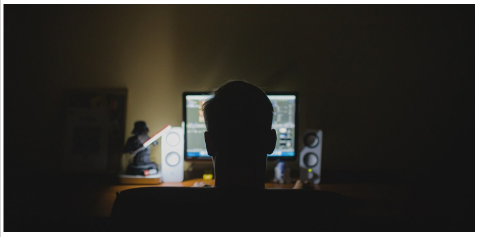
Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Pour Nicolas Reys de la société de conseil en gestion des risques Control Risks, la question doit être soulevée en conseil d'administration.



L'ancien directeur du FBI Robert Mueller déclarait en 2014: « il y a seulement deux types d'entreprises: celles qui ont été piratés et celles qui le seront un jour. » Ce message devient de plus en plus réel. L'attaque récente sur le principal fournisseur de services de messagerie de paiements pour les institutions financières SWIFT nous rappelle que même les organisations considérées les plus sûres ne sont pas infaillibles et que maintenant les cyberattaques font désormais partie intégrante du paysage du risque des entreprises modernes. Selon une étude récente, 1.673 brèches de données ont exposé plus de 707 millions de données diverses au cours de l'année 2015, à travers le monde. Une autre étude relève que 90% des grandes entreprises et 74% des petites et moyennes entreprises dans le monde ont subi une brèche de sécurité.

Peut être très coûteux

De nombreux dirigeants considèrent toujours la réponse à une cyberattaque comme un problème purement technique et non stratégique. Pourtant la fréquence et l'ampleur croissante des cyberattaques, ainsi que l'intérêt grandissant que les partenaires commerciaux et les autorités portent à la cybersécurité, exigent d'élever le problème au rang des conseils d'administration. Certes, le lexique associé aux cyberattaques peut être intimidant pour les chefs d'entreprises, des termes tels que « centre de commandement et de contrôle », « numéro de port TCP » et « injection SQL » peuvent laisser entendre qu'une cyber intrusion est un problème informatique et donc ne concernant pas le comité de direction. Toutefois, quel qu'en soit sa nature, ce type d'événement peut être très coûteux et une réponse mal gérée est susceptible d'augmenter de manière significative son impact commercial et opérationnel. L'Institut Ponemon estime que le coût moyen d'une fuite de données est de 3,79 millions de dollars par entreprise victime; en augmentation de 23% depuis 2013.

Préjudice de réputation

A l'extrémité de ce spectre, le distributeur américain Target, qui a subi une énorme perte de données clients en 2013, estime que le coût total de cette attaque s'est élevé à 162 millions de dollars. Un montant supplémentaire de 90 millions ayant par ailleurs été couvert par les assureurs du détaillant. Mais surtout, la marque a subi un préjudice de réputation considérable et Target a vu son rythme de croissance ralentir suite à cette crise. Il est donc possible que l'impact total sur l'entreprise sera encore plus significatif à moyen terme. D'ailleurs le PDG et le responsable de la sécurité des systèmes d'information (RSSI) de Target ont été licenciés à la suite de cet événement. Bien que comprendre les dimensions techniques de ce type de crise reste crucial pour les résoudre, il faut absolument prendre en compte les implications opérationnelles et commerciales associées aux cyberattaques.
Les gestionnaires de crise au sein de l'entreprise doivent s'interroger sur au moins trois points : « quel est l'impact opérationnel immédiat sur l'entreprise de cette attaque et avec quelle rapidité pouvons-nous revenir en ligne? Quelle est notre responsabilité juridique? Avons-nous un plan de communication en place? ». Le département informatique d'une entreprise est normalement en mesure de répondre à l'incident technique et de fournir les informations sur les accès ouverts, ce qui a été volé et ce qu'il faudra faire pour reconnecter les systèmes. Mais les informaticiens ont rarement l'expérience ou le mandat pour répondre aux questions de gestion opérationnelle qu'une cyberattaque suscite.

