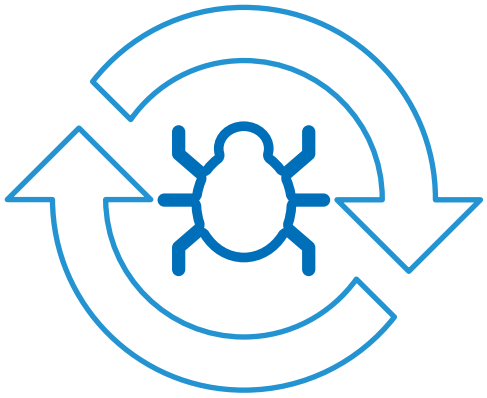
SOPHOS
Security made simple.

Menaces à la sécurité : quelles tendances pour 2015 ?

Nos prédictions pour la cybersécurité en 2015 et au delà

Par James Lyne, Responsable mondial de la recherche en sécurité, Sophos



La cybersécurité en 2015

La cybersécurité est en essor rapide, non seulement en tant qu'industrie, mais également comme sujet de préoccupation quotidien pour les utilisateurs, aussi bien professionnels que simples particuliers. Et pour cause : les risques d'infection évoluent tout aussi rapidement que la technologie, les criminels recherchant sans cesse de nouvelles façons d'exploiter la vulnérabilité des utilisateurs et des systèmes.

A cette période de l'année, il est de coutume de faire des prédictions concernant les évolutions des technologies et des menaces qui méritent votre attention durant l'année à venir. Certaines ne se manifesteront peut-être que bien plus tard, mais beaucoup commencent déjà à produire leurs effets. Il est en tous les cas utile de surveiller les tendances émergentes en matière de cybersécurité, et nous en avons retenu 10 qui auront selon nous un impact notable en 2015 et au-delà.

SOPHOS
Security made simple.

Pour accéder à des ressources supplémentaires rendez-vous sur
sophos.fr

De nouvelles mesures de prévention réduiront le nombre de vulnérabilités exploitables

Depuis de nombreuses années, les cybercriminels profitent des exploits pour discrètement déployer leur code malveillant. Alors qu'autrefois les menaces étaient principalement diffusées par des messages de spam, aujourd'hui la majorité des infections provient d'attaques Web et de vulnérabilités des navigateurs. Heureusement, Microsoft a mobilisé des ressources considérables pour mettre en place des mesures de prévention des risques. Parmi celles-ci se démarquent la protection PED (Protection de l'exécution des données, ou DEP en anglais), conçue pour bloquer l'exécution de code malveillant dans certaines parties de la mémoire de l'ordinateur, et l'ASLR (randomisation du format d'espace d'adresse), qui complique l'écriture de code malveillant en distribuant l'espace d'adressage de manière aléatoire. Il existe de nombreuses autres améliorations dans Windows 8 et 8.1 sur lesquelles vous pourrez vous informer en ligne si vous souhaitez en savoir plus.

Plus la distribution de code malveillant devient difficile, plus la valeur marchande des vulnérabilités d'applications et de plates-formes prisées telles qu'Internet Explorer et Windows 7 augmente, donnant lieu à un début de changement dans le comportement des cybercriminels. Ceci nous permet d'effectuer un certain nombre de prédictions sur les tendances à suivre. Les informations concernant les vulnérabilités majeures sont vendues pour mener des attaques plus ciblées et déployées de manière plus sélective, laissant moins d'options à beaucoup de cybercriminels.

Nous constatons par conséquent un retour à l'ingénierie sociale, avec des techniques toujours plus efficaces à mesure que les cybercriminels innovent dans le domaine des charges virales. Ceux-ci concentreront peut-être également plus d'efforts sur des plates-formes autres que celles de Microsoft, moins bien protégées. Sachez également qu'un grand nombre d'utilisateurs continueront d'utiliser des plates-formes plus anciennes telles que Windows XP. La mise en place des nouvelles techniques de protection citées plus haut a entraîné une augmentation massive de la valeur des exploits sur le marché noir, et poussé cette industrie illicite à encore davantage de discrétion. En 2015, restez donc attentifs aux techniques d'ingénierie sociale, plus simples et néanmoins efficaces. N'hésitez pas à revoir votre stratégie d'installation des correctifs et vos processus de maîtrise des systèmes non-Microsoft.

Les attaques ciblant l'Internet des Objets passeront du stade de prototypes à celui de risques bien réels

En 2014, nous avons constaté que les fabricants d'équipements connectés (l'Internet des Objets) n'ont pas mis en œuvre le minimum de sécurité indispensable, preuve qu'ils n'ont rien appris des douloureuses erreurs passées de l'industrie informatique, ou les ont tout simplement ignorées dans leur hâte de gagner des parts de marché.

