GÉOPOLITIQUE PROFONDE

VEILLE ET SYNTHÈSE STRATÉGIQUES SUR LES ENJEUX DE CE MONDE

ACTUALITÉS CONCERNANT LA SÉCURITÉ INFORMATIQUE

Les principales cybermenaces

Au niveau des menaces les plus courantes actuellement, ce sont toujours les attaques de botnets qui restent persistantes. Un tout récent rapport du Centre de Recherche sur les Menaces de CenturyLink, Inc. révèle avoir détecté, au cours de l'année 2017, 195 000 menaces/jour en moyenne touchant environ 104 millions de cibles uniques par le biais de botnets. La France fait partie des 5 pays européens au plus fort volume de trafic Internet malveillant. Les cibles touchées sont des serveurs, des ordinateurs, des appareils mobiles et tout appareil connecté à Internet. Le Centre recommande plus de vigilance aux entreprises, gouvernements et consommateurs face aux risques découlant de ce style d'attaques. Les botnets peuvent servir au spam, au hameçonnage pour voler des données sensibles, aux virus informatiques, aux attaques informatiques par déni de service (DDoS) ou aux *BruteForcing* (trouver des mots de passe d'utilisateurs).

Cylance Inc. a également publié son rapport sur les principales cybermenaces mondiales sur la base des expériences de ses clients en 2017. Les attaques à grande échelle continuent de croître, particulièrement les ransomware dont le nombre s'est multiplié par 3 l'année dernière. Ils ciblent principalement le secteur de la santé et l'industrie alimentaire. Les vecteurs d'attaques les plus courants restent le phishing et le téléchargement de pièces infectées. Une croissance exponentielle des variantes de malware avec une courte durée de vie et des changements très réguliers rendent également la lutte difficile. À noter que 50 à 70 % des attaques de 2017 ont exploité des vulnérabilités connues et signalées plus de neuf mois auparavant. Les menaces les plus fréquentes basées sur DNS (*Domain Name System*) ont changé en 2018 par rapport à l'année précédente. Les malware exploitant le DNS sont les menaces les plus courantes avec le phishing (36 %), suivis par les attaques par déni de service (20 %), la saturation (*lockup*) de domaine (20 %), et le DNS tunneling (20 %).

En 2017, le secteur financier est désormais le secteur le plus attaqué à l'échelle mondiale, selon le rapport annuel GTIR (*Global Threat Intelligence Report*) de NTT Security. Les offensives sont passées de 14 % à 26 % en un an (2016-2017). Le secteur technologique a également connu une recrudescence de problèmes avec une augmentation d'environ 25 % des atteintes par rapport à 2016, ce qui représente 19 % des agressions cyber dans le monde. À l'inverse, le secteur gouvernemental est bien moins touché (-5 %). Notons une fois de plus, une fulgurante croissance des ransomwares, avec une augmentation de 350 % des détections.

Selon de récents rapports, le nombre de failles logicielles documentées a atteint un niveau record en 2017, avec 14 % d'augmentation par rapport à l'année précédente (19 954 contre 17 147 en 2016). L'exploitation de vulnérabilités connues du public est une cause majeure de problèmes de sécurité, comme dans le cas du piratage d'Equifax ou du ransomware WannaCry. Selon le cabinet PwC, ce genre d'incidents de cybersécurité génèrent des coûts de 2,5 M$ en moyenne en 2015.

Les résultats du rapport trimestriel de sécurité (le *Global Threat Landscape Report*) de Fortinet sont plus nuancés. L'étude note que si les ransomwares sont toujours une réelle menace pour les entreprises (de plus en plus nombreux et sophistiqués), il semble que certains cybercriminels préfèrent largement utiliser les systèmes à des fins de minage de cryptomonnaies plutôt que de rançonnage. Les malwares de minage de crypto ont plus que doublé sur le trimestre, passant de 13 % à 28 %. Le cryptojacking (détournement de ressources de systèmes à des fins de minage de bitcoin et monero notamment) s'est particulièrement bien imposé au Moyen-Orient, en Amérique latine et en Afrique. Le ransomware GandCrab découvert en janvier 2018 fait la synthèse en utilisant le cryptoactif dash pour le paiement des rançons. De même que BlackRuby et SamSam sont deux variantes de logiciels de rançon des plus actives au premier trimestre 2018.