Brèches souvent détectées par des tiers

D'autant que, les « cyberattaques » peuvent rapidement prendre des proportions médiatiques mal maîtrisées puisque Mandiant relève que 53% des brèches de sécurité informatique sont détectées par des tiers plutôt que par les victimes.
Comment se protéger? D'abord en comprenant les capacités et motivations des acteurs prenant pour cible votre entreprise afin de formuler un plan de gestion de crise adapté et proportionné, envisageant les scénarios de crises les plus probables ainsi que les plus dangereux pour votre entreprise. Il est ainsi souhaitable d'établir avant une cyberattaque, un plan de gestion de crise et des procédures bien documenté. Assurez-vous que la réponse à l'incident technique soit complète et s'accompagne d'un plan de gestion commerciale et opérationnelle. Vérifiez donc que tous les acteurs principaux de l'entreprise connaissent ce plan et qu'ils peuvent rapidement l'actionner. Testez son fonctionnement en vous exerçant dans des conditions réelles, et posez-vous les questions suivantes: Tout le monde peut-il être contacté? Connaissent-ils leurs rôles et responsabilités face à une telle crise? Enfin soyez prêts, à vous procurer le soutien de spécialiste en gestion de crise pour vous aider si vous ne disposez pas des capacités techniques, juridiques, de communications, ou de gestion de crises nécessaires en interne.
Les attaques cybercriminelles ont doublé entre 2014 et 2015, il n'est donc plus possible d'ignorer la menace. Même si vous êtes une entreprise bien protégée, une cyberattaque a toute les chances de vous affecter dans un futur proche. La question n'est déjà plus « quand aura lieu une attaque? », mais plutôt « êtes-vous prêts à réagir? »
Nicolas Reys de la société de conseil en gestion des risques Control Risks.

Article original de Challenges.fr

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Techniques et astuces pour la robustesse de vos mots de passe

Techniques et astuces pour la robustesse de vos mots de passe

Les experts en cybersécurité ont tendance à être quelque peu cyniques envers les utilisateurs « lambda », particulièrement lorsqu'il s'agit du choix des mots de passe. Cependant, selon certains experts en sécurité informatique au sein du CyLab, l'Institut Security & Privacy de l'Université de Carnegie Mellon, les utilisateurs ordinaires ne semblent pas être aussi stupides qu'il n'y paraît. En effet les erreurs commises peuvent être classées en 4 catégories spécifiques. Le travail de sensibilisation nécessaire ne devrait pas être une tâche insurmontable.

