Est-ce que la campagne présidentielle d’Emmanuel Macron a été vraiment piratée par les Russes ?

	Est-ce que la campagne présidentielle d’Emmanuel Macron a été vraiment piratée par les Russes ?

Une société de cybersécurité affirme qu'un groupe de hackers russes a tenté de déstabiliser la campagne d'Emmanuel Macron, confirmant les dires de l'équipe du candidat.

L'équipe d'Emmanuel Macron dénonçait, en février, « *plusieurs milliers d'attaques* » contre ses structures informatiques. Dans un rapport consulté par *Libération* et *20 Minutes*, lundi 24 avril, la société de cybersécurité Trend Micro confirme que le mouvement En marche ! a été la cible, pendant les derniers mois de la campagne présidentielle, de pirates informatiques identifiés comme appartenant au groupe de hackers russes Fancy Bear.

Que sait-on de ces tentatives de piratage ?

Entre le 15 mars et le 17 avril, selon *Libération*, la société Trend Micro « *a repéré quatre sites web reproduisant des pages d'accueil de services en ligne Microsoft, avec des adresses destinées à tromper les utilisateurs* ». Les noms de domaine suivants ont été créés : onedrive-en-marche.fr, mail-en-marche.fr, portal-office.fr et accounts-office.fr. L'objectif de ces noms, dont deux imitent le nom du site officiel d'Emmanuel Macron (en-marche.fr), est d'inciter les destinataires d'un mail frauduleux à se connecter et renseigner identifiant et mot de passe…

Connaît-on les conséquences de ce piratage ?

L'équipe d'Emmanuel Macron affirme que ces manœuvres n'ont pas eu d'effet. Contacté par *20 Minutes*, Mounir Mahjoubi, responsable numérique de la campagne En marche !, assure qu'« *aucune de ces boîtes mail n'a été hackée* ». « *Nous avions détecté ces noms de domaine et plusieurs autres*, poursuit Mounir Mahjoubi. *Certaines personnes ont cliqué sur les liens, mais n'ont renseigné ni identifiant ni mot de passe* », explique-t-il encore à *Libération*, et aucune donnée n'a été volée…[lire la suite]

« En général on ne sait pas qui attaque », explique le directeur général de l'ANSSI. « Les attaques peuvent venir d'absolument partout. Mieux vaut se demander comment faire pour se protéger ».

Denis JACOPINI : A ce jour, nous n'avons aucune certitude sur les auteurs de l'attaque de TV5 monde en avril 2015. Bientôt 2 ans plus tard, les preuves recueillies ne sont pas suffisantes pour accuser Russes, Chinois ou d'autres états. Alors quelques jours ou quelques semaines à la suite des élections Françaises ne suffiront pas à nous assurer de l'identité des auteurs de ces ingérences. On peut avoir des doutes, mais nous auront difficilement des certitudes.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Présidentielle : trois questions sur les soupçons de piratage informatique ciblant En marche !*

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

Qu’est ce que le Smishing ?

	**Qu’est ce que le Smishing ?**

Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Tout comme le phishing, un message à caractère urgent est envoyé à un utilisateur pour qu'il entreprenne une action. Lors d'un Smishing, c'est un message texte qui est envoyé à un utilisateur sur son téléphone. Le texte du message demande généralement à l'utilisateur d'appeler un numéro de téléphone ou de se rendre sur un site Internet pour effectuer une action précise. La plupart du temps, lorsque vous composez ce numéro de téléphone, vous êtes automatiquement redirigé vers un serveur vocal interactif. Il est demandé à l'utilisateur de fournir des informations personnelles (mot de passe) ou bancaires (numéro de carte bancaire).

Souvent, cette forme de phishing implique un message de texte dans un SMS ou dans un numéro de téléphone. Le numéro de téléphone comporte un message automatisé à partir duquel vos informations commencent à être réellement recueillies. Ce qui rend particulièrement effrayant le smishing, c'est que l'on a plutôt tendance à faire confiance à un SMS qu'à un e-mail. La plupart des gens sont conscients des risques encourus pour la sécurité lorsqu'on clique sur des liens contenus dans des e-mails. Mais c'est moins le cas lorsqu'il s'agit de SMS.