La France est particulièrement sous la menace de cyberattaques. Un accroissement notable d'outils d'attaques sophistiqués aux effets de plus en plus ravageurs a sévi en 2017. Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), cette même année, la France a totalisé, « *2 435 signalements d'événement de sécurité numérique (1 621 traités), 20 incidents majeurs de sécurité, 12 opérations de cyberdéfense face à des menaces et compromettant les opérations liées* [à] *l'activité d'une organisation d'importance vitale (OIV) ou fortement sensible, et, enfin, trois crises publiques majeures (menace sur l'élection présidentielle, rançongiciel Wannacry et attaque à des fins de sabotage NotPetya)* ». Les résultats de l'enquête de Bessé & PwC montrent que les dirigeants français d'entreprises de taille intermédiaire (ETI) sont mieux informés et sensibilisés au risque cyber, car 76 % des sondés déclarent avoir subi au moins un incident cyber en 2017.

Les malwares les plus prolifiques du mois d'avril dernier en France sont Coinhive (cheval de Troie pour extraire de la cryptomonnaie Monero), Roughted (publicité malveillante

à grande échelle, escroqueries, kits d'exploitation de vulnérabilité et ransomwares), Cryptoloot (cryptomining exploitant tous types de monnaies virtuelles), Necurs (botnet le plus actif au monde avec 6 millions de bots estimés en 2016 propageant surtout des chevaux de Troie bancaires et des ransomwares), JSEcoin (mineur JavaScript intégré à n'importe quel site Web), Conficker (ver informatique qui cible le système d'exploitation Windows pour récupérer des données comme les mots de passe), Fireball (logiciel publicitaire détourneur de navigateur qui change le moteur de recherche par défaut, installe des pixels de suivis ou télécharge des logiciels malveillants), Nivdort (cheval de Troie ciblant l'OS Windows pour subtiliser mots de passe, informations/paramètre système, adresse IP, configuration du logiciel, localisation approximative et collecte des frappes de touches dans certaines versions pour modifier les paramètres DNS), Virut (un des principaux distributeurs de botnets et de logiciels malveillants sur Internet utilisé pour des offensives DDoS, du spam, du vol de données et de la fraude) et enfin Pirrit (adware qui inclut les capacités d'un outil d'administration à distance pour injecter du code JavaScript directement dans le navigateur).

Cyberespionnage, gouvernements et secteur privé

Selon un rapport de l'entreprise de sécurité mobile US Lookout et du groupe de défense des droits numériques US Electronic Frontier Foundation, la Direction générale de la sécurité générale du Liban (GDGS), soit les services de renseignement libanais, est soupçonnée d'avoir utilisé les smartphones de milliers de personnes en tant qu'outil de cyberespionnage. Plus de 10 opérations cyber auraient été menées dans au moins 21 pays depuis 2012, principalement sur les utilisateurs de téléphones Android (Google). Selon l'analyse, il s'agirait d'un des premiers exemples connus de piratage informatique à grande échelle de téléphones intelligents plutôt que d'ordinateurs.

Le Mossad, (service de renseignement extérieur israélien), le Shin Bet (service de sécurité intérieure israélien) et Tsahal, (l'armée de défense d'Israël) coopèrent de plus en plus avec le secteur privé pour optimiser leurs performances dans le cyberespace. Le Mossad s'intéresse particulièrement aux technologies robotiques (pour utilisation terrestre, maritime et aérienne), aux technologies de l'énergie et aux batteries, aux outils de cryptage de l'information à haute vitesse, aux logiciels pour identifier les traits de personnalité à des fins de profilage de personnalité, basés sur le comportement et l'activité en ligne, à l'apprentissage automatique et à l'automatisation pouvant aider à synthétiser les documents, les cataloguer et traiter les données dans diverses langues.

