares de type Web : plus sophistiqués, variés et camouflés

L'année 2013 a vu une croissance des kits d'exploits et les attaques dangereuses visant les serveurs Web, entraînant une hausse des téléchargements passifs.

Comme nous l'avons déjà mentionné dans notre section sur les malwares pour Linux, les attaques sous forme de modules malveillants Apache ont fortement augmenté cette année. Une fois installé sur le site légitime piraté, le module exploite les failles connues du navigateur pour lancer des téléchargements passifs.

Darkleech attaque les serveurs Web

Le malware Web le plus important cette année fut Darkleech, qui en l'espace de 5 mois avait déjà infecté plus de 40 000 domaines et adresses IP, dont 15 000 au mois de mai. Des sites Web importants tels que ceux du Los Angeles Times et de Seagate ont été touchés. Les serveurs Web infectés par Darkleech sont responsables d'avoir distribué des malwares extrêmement virulents tels que le ransomware Nymaim, qui après avoir chiffré les fichiers de l'utilisateur, lui demande $300 en échange de la clé.[34] Nous avons découvert que 93% des sites infectés par Darkleech exécutaient Apache.[35]

En mars 2013, Darkleech et d'autres attaques associées constituaient presque 30% de toutes les menaces Web détectées sur les machines et appliances Web des clients, soit la menace la plus importante de sa catégorie.

Certaines de ces attaques sont conçues pour être difficiles à reproduire. Elles peuvent par exemple n'être lancées qu'une fois sur dix, portant l'administrateur à croire que le problème, si toutefois il y en a un, ne provient pas du système local. Darkleech garde des listes noires pour s'assurer que chaque adresse IP ne soit sollicitée qu'une seule fois. Beaucoup de criminels évitent également de frapper les adresses IP qu'ils soupçonnent appartenir au domaine de la sécurité ou aux moteurs de recherche.

En savoir plus

- Choisir votre fournisseur d'hébergement
- Malware B-Z: Inside the Threat From Blackhole to ZeroAccess
- Les cinq étapes d'une attaque de malware Web
- Malware 101

Ces attaques envers les serveurs Web soulignent le besoin d'une meilleure collaboration entre les éditeurs de sécurité et les hébergeurs de sites Web, pour mieux comprendre les attaques aussi complexes et subtiles que Darkleech. Du point de vue technique, celles-ci sont déjà exceptionnellement difficiles à détecter. Nous avons aidé plusieurs hébergeurs à nettoyer leurs serveurs. Mais comme l'hébergement est une activité à faible marge, il n'est pas rare que ceux-ci remplacent les serveurs infectés par de nouveaux serveurs virtuels plutôt que de diagnostiquer la cause du problème. Et puisqu'ils ne prennent pas le temps de comprendre, le problème se transmet rapidement sur les nouveaux serveurs.

Il est donc conseillé de se renseigner sur les procédures que suit son hébergeur en cas d'infection, et s'il a des mesures en place pour éviter la réinfection.

Davantage de « malvertising »

On appelle "malvertising" les annonces malveillantes distribuées sur les réseaux publicitaires et sites Web légitimes. Ce phénomène, qui existe depuis longtemps, a connu une recrudescence en 2013, touchant même des grands sites tels que YouTube.

De nos jours, il apparaît le plus souvent sous forme de contenu Flash malveillant. Si l'utilisateur clique sur l'annonce Flash, il risque d'être réorienté vers un site malveillant grâce à du code ActionScript. Un très bon exemple de cheval de Troie récent est Troj/SWFRed-D. Présent dans de nombreuses publicités YouTube en 2013, celui-ci redirige l'utilisateur vers le kit d'exploit Styx, ce qui explique pourquoi ce dernier est devenu aussi courant ces derniers temps (voir le tableau ci-dessous).

L'annonce contenant du code ciblant les failles dans le lecteur Flash du client, il peut même infecter les utilisateurs Flash sans les rediriger.

Au-delà de Blackhole : tout un monde de kits d'exploits

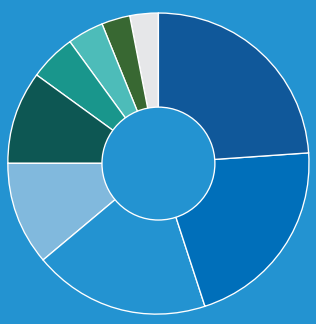
Notre rapport 2012 couvrait en profondeur Blackhole, le kit d'exploit d'avant-garde qui permettait aux auteurs de malwares de distribuer potentiellement n'importe quelle charge virale. Bien que ce kit existe toujours (il est d'ailleurs utilisé dans les attaques Darkleech dont nous avons parlé ci-dessus), il n'est plus unique en son genre.

Plusieurs groupes de criminels ont réussi à créer de nouveaux kits d'exploits ultra-puissants basés sur les innovations de Blackhole, sans avoir à le rétroanalyser. Récemment, Blackhole n'était que 8ème du classement des malwares les plus répandus. Avec l'arrestation de son auteur présumé, M. Paunch,[36] il est probable qu'il perde encore plus de places. Notons que cette arrestation a mené à l'augmentation immédiate des prix de Neutrino, l'un de ses concurrents.[37]

Kits d'exploits : Blackhole à la traine derrière des modèles plus évolués

Blackhole, qui dominait le monde en 2012, a été dépassé par de nouveaux kits tels que Neutrino et Redkit en 2013.

Neutrino	24%	SweetOrange	11%	Nuclear	4%
Kit inconnu	21%	Styx	10%	Blackhole/Cool	3%
Redkit	19%	Glazunov/Sibhost	5%	Autres	3%



NB : les pourcentages sont arrondis à l'unité supérieure.
Source : SophosLabs

En savoir plus
Preventing website compromises

L'avènement de Redkit

Tandis que Blackhole cible les failles de Java, de PDF et de Flash, une multitude de nouveaux kits se concentrent uniquement sur Java. C'est le cas de Redkit, qui cible les sites Web légitimes et qui était par ailleurs à l'origine du piratage du site de la NBC en février 2013,[38] et de la distribution de spam suite aux attentats du marathon de Boston. En juillet 2013, il se trouvait en tête des kits les plus utilisés, constituant 42% des détections ce mois-là.