Ne cliquez jamais sur les liens contenus dans ces messages et ne rappelez jamais ces numéros.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Que sont le Smishing et le Vishing ? | Aide Homelidays*

Toutes les sirènes d'urgence de Dallas piratées et déclenchées

Toutes les sirènes d'urgence de Dallas piratées et déclenchées

---

Tornade imminente ? Menace non identifiée mais liée aux récents bombardements américains en Syrie ? Dans la nuit du vendredi 7 au samedi 8 avril, les habitants de Dallas, au Texas, ont eu tout le temps de se demander pourquoi les 156 sirènes habituellement utilisées pour avertir d'un danger météorologique ont retenti pendant plus d'une heure et demie, entre 23h40 et 1h20.

Si la municipalité a parlé dans un premier temps de « *dysfonctionnement* », elle a fini par reconnaître qu'il s'agissait d'un piratage, dont le ou les auteur(s) reste(nt) à ce jour non identifié(s).
En pleine nuit, Dallas a donc pris des airs de ville submergée par une catastrophe de grande ampleur, comme le montrent les vidéos postées par différents habitants sur les réseaux sociaux, qu'ils soient ouvertement inquiets ou s'interrogent plus ou moins ironiquement : « *Vous vous êtes déjà demandé à quoi ressemblait la fin du monde ?* » D'autant qu'il était impossible d'échapper aux sirènes, celles-ci retentissant du nord au sud de la ville, selon la disposition voulue par la municipalité.

L'IDENTITÉ DU OU DES HACKER(S) RESTE INCONNUE

Les sirènes ont retenti une quinzaine de fois pendant 1 minute 30 à chaque nouveau déclenchement, alors que les équipes techniques de la ville les éteignaient en vain, comme l'explique Sana Syed, porte-parole de la municipalité : « *À chaque fois que nous pensions les avoir éteintes, les sirènes sonnaient de nouveau car le hacker nous piratait en continu* ». Résignée, la ville a finalement désactivé entièrement le système d'alarme, y compris pendant le week-end : il doit être relancé à temps pour les tornades attendues cette semaine.
Quant à l'identité du ou des pirate(s), le mystère reste entier. « *Nous sommes convaincus que le piratage provient de la région de Dallas car vous devez nécessairement être à proximité du signal pour le déclencher* » souligne Sana Syed. Rocky Vaz, directeur du Bureau de gestion des urgences de Dallas, se montre assez pessimiste sur les chances de retrouver le coupable, une recherche qu'il assimile à trouver « *une aiguille dans une botte de foin* » contrairement au maire de la ville, Mike Rawlings, qui affirme que les autorités « *retrouveront et poursuivront le responsable, quel qu'il soit* ». La municipalité a notamment demandé l'aide de l'Agence de régulation des télécoms pour mener l'enquête…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Un hacker déclenche toutes les sirènes d'urgence de Dallas, les habitants paniquent — Tech — Numerama*

Un virus vous force à jouer à un jeu vidéo pour débloquer votre ordinateur

Un virus vous force à jouer à un jeu vidéo pour débloquer votre ordinateur

---

Au lieu d'honorer une demande de rançon, les victimes de ce logiciel malveillant doivent se procurer un jeu vidéo et atteindre un certain score en « mode dément » pour récupérer leurs données.
par Jamal El Hassani

Voilà la preuve que certains hackers nuisent à leur prochain dans le simple but de s'amuser. Un pirate a créé un logiciel de rançon assez original et qui ne lui rapportera pas un sou. Habituellement, les « ransomware » ou rançongiciels, sont des programmes qui chiffrent toutes les données présentes sur un appareil électronique, les rendant inaccessibles. Pour récupérer ses données, la victime doit payer, sans quoi les pirates menacent souvent de les détruire.
Mais finalement, l'argent n'est pas la manière la plus difficile de se débarrasser des ces programmes, pour ceux qui en ont les moyens. Le pirate a donc préféré rendre la vie impossible à ses victimes en les obligeant à atteindre un certain score dans un jeu vidéo réglé sur un niveau de difficulté très élevé. Son malware, baptisé resenWare, a été repéré par Malware Hunter Team, un site spécialisé dans la traque de ces logiciels malveillants, qui n'avait jamais rien vu de la sorte.

