Connaissez-vous les fichiers Prefetch ?

Que sont les fichiers Prefetch ?

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme.

Un mot sur les fichiers Prefetch

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme sur le système et éventuellement l'emplacement depuis lequel il a été exécuté.
Pour rappel, les fichiers Prefetch *.pf, introduits sous Windows XP et localisés dans %SystemRoot%Prefetch, sont utilisés par le système d'exploitation pour caractériser les applications exécutées par le système et l'utilisateur.
Cette fonctionnalité permet de déterminer les pages mémoires de code utilisées par un programme afin de les charger préalablement lors de l'exécution de ce dernier. L'objectif ainsi visé est d'éviter un maximum d'accès disque. Par défaut, le Prefetch est désactivé pour tous les programmes sur les environnements Windows Server.

Ce paramètre est stocké dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnablePrefetcher
Windows Vista et SuperFetch

Introduit avec le noyau de Vista, SuperFetch est un procédé de gestion de la mémoire, à l'image du Prefetcher introduit sous XP. SuperFetch vise à améliorer les performances générales du système via un mécanisme de prédiction d'utilisation des pages mémoire de code en fonction de scénarios temporels (exécution en semaine ou week-end, utilisation entre 6 heures et midi, midi et 18h, 18h et minuit).
Prefetch ne se base que sur l'activité récente du système pour charger préalablement des données. Si une application utilise intensivement la mémoire, l'historique d'utilisation des pages sera faussé. SuperFetch tente d'optimiser ce modèle de gestion mémoire par le composant de rééquilibrage (rebalancer), qui permet de prioriser à nouveau la liste des pages mémoire en fonction de leur historique d'utilisation et des scénarios temporels établis.
Les fichiers Ag*.db constituent une base d'informations sur l'historique d'utilisation des programmes et de leurs pages mémoire de code. Par abus de langage, ils sont nommés fichiers SuperFetch, bien que ce terme englobe le procédé de gestion mémoire optimisé dans son ensemble. A l'instar des fichiers Prefetch, ils se trouvent dans le dossier %SystemRoot%Prefetch.
Comme pour Prefetcher, le SuperFetch est désactivé par défaut pour tous les programmes sur les environnements Windows Server.

Le paramètre est contenu dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnableSuperfetch

Initialement, enablePrefetcher et enableSuperfetch étaient désactivée par défaut sur Windows 7 sur les systèmes équipés de disques SSD, afin d'améliorer la durée de vie des premiers modèles de disque. L'option enablePrefetcher a été réactivée par défaut à partir de Windows 8, mais ce n'est pas le cas pour SuperFetch.

Utilité des artefacts d'exécution de programme

Dans le cadre d'une investigation lors d'un incident de sécurité informatique, l'analyste sera intéressé de savoir si un programme a été exécuté (le nombre de fois, la date, la fréquence et l'emplacement). Cela peut mettre en avant un comportement malveillant si une application suspecte est utilisée, ou déterminer la légitimité d'une autre par une étude statistique.

Les fichiers Prefetch peuvent être décodés avec les outils suivants :
Pf de TzWorks (payant) ;
CrowdResponse de CrowdStrike (gratuit) ;
Windows file analyzer de Mitec (gratuit) ;
le greffon prefetch de RegRipper (libre et gratuit) ;
Prefetch-parser de Airbus DS (libre et gratuit).

Les fichiers SuperFetch peuvent être partiellement décodés avec les outils suivants :
CrowdResponse de CrowdStrike (gratuit) ;
Superfetch-dumper de Rewolf (libre et gratuit).

Documentation
http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-037
http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-044
https://technet.microsoft.com/en-us/magazine/2007.03.vistakernel.aspx
https://www.crowdstrike.com/blog/crowdresponse-application-execution-modules-released
M. Russinovitch, D. Solomon, A. Ionescu. Windows Internals vol.2. Microsoft Press. p.338
https://github.com/libyal/libagdb/blob/master/documentation/Windows SuperFetch (DB) format.asciidoc

---

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-051*

Un phishing et Lastpass s’en est allé

Un phishing et Lastpass s’en est allé

Lors de la conférence Shmoocon, un chercheur a présenté une attaque de phishing particulièrement convaincante visant les services du gestionnaire de mot de passe Lastpass. En réaction, les mesures de sécurité ont été rehaussées par l'éditeur du service.