La méthodologie de CyLab est la suivante : montrer aux gens des mots de passe par paires, et leur demander lesquels leur semblent les plus robustes. Ensuite, établir une corrélation entre leurs réponses et l'efficacité effective de ces derniers en utilisant *les méthodes les plus actuelles pour craquer les mots de passe*. Au final, sur 75 paires, les participants en ont correctement sélectionné 59. Il s'agit de 79%, soit en pratique un « B ».
Il est vrai que l'échantillon des 165 utilisateurs du CyLab est certainement un peu plus technique que d'autres utilisateurs : ils ont été recrutés en ligne via le système du Turc Mécanique d'Amazon. De plus, CyLab ne dit pas en substance que tous les utilisateurs atteindront ce score, mais seulement que certains peuvent y arriver. Enfin, pour conclure, ces scores ne sont pas alarmants.
Les personnes sondées par CyLab savaient que des mots de passe sont robustes lorsque :
• Les majuscules sont utilisées au milieu du mot, plutôt qu'au début.
• Des chiffres et des symboles sont situés au milieu du mot plutôt qu'à la fin.
• Des séquences de chiffres aléatoires sont insérées à la place d'autres plus évidentes, telles que l'année en cours par exemple.
• Des noms sont ajoutés, différents des traditionnels prénoms et noms.
• Des noms faisant parties de la vie privée ne sont pas utilisés, tels que les prénoms de vos enfants.
• Des mots faisant référence de manière évidente au site ou au compte que vous êtes en train de protéger ne sont pas utilisés.
Bien sûr, il en reste 21% qui n'ont pas réussi à faire la distinction. Cela laisse en effet de belles opportunités **aux cybercriminels pour craquer vos mots de passe**. Quelles ont donc été les plus grosses erreurs commises ? :
1. **Les participants ont ajouté des chiffres à leurs mots de passe, en plus des lettres, en pensant les renforcer**. Dommage ! Les hackers savent bien que les internautes très souvent rajoutent à la fin des chiffres, du coup « brooklynqy » est plus sécurisé que « brooklyn16 ».
2. **Les participants ont pensé que le fait de changer tout simplement des lettres en chiffres rendrait leurs mots de passe plus robuste.** Dommage ! Les craqueurs de mots de passe « exploitent de plus en plus la tendance des utilisateurs à faire des substitutions prévisibles », ainsi « punk4life » n'est pas plus sûr que « punkforlife ».
3. **Les participants ont surestimé la sécurité procurée par les séquences présentes au niveau de leur clavier.**Dommage ! Les hackers de nos jours recherchent très rapidement les séquences des claviers telles que « qwertyuiop », tout comme d'autres patterns classiques, et pas seulement à base de mots.
4. **Les participants ont mal appréhendé la popularité de certains mots ou de certaines phrases.** Selon le CyLab, par exemple, les utilisateurs ont pensé que « ieatkale88 » et « iloveyou88 » étaient équivalent d'un point de vue sécurité. Pas vraiment : les craqueurs de mots de passe ont besoin de plus d'un milliard de tentatives en plus pour en venir à bout de « ilovekale ». Il est plus sûr de choisir un mot isolé rare plutôt qu'une phrase intégrant « iloveyou » or « ilove ». Les mots de passe utilisant le mot « love » sont incroyablement répandus …ce qui est plutôt une bonne intention si vous n'êtes pas responsable de la cybersécurité d'un site.
Qu'est ce qui pourrait aider les utilisateurs pour éviter les mauvaises stratégies de choix des mots de passe ? Selon l'auteur de l'étude :
Une méthode qui semble être très efficace pour assister les utilisateurs dans l'évaluation de leurs mot de passe, vis-à-vis des pratiques courantes, est de leur fournir des feedbacks ciblés et explicites pendant la phase de création. Les calculateurs actuels de la force d'un mot de passe indiquent simplement aux utilisateurs si un mot de passe est faible ou fort, mais ne mentionne pas les raisons.
Les futurs travaux dans ce domaine pourraient s'inspirer d'une récente étude qui montrait la possibilité pour les utilisateurs de finir automatiquement le mot de passe partiel qu'ils viennent de taper … et pourrait également se baser sur une autre étude utilisant des arguments de motivation ou encore la pression de collègues pour inciter les utilisateurs à créer des mots de passe plus robustes.
Article original de Sophos France

Réagissez à cet article

Original de l’article mis en page : Robustesse des mots de passes : techniques et astuces

---

La double authentification de Google contournée par des hackers

La double authentification de Google contournée par des hackers

---

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient.

Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

---

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

Réagissez à cet article

Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

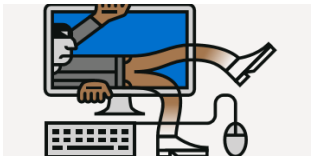
---

77 % des entreprises totalement impuissantes face aux cyberattaques

77 % des entreprises totalement impuissantes face aux cyberattaques

---

Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés dans ce domaine, et note même un recul….

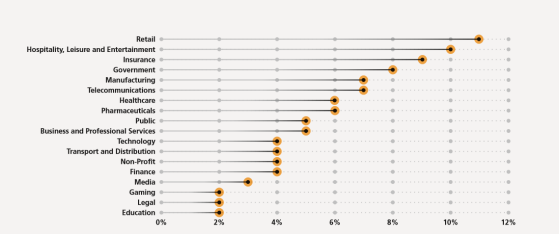


Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le monde. Son édition 2016, qui décrypte les tendances de ces trois dernières années souligne le peu de progrès réalisés par les entreprises dans leur lutte contre les menaces, et note même une légère hausse du nombre d'entre elles mal préparées qui s'élève à 77 %. Face à des attaques d'envergure, elles doivent le plus souvent solliciter une intervention extérieure. Seules 23 % des organisations seraient donc en mesure de se défendre efficacement contre des incidents de sécurité majeurs.