Tawfiq Tirani, ancien n° 1 de l'Agence Générale Palestinienne des Services d'Intelligence (de 1994 à 2008), les services de renseignement palestiniens, affirme que le gouvernement de Cisjordanie a travaillé main dans la main avec la CIA pour mettre sur

écoute plusieurs milliers de personnes sans contrôle légal. Il a introduit une plainte contre l'Autorité Palestinienne demandant qu'une enquête soit initiée sur ces écoutes.

Utilisé depuis 2012 pour exfiltrer discrètement des données gouvernementales et d'individus dans des pays en guerre ou politiquement instables (Irak, Somalie, Afghanistan, Libye, RDC, Yémen…), le logiciel de cyberespionnage (malware) Slingshot continue d'être actif (au moins une centaine de lésés) dans les pays les plus instables du Moyen-Orient et d'Afrique.

Le gouvernement luxembourgeois veut accroître les capacités techniques de son Service de renseignement de l'État (SRE) pour surveiller et conserver des données téléphoniques et informatiques. Le budget de l'entité passera de 3,3 M€ en 2018 à 5,1 M€ en 2019 (64 % d'augmentation) pour atteindre 5,4 M€ en 2021.

Aadhaar est une base de données biométrique mise en place par l'État indien, en partenariat avec la société française Idemia (anciennement Morpho) en 2010. Cette base de données attribue aux résidents du pays un numéro unique à 12 chiffres associés à leurs empreintes digitales, photo du visage et scan de l'iris. Aujourd'hui indispensable pour toute démarche administrative, ce *Big Brother* indien regroupe les informations personnelles de près de 1,2 milliard de personnes (99 % de la population adulte du pays). Toute personne vivant en Inde depuis plus de six mois, y compris étrangères, peut obtenir gratuitement une carte d'identité. Human Rights Watch et Amnesty International dénoncent des « *violations du droit à la vie privée* » et soulignent une surveillance étatique accrue « *avivée par l'absence de lois pour protéger les données personnelles en Inde et le manque de contrôle judiciaire ou parlementaire sur les activités des services de renseignement* ». De plus, un chercheur en cybersécurité avait découvert que des centaines de milliers de numéros Aadhaar avaient été publiés en ligne en février 2017. En 10 minutes et pour 500 roupies (6,4 €), le fameux journal indien *The Tribune* a également pu accéder via un intermédiaire anonyme à des données personnelles associées à des numéros du système d'identification de la population (noms, adresses, photos, numéros de téléphone, adresses mail), selon un article de janvier 2018. La Cour suprême de l'Inde devra prochainement trancher sur la comptabilité du fichage de la population avec la Constitution du pays. Selon *Diploweb*, ce programme illustre la montée en puissance des capacités de contrôle technologique au bénéfice des autorités publiques et des intérêts commerciaux privés.

L'agence de renseignement NSA déclare que 534 millions de communications (conversations téléphoniques, SMS) ont été épiées en 2017 aux États-Unis. Un chiffre qui a été multiplié par trois par rapport à celui de l'année précédente. De plus, l'activité sur Internet de quelques 130 000 étrangers (+ 25 % par rapport à 2016) s'ajoute à ces interceptions de la NSA. Durant ces deux dernières années, 1 500 personnes ont été particulièrement surveillées pour des questions de sécurité nationale. Selon la CIA, la sur-

veillance numérique est tellement efficace qu'elle se substitue largement à la simple filature dans une bonne trentaine de pays.

La spécialiste en cybersécurité **Kelly Shortridge** (BAE Systems) a constaté que le navigateur Google Chrome scanne en permanence les fichiers présents sur les ordinateurs de ses utilisateurs qui fonctionnent sous le système Windows. La faute au programme Chrome Cleanup Tool qui scanne l'ordinateur en recherchant des programmes malfaisants et envoie les métadonnées à Google.

Selon une nouvelle étude de vpnMentor, 50 fournisseurs de VPN sur 280 disponibles ont partagé des données personnelles de leurs utilisateurs avec Facebook sans qu'ils ne le sachent. Ceci a été réalisable par le biais du pixel de Facebook, un plug-in de reciblage (*retargeting*) qui sert à optimiser la publicité sur le réseau social et sur le Net en général.