Le jeu auquel il faut jouer est *Undefined Fantastic Object*, un titre japonais sorti sur PC en 2009 dans lequel on tire sur des vagues d'ennemis successives en évitant leur projectiles. Comme on peut le voir sur cette vidéo du jeu en mode « dément », la difficulté choisie par les pirates, le challenge a l'air relevé.

Il faut s'acheter le jeu

Mais avant de réussir à atteindre le score requis, encore faut-il mettre la main sur le jeu: le logiciel malveillant ne fournit pas de copie de *Undefined Fantastic Object*, c'est à la victime de se l'acheter.
Heureusement, les chasseurs de malwares ont trouvé une faille dans ce programme. Le logiciel met en garde ceux qui essaieraient de tricher, affirmant que cela détruira la clé de chiffrement, seul moyen de récupérer les données. Mais ces menaces sont un mensonge. Il est en fait possible de tricher en se rendant dans les fichiers du jeu pour modifier son score afin de dépasser celui que requiert le malware pour récupérer ses données…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

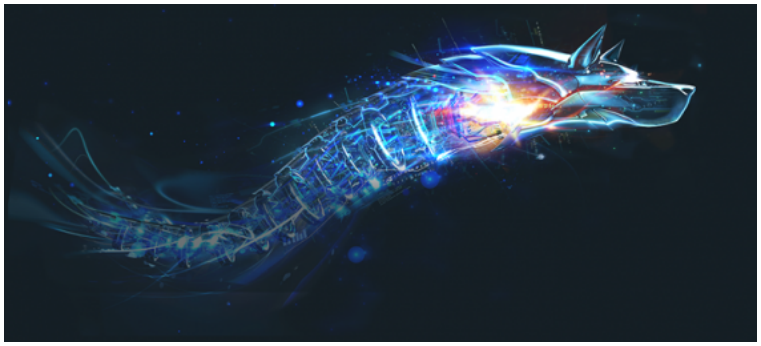
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Ce malware vous force à jouer à un jeu vidéo pour débloquer votre ordinateur – SFR News*

Victime du ransomware Bart ? Bitdefender publie un outil gratuit de déchiffrement

	**Victime du ransomware Bart ? Bitdefender publie un outil gratuit de déchiffrement**

L'outil proposé par Bitdefender fonctionne avec tous les échantillons connus. Le ransomware Bart, qui chiffre les appareils sans avoir besoin de connexion Internet, a été analysé par les chercheurs des Bitdefender Labs. Les victimes de ce malware peuvent désormais télécharger l'outil gratuit de déchiffrement afin de récupérer leurs données perdues.

Communiqué de presse – Alors que ce ransomware a été détecté en circulation pour la première fois en juillet 2016, Bitdefender est le seul éditeur de solutions de sécurité à proposer un outil de déchiffrement pour toutes les versions de Bart. L'outil de déchiffrement du ransomware Bart permet de déchiffrer les fichiers avec des extensions « .bart.zip », « .bart » et « .perl » et est également téléchargeable sur le site Internet « No More Ransom » depuis le 4 avril 2017.
Cet outil est le fruit d'une collaboration entre Bitdefender, Europol et la police roumaine en soutien à l'initiative « *No More Ransom* » lancée par le Centre européen de lutte contre la cybercriminalité d'Europol.

Le fonctionnement du ransomware Bart
Contrairement à d'autres familles de ransomwares, Bart chiffre les fichiers des victimes sans avoir besoin de recourir à une connexion Internet. Cependant, le processus de déchiffrement nécessite pour sa part une connexion Internet afin d'accéder au serveur de commande et contrôle (C&C) de l'attaquant, de pouvoir transférer des bitcoins et recevoir la clé de déchiffrement.
Alors que les premières versions de Bart se limitaient à un chiffrement plutôt rudimentaire, tel que la création d'archives .zip protégées par mot de passe, les nouvelles versions vont bien au-delà cette méthode.