Le retail le plus touché par les incidents

Après des années passées en tête des secteurs les plus touchés dans les précédents rapports GTIR, la finance cède sa place à la grande distribution qui enregistre 22 % des interventions sur incidents (contre 12 % l'année passée) de NTT Com Security. La grande distribution a été particulièrement exposée aux attaques de spear phishing. Parce qu'elles brassent d'importants volumes de données personnelles, dont des informations bancaires, les organisations de ce secteur constituent une cible particulièrement attractive, et ce au point d'enregistrer le plus fort taux d'attaques par client. Le secteur financier a représenté 18 % des interventions.

En 2015, le groupe NTT a également noté une augmentation des attaques à l'encontre du secteur de l'hôtellerie, des loisirs et du divertissement. Tout comme la grande distribution, ce secteur draine aussi de gros volumes d'informations personnelles, y compris des données de cartes bancaires. De même, le niveau relativement élevé des transactions dans le milieu (hôtels, stations touristiques…) suscitent la convoitise des attaquants. Avec sa palette de programmes de fidélité, l'hôtellerie est une vraie mine d'informations personnelles. Plusieurs violations de sécurité ont d'ailleurs défrayé la chronique en 2015 : Hilton, Starwood ou encore Hyatt.



Les attaques par secteur – 2015

Hausse de 17 % des menaces internes

A quels types d'incidents NTT Com Security a-t-il été confronté ? Les violations de sécurité ont représenté 28 % des interventions en 2015, contre 16 % en 2014. Un grand nombre d'incidents concernaient des vols de données et de propriété intellectuelle. Les menaces internes ont connu de leur côté une véritable envolée, passant de seulement 2 % en 2014 à 19 % en 2015. Elles résultent le plus souvent d'une utilisation abusive des données et ressources informatiques par des salariés ou prestataires externes.

En 2015, 17 % des interventions de NTT Com Security se sont produites sur des attaques par spear phishing, alors qu'elles représentaient moins de 2 % auparavant. Basées sur des tactiques sophistiquées d'ingénierie sociale, comme l'utilisation de fausses factures, ces attaques visaient principalement des dirigeants et autres personnels de la fonction comptabilité-finance.

Enfin, le GTIR 2016 a enregistré un recul des attaques #DDoS par rapport aux années précédentes. Elles ont reculé de 39 % par rapport à 2014. Le rapport attribue cette baisse aux investissements réalisés dans les outils et services de défense contre ce type d'agression.

A noter cependant une augmentation des cas d'extorsion, où les victimes d'acquittent d'une rançon pour lever les menaces ou stopper une DDos en cours.

Top 10 External Vulnerabilities	
Outdated PHP Version	8%
Cross-Site Scripting (CSS/XSS)	7%
Outdated Apache Web Server	7%
SSL/TLS Information Disclosure	6%
Web Clear Text Username/Password	5%
Weak SSL/TLS Ciphers/Certificate	5%
Outdated Apache Tomcat Server	4%
Weak/No HTTPS cache policy	4%
Cookie without HTTPOnly attribute set	3%
SSL Certificate Signed using Weak Hashing Algorithm	3%

Top 10 Internal Vulnerabilities	
Outdated Java Version	51%
Outdated Adobe Flash Player	11%
Outdated Adobe Reader and Acrobat	5%
Outdated Microsoft Windows	3%
Outdated Microsoft Internet Explorer	3%
Outdated Mozilla Firefox	2%
Outdated Microsoft Office	1%
Outdated Linux Kernel	1%
Outdated Novell Client	1%
Outdated OpenSSH Version	1%

Top 10 des vulnérabilités internes et externes – 2015. Parmi l'ensemble des vulnérabilités externes identifiées, le top 10 compte pour 52 % des cas recensés. Les 48 % restants étaient composés de milliers de vulnérabilités. Parmi l'ensemble des vulnérabilités internes identifiées, le top 10 compte pour 78 % des cas recensés. Ces 10 vulnérabilités internes étaient directement liées à la présence d'applications obsolètes sur les systèmes visés.