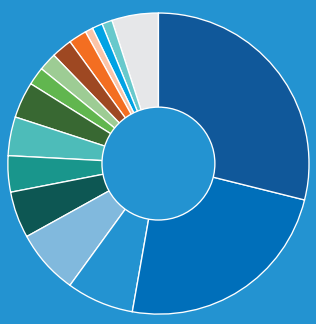
Tout comme les téléchargements passifs traditionnels, Redkit réoriente les utilisateurs vers un site d'exploit. L'utilisateur passe tout d'abord par un autre serveur, légitime mais piraté. Puis il est dirigé vers une page d'accueil .htm ou .html piratée contenant un fichier Java JAR malveillant (format également utilisé pour distribuer les applets Java).

La victime présume que le contenu malveillant provient du serveur Web piraté utilisé dans la deuxième étape de redirection, mais il est en fait stocké ailleurs pour éviter d'être détecté. En effet, les serveurs Web exécutent un utilitaire PHP relié à une commande Redkit distante et un serveur de contrôle. L'utilitaire met à jour la liste des sites infectés toutes les heures, réorienteles victimes vers les « bons sites » et veille à ce que le contenu malveillant le plus récent soit livré depuis sa source réelle.[39]

Charges virales des kits d'exploits, juin 2013 : les kits d'exploits peuvent distribuer pratiquement n'importe quoi. Voici les charges les plus courantes

Les kits d'exploits ont pour but de distribuer une multitude de charges virales: à partir de juin 2013, les ransomwares et le botnet ZeroAccess étaient les plus courants.

Ransomware	29%	Karagany	4%	Tobfy	1%
ZeroAccess	24%	FakeAV	4%	Tranwos	1%
Fareit	7%	Simda	2%	Andromeda	1%
Moure	7%	Dofoil	2%	Autre	5%
Shylock	5%	Medfos	2%		
Zbot	4%	Redyms	2%		



NB : les pourcentages sont arrondis à l'unité supérieure.
Source : SophosLabs

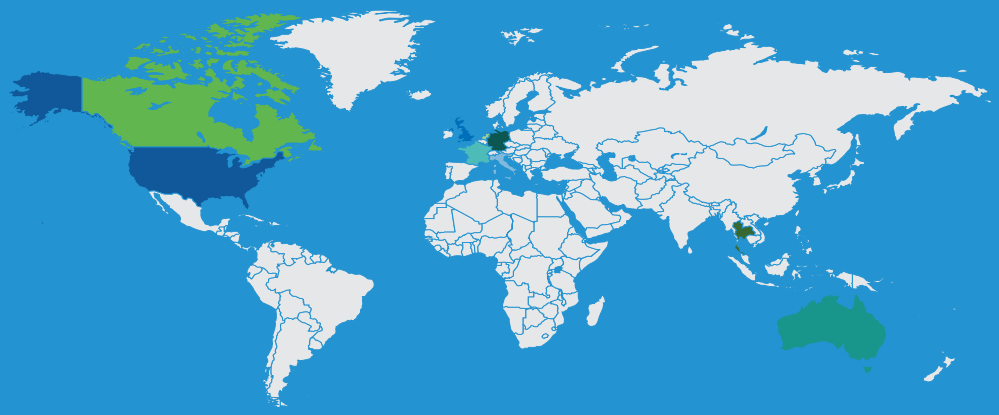
Redkit agit en tant que botnet pour contrôler les serveurs Web qui interagissent avec plusieurs milliers d'utilisateurs. Comme ces serveurs tournent 24h/24 et 7j/7 et touchent autant d'utilisateurs, ils sont très précieux pour ceux qui souhaitent livrer des attaques par DDoS ou distribuer des volumes importants de malwares.

Mais Redkit n'est pas le seul exploit récent qui cible les serveurs Web. Le kit Glazunov a été détecté chez des hébergeurs partout dans le monde. Le tableau en page 15 montre que celui-ci constituait 5,47% de toutes les détections de kits d'exploit pendant le troisième trimestre 2013. Il est connu pour la distribution de ransomwares dangereux. Deux kits émergents, Sibhost et Flimkit, sont tellement similaires qu'ils proviennent probablement de la même source.

Propagation mondiale de Zbot

En 2013, la charge virale du kit d'exploit Zbot s'est répandue aux Etats-Unis, en Europe et en Australie, constituant 31% des détections américaines, 23% des détections en Grande-Bretagne, et 12% des détections italiennes.

Systèmes d'extrémité	
Etats-Unis	2,322
Royaume-Uni	1,749
Italie	884
Allemagne	693
Australie	365
France	188
Thailande	156
Canada	144
Pays-Bas	135
Singapour	84
Autres	795



Source : SophosLabs

Conseils pratiques pour protéger votre serveur Web et vos clients

Adoptez une protection multi-niveaux. Associez une solution de détection des malwares à jour avec un filtrage Web et une solution de détection en cours d'exécution et prévention des intrusions au niveau des systèmes.

Installez rapidement les correctifs. Bien que l'on entende surtout parler des attaques « du jour zéro » (zero-day), la grande majorité des attaques profitent de vulnérabilités anciennes dont les correctifs n'ont pas été installés par l'utilisateur.

Limitez ou supprimez Java sur le client. En 2013, de nombreux auteurs de botnets ou d'exploits se sont éloignés de Flash et PDF pour se concentrer sur Java, qui possède un plus grand nombre de vulnérabilités. Déterminez donc si vous avez réellement besoin d'avoir Java sur vos clients.

Réduisez la surface d'attaque en évitant ou en supprimant les plug-ins superflus, comme par exemple les plugins WordPress que vous n'utilisez pas.

Protégez vos identifiants de connexion. Utilisez des mots de passe uniques, et assurez-vous d'avoir changé tous les mots de passe administrateur par défaut.

Menaces ciblant les comptes financiers

Nous rencontrons de plus en plus d'attaques persistantes et ciblées, pour la plupart visant les comptes financiers.