La Direction générale des finances publiques (DGFIP) a fait l'erreur d'utiliser la plateforme YouTube pour héberger une vidéo d'information sur le prélèvement à la source, en la rendant obligatoire à visionner pour accéder au site et déclarer ses revenus. L'État transmet donc indirectement à Google, propriétaire de YouTube, les données des internautes français.

La Commission nationale de l'informatique et des libertés (CNIL) a mis en demeure la société Direct Énergie à propos de ses compteurs Linky controversés (contestés par les usagers dans pas moins de 300 villes et communes françaises). Selon elle, le consentement des clients pour la collecte de leurs données de consommation personnelles toutes les demi-heures ne serait pas « *libre, éclairé et spécifique* ». Encore 35 millions de compteurs Linky doivent être déployés sur la totalité du territoire d'ici 2021, alors que 7 millions sont actuellement en place. Une proposition de loi visant à permettre aux consommateurs et aux municipalités de refuser l'installation du compteur a en effet été déposée le 16 mai 2018 à l'Assemblée nationale. Actuellement, les installations de Linky sont obligatoires.

Le cerveau ukrainien d'un groupe de cybervoleurs russes ou ukrainiens, qui aurait dérobé près de 1 Mds € à des banques, a été arrêté en Espagne fin mars 2018. Le groupe opérait depuis plus de cinq ans en se servant de logiciels malveillants sophistiqués (appelés Carbanak et Cobalt) qu'ils créaient eux-mêmes. Les pirates se faisaient passer pour des entreprises légitimes et envoyaient massivement à des employés de banque des courriels avec une pièce jointe malveillante. Une fois téléchargé, ce logiciel malveillant leur permettait de contrôler à distance des distributeurs de billets. Chaque opération pouvait rapporter plus de 1,5 M$ en moyenne. Des bénéfices immédiatement convertis en cryptomonnaies de type bitcoin, pour ensuite acquérir des biens matériels (voitures de luxe, maisons…). Ils ont pu accéder à la quasi-totalité des banques de Rus-

sie et extraire de l'argent d'une cinquantaine d'entre elles. Le groupe a ciblé plus de 100 institutions financières dans 40 pays (Biélorussie, Azerbaïdjan, Kazakhstan, Ukraine, Taïwan…).

Les récentes failles de sécurité

Des chercheurs du *MIT Technology Review*, le magazine du Massachusetts Institute of Technology, ont découvert 147 failles de sécurité dans 34 applications du Play Store Google (Android). Ces applis sont notamment utilisées par des entreprises comme Siemens et Schneider Electric pour contrôler des processus industriels. Des vulnérabilités qui permettraient à des pirates informatiques d'infecter un périphérique mobile avec un code malveillant afin qu'il délivre des commandes aux serveurs qui contrôlent de nombreuses machines. Ces risques informatiques sont un réel danger pour le milieu industriel, car une personne mal intentionnée pourrait faire croire par exemple qu'une machine fonctionne à une température sécuritaire alors qu'elle surchauffe. Des instabilités ont été découvertes dans le système d'acquisition et de contrôle de données (SCADA - système de télégestion à grande échelle) des technologies industrielles de Siemens. Certaines d'entre elles donnent l'opportunité à un belligérant de «*provoquer un déni de service à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données*» (3 mai 2018). D'autres faiblesses dans le système SCADA de Schneider Electric peuvent permettre à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et un contournement de la politique de sécurité (25 mai 2018).

Près de 700 000 données des lecteurs de *L'Express* (60 go contenant noms, prénoms, adresses mails et professions) étaient accessibles en ligne sans mot de passe durant plusieurs semaines. Alors que le média avait été averti de cette fuite, il n'a pas réagi, laissant la base de données et son contenu téléchargeables par tout un chacun pendant un mois. Des entités malveillantes ont tenté à plusieurs reprises d'obtenir une rançon, notamment en bitcoin, en échange des données.