Article original de Juliette PAOLI

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cyberattaques : 77 % des entreprises totalement impuissantes | Solutions Numériques

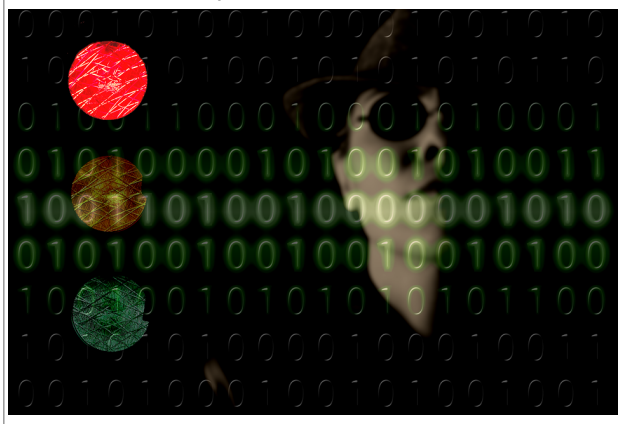
---

Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

---

D'après les informations de FireEye, le malware Irongate, qui vise les systèmes de contrôle des procédés industriels ressemble en certains points au terrible ver Stuxnet. Cette découverte est une nouvelle source d'inquiétude pour les membres de la communauté de la sécurité de l'information et elle vient confirmer la nécessité du perfectionnement des systèmes de détection des malwares qui attaquent les infrastructures critiques.



Les chercheurs ont également signalé qu'Irongate ne constituait pas une menace sérieuse pour l'instant car il fonctionne uniquement dans des environnements simulés. Ceci étant dit, FireEye indique que ce malware est passé inaperçu pendant des années alors qu'il figurait pendant tout ce temps dans la base VirusTotal. « La compétence du secteur dans le domaine de l'identification et de la détection des menaces s'améliore, mais elle n'a pas encore atteint un niveau satisfaisant comme le montrent ces exemples » constate Rob Caldwell, directeur du groupe d'analyse FireEye Labs Advanced Reverse Engineering (FLARE). Il poursuit en expliquant qu'il faut absolument mieux comprendre ce que représentent les menaces pour les systèmes de contrôle des procédés industriels, comment les détecter et comment améliorer la protection contre celles-ci. »

D'après FireEye, le malware qu'elle a identifié se distingue par sa capacité à mener une attaque de type homme du milieu contre l'entrée et la sortie des procédés et à attaquer l'application qui exécute des opérations sur les processus dans les environnements simulés. Un système compromis par Irongate permet aux attaquants de substituer les contrôles industriels à l'insu de l'opérateur du système. Des techniques semblables ont déjà été utilisées par le passé pour mettre hors service des infrastructures critiques diverses, depuis des réseaux de distribution d'électricité jusqu'aux contrôleurs logiques de centrifugeuses dans le secteur nucléaire.

Les chercheurs ont découvert une exemplaire d'Irongate vers la fin de l'année 2015 sur VirusTotal alors qu'ils recherchaient des droppers compilés à l'aide PyInstaller. L'échantillon trouvé ressemblait très fort aux malwares qui visaient les systèmes d'automatisation industrielle et autres systèmes de contrôle des procédés industriels. Il se fait que ce modèle avait été chargé pour analyse en 2012, mais aucun logiciel antivirus ne l'avait reconnu.

L'analyse a démontré que le malware utilise une technique de l'homme du milieu qui permet de réaliser des attaques contre une application personnalisée de l'utilisateur qui fonctionne dans un milieu de modélisation des contrôleurs logiques programmables Step 7 de Simens Les experts ont découvert également une bibliothèque dynamique capable de masquer le comportement malveillant du code exécutable. Cette DLL est capable d'enregistrer cinq secondes du trafic « normal » provenant du contrôleur logique programmable modélisé ; l'attaquant peut reproduire ce fragment afin de masquer le transfert des données codées en dur vers l'équipement d'imitation.

Les chercheurs ont été surpris de voir que pour rendre l'analyse plus difficile, ce malware spécialisé se comporte comme un malware traditionnel : lorsqu'il est exécuté sur une machine virtuelle ou dans un bac à sable (Cuckoo), il passe en mode de veille et refuse de s'exécuter.