Bien qu'ils ne soient pas en mesure de quantifier la hausse, les SophosLabs constatent de plus en plus d'attaques visant des entreprises et des institutions spécifiques ; certaines d'entre elles n'étaient pas jusqu'alors considérées à risque. Ces attaques cherchent plus particulièrement à pirater des comptes financiers, ce qui explique pourquoi les détourneurs de fonds sont intéressés par les méthodes utilisées par les menaces avancées persistantes (APT).

Plugx, Blame et Simbot : prenez garde aux apparences trompeuses

Certaines attaques ciblées tentent de se faire passer pour des applications légitimes. Nous voyons notamment des attaques dangereuses qui dérobent les certificats et qui chargent des contenus malveillants à l'aide des composants sains du système d'exploitation Windows ou d'éditeurs tiers. Le code malveillant est ensuite exécuté par un processus fiable, ce qui trompe le pare-feu en lui faisant penser que le trafic sortant est légitime.

Gabor Szappanos, chercheur principal à Sophos, explique que ces attaques ciblées parviennent à rester indétectées pendant des mois en minimisant l'impact sur le système, en gardant tout sous forme chiffrée et en s'alignant de près sur des applications saines. Ces techniques laissent présager qu'à l'avenir, les attaques seront encore plus difficiles à détecter.[40]

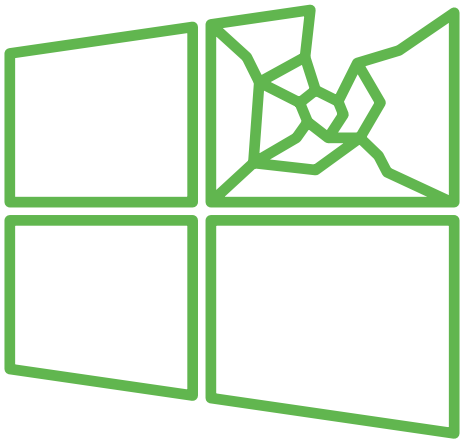
En savoir plus
APTs

Plugx, par exemple, repose sur l'usurpation d'applications sainessignées numériquement. Il exploite les vulnérabilités des DLL Windows, plaçant la librairie malveillante à côté de l'application. Quand l'application est exécutée, elle charge la DLL malveillante dans le fichier courant plutôt que dans la DLL saine située dans le fichier système.[41] Cette vulnérabilité est le résultat d'une particularité de Windows. La modifier causerait l'échec d'une multitude d'applications légitimes.[42] Il semblerait donc que nous devions composer avec cette vulnérabilité pendant encore longtemps.

Un autre spécimen, Blame, cache son contenu malveillant au cœur d'une DLL composée de plusieurs projets open source, dont l'encodeur MP3 LAME, qui sert de leurre en ajoutant suffisamment de code sain pour camoufler le code malveillant.

Simbot, lui, est l'exemple classique du nouveau modèle d'attaque dit "BYOT" (Bring your own Target, ou "apportez votre propre cible"). Il contient une application saine mais vulnérable, démarrée par une ligne de commande extrêmement longue, menant à l'exécution d'un utilitaire malveillant qui déchiffre et charge la principale charge virale.

Bien que l'exploitation d'applications vulnérables ne soit pas une tactique récente, Simbot se différencie par le fait qu'il l'utilise à chaque démarrage sur des systèmes déjà infectés pour garantir l'exécution d'une application saine, et que le code malveillant soit uniquement exécuté via l'exploit. En utilisant sa propre application, Simbot ne dépend pas de l'application en cours d'installation sur le système, et fonctionne même si celle-ci a été corrigée dans une version ultérieure. Cette approche permet à Simbot de laisser très peu de traces.



Windows : le danger croissant des systèmes non corrigés

A partir d'avril 2014, il n'y aura plus de correctifs pour Windows XP et Office 2003. Les correctifs Windows sont néanmoins un problème de taille dans les domaines spécialisés tels que les terminaux de paiement et les équipements médicaux.

On parle tellement d'Android et du Web actuellement que l'on oublie que plus d'un milliard d'ordinateurs fonctionnent toujours sous Windows. Bien que la plupart d'entre eux soient mis à jour et corrigés par l'outil automatique Microsoft Update, il existe encore des failles inquiétantes. Ce chapitre portera sur trois problèmes particuliers : l'arrêt annoncé des correctifs pour Windows XP et Office 2003; les terminaux de paiement (POS) sans correctifs ou non corrigibles; et l'omniprésence de malwares sur les équipements médicaux sans correctifs qui fonctionnent sous diverses versions de Windows.

Selon NetMarrketShare, en septembre 2013, plus de 31% de tous les PC utilisaient encore Windows XP,[43] la version populaire du système d'exploitation lancée en 2001. Microsoft a publié de nombreux communiqués informant ses utilisateurs qu'il cesserait d'éditer des mises à jour de sécurité à partir du 8 avril 2014.[44]

Si vous, ou vos employés, exécutez ce système, prenez garde. Selon le Trustworthy Computing Director de Microsoft, certaines failles présentes dans les nouvelles versions seront rétrocompatibles avec Windows XP. Ces vulnérabilités existeront toujours dans Windows XP même lorsque Microsoft les aura corrigées dans Windows Vista, Windows 7 ou Windows 8.[45]

En savoir plus

Cinq recommandations pour réduire les risques des menaces Web modernes

Naked Security podcast: The End of XP

L'arrêt des correctifs pour Windows XP affecte les points de vente et les appareils médicaux

A mesure que la vulnérabilité des systèmes suscite de plus en plus d'inquiétudes, l'attention se porte sur les autres catégories de périphériques qui exécutent Windows. Certains de ces systèmes exécutent Windows XP ou des versions plus anciennes telles que Windows 2000. Même les entreprises qui installent méticuleusement les correctifs ne pourront plus se protéger. D'autres appareils exécutent des versions plus récentes de Windows, mais leurs propriétaires ou fabricants ne fournissent pas de correctifs adéquats.