En avril 2017, la clef USB d'une jeune femme appelée Mina B. (fichée S) a été examinée dans le cadre d'une enquête judiciaire. Le support contenait des fichiers de police sensibles, dont notamment une liste datant de 2008 de 2 626 agents du renseignement. Cette liste, préalablement effacée de la clef USB, a été restaurée par les enquêteurs. Elle contient les noms, matricules et affectations de l'ensemble des agents du corps des gradés et gardiens nommés lors de la Commission administrative paritaire nationale (CAPN) du 19 juin 2008. Les individus listés sont issus de la Direction centrale des Renseignements généraux (DCRG) et de la Direction de la Surveillance du territoire (DST), deux services partiellement fusionnés pour créer la Direction générale de la Sécurité

intérieure (DCRI).

La plus grande banque d'Australie, la Commonwealth Bank, a admis jeudi 3 mai 2018 avoir égaré les données financières d'environ 20 millions de ses clients. La banque n'a pas été en mesure de retrouver deux bandes de données magnétiques censées être détruites et sur lesquelles étaient stockés des noms, adresses, numéros de compte et les détails de transactions financières enregistrées entre 2000 et 2016. Ces données ont pu être détruites par un sous-traitant après la fermeture de son centre de données, bien qu'aucun document ne puisse le prouver. Aucun des systèmes informatiques, plateformes technologiques, applications et autres sites Internet n'ont été compromis selon cette société, qui est la première entreprise par la capitalisation boursière du pays. L'affaire tombe alors qu'elle est soupçonnée de dizaines de milliers d'atteintes à la loi à propos de blanchiment d'argent, financement de terrorisme et manipulations de taux interbancaires de référence. Trois autres grandes banques australiennes, National Australia Bank, Westpac et ANZ, sont également concernées par une commission d'enquête royale sur des flux financiers illicites.

Fin avril 2018, Kaspersky Lab (société privée russe spécialisée dans la sécurité des systèmes d'information) a détecté un exploit encore inconnu jusqu'alors. Un exploit est une forme de logiciel qui se sert des bugs ou des vulnérabilités d'autres logiciels pour infecter des victimes avec un code malveillant. L'exploit découvert par l'entreprise moscovite en question utilise une vulnérabilité zero-day CVE-2018-8174 pour Internet Explorer pour des attaques ciblées. Voici la démarche d'infection : la victime reçoit d'abord un document Microsoft Office RTF malveillant qui, après ouverture, télécharge l'exploit c'est-à-dire une page HTML avec un code malsain. Ce code déclenche un bug UAF de corruption de la mémoire et un shellcode, qui télécharge le programme hostile, est alors exécuté forçant ainsi le chargement d'Internet Explorer, peu importe le navigateur habituellement utilisé par la victime. À propos de Kaspersky Lab, c'est au tour du gouvernement néerlandais de bannir, à l'instar des USA, le logiciel antivirus de l'éditeur russe pour motif d'espionnage et de sabotage au profit de Moscou. Kaspersky Lab a contesté les accusations et a rappelé que cette décision a été annoncée au moment où il a décidé de transférer une partie de ses services de la Russie vers la Suisse.

Le 16 avril dernier, les chercheurs de ce spécialiste russe de la sécurité informatique ont également découvert un nouveau malware Android diffusé par *Domain Name System* (DNS Hijacking). Dénommé Roaming Mantis, le logiciel malveillant a pour objectif de subtiliser des informations comme des identifiants, ainsi que donner aux pirates un contrôle intégral des appareils infectés. Le malware visait principalement les smartphones en Asie, mais a inclus en à peine un mois l'Europe et le Moyen-Orient, en y ajoutant du phishing pour les appareils iOS et du minage de cryptomonnaies sur PC.

Les transcripteurs de Cortana, l'assistant vocal de Microsoft, sont recrutés directement

