Revue d'actualité

11/06/2019

OSSIR

Préparée par

*Étienne **B**audin @etiennebaudin*
*Arnaud **S**OULLIE @arnaudsoullie*

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-053 Vulnérabilités dans Internet Explorer (8 CVE)

- Exploit:
  - 1 x Vol de session
  - 5 x Exécution de code à distance
  - 1 x Vol d'informations
  - 1 x Contournement de restrictions de sécurité
- Crédits:
  - Wenxu Wu (@ma7h1as) of Tencent Security Xuanwu Lab (CVE-2019-0921)
  - Juan Pablo Lopez Yacubian (CVE-2019-0929)
  - Krishnakant Patil and Siddhant Badhe - Project Srishti working iDefense, Accenture (CVE-2019-0930)
  - ? (CVE-2019-0995)
  - Four Fire (CVE-2019-0884)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0911, CVE-2019-0918)
  - Arthur Gerkis of Exodus Intelligence (@ax330d) working with Trend Micro's Zero Day Initiative working Trend Micro's Zero Day Initiative (CVE-2019-0940)

MS18-054 Vulnérabilités dans Edge (18 CVE)

- Exploit:
  - 17 x Exécution de code à distance
  - 1 x Élévation de privilèges
- Crédits:
  - Liu Long of Qihoo 360 Vulcan Team (CVE-2019-0926)
  - Arthur Gerkis of Exodus Intelligence (@ax330d) working Trend Micro's Zero Day Initiative (CVE-2019-0938)
  - Four Fire (CVE-2019-0884)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0911, CVE-2019-0912)
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933)
  - Bruno Keith (CVE-2019-0922)
  - Zhiyi Zhang from Codesafe Team of Legendsec at Qi'anxin Group (CVE-2019-0923)
  - fluoroacetate (@fluoroacetate) working Trend Micro's Zero Day Initiative (CVE-2019-0937)
  - Arthur Gerkis of Exodus Intelligence (@ax330d) working with Trend Micro's Zero Day Initiative working Trend Micro's Zero Day Initiative (CVE-2019-0940)

Dont 3 communes avec IE:

- CVE-2019-0940
- CVE-2019-0911
- CVE-2019-0884

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-055 Vulnérabilités dans RDP (1 CVE)

- Affectés
  - Windows 7
  - Windows 2008
  - Patchs pour XP/2003 disponible également
- Exploit:
  - 1 x Exécution de code à distance
  - Pas d'action utilisateur nécessaire, **wormable**
  - POC existant (visible via le score CVSS)
- Crédits:
  - The UK's National Cyber Security Centre (NCSC) (CVE-2019-0708)

- Nommée Bluekeep
- de nombreux scans du port RDP identifiés sur Internet (Greynoise, Onyphe, etc.)
- de nombreux faux codes d'exploitation partagés sur Github
- Un PoC menant à un DOS partagé ("facile" de le transformer en RCE)
- Aucun code public pour l'heure
- Des codes d'exploitation privés existent

https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

https://twitter.com/GossiTheDog/status/1128431661266415616?s=03

https://twitter.com/0xffff0800/status/1129215041432096773?s=03

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-056 Vulnérabilité dans Windows DHCP Server (1 CVE)

- Affectés
  - Windows Server 2008
  - Windows Server 2012
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server, version 1803
  - Windows Server, version 1903
- Exploit:
  - 1 x Exécution de code à distance
- Crédits:
  - Mitch Adair, Microsoft Windows Enterprise Security Team (CVE-2019-0725)

MS19-057 Vulnérabilité dans SQL Server (1 CVE)

- Affectés
  - Microsoft SQL Server 2017 (CU+GDR)
  - Microsoft SQL Server 2017 (GDR)
- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - ? (CVE-2019-0819)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilité dans Kerberos (1 CVE)

- Affectés
  - Toutes versions de Windows
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Andrew Bartlett of Catalyst and the Samba Team (CVE-2019-0734)

MS19-058 Vulnérabilité dans Windows Kernel (1 CVE)

- Affectés
  - Toutes versions de Windows
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0881)

MS19-058 Vulnérabilités dans Microsoft Office SharePoint (8 CVE)