J'ai moi-même piraté des routeurs sans-fil au moyen d'attaques Web telles que l'injection SQL, des caméras de vidéosurveillance sans dispositif de verrouillage et des bornes WiFi sans identifiants de connexion, entièrement ouvertes sur le réseau. Ces failles ont fait l'objet d'une multitude de conférences dans le domaine de la sécurité sans pour autant jusqu'à présent susciter un intérêt notable de la part des cybercriminels. Attendons-nous donc à rencontrer des attaques plus sérieuses en dehors des exploits de type "preuve de concept" qu'étudient actuellement les chercheurs en sécurité.

Faute d'implémenter des protections plus robustes, les attaques ciblant les appareils de grande consommation pourraient avoir des conséquences de grande envergure. Il est crucial que l'industrie de la sécurité informatique évolue pour inclure ces appareils, que leurs fabricants reconnaissent enfin l'importance de la sécurité (comme Microsoft a dû le faire par le passé) et que les utilisateurs prennent conscience du problème afin que la sécurité devienne une exigence commerciale et non une pensée après-coup.

Il est par ailleurs possible que les cybercriminels aient jusqu'à présent négligé l'Internet des Objets, n'ayant pas encore trouvé de modèle leur permettant d'en profiter financièrement. Mais plus l'usage de ces appareils se diversifiera, plus le risque de piratage deviendra présent; et au rythme d'évolution technologique actuel, les fabricants n'auront vraisemblablement pas le temps de sécuriser les appareils avant que les attaques ne commencent à déferler. Pire encore, et contrairement à Microsoft, ces fabricants d'objets connectés ne disposeront peut-être pas de l'infrastructure nécessaire pour distribuer des correctifs en temps voulu.

Le chiffrement deviendra une pratique courante, mais tout le monde ne s'en réjouira pas

En 2013, nous avions prédit que le chiffrement intégral deviendrait la pratique par défaut des éditeurs de systèmes d'exploitation et de solutions de sécurité. Cette tendance s'est réalisée en grande partie.

Le chiffrement est devenu une pratique largement courante en raison d'une préoccupation généralisée pour la sécurité et la confidentialité, causée par la médiatisation d'une multitude d'incidents d'espionnage et de fuites de données.

Par exemple, de nombreuses applications Android effectuent le chiffrement local des données sur le périphérique, ainsi que lorsqu'elles se connectent à Internet. Ce nombre a considérablement augmenté au cours des deux dernières années : c'est une grande réussite dans le domaine de la sécurité.

Malheureusement, bien que beaucoup des applications concernées utilisent SSL (entre autres), très peu d'entre elles l'implémentent correctement. La plupart n'utilisent pas le "certificate pinning", réduisant par conséquent l'efficacité du chiffrement. La différence entre un chiffrement réellement efficace et un chiffrement "de façade" est certes dans les détails, mais il faut bien dire que le chiffrement de la plupart des applications n'est pas entièrement fiable.

De plus en plus d'entreprises et de particuliers souhaitent chiffrer les données transférées vers le Cloud depuis un PC ou un mobile, et il est crucial que ceux-ci posent des questions plus précises que simplement « est-ce que c'est chiffré ? ». Les normes et les processus d'audit ne suffisent pas toujours à vérifier tous les détails, comme dans le cas de DES, jugé insuffisant bien trop tard.

En attendant, certains services de police et de surveillance s'opposent au chiffrement généralisé des données, argumentant que celui-ci pourrait avoir un effet inverse sur la sécurité. Bien que ceux-ci avancent indubitablement un argument de taille, il ne serait pas raisonnable de sacrifier la confidentialité des données pour simplement satisfaire des objectifs de surveillance en vue de vérifier l'application des lois.

Le chiffrement soulève un problème intéressant pour les fournisseurs de solutions de sécurité réseau indépendants, car le trafic chiffré ne peut pas être intercepté et analysé au niveau des passerelles. Il est donc fortement probable que ceci fasse changer la manière dont les éditeurs protègent les réseaux dans les années à venir.