Les terminaux de paiement (POS) utilisent fréquemment Windows pour gérer toutes leurs transactions. Bien que la règlementation exige l'installation rapide des correctifs, certains appareils font l'objet de mises à jour irrégulières, surtout dans les petits commerces qui ne bénéficient pas d'un support informatique sophistiqué.[46] Bien des systèmes de POS ont choisi Windows XP pour sa popularité et sa durabilité. Certains d'entre eux pourraient exécuter une nouvelle version de Windows, mais selon l'expert en systèmes de paiement Walter Conway, d'autres ont été conçus spécialement pour Windows XP.[47]

Les risques sont donc biens réels. En décembre 2012, Visa informait les commerçants de l'existence de Dexter, un malware pour Windows conçu spécialement pour s'attaquer aux terminaux de paiement. Celui-ci détournait les données stockées sur les bandes magnétiques et les envoyait vers un serveur de C&C.[48]

De graves problèmes de sécurité sont aussi apparus dans les appareils médicaux. En juin 2013, après avoir fait l'objet d'une grande polémique, la Food and Drug Administration américaine révélait que de nombreux appareils médicaux avaient été soit infectés soit désactivés par des malwares. Ceux-ci avaient dans certains cas accéder aux données des patients, aux systèmes de surveillance et avaient même atteint des appareils portés par les patients.[49]

Ces problèmes sont causés par le fait que de nombreux fabricants n'ont pas distribué les mises à jour de sécurité et les correctifs nécessaires aux plates-formes concernées. Mais comme dans le cas des terminaux de paiement, Microsoft ne peut pas être tenu responsable du manque de sérieux des fabricants, qui devraient s'engager à certifier la compatibilité de leurs appareils avec les derniers correctifs. Mais dès l'arrêt des mises à jour de sécurité pour Windows XP, même les fabricants avec des procédures de certification fiables n'auront plus de correctifs Windows XP à tester.

Quelle est l'étendue réelle du problème ? Selon la MIT Technology Review publiée fin 2012, les équipements médicaux deviennent truffés de malwares."[50] Au Beth Israel Deaconess Medical Center à Boston, "664 appareils médicaux fonctionnent sous des versions anciennes de Windows, que les fabricants refusent de modifier et que l'hôpital n'a pas l'autorisation de changer—même pour ajouter des logiciels antivirus... Ils sont donc souvent touchés par les malwares, à tel point qu'un ou deux appareils par semaine doivent être déconnectés pour nettoyage."

Pour terminer, signalons que Windows XP ne sera pas le seul produit phare de Microsoft à perdre ses mises à jour le 8 avril 2014. Ce sera aussi le cas de Microsoft Office 2003. Toujours en utilisation courante, Office 2003 était la dernière version à supporter les anciens formats de documents Microsoft, qui ne sont toujours pas considérés fiables même après trois service packs. Malheureusement, les utilisateurs de Vista et Windows 7, des systèmes pourtant fréquemment mis à jour, courent le risque de rester vulnérables pendant les années à venir étant donné que Office 2003 est inclus dans ces systèmes d'exploitation.

Le spam se réinvente

Encore une année de spam. Le risque de sécurité ne disparaît jamais.

Les cybercriminels continueront à profiter des courriels tant qu'ils existeront. Certains messages de spam sont juste indésirables. D'autres sont connectés à des arnaques financières que la plupart d'entre nous avons appris à ignorer. D'autres, en revanche, sont très dangereux.

Certaines des tactiques favorites des spammeurs semblent être là pour durer, telles que le spam-image (par ex. les tentatives de vendre des fausses Rolex) et le spam lié à l'actualité (par ex. l'attaque terroriste du marathon de Boston en avril 2013).

D'autres formes de spam semblent être cycliques. Elles deviennent passées de mode puis reviennent quelques années plus tard. Par exemple, en 2013, nous avons assisté au retour des arnaques de "pump-and-dump".

Le retour des arnaques de "pump-and-dump"

Le "pump-and-dump" consiste à disséminer des fausses informations concernant une action en bourse qui serait prétendument sur le point d'augmenter. Les criminels profitent ensuite du courant acheteur ainsi créé pour vendre leurs titres (achetés à bas prix) et en récolter les bénéfices. Il y a quelques années, il y avait des jours où plus de 50% des messages de spam détectés pouvaient être attribués au "pump-and-dump". Mais ces messages furent presque entièrement éradiqués par une campagne de répression de la Commission boursière américaine.

Début 2013, ces messages ont pourtant commencé à réapparaître par à-coups, représentant de 1 à 7% du spam entre le 17 et le 31 janvier, de 5 à 15% entre le 16 et le 20 février, et de 5 à 20% au mois de mars. Puis ils se sont calmés jusqu'à la fin du mois de juin, avant de revenir de plus belle : entre juillet et septembre, les volumes étaient d'environ 10-20% par jour, avec des pointes occasionnelles allant jusqu'à 50%.

En savoir plus

Qui espionne votre messagerie

Ne laissez pas les pertes de données anéantir votre budget

Certains disent que l'on ne peut pas être trop rond ou trop mince, et c'est vraisemblablement l'opinion des auteurs de la deuxième plus grande campagne de spam de l'année : une arnaque portant sur un produit d'amaigrissement nommé "greencoffee". Ces messages imitent de vrais bulletins d'informations et citent des médecins vus à la télévision tels que le Dr. Oz pour plus de crédibilité. Malheureusement, les utilisateurs qui se font piéger sont dirigés vers des domaines qui ont pour seul but d'inciter à l'action avant d'être redirigés vers le site principal de l'arnaque.

Serveurs distribués et spam "snowshoe"

Les spameurs sont continuellement susceptibles de voir leur spambots et leurs serveurs de spams interrompus. Pour y remédier, ceux-ci cherchent activement à couvrir leurs traces.

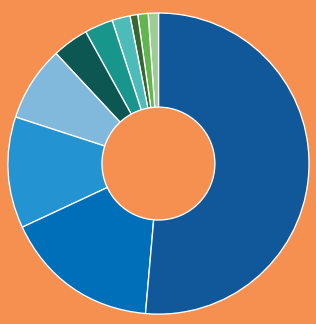
En 2013, beaucoup de spammeurs ont utilisé des techniques de "snowshoe", que nos filtres antispam sont heureusement capables de détecter. Le terme "snowshoe" (en français : raquette à neige) fait allusion au fait que les spammeurs répartissent leur charge sur une surface plus large pour l'empêcher de s'enfoncer.

