

Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

✕	Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs
---	--

Script kiddies and online criminals around the world have reportedly started exploiting NSA hacking tools leaked last weekend to compromise hundreds of thousands of vulnerable Windows computers exposed on the Internet.

Last week, the mysterious hacking group known as Shadow Brokers leaked a set of Windows hacking tools targeting Windows XP, Windows Server 2003, Windows 7 and 8, and Windows 2012, allegedly belonged to the NSA's Equation Group.

What's Worse?

Microsoft quickly downplayed the security risks by releasing patches for all exploited vulnerabilities, but there are still risks in the wild with unsupported systems as well as with those who haven't yet installed the patches.

Multiple security researchers have performed mass Internet scans over the past few days and found tens of thousands of Windows computers worldwide infected with **DoublePulsar**, a suspected NSA spying implant, as a result of a free tool released on GitHub for anyone to use.

Security researchers from Switzerland-based security firm Binary Edge performed an Internet scan and detected more than 107,000 Windows computers infected with DoublePulsar.

A separate scan done by Errata Security CEO Rob Graham detected roughly 41,000 infected machines, while another by researchers from Below0day detected more than 30,000 infected machines, a majority of which were located in the United States.

The impact ?

DoublePulsar is a backdoor used to inject and run malicious code on already infected systems, and is installed using the **EternalBlue** exploit that targets SMB file-sharing services on Microsoft's Windows XP to Server 2008 R2.

Therefore, to compromise a machine, it must be running a vulnerable version of Windows OS with an SMB service expose to the attacker.

Both DoublePulsar and EternalBlue are suspected as Equation Group tools and are now available for any script kiddie to download and use against vulnerable computers.

Once installed, DoublePulsar used hijacked computers to sling malware, spam online users, and launch further cyber attacks on other victims. To remain stealthy, the backdoor doesn't write any files to the PCs it infects, preventing it from persisting after an infected PC is rebooted...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs*

Les services Cloud au centre d'attaques d'entreprises par APT10

✕	Les services Cloud au centre d'attaques d'entreprises par APT10
---	---

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. « *Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience* », a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme « *l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées* ». Pas moins.

✘ De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. « *PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles* », indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

Forum International de la Cybersécurité 24 et 25 janvier 2017 à LILLE

✕	Forum International de la Cybersécurité 24 et 25 janvier 2017 à LILLE
---	---

Lille grand palais accueille à partir de ce mardi 24 janvier à 09:30 la 9ième édition du Forum International de la Cybersécurité.

Favoriser l'innovation

Résolument tournée vers l'innovation, les écoles Epitech ont développé au sein de chaque campus des Innovation, des espaces dédiés aux expérimentations, au prototypage et au développement de projet innovants. Ces Hub reposent sur une méthodologie collaborative et transversale, reposant sur 5 domaines de compétences permettant de balayer le champ des innovations dont celui de la sécurité.

Ainsi, situé au sein de l'Espace Carrières, réunissant des écoles spécialisées, des étudiants d'Epitech et des encadrants pédagogiques proposeront des démonstrations d'attaques/défense lors des Hacking Trucks du Forum.

Les démonstrations proposées par l'Epitech :

- Démonstration de la facilité d'interception et d'altération des communications sur le(s) réseau(x) GSM et/ou Wi-Fi, par l'interception de SMS, de conversations vocales (pour le GSM) et autres communications quelconques (pour le Wi-Fi),
- Démonstration Ransomware : Démonstration du mode opératoire et des conséquences d'une campagne d'attaque par rançongiciel,
- Hacking Live : Démonstration d'une attaque en live d'une plateforme CMS Web, de la découverte de la faille Web jusqu'à la prise de contrôle du serveur l'hébergeant,
- Poisontap : À l'aide d'un matériel peu coûteux, il suffira de quelques minutes à nos étudiants démonstrateurs pour siphonner les communications d'un ordinateur, même verrouillé. Ces démonstrations ont pour but de sensibiliser tout visiteur sur la protection des données, notamment avec le développement des usages et des nouvelles technologies afin que les consommateurs soient de plus en plus soucieux de leur sécurité tout en gardant un confort d'utilisation. Le FIC est un événement gratuit dont l'inscription est soumise à la validation des organisateurs...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Lille FIC 2017

Et si la publicité sur Internet était aussi infectée par des malwares ?

x	Et si la publicité sur Internet était aussi infectée par des malwares ?
---	---

Les chercheurs ESET viennent de découvrir Stegano, un nouveau kit d'exploitation se propageant via des campagnes publicitaires. De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés.

Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.

Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.

Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible **permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur.**

« **Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware,** » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.

« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.

Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.

Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovsky, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute la France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Une série de clics suffisent à vous identifier

✖	Une série de clics suffisent à vous identifier
---	--

Corréler l'historique des pages Web visitées aux profils Twitter permet d'identifier les internautes, expliquent des chercheurs de Princeton et de Standford. Ou quand le Big Data vient lever ce qui restait d'anonymat sur le Web.

L'anonymat sur Internet, un vœu pieux ? C'est en somme la démonstration d'une équipe de chercheurs des universités de Princeton et Standford. Ces derniers ont imaginé une extension pour le navigateur Chrome qui permet aux utilisateurs de prendre conscience de l'intérêt des traces qu'ils laissent sur le Net pour des publicitaires ou des espions. L'utilitaire, appelée Footprints, collecte les liens cliqués par l'utilisateur au cours des 30 derniers jours et, à partir de ces seules informations, renvoie une liste de 15 profils Twitter susceptibles de coller à cet usage. Ensuite, l'extension s'efface d'elle-même, assurent les chercheurs.

Professeur assistant à l'université de Standford, Sharad Goel explique que l'objectif de cet outil est avant tout éducatif : « *nous n'envisageons pas de rendre cet outil accessible à d'autres, il s'agit avant tout de réveiller les consciences.* » Un outil de ce type permettrait par exemple à une entreprise traçant déjà ses utilisateurs – soit la totalité des sites marchands notamment – de deviner l'identité des internautes, par corrélation avec leur usage d'un réseau social. En effet, si les publicitaires ou les spécialistes du marketing analysent déjà les traces laissées par les utilisateurs pour personnaliser l'expérience des clients online, ils ne sont en général pas en mesure de remonter jusqu'à l'identité réelle de l'internaute. Les chercheurs montrent que cette anonymat déjà tout relatif pourrait en pratique être levé, grâce à des analyses statistiques et au Big Data.

Dis-moi ce que tu cliques, j'en déduirai qui tu es

Dans un billet de blog, une étudiante de Standford ayant participé à la conception de Footprints, Jessica Su, explique le principe de la méthode : « *Partant de la combinaison unique de pages Web qu'un individu a visitées, nous déterminons les fils de réseau social similaires à cet historique, calculant une liste d'utilisateurs qui ont toutes les chances d'avoir produit cette série de clics. De cette façon, nous pouvons relier l'identité réelle d'une personne à un jeu de liens visités, y compris les liens qui n'ont jamais été postés publiquement sur aucun réseau social.* »...[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Une série de clics et Twitter suffisent à vous identifier

Cybersécurité et Cyberdéfense : leviers de l'intelligence économique



La transition numérique en
Afrique étroitement liée à
l'intelligence économique

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.

Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.

De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberspace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.

Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant...[lire la suite]

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : **Cybersécurité et Cyberdéfense : leviers de l'intelligence économique. »**