Des failles importantes dans des logiciels très répandus seront découvertes, après avoir échappé à la vigilance des éditeurs de sécurité ces 15 dernières années

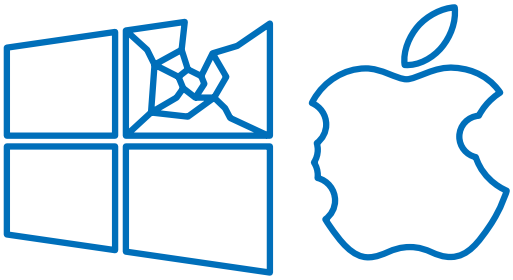
Nous avons assisté cette année à la découverte d'un nombre de bugs considérables sur des plates-formes non Microsoft, pourtant surveillées par de nombreux acteurs du domaine de la sécurité. De Heartbleed à Shellshock, il est devenu évident que des portions importantes de code instable sont présentes dans de nombreux systèmes actuels.

De nombreux utilisateurs ont été choqués de découvrir que le projet OpenSSL, à l'origine de logiciels extrêmement courants et intégrés à plus d'endroits que l'on ne s'imagine, ne disposait pas toujours des ressources nécessaires pour effectuer des audits et des vérifications de code adéquats.

Bien que la plupart de ces défauts n'atteindront vraisemblablement pas la même sévérité que ceux rencontrés en 2014, ils représentent tout de même un défi intéressant pour les entreprises. Celles-ci ont développé et mis en place des protocoles pour distribuer les correctifs ou gérer les risques présents sous Windows, mais pas pour les autres plates-formes, comme on a pu le constater par la lenteur de leur réactivité à Heartbleed. De nombreuses marques sont encore vulnérables plusieurs mois après que l'affaire ait été exposée par la presse.

Malheureusement, je ne suis pas sûr que l'incident ait servi de leçon aux entreprises. Les utilisateurs des systèmes non Microsoft risquent donc d'être exposés longtemps à d'autres vulnérabilités que l'on n'a pas encore découvertes.

Les évènements de 2014 ont accru l'intérêt des criminels pour les plates-formes et logiciels moins courants. Préparez votre stratégie de sécurité dès maintenant. La plupart des procédures en place actuellement devront être modifiées.



De nouvelles réglementations obligeront à divulguer plus de cas d'atteintes au traitement des données, particulièrement en Europe

La législation évolue lentement par rapport aux technologies et à la sécurité informatique, mais des changements majeurs du cadre législatif sont sur le point d'être mis en place. Après des années de discussions autour de sujets tels que la divulgation obligatoire des fuites de données, les officiers de protection des données et les sanctions financières en cas de non-conformité, l'Union Européenne prévoit l'adoption d'une nouvelle règlementation bien plus sévères courant 2015, qui entrera en application à partir de 2016.*

Des sondages récents recueillis en Europe révèlent que la majorité des entreprises ignorent l'existence des changements prévus, en dépit du fait que ceux-ci introduiraient la possibilité de sanctions financières pouvant aller jusqu'à 100 millions d'Euros ou 5% du chiffre d'affaires mondial annuel pour des non-conformités en matière de protection des données à caractère personnel. 77% des personnes interrogées ignoraient même si leur entreprise était conformes aux normes actuelles, sans parler des normes à venir. Il est probable que ces changements déclencheront la mise à niveau de règlements concernant la protection des données dans d'autres juridictions.

Les lois concernant le cybercrime par exemple présentent des problèmes de taille : celles-ci sont implémentées au niveau national alors que le cybercrime est un problème international. Les limitations et la pertinence de lois nationales telles que l'acte CFAA (Computer Fraud and Abuse Act) aux États-Unis, et ses équivalents internationaux, risquent de susciter de plus en plus de plaintes en 2015. Il n'en reste pas moins qu'une approche plus globale n'est pas prévue dans un avenir proche.

***Cette règlementation n'en étant encore qu'à l'état de projet, les délais et l'étendue de celle-ci sont susceptibles de changer. Il est toutefois très probable que celle-ci soit adoptée telle quelle.**

Les pirates prendront pour cible de plus en plus les systèmes de paiement mobile, même si les systèmes de paiement traditionnels resteront encore leurs cibles de prédilection

Les systèmes de paiement mobiles ont fait beaucoup parler d'eux en 2014 avec le lancement d'Apple Pay. Ces nouveautés feront sans aucun doute l'objet d'inévitables erreurs d'implémentation. La première proposition d'Apple semble néanmoins offrir plus de convivialité et une meilleure sécurité que la plupart des systèmes par cartes de paiement, surtout aux États-Unis où les protections anti-fraude sont plutôt archaïques.