Les spammeurs qui emploient cette technique distribuent donc leurs messages vers de nombreux adresses IP, sites Web et sous-réseaux. Certains inondent une seule adresse IP avant de passer à une autre adresse, souvent dans le même secteur géographique. Ces stratégies tentent de contourner les systèmes de détection basés sur les gros volumes utilisés par les hébergeurs de messagerie, et profitent des failles du CAN-SPAM Act de 2003, la loi anti-spam américaine.[51]
Le spam snowshoe constitue une grande majorité des courriels indésirables dans les entreprises qui ne sont pas équipées d'un système de filtrage fiable.

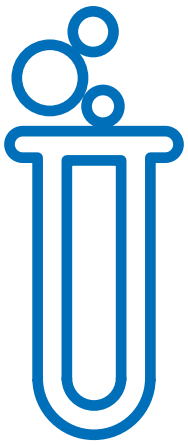
Juin 2013 : le spam en pièce jointe, ou comment télécharger une montagne d'ennuis

En juin 2013, Fareit et Andromeda étaient les deux principaux malwares distribués en pièce jointe. Fareit (également connu sous les noms Pony ou Ponik) télécharge souvent Zeus en P2P, mais recueille également des mots de passe stockés dans les logiciels de messagerie et les clients FTP. Andromeda télécharge d'autres malwares tels que Zeus en P2P, des spambots et ZeroAccess, et parfois aussi ses propres modules afin d'infecter les partages réseau et les périphériques portables.

Fareit	52%	Donx	4%	DarkComet	1%
Andromeda	17%	Bublik	3%	Banload	1%
Zbot	12%	Ransomware	2%		
Dofoil	8%	DnetBckdr	1%		



NB : les pourcentages sont arrondis à l'unité supérieure
Source : SophosLabs



SophosLabs : comment garder une longueur d'avance sur les attaques les plus complexes de notre époque

A mesure que les attaques de malwares deviennent plus complexes et discrètes, les éditeurs de sécurité doivent faire preuve de plus d'intelligence, de flexibilité et de rapidité. C'est précisément ce que font les SophosLabs.

Autrefois, les éditeurs de sécurité détectaient les malwares en identifiant les signatures des logiciels malveillants. Les criminels pouvaient donc facilement éviter la détection en créant des attaques polymorphes qui généraient des malwares uniques pour chaque ordinateur ciblé.

Certaines attaques polymorphes sont faciles à éviter. Le filtrage de la messagerie par exemple peut dans la majorité des cas bloquer les attaques distribuées en pièce jointe. Mais aujourd'hui, les attaques les plus dangereuses sont composées d'une multitude d'éléments complexes répartis sur l'intégralité du Web. Et comme ce rapport l'explique, les criminels adoptent désormais des techniques puissantes pour résister à la détection.

La meilleure solution est de les contrer avec une protection multi-niveaux. Nous investissons beaucoup d'efforts dans la détection et le blocage des sites qui hébergent des kits d'exploits et du contenu malveillant. Nous avons construit différents niveaux de détection destinés à détecter des composants spécifiques des kits d'exploits, tels que les redirections de JavaScript camouflé, les Java JARs piratés et les documents infectés. Bien qu'aucun niveau ne puisse offrir une protection intégrale à lui seul, ensemble, ils sont très efficaces.

En savoir plus
Les SophosLabs

Nous développons également des protections encore plus robustes, basées entre autres sur la détection selon le contexte, qui analyse simultanément les informations sur les fichiers en cours de téléchargement et les sites d'où ils proviennent. Pris séparément, un fichier ou une source ne suffisent pas à diagnostiquer une menace. En revanche, l'association des deux informations peuvent révéler des comportements subtils associés à des menaces connues, ce qui active notre logiciel sans risquer d'occasionner de faux positifs.

Un dernier niveau de protection, la détection en cours d'exécution, couvre les rares éventualités où le malware réussirait à déjouer les autres défenses. Nous guettons les signes d'un malware en cours d'exécution. Nous recherchons les comportements suspects des programmes. Nous comparons ces informations avec les résultats d'analyses précédentes du fichier exécutable en question. Par exemple, un fichier qui avait éveillé de légers soupçons au téléchargement pourrait se comporter de manière encore plus suspecte par la suite. Ceci entraînerait son blocage.

Les nouvelles versions de notre appliance de sécurité réseau utilisent les mêmes techniques pour bloquer les périphériques qui montrent des signes d'infection, tels que les appareils agissant comme s'ils étaient sous le contrôle d'un botnet. Sophos UTM 9.2 inspecte les paquets réseau, identifie les machines qui tentent de se connecter à des domaines illicites, et reconnaît les fichiers de configuration malveillants transmis via HTTP depuis les botnets vers les machines infectées.

Comme les serveurs de C&C et les malwares évoluent à vitesse fulgurante, les produits Sophos distribuent des mises à jour instantanées "in-the-cloud".

Les SophosLabs traitent d'importantes quantités de données pour garder une longueur d'avance sur les cybercriminels. Nous recueillons tous les jours des milliards de données sur des ordinateurs aux quatre coins du globe. Notre infrastructure ultra-sophistiquée nous permet d'analyser ces données et d'identifier les menaces émergentes dans les délais les plus brefs, en corrélant toutes les données qui nous parviennent des machines et des serveurs protégés. Elle nous permet également de développer une meilleure protection en recueillant les fichiers binaires, les URL et la télémétrie.

Pour ceux d'entre vous qui ont des connaissances techniques, notre infrastructure est basée sur Hadoop. Ce logiciel open source s'inspire d'idées lancées par Google et Yahoo, idéales pour les entreprises telles que Facebook, Twitter, eBay, et Sophos, qui ont d'importantes quantités de données à analyser rapidement.

Tendances à suivre en 2014

Par les SophosLabs

Entre des avancées technologiques considérables et la polémique qui a entouré la NSA, l'année 2013 a été haute en évènements pour les observateurs de tendances. L'analyse de tous ces évènements nous a permis d'en extraire les tendances de l'année à venir.

Attaques sur les données professionnelles et privées dans le Cloud

Les services dans le Cloud, où de plus en plus d'entreprises gèrent désormais leurs données client, leurs projets internes et leurs biens financiers, jouissent d'une popularité croissante. Nous nous attendons donc à voir émerger une multitude d'attaques contre les ordinateurs, les périphériques mobiles et les identifiants de connexion, visant à accéder aux Clouds d'entreprise et privés.