« Bien que Stuxnet soit plus complexe sur le plan technique, Irongate possède quelques traits similaires » a déclaré Sean McBride, analyste antivirus principal chez FireEye. Pour être plus précis, il a noté que ces deux malwares sont destinés à attaquer un système particulier de gestion et ils utilisent des outils de protection contre la détection : Stuxnet est capable de détecter la présence d'un logiciel antivirus et Irongate, celle d'une machine virtuelle. Toutefois, à la différence de ses rares confrères commeBlackEnergy, Havex, et même Stuxnet, Irongate n'est pas très répandu dans la pratique : il fonctionne seulement dans les environnements simulés orientés sur les systèmes Siemens.

Qui est donc à l'origine de ce malware et quel est son objectif ? FireEye avance trois hypothèses en réponse. Tout d'abord, les experts supposent que son auteur peut avoir nourri l'espoir que quelqu'un transfèrerait ce code depuis l'environnement simulé et commencerait à l'utiliser dans son environnement de travail. Il est également possible qu'Irongate soit un modèle expérimental et que son créateur a décidé de vérifier à quel point il était facile de le détecter via les services VirusTotal. La troisième hypothèse est celle considérée comme la plus probable par FireEye : un expert en sécurité de l'information a oublié qu'il avait soumis ce code à une vérification il y a un certain temps.

« Il convient de fournir de plus gros efforts dans le secteur pour détecter les menaces qui visent les systèmes de contrôle des procédés industriels » conclut Dan Scali, conseiller principal de la division conseil de FireEye sur les questions de sécurité des systèmes d'automatisation industrielle. « Globalement, il n'y a pas eu de gros progrès dans la résolution des problèmes posés par Irongate depuis Stuxnet. Dans la mesure où l'accès à de tels attaques se démocratise, le thème de l'adéquation des mesures de protection est source de préoccupation.

Réagissez à cet article

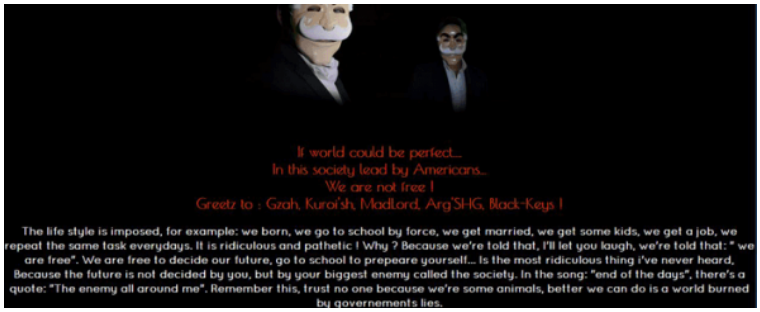
Original de l’article mis en page : Un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet – Securelist

---

Déffaçage (piratage) du site Internet des espaces de la CAF

Déffaçage (piratage) du site Internet des espaces de la CAF

Barbouillage de sites – Plusieurs pirates informatiques se sont amusés à modifier des espaces Internet appartenant à la CAF.



Barbouillage de sites – Samedi 11 juin, vers 16 heures, plusieurs sites Internet appartenant à la Caisse des Allocations Familiales Françaises se sont retrouvées modifiés, du barbouillage de sites, par trois pirates informatiques « différents » : Mad Lord, ArG'Sh et Sneaky. Les sites impactés (ils étaient tous sur le même serveur) : lacafrecrute.org, lacafrecrute.com, fraude-caf.fr et lacaf.com.Les adolescents ont taggué les espaces ainsi infiltrés.

Barbouillage de sites

*Dans le premier cas, celui de lacaf.com, le pirate indique que « **Si le monde pouvait être parfait … sans corruption, duperie … Ensemble, nous pouvons agir pour créer** !« . Dans le site dédié à la lutte contre la Frauce, ArG'SH affiche une jeune fille tirée d'un manga et une tirade sur la corruption des gouvernements. Même son de cloche pour lacafrecrute.com, espace dédia aux offres d'emplois à la CAF [le site lacafrecrute.fr fonctionne, NDR] , modifié par Sneaky. Les adresses Internet des sites impactés sont redirigées vers l'url officiel de la Caisse des Allocations Familiales : caf.fr. D'après mes constations, les données privées et sensibles appartenant aux allocataires n'ont pas été impactées.*
Article original de Damien BANCAL