Le phishing n'est pas toujours un problème situé entre le clavier et la chaise. C'est en tout cas la thèse défendue par le chercheur Sean Cassidy, qui a présenté ce week-end lors de la conférence Shmoocon une attaque de cette catégorie particulièrement convaincante et capable de tromper les utilisateurs les plus aguerris du gestionnaire de mot de passe Lastpass.

L'attaque, baptisée « Lostpass » exploite plusieurs vulnérabilités présentes sur le service de gestion des mots de passe : il s'agit tout d'abord pour l'attaquant d'attirer l'utilisateur sur un site malicieux, puis d'afficher une notification indiquant à l'utilisateur que celui-ci a été déconnecté de Lastpass. Une fois celle-ci affichée, l'utilisateur est ensuite redirigé vers une page de login quasi identique à celle affichée par Lastpass en cas de déconnexion. L'attaquant peut exploiter un bug notamment présent dans Chromium afin de disposer d'un nom de domaine quasi similaire à celui utilisé pour les extensions chrome du même type que celles utilisées par Lastpass.

L'attaquant peut ensuite exploiter l'API ouverte de Lastpass pour vérifier si les identifiants entrés par l'utilisateur sont valides et pour savoir si celui-ci a activé un système d'identification à double facteur : si tel est le cas, l'attaquant peut également présenter une invite copiée sur celle proposée par le service de gestion de mot de passe et qui lui permet de récupérer par la même occasion le token généré par la double authentification. Une fois les identifiants récupérés, l'attaquant peut accéder au reste des mots de passe stockés par l'utilisateur, ou modifier les paramètres de sécurité du compte afin de faciliter d'éventuelles futures attaques.

Un problème entre la chaise et le clavier ?

Les équipes de Lastpass ont été mises au courant de ce scénario d'attaque au cours de l'été 2015 et ont depuis mis en place plusieurs mesures afin de protéger les utilisateurs. La société a ainsi mis en place un système de vérification par mail lorsque l'utilisateur se connecte depuis un appareil inconnu, ce qui permet selon Lastpass de réduire considérablement les attaques de ce type.

La société précise également revoir le fonctionnement de son extension :
celle-ci s'appuie en effet sur des notifications Viewport pour informer ses utilisateurs, une technique facile à imiter pour un attaquant qui souhaiterait tromper un utilisateur. Un comportement que Lastpass entend corriger afin de réduire un peu plus le risque de confusion entre véritables notifications et notifications malicieuses émanant du site visité.
Pour Sean Cassidy, le problème souligné par ce scénario est tout aussi critique qu'une vulnérabilité classique, mais celui-ci regrette que les attaques de type phishing soient trop souvent reléguées au simple rang des problèmes liés à l'utilisateur. Dans sa démonstration en effet, la différence entre les pages légitimes et les pages malicieuses utilisées par un attaquant est minime. Seule une infime différence de trois caractères dans une url et quelques différences typographiques séparent ici le vrai du faux, ce qui rend l'attaque bien plus inquiétante.

Réagissez à cet article

Source : *Lastpass : un phishing presque parfait*

Mots de passe : nos conseils pour une sécurité maximum

Mots de passe : nos conseils pour une sécurité maximum

password, admin, 123456, abcdef, qwerty, j'en passe et des meilleures… Voilà des mots de passe encore bien utilisés si l'on en croit le palmarès 2013 des 25 mots de passe les plus fréquents (publié par la société SplashData, éditrice de logiciels). Mais de véritables passoires en termes de sécurité ! A l'heure du cloud et des services Web qui numérisent toujours un peu plus nos vies, la vigilance ne saurait souffrir de négligences. De l'importance de sécuriser ses mots de passe, nous vous expliquons le pourquoi et le comment.

Paranoïa, quand tu nous gagnes…

On a beau être d'un naturel plutôt stoïque, la lecture du rapport P@$$1234: the end of strong password-only security publié en janvier 2013 par le cabinet d'expertise Deloitte donne tout de même quelques sueurs froides… Il s'appuie sur un travail intéressant de Mark Burnett (du site Xato.net), lequel a décortiqué une liste de 6 millions de duos login plus mot de passe uniques pour en extraire des statistiques.

- 98,8 % de cette base d'utilisateurs emploient les 10 000 mots de passe les plus fréquents ;
- 91 % se concentrent sur 1 000 mots de passe ;
- 40 % font avec 100 mots de passe ;
- 14 % (soit 840 000 personnes tout de même) piochent dans le top 10 !