Bien que l'on ne puisse pas prédire de manière absolue la forme que prendront ces attaques, il est fort probable qu'il s'agisse entre autres de ransomwares qui prendront en otage les données et les documents locaux hébergés dans le Cloud. Ces attaques ne chiffreront pas forcément les données mais pourraient prendre la forme de chantage, en menaçant l'utilisateur de divulguer ses données confidentielles s'il ne paie pas.

Il sera plus important que jamais d'utiliser un mot de passe solide et de bonnes politiques concernant l'accès aux données stockées dans le Cloud. Votre sécurité repose entièrement sur votre maillon le plus faible, soit vos machines Windows ou l'attitude de vos employés envers la sécurité.

Techniques de menaces persistantes avancées au service du détournement de fonds

Nous nous attendons à voir les groupes de détourneurs de fonds améliorer leurs techniques en s'inspirant du succès des menaces persistantes avancées dans le domaine de l'espionnage industriel. Ces techniques sont déjà utilisées au service de la distribution de malwares.

En savoir plus
Ingénierie sociale

Plus les éditeurs de sécurité progressent dans les niveaux de protection, la sécurité des systèmes d'exploitation et la sensibilisation des utilisateurs, plus les cybercriminels sont forcés de rentabiliser au maximum chacune de leurs opérations. Il est donc possible que les attaques futures soient composées de plusieurs éléments et méthodes de distribution, conçues pour cibler un public plus restreint. Les malwares adopteront en tous cas de plus en plus de particularités des APT en 2014.

Les malwares pour Android, de plus en plus complexes, chercheront de nouvelles cibles
En 2013, nous avons assisté à la croissance exponentielle des malwares pour Android, non seulement en termes de nombre de familles différentes et d'échantillons, mais aussi en termes de nombre d'appareils frappés sur l'ensemble du globe.

Bien que les nouvelles fonctionnalités de sécurité d'Android fassent progressivement réduire les taux d'infection, il faudra longtemps avant qu'elles ne soient adoptées unanimement, laissant de nombreux utilisateurs à la merci des attaques d'ingénierie sociale. Les cybercriminels continueront à explorer de nouvelles voies pour monétiser les malwares pour Android. Bien que leurs options soient plus limitées sur cette plate-forme que sur Windows, les appareils mobiles offrent l'avantage non négligeable de pouvoir servir de base de lancement pour des attaques visant les réseaux sociaux et les plates-formes dans le Cloud.

Pour réduire les risques d'infection, imposez donc une politique de BYOD ("bring your own device" ou "apportez votre propre périphérique") visant à bloquer le chargement d'applications mobiles depuis des sources inconnues et à imposer une protection antimalware.

Les malwares se diversifient et se spécialisent
Les différents types de malwares à caractère financier reflètent la diversité des secteurs géographiques et des régions économiques d'où ils proviennent. Nous distinguons des techniques d'ingénierie sociale, des options de monétisation des malwares et des objectifs différents selon les pays. Les malwares adaptés à des publics différents (par exemple le grand public et les entreprises) continueront à croître en 2014. Nous verrons vraisemblablement apparaître des attaques conçues spécialement pour s'attaquer à différents degrés de défense ou de valeur cibles.

Les données personnelles en danger sur les applications mobiles et les réseaux sociaux
La sécurité des mobiles en général continuera à faire couler de l'encre en 2014. L'adoption croissante de nouvelles applications de communication personnelles et professionnelles élargit la surface d'attaque pour les arnaques basées sur l'ingénierie sociale et les tentatives d'exfiltration de données. Votre carnet d'adresses et votre graphique de connexions sociales sont précieux aux yeux des cybercriminels en tous genres. Veillez donc à les protéger comme il se doit, grâce au contrôle des applications mobiles et Web pour les professionnels.

Les cyberdéfenses en ligne de mire
Dans la lutte interminable entre cybercriminels et éditeurs de sécurité, nous nous attendons à voir apparaître de nouvelles armes destinées à tester les derniers mécanismes de cyberdéfense. Les services de réputation, les bases de données pour la sécurité du Cloud, les listes blanches et les couches de sandboxing feront tous l'objet de nouvelles attaques. Il y aura plus de malwares comportant des signatures volées; de tentatives de compromettre les données de sécurité, les analyses télémétriques, la détection en environnement sandbox et les techniques de contournement; et une utilisation plus répandue d'outils légitimes à des fins malveillantes.

Des malwares 64-bits
Avec l'adoption croissante des systèmes d'exploitation 64-bits, nous nous attendons à rencontrer plus de malwares destinés exclusivement à ces systèmes.

Les kits d'exploits restent la principale menace pour Windows

Bien que les récentes améliorations du système d'exploitation Windows placent la barre un peu plus haut pour les développeurs d'exploits, Microsoft n'a pas encore gagné la guerre.

Avec l'arrêt de ses mises à jour de sécurité, Windows XP est en passe de devenir une cible de choix pour les cybercriminels. Quelles sont les chances que Windows 7 domine le panorama des systèmes d'exploitation pendant aussi longtemps ? Combien de temps faudra-t-il pour que la majorité des machines passent à des versions plus récentes de Windows, dotées de meilleures fonctionnalités de sécurité ?

Bien que la distribution de menaces reposant sur une interaction avec l'utilisateur (ingénierie sociale) continue à être un vecteur important d'infection, les auteurs de malwares devront affiner leurs techniques pour inciter leurs victimes à exécuter la charge malveillante, car les utilisateurs sont devenus plus habiles dans l'art de distinguer entre le malveillant et le bénin. Les criminels devront donc créer des leurres plus ciblés et plus convaincants.

Le matériel, l'infrastructure et les logiciels compromis à la source

Plusieurs évènements cette année (comme les révélations concernant l'espionnage mené par le gouvernement et certaines entreprises, ainsi que l'existence de portes dérobées) ont prouvé que la vaste infrastructure sur laquelle nous opérons tous est non seulement susceptible d'être compromise, mais qu'elle l'est déjà actuellement. Il sera donc essentiel de réévaluer les technologies et les entités auxquelles nous confions nos données.