Voici comment fonctionne Bart :
• Il supprime les points de restauration du système
• Il génère une clé de chiffrement en se basant sur les informations de la machine de la victime
• Il comptabilise tous les fichiers et les chiffre à l'aide de la clé générée
• Il utilise une master key pour chiffrer la clé utilisée pour chiffrer les fichiers (qui devient l'identifiant unique de la victime, l'UID)
• Il affiche l'avis de rançon et redirige vers un site Internet .onion (l'URL contient l'UID de la victime)…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Bitdefender publie un outil gratuit de déchiffrement du ransomware Bart | UnderNews*

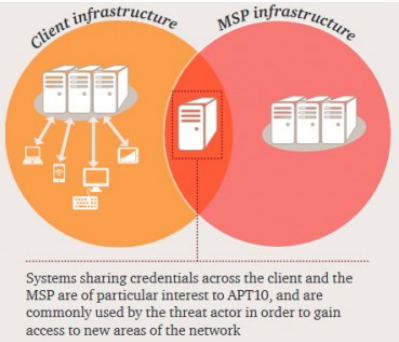
Les services Cloud au centre d'attaques d'entreprises par

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

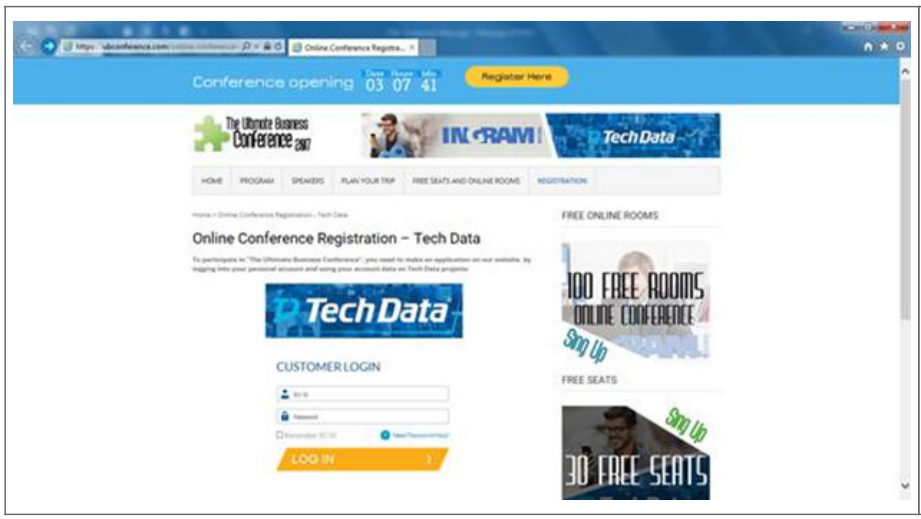
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux



Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

---

Chers revendeurs informatiques, attention à la nouvelle arnaque. Les intentions des pirates ne sont pas encore connues, mais les intentions sont forcément malveillantes.

En tant que revendeur informatique, il est fort probable que vous commandiez votre matériel destiné à la revente ou non chez les principaux et parmis les plus anciens grossistes et importateurs Français : Ingram ou Techdata.
Une récente communication de Techdata, qui nous a été remontée par un précieux partenaire Parisien, nous informe que Techdata vient de lancer l'alerte suivante auprès de ses clients :

Cher client,
Il a été porté à notre connaissance que certains Clients de TECH DATA ont reçu des emails comportant un lien internet vers un site web frauduleux leur demandant :
– de s'inscrire à une conférence dans laquelle TECH DATA et d'autres distributeurs participeraient,
– de fournir des informations type login et mot de passe de TECH DATA ainsi que d'autres informations sensibles.
Le site Web apparaît comme indiqué ci-dessous :