Et le problème de ces mots de passe ultra bateau, dont « password » et « 123456 », c'est qu'ils représentent le degré zéro de sécurité, puisqu'ils seront les premiers à être testés par tout hacker qui se respecte. Le souci de sécurité n'est visiblement pas encore rentré dans toutes les têtes…

Pour mieux se protéger de l'ennemi, il faut tenter de le comprendre. Comment les hackeurs fonctionnent dans les grandes lignes ? Quatre scenarii sont à envisager : le piratage en direct, le vol de bases de données, le phishing (ou plus globalement le *social engineering* précise Paul Rascagnères, analyste malware chez l'éditeur d'antivirus G DATA) et les virus.

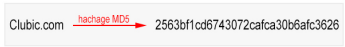
Le premier, qui consiste à tester tous les mots de passe possibles et imaginables dans une interface de connexion sur la base d'un identifiant connu, n'est plus possible aujourd'hui ou très rarement. Cela, parce que la grande majorité des sites sérieux bloquent les comptes au bout de quelques tentatives ratées, trop peu nombreuses même pour un mot de passe évident (quoique avec password et 123456…).

Non, le gros des dangers tient dans le vol, les virus et le *social engineering*. Pour ce dernier, une sorte de vol avec consentement non éclairé, la complexité d'un mot de passe n'a pas d'intérêt : le hackeur se fait passer pour quelqu'un d'autre (email, coup de fil ou faux site officiel), et s'il parvient à duper l'utilisateur, il en profite pour récupérer ses identifiants, en clair. La pratique est courante, les données sont ensuite utilisées ou revendues sur des marchés parallèles. Le seul remède dans ce cas, c'est la vigilance. Idem pour l'aspect virus, un malware avec keylogger peut intercepter vos saisies au clavier ou chiper les identifiants stockés dans le navigateur par exemple : votre ordinateur doit être protégé par un antivirus, à jour, et en programmant des analyses régulières.

? Un hash qui part d'autant plus vite en fumée que le mot de passe est simple ?

C'est en matière de vol qu'il est intéressant de comprendre les mécanismes. Tous les couples identifiants / mots de passe des services Web sont stockés sur les serveurs des entreprises respectives, et forment ainsi autant de bases de données. Ces vols sont assez ponctuels mais malheureusement massifs (par milliers voire millions d'entrées). Très rarement (et normalement pas en France puisque c'est illégal), ces bases de données sont stockées en clair. Si dérobade il y a, la complexité du mot de passe sera vaine.

Mais dans la majorité des cas, les identifiants et mots de passe sont hachés, c'est-à-dire brouillés par un algorithme. Quand quelqu'un veut se connecter à son service, le mot de passe qu'il entre est également haché en temps réel, puis comparé à celui stocké sur les serveurs. Les hackeurs qui se procurent pareilles bases de données vont devoir utiliser des logiciels spécifiques pour déterminer quelle fonction de hachage (hash en anglais) a été utilisée, après quoi ils peuvent automatiser les tests. Tests qui vont consister à choisir un mot, le hacher, le comparer à l'empreinte hachée de la base de données volée : s'il y a correspondance, le mot de passe est trouvé, sinon il faut tester un autre mot, etc. Un hash qui part d'autant plus vite en fumée que le mot de passe est simple.



En hachant un mot via un algorithme, on obtient une empreinte de ce type. Il existe plusieurs algorithmes, proposant des niveaux de sécurité plus ou moins élevés : MD5, SHA-1, SHA-2, etc…

Le hasard fait parfois bien les choses, mais les statistiques les font encore mieux. Pour éviter de tâtonner au doigt mouillé, les hackeurs recourent à des dictionnaires, ou mieux encore, à des listings de mots de passe qui ont été établis au fil des différents vols de données, comme la base du réseau communautaire RockYou.com et ses 32 millions d'entrées évaporées dans la nature en 2009. De vrais mots de passe, couramment employés, et qui ne changent pas beaucoup, comme en témoigne la constance des palmarès des mots de passe les plus fréquents, d'une année sur l'autre. Les cas de vols de données ne manquent pas : Ebay,Orange, Domino's Pizza ou encore Adobe pour les exemples les plus récents.

Vends forfait 4G pas cher, avec livraison à domicile. Seul moyen de paiement accepté : l'abonnement annuel.

Les listings contiennent des mots simples, les logiciels pirates proposent donc des règles complexes. Mais faciles à mettre en oeuvre d'après le journaliste Nat Anderson. Son expérience est instructive. En tentant de se mettre dans la peau d'un hacker, il a potassé le fonctionnement des logiciels pirates, et notamment de Hashcat, qui sont, sans surprise, très bien conçus.