Les découvertes de 2013 ne sont probablement que le sommet de l'iceberg, et il est possible que d'autres révélations de ce genre fassent l'actualité en 2014. La plupart des entreprises n'ont pas la possibilité ou les ressources de rechercher des portes dérobées : suivez donc de près le travail des chercheurs en sécurité et la presse spécialisée pour plus d'informations.

Le piratage se généralise

Nous utilisons de nos jours de plus en plus d'appareils différents, tous susceptibles de contenir des données professionnelles confidentielles. Mais les technologies de sécurité conçues pour ces appareils ne sont pas aussi bien développées que celles de l'environnement PC.

Pour ceux qui souhaitent nous nuire, les périphériques intégrés dans les maisons, les bureaux et même les villes, sont des cibles intéressantes. Et les nouvelles monnaies et moyens de paiement électroniques sont tout aussi attrayants que les cartes de crédit.

Nous ne nous attendons pas à des attaques importantes contre "l'Internet des objets" en 2014, mais nous prévoyons une augmentation des vulnérabilités et des exploits de type "preuve-de-concept".

En conclusion

Les créateurs de malwares, de kits d'exploits et de botnets ont fait preuve de plus d'efficacité et d'agressivité en 2013. Ils ont développé de nouvelles formes d'attaques et de techniques de camouflage, ont identifié de nouvelles cibles et ont remis d'anciennes approches au goût du jour.

Ces nouvelles attaques vont exiger plus d'intelligence de la part de tous pour s'en défendre. Sophos travaille sans relâche pour concevoir des méthodes de détection plus sophistiquées, livrant des mises à jour en temps réel depuis le Cloud et permettant de protéger tous les périphériques nouvelle génération que vous, ou vos utilisateurs, choisissez d'adopter.

Que vous soyez un professionnel de l'informatique, un entrepreneur ou un utilisateur individuel, il y a de grandes chances que vos connaissances en matière de sécurité s'améliorent constamment. Veillez à protéger tous vos systèmes quelle que soit la plate-forme utilisée. Réduisez la surface d'attaque en supprimant les plates-formes telles que Java lorsque vous ne les utilisez pas. Installez systématiquement tous les correctifs, car la plupart des attaques ciblent les anciennes vulnérabilités. Ne négligez jamais le b.a.-ba de la sécurité : utilisez des mots de passe solides, apprenez à vos utilisateurs comment déjouer les pièges de l'ingénierie sociale, etc.

La lutte contre les cybercriminels n'est pas prête de s'arrêter, mais si vous restez vigilent, appliquez les meilleures pratiques en matière de sécurité, faites un usage intelligent des technologies et vous armez du meilleur soutien, vous réussirez à protéger votre entreprise. Chez Sophos, nous avons tout ce qu'il faut pour vous aider et restons à votre entière disposition.

Sources (en anglais)