Les cybercriminels seront donc à la recherche de failles dans ces systèmes, même si les versions actuelles sont dotées de fonctions de sécurité très pertinentes : des équipements conçus pour empêcher l'extraction d'informations; une authentification par code confidentiel, mot de passe ou empreinte digitale (plus fiable qu'une signature); un jeton représentant l'autorisation de l'utilisateur (ceci évite que les pirates ne volent l'équivalent d'un numéro de carte bleue qu'ils peuvent utiliser à répétition, même s'ils parviennent à s'infiltrer dans le portefeuille électronique de l'utilisateur).

Il va sans dire que ces systèmes de paiement sont bien plus fiables qu'une carte, facile à reproduire. Les fuites telles que celle subie récemment par le spécialiste de la grande distribution Target prouvent la vulnérabilité des systèmes utilisés à l'heure actuelle aux États-Unis. Les nouveaux systèmes seront plus résistants au vol. Attendons-nous donc à ce que les cybercriminels continuent à abuser des cartes de paiement traditionnelles pendant encore longtemps. De notre côté, nous continuerons à vous informer des faiblesses dans les nouveaux systèmes et des nouvelles tactiques de piratage conçues pour en tirer profit.

7

Le déficit de compétences continuera de s'accroître : les capacités de réponse aux incidents et l'éducation resteront les premières priorités

De plus en plus d'attaques et de fuites de données sont couvertes dans la presse, une tendance qui ne semble pas près de ralentir. A mesure que la législation changera, de plus en plus d'entreprises seront forcées d'admettre leurs erreurs publiquement.

Plus la technologie s'impose dans la vie courante et l'économie mondiale, plus les gouvernements et l'industrie reconnaissent un le déficit critique d'expertise en la matière.

L'écart est par ailleurs en augmentation constante; certains gouvernements prédisent même qu'ils ne pourront pas satisfaire la demande en professionnels de la sécurité avant 2030. Étant donné le nombre croissant d'incidents et de fuites à gérer, il y a une forte demande pour ce genre de profil.

Il est donc urgent que l'industrie fasse la promotion des opportunités de carrière existant dans cette filiale et que les entreprises réfléchissent à leur stratégie de recrutement.

Des kits d’exploits et autres services d’attaques verront le jour pour les mobiles (et autres plateformes)

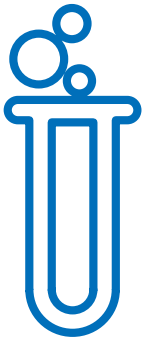
Au cours des dernières années, le monde du cybercrime a vu l'apparition d'une multitude de produits et de services facilitant le piratage et les escroqueries. Certains de ces "crime packs" incluent désormais les plates-formes mobiles, sans pour autant se spécialiser sur ce domaine.

Mais avec la popularité croissante des appareils mobiles (et les données de plus en plus convoitables qu'ils contiennent), des outils de piratage spécifiques ne tarderont pas à voir le jour, et iront peut-être même jusqu'à s'étendre à l'Internet des Objets.

A l'heure actuelle, la plupart des malwares en dehors de Windows visent Android, et se font passer pour des applications légitimes pour inciter l'utilisateur à les installer. Bien que les cybercriminels continueront à utiliser cette technique, le système d'installation des applications validées est plus strict, rendant plus difficile le chargement furtif d'applications malveillantes. On peut s'attendre à ce que les criminels réagissent en développant des exploits pour les plates-formes concernées ainsi que des kits leur permettant de commercialiser et donc de simplifier l'infiltration.

Notons tout de même que les versions plus récentes des logiciels mobiles intègrent des contrôles de sécurité tels que l'ASLR (userland et Kernel) et des fonctionnalités de bac à sable (sandboxing). Bien que ces plates-formes soient loin d'être parfaites et que de nombreux utilisateurs exécutent encore des versions anciennes qui n’intègrent aucune fonctionnalité de sécurité, la mise à jour automatique est de plus en plus courante. Ceci permet de dissuader les attaques contre ces plates-formes : le volume d'exploits est toujours bien plus important pour PC que pour mobile.

Il est donc probable que les cybercriminels continueront à étudier le marché du mobile, et réussiront au cours des deux prochaines années à commercialiser des produits innovants pour l'exploitation de plates-formes autres que le PC.



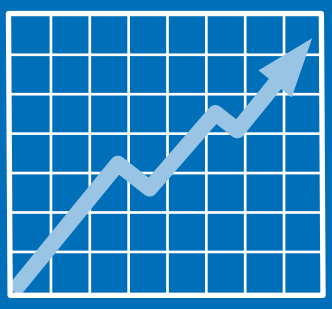
L'écart continuera à se creuser entre le niveau de sécurité des systèmes de contrôle industriels (ICS et SCADA) et celui des environnements informatiques de bureaux ordinaires

Les systèmes de contrôle industriels (ICS) ont typiquement 10 ans de retard sur le niveau de sécurité des environnements informatiques de bureaux ordinaires. Ces plates-formes manquent souvent de processus d'authentification, de chiffrement et de systèmes de vérification. La méthode de protection la plus fiable est de les isoler sur des réseaux séparés.