Veuillez noter que ce site web n'est d'aucune façon associé à TECH DATA. La sécurité de nos partenaires est une priorité pour TECH DATA et nous n'autorisons aucun tiers à collecter les identifiants de connexion de nos clients.
Aussi, actuellement nous œuvrons avec les autorités compétentes pour la fermeture de ce site frauduleux.
A ce jour, à notre connaissance les clients européens ne semblent pas affectés, ce site frauduleux visant les clients américains principalement.
Cependant, nous comptons sur votre vigilance et vous remercions de nous informer dans le cas où vous recevriez des emails contenant des liens vers ce site internet ou similaires en vous adressant à l'adresse suivante : itsecurity@techdata.com
Nous attirons votre attention sur la sophistication et l'augmentation de la cybercriminalité (phishing), dès lors restez vigilants.
Nous vous remercions de votre attention et collaboration.
Tech Data Europe

Comme vous pouvez le remarquer, à l'instar de KPMG pourtant spécialisé en audit et conseil dans de nombreux domaines dont la sécurité informatique, pourtant victime d'une arnaque au Président leur ayant coûté plusieurs millions d'Euros (7,6) en 2014, les professionnels de l'informatique sont aussi la cible des pirates.
Nous espérons que, même si la plupart n'ont pas assisté à nos conférences de sensibilisation à la Cybercriminalité, ils sauront à quoi ressemble le loup pour ne pas le laisser rentrer dans la bergerie.

Denis JACOPINI

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *E-mailing Tech Data France*

Alerte : un ransomware sur Android trompeur arrive à

échapper aux antivirus

	Alerte : un ransomware sur Android trompeur arrive à échapper aux antivirus

Des chercheurs en sécurité ont trouvé un ransomware pour Android, capable d'éviter la détection par les antivirus. Il n'est dans l'absolu pas considéré comme très dangereux mais, comme certains malwares actuels, pourrait représenter une tendance.
L'histoire des malwares n'est pas nouvelle. Si l'on en croit un rapport publié en février par Eset (éditeur notamment de NOD32), le nombre d'attaques par ce vecteur a augmenté de 50 % en 2016 sur la plateforme de Google. Une conjonction de facteurs en est responsable, mais l'utilisation des boutiques tierces et les méthodes visant à tromper l'utilisateur sont clairement les plus présentes.

Des évolutions que l'on retrouve dans un nouveau ransomware découvert par la société ZScaler.
Rappelons – s'il est encore besoin de le faire – qu'il s'agit d'un logiciel malveillant dont l'objectif est de chiffrer les données de l'utilisateur puis de lui réclamer une rançon. Il peut payer et avoir une chance de les retrouver, ou refuser et faire avec les conséquences. Les sauvegardes régulières et une bonne hygiène informatique sont les deux seules armes vraiment efficaces contre ce type de menace.

Un compte à rebours de quatre heures

…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Android : un ransomware trompeur arrive à échapper aux antivirus*

Alerte : Une publicité sur Skype propage un rançongiciel

Alerte : Une publicité sur Skype propage un rançongiciel

Selon plusieurs utilisateurs, un logiciel malfaisant serait répandu via une publicité sur Skype par Roman De Schrijver

© Reddit

La publicité en question se présente comme une fausse page web d'Adobe. Ensuite, une fenêtre émergente surgit demandant de mettre à jour Adobe Flash Player. Si les utilisateurs se laissent tenter, c'est en réalité un maliciel qui s'installe sur leur ordinateur. Selon toute vraisemblance, ce maliciel est plutôt un rançongiciel (ransomware), à savoir un programme qui verrouille votre ordinateur et crypte vos données, de telle sorte que vous ne puissiez vous-même plus y accéder.

On ne sait pas encore à ce jour combien de victimes la fausse publicité a faites. Ce n'est du reste pas la première fois que les utilisateurs de Skype sont confrontés à ce genre d'annonce factice. Quoi qu'il en soit, il vous est toujours conseillé de rester vigilant vis-à-vis de ce que vous téléchargez et des liens sur lesquels vous cliquez.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Une publicité sur Skype propage un rançongiciel – ICT actualité – Data News.be*