en ligne via un test et suivent une formation en ligne. En cas de réussite, aucun contrat de travail ni de confidentialité n'est signé. Les travailleurs sont indépendants et ont accès aux masses de données collectées par Cortana, c'est-à-dire les enregistrements vocaux de tous ces utilisateurs, pour les traiter un à un. Un texte s'affichait avec ce que Cortana avait compris de l'enregistrement et le transcripteur doit corriger la grammaire, l'orthographe, etc. Noms, adresses, conversations personnelles, numéros de sécurité sociale, recherches en ligne, conversations en ligne (Xbox ou Skype pour ceux qui utilisent un service de traduction instantanée), questions personnelles à Cortana et diverses informations sont donc accessibles sur la plateforme de travail. Cortana enregistre également, de façon non sollicitée, des conversations qui ne devaient pas être enregistrées qu'il faut néanmoins traiter : Microsoft récupère les données dans tous les cas. Les logiciels à activation vocale tels Cortana, Siri ou Alexa sont des agents conversationnels artificiels qui demandent une grande dimension de travail humain. Les travailleurs précaires qui trient nos requêtes, écoutent nos propos, sont situés en France ou peuvent être issus de pays francophones comme la Tunisie, le Maroc ou Madagascar. De même, un couple a constaté qu'une de ses conversations avait été enregistrée à son insu par l'enceinte connectée Echo qui l'a transmise à un employé du mari. Il s'agirait d'une erreur selon le constructeur Amazon. Notons également que tout juste après son lancement, la serrure connectée Amazon Key (un dispositif de livraison à domicile) a immédiatement été piratée.

Les vulnérabilités relevées par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT)

- Une vulnérabilité pouvant provoquer une atteinte à la confidentialité des données a été découverte dans Microsoft Windows (27 avril 2018). Un déséquilibre a été découvert dans Microsoft Windows Host Compute Service Shim (hcsshim). Il permet à un attaquant de provoquer une exécution de code arbitraire à distance (03 mai 2018). Le 8 mai 2018, Microsoft a annoncé ses mises à jour mensuelles de sécurité : 67 vulnérabilités ont été corrigées, dont 22 considérées comme critiques, 45 comme importantes et 2 comme faibles. Elles concernent Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office, Services Microsoft Office et Microsoft Office Web Apps, ChakraCore, Adobe Flash Player, Cadriciel .NET, Microsoft Exchange Server. Des vulnérabilités ont été corrigées dans Microsoft Windows concernant une divulgation d'informations, une élévation de privilèges, un contournement de la fonctionnalité de sécurité et une exécution de code à distance (09 mai 2018). De même que dans Microsoft .NET, des failles telles qu'un déni de service et un contournement de la fonctionnalité de sécurité ont été rectifiées (09 mai 2018). Dans Microsoft Internet Explorer (09 mai 2018), Microsoft Edge (09 mai 2018) et Microsoft Office (09 mai 2018) sont présents des problèmes de divulgation d'informations, des possibilités d'exécution de code à dis-

tance et de contournement de la fonctionnalité de sécurité. Des risques de divulgation d'informations, d'élévation de privilèges, d'exécution de code à distance et d'usurpation d'identité ont été corrigées dans plusieurs versions de Microsoft Exchange Server et Microsoft Infopath 2013, ainsi que dans C SDK, C # SDK et ChakraCore Java SDK pour Azure IoT, le cloud de l'Internet des objets de Microsoft (09 mai 2018). Une dernière vulnérabilité a été découverte dans Microsoft PowerPoint. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance (24 mai 2018).

- Dans Google Chrome, plusieurs vulnérabilités permettant à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur (27 avril 2018, 09 mai 2018 et 22 mai 2018) et une élévation de privilèges (11 mai 2018) ont été relevées. D'autres failles ont été découvertes dans Google Android pouvant amener à l'exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité (09 mai 2018).

- Des faiblesses permettant l'exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité ont été annoncées pour le navigateur Mozilla Firefox au 09 mai 2018. D'autres failles ont été relevées dans Mozilla Thunderbird pouvant amener à un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service (22 mai 2018).

- Une fragilité pouvant provoquer une exécution de code arbitraire à distance a été découverte dans le Norton Core, le routeur sécurisé pour protéger les objets connectés de la maison de Symantec (2 mai 2018).

- Produits Cisco : des vulnérabilités permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité (03 mai 2018 et 17 mai 2018).