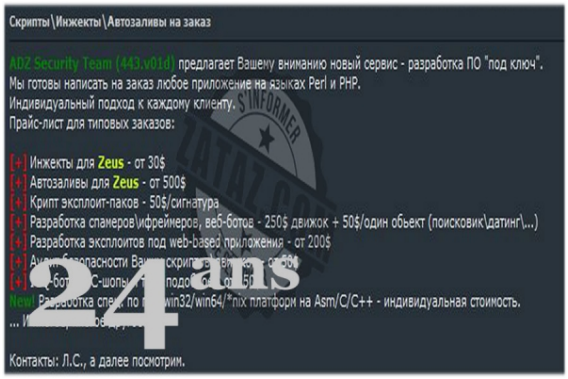
Réagissez à cet article

Original de l'article mis en page : Barbouillage de sites ! Des espaces de la CAF piratés – ZATAZ

Prison ferme pour les auteurs de SpyEye botnet

Prison ferme pour les auteurs de SpyEye botnet

Le code malveillant SpyEye botnet a fait de gros dégâts en son temps. Les deux auteurs, Russe et Algérien, de ce kit informatique dédié à l'espionnage viennent d'écoper de 24 ans de prison ferme.



Les deux pirates Russe et Algérien cachés derrière le code malveillant SpyEye ont été reconnus coupables par la justice américaine d'avoir fabriqué et vendu ce kit malveillant dont le but premier était d'infiltré les ordinateurs pour espionner et voler les données des machines infiltrées.

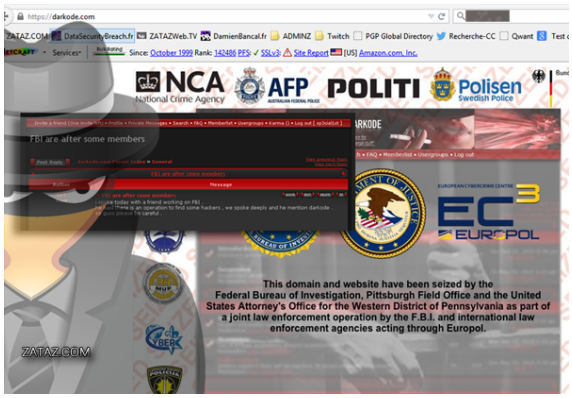
Le prix de SpyEye botnet

Les deux pirates ont été condamnés à 24 ans de prison ferme (les deux peines cumulées). Une condamnation forte pour un outil, aussi baptisé Zeus, qui a permis d'infecter des centaines de milliers d'ordinateurs de par le monde. Une peine de neuf ans et six mois pour Aleksandr Andreevich Panin (27 ans), connu sur la toile sous le pseudonyme de « Gribodemon » et « Harderman ». Le FBI avait lancé un « Wanted » sur la tête de Panin de 3 millions de dollars. En juin 2015, l'ensemble des interactions de Zeus / SpyEye avait été stoppé par le FBI, Europe et Eurojust. Plusieurs dizaines de personnes ont été arrêtés, de l'utilisateur de SpyEye aux blanchisseurs d'argent volé.

L'Algérien Hamza Bendelladj, alias Bx1 a écopé de 15 ans. Ce dernier, âgé de 27 ans, était le partenaire d'affaires de Panin. Ce ressortissant algérien avait plaidé coupable en Juin 2015. Il avait modifié SpyEye pour réaliser son propre outil malveillant qui lui a permis de voler 200.000 numéros de carte de crédit. Bendelladj, baptisé « Le pirate souriant » avait été arrêté à Bangkok, en janvier 2013. Extradé aux USA en mai 2013. Il vient de perdre définitivement son grand sourire !
Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.

Dans les outils proposés par les pirates, des ransomwares, comme Locker

Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.



SpyEye, comme j'avais pu vous le montrer à l'époque [1e capture écran de cet article], était commercialisé dans le black market, dans une boutique baptisée à l'époque DarkCode.
Article original

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Prison ferme pour les auteurs de SpyEye botnet

---

32 millions de mots de passe Twitter dérobés

	32 millions de mots de passe Twitter dérobés

---

Après LinkedIn, MySpace et Tumblr, Twitter a lui aussi été victime d'un piratage massif. 32,8 millions de comptes seraient affectés.