En quelques clics, on peut étoffer la recherche, de sorte à ce que sur un mot de passe comme « clubic » (à tout hasard), le logiciel teste également des ajouts de chiffres ou de lettres (« clubic10 » ou « clubicz »), mais aussi l'ordre inversé (« cibulc »), les ajouts de préfixes et suffixes courants (man, 123, mad, me…), la version *leet*, c'est-à-dire avec des caractères alphanumériques ASCII (« (|_ |_| |3 | (») voire des inversions de lettres. De quoi multiplier les chances du malfaiteur d'arriver à ses fins.


Le logiciel Hashcat

? Un mot de passe à 8 caractères hacké en 5 h 30 ?

Plus efficace encore mais exigeante en ressources, la bonne vieille attaque de force brute. Sur une quantité donnée de caractères, mettons six, la technique un brin bourrine consiste à hacher et tester « aaaaaa », puis « aaaaab », etc. Sachant qu'un clavier français peut produire 142 caractères (avec tous les accents, la casse, les symboles, les chiffres, et encore 103 si on exclut les accents) et que la statistique est exponentielle, ça nous fait 8 198 418 170 944 de combinaisons possibles (8 200 milliards pour ceux qu'autant de chiffres perturberait). Dans l'exemple donné par l'étude du cabinet Deloitte, un mot de passe à 8 caractères (6,1 millions de milliards de possibilités sur un clavier américain à 94 caractères) pourrait être hacké en 5 h 30 par une configuration dédiée haut de gamme (estimée à 30 000 $ en 2012), mais en près d'un an avec un PC correct de 2011.

Représentation visuelle de ces chiffres astronomiques

Le petit point noir, c'est le nombre de combinaisons à 8 caractères, le gros point bleu c'est avec 10 caractères. Les joies de l'exponentiel !

Voilà donc la clef : plus un mot de passe est complexe (avec des caractères spéciaux, un séquençage aléatoire, etc.) et long, plus le hacker aura du fil à retordre. Rien qu'en passant à 10 caractères, courbe exponentielle oblige, on fait grimper les combinaisons sur un clavier français à 3 333 369 396 234 118 349 824 (3 333 milliards de milliards !!!). La même machine de compétition mettrait alors 343 ans pour tester toutes les combinaisons… A cette parade, les hacker répondent par le crowd-hacking : ils confient des fragments de calculs à faire à des milliers de PC normaux infectés (les fameux PC zombies). C'est supposé aller beaucoup plus vite ainsi, mais bon, les hackers préfèrent tout de même les mots de passe courts et basiques.

? nous peinerions à retenir plus de sept chiffres dans notre mémoire à court terme ?

Le remède est simple, sa mise en oeuvre plus délicate. D'après une étude de l'Université de Toronto que cite le rapport Deloitte, les êtres humains limités que nous sommes peinerions à retenir plus de sept chiffres dans notre mémoire à court terme, et même plus que cinq en prenant de l'âge. L'ajout de symboles, de lettres majuscules et minuscules produirait un mix encore moins aisé à retenir. Le rapport se fait plus accablant en ajoutant que la nature humaine a tendance à suivre des schémas de pensée limités par rapport aux possibilités offertes. La majuscule ? En première position dans les mots. Les chiffres ? À la fin. Des 32 symboles présents sur un clavier américain ? Une demi-douzaine seulement est utilisée. De quoi rendre l'aléa théorique plus prédictif pour les hackers. Rien de nouveau cependant. A moins que… le rapport ne pointe du doigt un nouveau frein, imputable aux usages mobiles. L'absence ou la moindre accessibilité des caractères spéciaux sur les claviers des smartphones amène le nomade à simplifier son mot de passe. Tout comme le temps de saisie supérieur qui inciterait un quart des personnes sondées à utiliser un mot de passe plus court pour gagner du temps. De 4 à 5 secondes pour taper un mot de passe de 10 caractères sur un clavier standard d'ordinateur, il faudrait entre 7 et 30 secondes pour faire la même chose depuis un smartphone tactile.

Réagissez à cet article

Source : *Mots de passe : nos conseils pour une sécurité maximum*

Alerte : Vulnérabilité zero-day qui affecte des millions de systèmes Linux et Android

Alerte : Vulnérabilité zero-day affecte des millions de systèmes Linux et Android

---

Le fournisseur en sécurité Perception Point a découvert une vulnérabilité zero-day présente dans le code source de Linux depuis 2012. Touchant des dizaines de millions de postes de travail et serveurs Linux 3 et 64-bit, mais également tous les terminaux Android 4.4 ou supérieurs, cette vulnérabilité sera corrigée sous peu.