- Quasiment tous les systèmes d'exploitation ou de virtualisation logiciel des processeurs Intel (affectant tous les OS) ont une faille à cause d'une erreur de compréhension du manuel du développeur. C'est encore pire sur les processeurs AMD, où la brèche permet d'exécuter du code. Sur Intel, elle permet à l'attaquant d'escalader les privilèges sur Windows et macOS, tandis qu'elle peut faire planter Linux dans les configurations de Xen (logiciel libre de virtualisation de systèmes d'exploitation) et de FreeBSD (système d'exploitation UNIX libre).

- 7-Zip : problème d'exécution de code arbitraire à distance (04 mai 2018).

- PHP : complication de sécurité non spécifiée par l'éditeur et un déni de service (27 avril 2018).

- Noyau Linux de SUSE : des brèches permettent à un attaquant de provoquer une

exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données (26 avril 2018). Souci d'exécution de code arbitraire, de déni de service et d'atteinte à l'intégrité des données (09 mai 2018). Des ouvertures involontaires permettent au pirate de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire et un déni de service (17 mai 2018), ainsi qu'une atteinte à la confidentialité des données et une élévation de privilèges (25 mai 2018).

- Noyau Linux de RedHat : atteinte à l'intégrité des données et à la confidentialité des données (26 avril 2018). Un individu malintentionné pouvait également provoquer un déni de service, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données (09 mai 2018) ou encore une atteinte à la confidentialité des données (22 mai 2018 et 25 mai 2018).

- Noyau Linux d'Ubuntu : problème d'exécution de code arbitraire, de déni de service et d'élévation de privilèges, ainsi que des possibilités pour un attaquant de provoquer une exécution de code arbitraire à distance. (09 mai 2018).

- Adobe Flash Player : un attaquant pouvait provoquer une exécution de code arbitraire à distance (09 mai 2018).

- Citrix XenServer : des failles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à l'intégrité des données (09 mai 2018).

- Citrix XenMobile : des vulnérabilités permettent au belligérant de provoquer un problème de sécurité non spécifié par l'éditeur et un contournement de la politique de sécurité (22 mai 2018).

- Xen : problème de déni de service et d'élévation de privilèges (09 mai 2018).

- Twitter : jeudi 3 mai dernier, un problème de sécurité a été dévoilé par la société qui a conseillé à ses usagers de changer leurs mots de passe par mesure de sécurité.

- Fortinet FortiOS : un pirate peut provoquer une atteinte à la confidentialité des données et une élévation de privilèges (22 mai 2018). De même pour les produits Fortinet (17 mai 2018).

- BIND : problème de déni de service à distance (22 mai 2018).

- Produits Tenable : souci de sécurité non spécifié par l'éditeur (22 mai 2018).

- Wireshark : problème de déni de service à distance (23 mai 2018).

- S/MIME et OpenPGP : le 14 mai 2018, une faille nommée EFAIL était rendue publique par des chercheurs des universités allemandes de Münster et Bochum, ainsi que de l'entreprise NXP Semiconductors. Des offensives sont réalisables contre les protocoles de sécurisation des échanges de courriels S/MIME et OpenPGP pour récupérer le texte clair d'un courriel protégé par chiffrement (23 mai 2018).

- Joomla ! : failles permettant au pirate de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données (23 mai 2018).

- Moodle : exécution de code arbitraire à distance possible, en plus d'un déni de service et d'un contournement de la politique de sécurité (25 mai 2018).

- VMware Workstation et Fusion : déni de service, atteinte à la confidentialité des données et élévation de privilèges (25 mai 2018).

- BMW : Des hackeurs chinois ont relevé 14 failles de sécurité dans une série de modèles du constructeur automobile allemand BMW. Elles permettaient de modifier à distance le fonctionnement interne du véhicule. L'Allemand a travaillé conjointement avec ce groupe de hackeurs chinois pour améliorer la sécurité de ses voitures.

Franck Pengam, Mai 2018.

- SITE : https://www.geopolitique-profonde.com

- FACEBOOK : https://www.facebook.com/geopolitiqueprofonde

- YOUTUBE : https://www.youtube.com/user/FranckPengam

https://www.geopolitique-profonde.com

MENTIONS LEGALES
Géopolitique Profonde
6 rue de Musset
75016 PARIS
Siren : 833 752 652
Contact : geopolitique.profonde@protonmail.com