1. ZeuS-P2P Monitoring and Analysis, v2013-06, NASK/CERT Polska, http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf
2. An Analysis of the Zeus Peer-to-Peer Protocol, Dennis Andriesse and Herbert Bos, VU University Amsterdam, The Netherlands, Technical Report IR-CS-74, rev. May 8, 2013, http://www.few.vu.nl/~da.andriesse/papers/zeus-tech-report-2013.pdf
3. Symantec Uses Vulnerability to Take Out Part of the ZeroAccess Botnet, CSO, http://www.csoonline.com/article/740626/symantec-uses-vulnerability-to-take-out-part-of-the-zeroaccess-botnet
4. CryptoLocker Ransomware - See How It Works, Learn about Prevention, Cleanup and Recovery, Sophos Naked Security, http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
5. Destructive Malware "CryptoLocker" on the Loose - Here's What to Do, Sophos Naked Security, 12 October 2013, http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/
6. With Carberp Source Code's Release, Security Pros Expect the Worst, CSO Online, 27 June 2013, http://www.csoonline.com/article/735569/with-carberp-source-code-s-release-security-pros-expect-the-worst
7. Carberp: The Never Ending Story, We Live Security, 25 March 2013, http://www.welivesecurity.com/2013/03/25/carberp-the-never-ending-story/
8. Shylock Financial Malware Back and Targeting Two Dozen Major Banks, ThreatPost, 18 September 2013, http://threatpost.com/shylock-financial-malware-back-and-targeting-two-dozen-major-banks
9. Cyber-thieves Blamed for Leap in Tor Dark Net Use, BBC News, 6 September 2013, http://www.bbc.co.uk/news/technology-23984814
10. Bitcoincharts.com, http://bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv
11. Back Channels and Bitcoins: ZeroAccess' Secret C&C Communications, James Wyke, Senior Threat Researcher, SophosLabs, Virus Bulletin, October 2013, http://www.sophos.com/en-us/medialibrary/PDFs/technical papers/Wyke-VB2013.pdf
12. The Delicate War Between Bitcoin Miners and Botnet Miners, Red Orbit, 28 March 2013, http://www.redorbit.com/news/technology/1112812519/bitcoin-miners-versus-botnet-miners-032813/
13. Botcoin: Bitcoin Mining by Botnet, Krebs on Security, 18 July 2013, http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/
14. GinMaster: A Case Study in Android Malware, Rowland Yu, SophosLabs Australia, Virus Bulletin, October 2013, http://www.virusbtn.com/pdf/conference_slides/2013/Yu-VB2013.pdf
15. Billion Dollar Botnets, Cathal Mullaney, Symantec, presented at Virus Bulletin, October 2013, http://www.virusbtn.com/conference/vb2013/abstracts/Mullaney.xml
16. Hey Android, Are You Frightened of FakeAV plus Ransomware? Rowland Yu, SophosLabs, October 2013
17. Revealed! The Top Five Android Malware Detected in the Wild, Graham Cluley, Sophos Naked Security, 14 June 2012, http://nakedsecurity.sophos.com/2012/06/14/top-five-android-malware/
18. Qadars: A New Banking Malware With a Fraudulent Mobile Application Component, 2 October 2013, http://www.lexsi-leblog.com/cert-en/qadars-new-banking-malware-with-fraudulent-mobile-application-component.html
19. Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html
20. Graphic inspired by The Scrap Value of a Hacked PC, Revisited, Krebs On Security, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/
21. CVE Details: WordPress Vulnerabilities, http://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/
22. Hacker Publishes Alleged Zero-Day Exploit for Plesk, Parity News, 6 June 2013, http://www.paritynews.com/2013/06/06/1112/hacker-publishes-alleged-zero-day-exploit-for-plesk/
23. Exclusive: Apple, Macs Hit by Hackers Who Targeted Facebook, Reuters, 19 February 2013, http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219
24. Microsoft Also Victim of Recent Watering Hole Attack, Help Net Security, 25 February 2013, https://www.net-security.org/secworld.php?id=14482
25. Mac Backdoor Trojan Embedded Inside Boobytrapped Word Documents, Sophos Naked Security, 30 March 2012, http://nakedsecurity.sophos.com/2012/03/30/mac-malware-backdoor/
26. Chinese Uyghur Dissidents Targeted by Mac Malware, Ben Weitzenkorn, TechNewsDaily, 15 February 2013, http://www.technewsdaily.com/16937-china-uyghur-attacks.html
27. New Mac Trojan Discovered Related to Syria, Intego, 17 September 2013, http://www.intego.com/mac-security-blog/new-mac-trojan-discovered-related-to-syria/
28. Mac Spyware: OSX/KitM (Kumar in the Mac), F-Secure, 22 May 2013, http://www.f-secure.com/weblog/archives/00002558.html
29. New Signed Malware Called Janicab, http://www.thesafemac.com/new-signed-malware-called-janicab/
30. OSX/FkCodec-A, Detailed Analysis, Sophos, 11 June 2013, https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/OSX~FkCodec-A/detailed-analysis.aspx
31. FBI Ransomware Now Targeting Apple's Mac OS X Users, Malwarebytes, 15 July 2013, http://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/
32. Apple Gets Aggressive - Latest OS X Java Security Update Rips Out Browser Support, Paul Ducklin, Sophos Naked Security, 18 October 2012, http://nakedsecurity.sophos.com/2012/10/18/apple-gets-aggressive-latest-os-x-java-security-update-rips-out-browser-support/
33. Apple Ships OS X 10.8.5 Security Update - Fixes "sudo" Bug At Last, Paul Ducklin, Sophos Naked Security, 13 September 2013, http://nakedsecurity.sophos.com/2013/09/13/apple-ships-os-x-10-8-5-security-update-fixes-sudo-bug-at-last/
34. Rampant Apache Website Attack Hits Visitors With Highly Malicious Software, Ars Technica, 3 July 2013, http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/
35. Rogue Apache Modules Pushing Iframe Injections Which Drive Traffic to Blackhole Exploit Kit, Fraser Howard, Sophos Naked Security, 5 March 2013, http://nakedsecurity.sophos.com/2013/03/05/rogue-apache-modules-iframe-blackhole-exploit-kit/
36. Blackhole Malware Toolkit Creator 'Paunch' Suspect Arrested, ZDNet, 9 October 2013, http://www.zdnet.com/blackhole-malware-toolkit-creator-paunch-arrested-7000021740/
37. Blackhole Exploit Kit Author Arrested in Russia, ComputerWorld, 8 October 2013, http://www.computerworld.com/s/article/9243061/Blackhole_exploit_kit_author_arrested_in_Russia
38. Lifting the Lid on the Redkit Exploit Kit, Fraser Howard, Sophos Naked Security, 3 May 2013, http://nakedsecurity.sophos.com/2013/05/03/lifting-the-lid-on-the-redkit-exploit-kit-part-1/
39. The Four Seasons of Glazunov: Digging Further into Sibhost and Flimkit, Fraser Howard, Sophos Naked Security, 2 July 2013, http://nakedsecurity.sophos.com/2013/07/02/the-four-seasons-of-glazunov-digging-further-into-sibhost-and-flimkit/
40. Hide and Seek - How Targeted Attacks Hide Behind Clean Applications, Gabor Szappanos, SophosLabs Hungary, October 2013, Virus Bulletin, http://www.virusbtn.com/conference/vb2013/abstracts/LM1-Szappanos.xml
41. Plugx "Malware Factory" Celebrates CVE-2012-0158 Anniversary with Version 6.0, Gabor Szappanos, Principal Researcher, SophosLabs, May 2013, http://sophosnews.files.wordpress.com/2013/05/sophosszappanosplugxmalwarefactoryversion6-rev2.pdf
42. The Windows DLL Loading Security Hole, Dr Dobbs Journal, 9 September 2010, http://www.drdobbs.com/windows/the-windows-dll-loading-security-hole/227400009
43. NetMarketShare, http://www.netmarketshare.com/
44. Windows XP SP3 and Office 2003 Support Ends April 8, 2014, Microsoft, http://www.microsoft.com/en-us/windows/endofsupport.aspx
45. The Risk of Running Windows XP After Support Ends, Tim Rains, Microsoft Security Blog, April 2014, http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx
46. Windows XP End of Life Affects PCI Compliance, Credit Card Processing Space, 6 March 2013, http://www.creditcardprocessingspace.com/windows-xp-end-of-life-affects-pci-compliance/
47. Windows XP End-of-Life Could Cripple PCI Compliance, Walter Conway, 6 February 2013, Storefront Backtalk, http://storefrontbacktalk.com/securityfraud/windows-xp-end-of-life-could-cripple-pci-compliance/
48. Dexter Malware Targeting Point-of-Sale (POS) Systems, Visa Data Security Alert, December 2012, http://usa.visa.com/download/merchants/alert-dexter-122012.pdf
49. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks, U.S. Food and Drug Administration, 13 June 2013, http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm
50. Computer Viruses Are "Rampant" on Medical Devices in Hospitals, MIT Technology Review, 17 October 2012, http://m.technologyreview.com/computing/41511/
51. Following the Tracks: Understanding Snowshoe Spam, Brett Cove, SophosLabs, http://sophosnews.files.wordpress.com/2011/10/vb2011-snowshoe2.pdf

Équipe commerciale France :
Tél. : 01 34 34 80 00
Courriel : sales@sophos.fr

Oxford (Royaume-Uni) | Boston (États-Unis)

1091-11.13DD fr-simple

SOPHOS