Une nouvelle vulnérabilité zero-day a été découverte permettant à des applications Android ou Linux d'escalader des privilèges et d'avoir un accès root, d'après un rapport publié ce matin par le fournisseur de solutions de sécurité Perception Point. « Elle affecte tous les téléphones Android sous KitKat (4.4) ou supérieurs », a fait savoir Yevgeny Pats, co-fondateur et CEO de Perception Point.

Toutes les machines dotées d'un noyau Linux 3.8 (ou supérieur) sont vulnérables, incluant des dizaines de millions de PC et serveurs Linux, aussi bien 32 que 64 bits. En tirant parti de cette vulnérabilité, des attaquants sont en mesure de supprimer des fichiers, accéder à des informations personnelles, et installer divers programmes.

Des correctifs disponibles via des mises à jour automatiques

Cette vulnérabilité, présente dans le code source de Linux depuis 2012 mais découverte seulement maintenant par Perception Point, n'a pour l'heure pas été exploitée. L'équipe Linux a été prévenue et des correctifs devraient être disponibles sous peu et seront installés via des mises à jour automatiques. Selon Yevgeny Pats, cette vulnérabilité zero-day (CVE-2016-0728) concerne le service keyrings facility permettant aux drivers de sauvegarder dans le noyau de l'OS des données de sécurité ainsi que des clés d'authentification et de chiffrement.

Réagissez à cet article

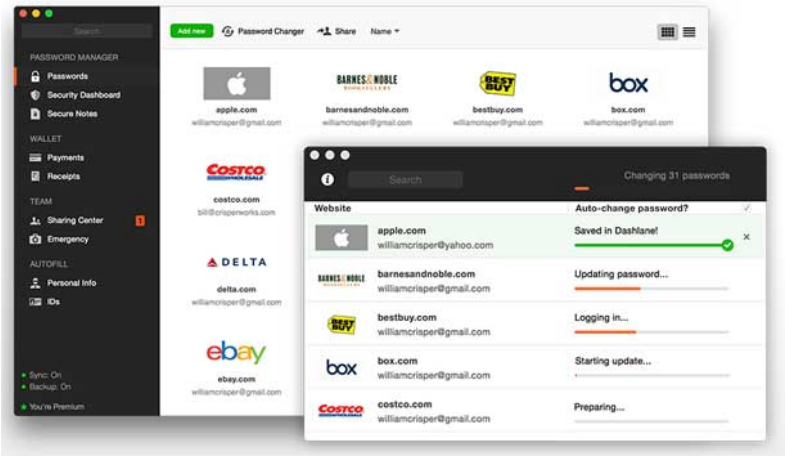
Source : *Une vulnérabilité zero-day affecte des millions de systèmes Linux et Android – Le Monde Informatique*

Article de Dominique Filippone avec IDG News Service

Dashlane : 500 mots de passe modifiés en un clin d’oeil

Dashlane : 500 mots de passe modifiés en un clin d’oeil

La nouvelle version de l'outil français des gestion des mots de passe propose d'automatiser la gestion des mots de passe. De quoi soulager des utilisateurs toujours plus sollicités sur le terrain de la sécurité.



La multiplication des services en ligne fait exploser le nombre de mots de passe utilisés par les professionnels. Au point de poser des problèmes de mémoires insolubles. Google réfléchit à les remplacer grâce au smartphone.

Dashlane propose le changement automatique de mot de passe pour 500 sites Web. (Source : Dashlane)

La pépite Dashlane propose elle une alternative au stockage manuel de plusieurs mots de passe en automatisant le stockage et la modification des mots de passe. Et la dernière version de l'outil permet de le faire pour 500 sites (au lieu de 75 jusqu'alors) et services web en un seul clic, avec la fonctionnalité Password Changer.

Banque et mot de passe

8 formats de documents sont désormais pris en charge : les applications, les bases de données, les documents financiers, les documents juridiques, les abonnements, les licences logicielles et les mots de passe Wi-Fi. Autres nouveautés de cette quatrièmes version de Dashlane, 7 langues différentes sont supportées et l'interface graphique a été revue de mnière à être identique quelque soit la plateforme (Mac, PC, iOS et Android). Autre amélioration, un moteur de recherche plus performant et un affichage des résultats sous divers formats.