Une nouvelle fuite de données pour un réseau social. Un hacker russe affirme avoir dérobé 379 millions d'adresses email et de mots de passe non chiffrés associés à des comptes Twitter. Identifié sous le pseudonyme Tessa88, il aurait mis en vente la base de données en question sur VK, le Facebook russe. LeakedSource, qui a révélé l'information, estime que 32,8 millions de comptes seraient effectivement compromis, une fois les doublons éliminés.

«Nous sommes convaincus que ces noms d'utilisateurs et les identifiants n'ont pas été obtenus par une violation des données Twitter. Nos systèmes n'ont pas été hackés», a déclaré un porte-parole de Twitter. La base de données serait donc le fruit d'une campagne de malware ciblant les particuliers pour récupérer leurs mots de passe.

Sollicité par Techcrunch, Troy Hunt, le fondateur de site haveibeenpwned.com qui permet de voir si une adresse mail fait partie d'une base de données piratée, émet des doutes par rapport à l'authenticité des données piratées: «Les piratages de comptes que nous avons vus jusqu'à présent sont très probablement le résultat de la réutilisation de données issues d'autres piratages», indique-t-il.

Une incitation de plus à modifier son mot de passe

Si Leakedsource propose de vérifier si vos identifiants et mots de passe sont dans leur base et de les retirer gratuitement, le plus simple reste encore de modifier son mot de passe.

Twitter a suggéré au passage de le complexifier, en suivant ses recommandations.

7 Juin

Twitter Support
@Support
To help keep people safe and accounts protected, we've been checking our data against what's been shared from recent password leaks.
Suivre

Twitter Support
@Support
Any time is a good time to make sure your account is secure, starting w[illegible] an updated password. More tipshttps://support.twitter.com/articles/76036
00:36 – 7 Juin 2016

Safe Tweeting: the basics
Keeping your account secure We want Twitter to be a safe and open community. This help page provides some information and tips to help you practice safe Tweeting and keep your acco
support.twitter.com
•
•
128128 Retweets
•
170170 j'aime

Selon la liste des données divulguées, bien trop de ***mots de passe*** *restent basiques et facilement trouvables. 123455 prend la première place du podium, suivi de 123456789, qwerty et du classique password.*
Ce piratage suit celui de MySpace, de Tumblr et de LinkedIn. ***100 millions de mots de passe*** *du réseau professionnel récupérés en 2012 ont été mis en vente mi-mai. Ce piratage avait valu à Mark Zuckerberg, adepte du mot de passe unique «dadada», de* ***voir ses comptes Twitter et Pinterest piratés****.*
Article original

Réagissez à cet article

Original de l’article mis en page : Un hacker russe prétend avoir dérobé des millions de mots de passe Twitter

---

La France dans le Top 10 du piratage informatique

La France dans le Top 10 du piratage informatique

NATIC Magazine vous fait une synthèse de l'actualité tournant autour des problématiques de cybersociété: Hacking, Sécurité, Codes malveillants, Piratage, Vie privée numérique, Protocole d'alerte, Alerte propagande, Web Tv, etc.

Le rapport annuel de Symantec sur le piratage informatique est une fois encore percutant. Selon le géant mondial de la cybersécurité, la France fait partie des 10 pays les plus concernés par les attaques informatiques. En 9ème position mondiale, le pays subit plus de 10 millions de tentatives avérées par an, en forte hausse d'une année sur l'autre.
Selon la version 2016 du rapport, les brevets technologiques et les trésors de propriété intellectuelle des grands groupes français attirent les meilleurs pirates mondiaux. Lancées par des concurrents, des activistes ou même des états, ces attaques visent également des PME ou même des particuliers ce qui est plus étonnant. Ces derniers sont très vulnérables notamment lorsqu'ils utilisent les réseaux sociaux. On observe en particulier une percée remarquable de l'utilisation des ransomwares ou rançongiciels – en hausse de 260% en France en 2015. Le phénomène prend de l'ampleur.
Dans le rapport de Symantec version 2016, le Top 3 des pays victimes de piratage en 2015 est constitué de la Chine, des Etats-Unis et de l'Inde.
Article original

Réagissez à cet article

Original de l’article mis en page : La France dans le Top 10 du piratage