Malheureusement, il arrive souvent que ces systèmes se retrouvent sur des réseaux ouverts vers l'extérieur : il suffit d'effectuer une analyse avec un outil tel que Shodan pour trouver un nombre surprenant de systèmes de contrôle connectés au Web. Heureusement, ceci n'a pas causé trop d'incidents jusqu'à présent.

Le problème est que la plupart des appareils et éditeurs concernés se sont accoutumés à des critères basés sur la résilience ou le contrôle, et n'ont pas encore acquis les réflexes de sécurité adoptées par d'autres domaines technologiques. Ils ont jusqu'à présent évité les attaques en pratiquant une stratégie d'isolement.

Bien que les plus grands éditeurs de systèmes de contrôle industriels commencent à prendre la sécurité plus au sérieux, l'écart avec les autres domaines technologiques ne fait que croître. Il est probable que des failles plus importantes soient exposées et exploitées par les cybercriminels au cours des années à venir, à mesure que leurs motivations progressent. Ceci entraînera certainement une évolution de la règlementation, un processus qui sera néanmoins long étant donné la complexité, la spécificité et le coût élevés de ces systèmes. Pour résumer, il s'agit d'un domaine à risque au sein duquel la sécurité n'est pas une priorité aussi importante que l'on pourrait le penser.



De nouvelles fonctionnalités dans les rootkits et botnets pourraient engendrer de nouveaux vecteurs d'attaque

La plupart des attaques rencontrées au cours des dernières années se produisaient au niveau de la couche applicative (y compris un grand nombre d'attaques par DDoS qui visaient la couche applicative plutôt que la couche transport). Les principaux protocoles tels que IPv4 sont en usage depuis si longtemps que leurs utilisateurs se sont habitués à leurs faiblesses et défauts de conception. Toutefois de grands changements s'annoncent. Une version entièrement nouvelle d'HTTP (2.0, qui succède à 1.1) arrive, et IPv6 est largement utilisé sans que la plupart des administrateurs ne le sachent.

Les plates-formes et protocoles que nous utilisons depuis des années font actuellement l'objet de changements de fond. Ceux-ci entraîneront sans doute de nouvelles failles que les cybercriminels pourront peut-être exploiter à leur profit. C'est une tendance générale dont nous avons déjà constaté les signes avant-coureurs. Le stack IPv6 de Windows 7 et Windows 8 comporte une vulnérabilité à une attaque par épuisement des ressources dont la plupart des utilisateurs ne connaissent pas l'existence. Celle-ci permet au criminel de monopoliser le processeur en envoyant un flux constant d'annonces aléatoires de routeurs. Avant que Microsoft ne corrige le problème, l'opération pouvait même faire tomber le système.

De façon plus générale, IPv6 réplique certaines failles déjà présentes dans IPv4. Il laisse par exemple la voie libre aux attaques de type "man in the middle" telles que l'infection ARP dans IPv4. Bien qu'il existe en théorie des dispositifs pour éviter ce genre d'attaque, ceux-ci n'ont pas encore été implémentés.

Les modifications matérielles de bas niveau tel que le passage à l'interface UEFI apporteront également leur lot de problèmes potentiels. Grâce à son environnement de démarrage amélioré, UEFI facilite la programmation par rapport à BIOS. En revanche, ce même environnement de démarrage ouvre la porte aux rootkit et aux botnets, et pourrait engendrer de nouveaux vecteurs d'attaque, ou permettre à des attaques existantes de devenir considérablement plus puissantes.

En résumé, il semblerait qu'en déployant ces technologies nous soyons sur le point de répéter les mêmes erreurs qu'auparavant, et nous sommes à l'aube de grands changements dans les normes technologiques. Nous vous tiendrons informés de la résurrection d'anciennes vulnérabilités ou de l'apparition de nouvelles catégories de failles majeures.

Équipe commerciale France :
Tél. : 01 34 34 80 00
E-mail : info@sophos.fr

Équipe commerciale Amérique du Nord :
Téléphone : 1-866-866-2802
E-mail : nasales@sophos.com

Équipe commerciale Benelux :
Tél. : Belgique +32 (0) 16 44 01 35,
Pays-Bas +31 (0) 162 480 240
Courriel : salesbenelux@sophos.com

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

SOPHOS