Côté moyen de paiement, 618 nouvelles banques internationales peuvent être utilisées dans les moyens de paiement. A noter que la version de base de Dashlane est proposées gratuitement, et que la version Premium 39,99 euros/an) permet de synchroniser les données sur mobile (nombre illimité d'appareils) et de les sauvegarder en mode sécurisé.

Réagissez à cet article

Source : *Dashlane : 500 mots de passe modifiés en un clin d'oeil*

Palmarès des mots de passe 2015

	**Palmarès des mots de passe 2015**

Comme chaque année, Splashdata dévoile les mots de passe les plus utilisés par les internautes, une liste qui est le fruit de données volées et rendues publiques. Sans surprise, « 123456 » et « password » se disputent toujours les deux premières places. Mais ce palmarès 2015 révèle aussi l'influence de Star Wars dans le choix des internautes.

Tous les ans à la mi-janvier, nous attendons avec impatience la réponse à cette question : l'humanité a-t-elle enfin compris que la plus grande des failles informatiques était un mot de passe trop simple à trouver ?
Mais cette fois encore, la déception est au rendez-vous : ces satanés « 123456 » et « password » trônent encore, là, tout en haut du classement.
Évidemment, on peut modérer ce sentiment en rappelant que la liste en question est obtenue en étudiant « seulement » deux millions de mots de passe échappés dans la nature. Comparé aux près de trois milliards d'internautes dans le monde, qui possèdent chacun plusieurs mots de passe (si, si, ça existe), cela reste faible.
Mais l'échantillon demeure représentatif, et on peut malheureusement imaginer que dans notre entourage proche, certains utilisent encore 12345678 (troisième du classement) ou même 12345 (qui rétrograde en cinquième position).

La tête de ce classement 2015 s'éloigne assez peu de celle du palmarès 2014, mais laisse tout de même de la place pour quelques nouveautés, dont le très original « welcome », directement propulsé en onzième position, immédiatement suivi par un autre promu, le très complexe « 1234567890 ».
Enfin, on note l'influence de la sortie de l'épisode 7 de *Star Wars* sur ce millésime 2015 : « princess » (en 21e position) et « solo » (23e) peuvent le laisser penser, alors que « starwars » (25e) ne laisse pas de place au doute.
Le classement en question :

- 1. 123456 (-)
- 2. password (-)
- 3. 12345678 (+1)
- 4. qwerty (+1)
- 5. 12345 (- 2)
- 6. 123456789 (-)
- 7. football (+3)
- 8. 1234 (-1)
- 9. 1234567 (+2)
- 10. baseball (-2)
- 11. welcome (nouveau)
- 12. 1234567890 (nouveau)
- 13. abc123 (+1)
- 14. 111111 (+1)
- 15. 1qaz2wsx (nouveau)
- 16. dragon (-7)
- 17. master (+2)
- 18. monkey (-6)
- 19. letmein (-6)
- 20. login (nouveau)
- 21. princess (nouveau)
- 22. qwertyuiop (nouveau)
- 23. solo (nouveau)
- 24. passw0rd (nouveau)
- 25. starwars (nouveau)

Réagissez à cet article

Source : *Palmarès des mots de passe 2015 : du classique, mais avec un peu de Star Wars*

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

---

Amnesty International a vivement critiqué mardi une nouvelle loi sur la cybercriminalité au Koweït qui, selon cette organisation, va restreindre davantage la liberté d'expression et doit être révisée.

Le texte, qui entre en vigueur mardi, « va s'ajouter à l'éventail de lois sur le web qui restreignent déjà le droit des Koweïtiens à la liberté d'expression et doit être révisé d'urgence », écrit l'organisation de défense des droits de l'Homme dans un communiqué.
La nouvelle législation prévoit la criminalisation d'une série d'expressions en ligne comportant notamment des critiques envers le gouvernement, des dignitaires religieux ou des dirigeants étrangers, relève Amnesty.
« Cette loi répressive » fait partie d'un éventail de législations destinées à « étouffer la liberté d'expression », a commenté Saïd Boumedouha, directeur adjoint d'Amnesty International pour le Moyen-Orient et l'Afrique du nord.
Des dizaines de personnes au Koweït ont été arrêtées et poursuivies en justice, certaines servant déjà des peines de prison, en vertu d'une autre législation pour des commentaires sur les réseaux sociaux.
Votée en juin, la nouvelle loi prévoit des peines de 10 ans de prison et des amendes allant jusqu'à 165.000 dollars pour des crimes en ligne, notamment ceux liés au terrorisme.
Pour le gouvernement, cette loi est nécessaire pour combler un vide juridique et réglementer l'utilisation des services en ligne tels que Twitter.
La peine minimale en vertu de la loi consiste en six mois de prison et 6.600 dollars d'amende pour celui qui ose, illégalement, « infiltrer un ordinateur ou un réseau électronique ».
« Les autorités koweïtiennes ne doivent pas appliquer cette loi jusqu'à ce qu'elle soit révisée pour se conformer aux obligations internationales du Koweït en matière de droits de l'Homme », a dit M. Boumedouha.
« Cette loi n'appartient pas au XXIe siècle », a-t-il ajouté, soulignant que « les Koweïtiens méritent mieux » qu'une telle législation.

Réagissez à cet article

Source : *Koweït: Amnesty critique la nouvelle loi sur la cybercriminalité – Internet – Notre Temps*

Comment l’industrie peut aussi anticiper les cyberattaques ?

Comment l’industrie peut aussi anticiper les cyberattaques ?

Les cyberattaques se multiplient ces derniers mois et ont augmenté de 51 % (*) cette année en France, en particulier à l'encontre des technologies de l'information (messageries hackées, serveurs victimes d'attaques #DDoS entre autres). Pourtant, un tout autre domaine suscite de nouvelles préoccupations : l'industrie.
Les systèmes industriels, ou Industrial Control System (ICS), désignant l'ensemble des moyens informatisés et automatisés assurant le contrôle et le pilotage de procédés industriels, subissent les mêmes menaces que dans le milieu IT.
Cependant, une attaque à l'encontre de l'ICS peut avoir des répercussions encore plus graves, non seulement sur l'industrie en elle-même, avec son corollaire de pertes financières, mais aussi, et surtout, sur l'homme et l'environnement.

Des réseaux vulnérables, car en flux tendus
Tandis que l'IT se soucie davantage de la confidentialité des données, les industriels se préoccupent essentiellement de la disponibilité et de la rentabilité de leur production. Il faut ainsi comprendre que pour des questions de coût, il est inconcevable pour un industriel de stopper sa production, nonobstant une menace imminente.

La dernière crise ukrainienne a illustré cette problématique. Malgré des bombardements massifs, le système de production n'a pas été arrêté. Les réseaux industriels sont d'autant plus vulnérables qu'il n'est pas possible d'effectuer de maintenance sur le système, puisqu'il est en cours de production.

Mais qui sont ces « pirates » qui tirent profit de ces vulnérabilités ?
Il s'agit de groupes bien organisés, de terroristes, qui s'attaquent directement à la vulnérabilité de l'État et des grandes entreprises. On parle d'une véritable cyberarmée qui s'attaque aux réseaux industriels de plusieurs manières : déni de services, prise de contrôle à distance des systèmes, vol de données, mise en faillite par détournement de fonds, pour n'en citer que quelques-uns. En 2003, la centrale nucléaire de Davis-Besse aux USA avait été la cible d'attaques DDoS.
Pour autant, la plupart des incidents de sécurité sont accidentels, liés par exemple à l'activation fortuite de malware se trouvant dans un mail, sur une clé USB ou encore des softwares mal sécurisés.
À l'échelle de l'industrie, les attaques peuvent entraîner des retards de production, un impact économique – consécutif au vol de secrets de fabrication – une perte d'image et de contrats. In fine, l'industriel se retrouve face à une véritable perte de compétitivité.
Les réseaux industriels étant en contact direct avec la vie humaine, celle-ci est également en danger. Ces attaques peuvent en effet entraîner des accidents physiques ; l'arrêt de la production d'énergie pouvant entraîner des coupures d'électricité dans les hôpitaux qui peuvent être critiques. À plus grande ampleur, la santé humaine et l'environnement sont également menacés dans le cas d'une attaque des systèmes nucléaires.
L'exemple le plus connu est celui de Stuxnet, un ver informatique découvert en 2010 et conçu pour attaquer une cible industrielle déterminée pour l'espionner. Le ver a affecté 45 000 systèmes informatiques, y compris des ordinateurs de la centrale nucléaire de Bouchehr ainsi que 15 000 ordinateurs et centrales situés en Allemagne, en France, en Inde et en Indonésie (**).

Les industriels ne sont pas suffisamment préparés à ces types d'attaques, car les moyens mis en œuvre sont limités et la sécurité est considérée comme annexe, dans la mesure où elle n'est pas fondamentale pour assurer les services. À cela s'ajoute qu'elle représente un coût additionnel pour la production, qui se répercute sur les consommateurs qui devront payer plus cher leurs eau, électricité et autres services.
Dès lors, quelles sont les mesures pour se prémunir de ces attaques ? Quels outils peuvent être mis en place ?
La loi est un instrument essentiel pour assurer la protection des ICS et aider à recréer de la confiance. La France a mis en place, en 2006, un décret qui définit 12 secteurs d'importance vitale comprenant notamment la gestion de l'eau, la santé, l'énergie, l'alimentation et les transports, des fondamentaux pour le fonctionnement d'un État.

« Le projet de loi de programmation militaire, prévu pour 2014-2019, précise qu'il est de la responsabilité de l'État d'assurer une sécurité suffisante des systèmes critiques des OIV (opérateurs d'importance vitale). À travers quatre mesures principales, il vise à établir un socle minimum de sécurité pour les organisations.
Il donne notamment au pouvoir exécutif la possibilité d'imposer aux OIV des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles.
Avec ce texte, qui sera examiné sous peu au Sénat, l'État fixera donc des règles en collaboration étroite avec l'ANSSI. Règles que les OIV seront tenus d'appliquer, à leur frais. Les sociétés mauvaises élèves seront susceptibles de se voir infligées une sanction pouvant aller jusqu'à 750 000 euros d'amende » (***).

Au-delà de cette législation, il est essentiel, pour retarder l'attaque, de mettre un point d'honneur à la sensibilisation de l'utilisateur dans la chaîne de production, mais aussi, et surtout, de la direction des industries, en l'incitant à appliquer de bonnes pratiques au quotidien et en investissant dans les hommes et les outils (firewall, anti-vers ou encore systèmes de détection d'intrus).
Cependant, même le plus puissant des firewalls n'est pas suffisant si l'on n'identifie et ne traite pas les menaces dans le détail, sur un service en particulier. Cela sous-entend qu'il y ait un opérateur qui assure la maintenance des systèmes d'informations, sans quoi les intrusions dans les réseaux industriels ne pourront être empêchées.

(*) Source : étude réalisée par le cabinet PwC
(**) Source : Wikipédia
(***) Source : Nextimpact.com

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*

Antivirus software could make your company more vulnerable

	Antivirus software could make your company more vulnerable !

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit

Imagine getting a call from your company's IT department telling you your workstation has been compromised and you should stop what you're doing immediately.
You're stumped: You went through the company's security training and you're sure you didn't open any suspicious email attachments or click on any bad links; you know that your company has a solid patching policy and the software on your computer is up to date; you're also not the type of employee who visits non-work-related websites while on the job. So, how did this happen?

A few days later, an unexpected answer comes down from the security firm that your company hired to investigate the incident: Hackers got in by exploiting a flaw in the corporate antivirus program installed on your computer, the same program that's supposed to protect it from attacks. And all it took was for attackers to send you an email message that you didn't even open.
This scenario might sound far-fetched, but it's not. According to vulnerability researchers who have analyzed antivirus programs in the past, such attacks are quite likely, and may already have occurred. Some of them have tried to sound the alarm about the ease of finding and exploiting critical flaws in endpoint antivirus products for years.
Since June, researchers have found and reported several dozen serious flaws in antivirus products from vendors such as Kaspersky Lab, ESET, Avast, AVG Technologies, Intel Security (formerly McAfee) and Malwarebytes. Many of those vulnerabilities would have allowed attackers to remotely execute malicious code on computers, to abuse the functionality of the antivirus products themselves, to gain higher privileges on compromised systems and even to defeat the anti-exploitation defenses of third-party applications.
Exploiting some of those vulnerabilities required no user interaction and could have allowed the creation of computer worms – self-propagating malware programs. In many cases, attackers would have only needed to send specially crafted email messages to potential victims, to inject malicious code into legitimate websites visited by them, or to plug in USB drives with malformed files into their computers.

Attacks on the horizon

Evidence suggests that attacks against antivirus products, especially in corporate environments, are both possible and likely. Some researchers believe that such attacks have already occurred, even though antivirus vendors might not be aware of them because of the very small number of victims.
The intelligence agencies of various governments have long had an interest in antivirus flaws. News website The Intercept reported in June that the U.K. Government Communications Headquarters (GCHQ) filed requests in 2008 to renew a warrant that would have allowed the agency to reverse engineer antivirus products from Kaspersky Lab to find weaknesses. The U.S. National Security Agency also studied antivirus products to bypass their detection, according to secret files leaked by former NSA contractor Edward Snowden, the website said.

Réagissez à cet article

Source : *Antivirus software could make your company more vulnerable | Computerworld*