- Exploit:
  - 1 x Vol d'informations
  - 2 x Élévation de privilèges
  - 4 x Vol de session
  - 1 x Exécution de code à distance
- Crédits:
  - ? (CVE-2019-0956)
  - Ashar Javed of Hyundai AutoEver Europe GmbH (CVE-2019-0957, CVE-2019-0949, CVE-2019-0950)
  - Ahmed Radi (CVE-2019-0958)
  - Huynh Phuoc Hung, @hph0var (CVE-2019-0963)
  - Nikola Kojić Ras-IT, Belgrade (CVE-2019-0951)
  - Ivan Vagunin, (CVE-2019-0952)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilités dans Microsoft Windows (7 CVE)

- Affectés
  - PowerShell Core 6.1
  - PowerShell Core 6.2
  - Toutes versions de Windows
- Exploit:
  - 4 x Élévation de privilèges
  - 1 x Vol d'informations
  - 1 x Contournement de restrictions de sécurité
  - 1 x Exécution de code à distance
  - CVE-2019-0863 (EdP) actuellement exploité dans la nature
- Crédits:
  - Gal De Leon of Palo Alto Networks (CVE-2019-0863)
  - ? (CVE-2019-0886)
  - Thomas Levering (CVE-2019-0942)
  - Matt Graeber of SpecterOps (CVE-2019-0733)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0885)
  - k0shl of Qihoo 360 Vulcan Team (CVE-2019-0931)
  - Abian Blome of ClawSec (CVE-2019-0936)

MS19-058 Vulnérabilités dans Microsoft JET Database Engine (13 CVE)

- Affectés
  - Toutes versions de Windows
- Exploit:
  - 13 x Exécution de code à distance
- Crédits:
  - Honggang Ren of Fortinet's FortiGuard Labs (CVE-2019-0893, CVE-2019-0898)
  - rgod of 9sg Security Team - rgod@9sgsec.com working Trend Micro's Zero Day Initiative (CVE-2019-0894, CVE-2019-0895, CVE-2019-0896)
  - Keqi Hu and Zhangjie from Chengdu Security Response Center of Qihoo 360 Technology Co. Ltd. (CVE-2019-0897)
  - Gal De Leon and Bar Lahav of Palo Alto Networks (CVE-2019-0899)
  - Bar Lahav and Gal De Leon of Palo Alto Networks (CVE-2019-0900, CVE-2019-0901, CVE-2019-0889, CVE-2019-0890, CVE-2019-0891)
  - Hardik Shah of McAfee (CVE-2019-0902)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilité dans Windows NDIS (1 CVE)

- Affectés
  - Windows 10
  - Windows 8.1
  - Windows Server 2012
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server, version 1803
  - Windows Server, version 1903
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Anthony LAOU HINE TSUEI (CVE-2019-0707)

MS19-058 Vulnérabilité dans Windows Diagnostic Hub (1 CVE)

- Affectés
  - Microsoft Visual Studio
  - Windows 10
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server, version 1803
  - Windows Server, version 1903
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Wayne Low of Fortinet's FortiGuard Labs (CVE-2019-0727)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilités dans Microsoft Office (4 CVE)

- Affectés
  - Toutes versions de Office
- Exploit:
  - 4 x Exécution de code à distance
- Crédits:
  - Keqi Hu and Zhangjie from Chengdu Security Response Center of Qihoo 360 Technology Co. Ltd. (CVE-2019-0945, CVE-2019-0946)
  - Bar Lahav and Gal De Leon of Palo Alto Networks (CVE-2019-0947)
  - Anonymous, working Trend Micro's Zero Day Initiative (CVE-2019-0953)

MS19-058 Vulnérabilités dans .NET Core (3 CVE)

- Exploit:
  - 3 x Déni de service
- Crédits:
  - Nemanja Mijailovic Nemanja Mijailovic's Blog (CVE-2019-0980)
  - Nemanja Mijailovic, Nemanja Mijailovic's Blog (CVE-2019-0981)
  - ? (CVE-2019-0982)

MS19-058 Vulnérabilités dans .NET Framework (2 CVE)

- Exploit:
  - 2 x Déni de service
- Crédits:
  - ? (CVE-2019-0820)
  - Keqi Hu and zhangjie from Chengdu Security Response Center of Qihoo 360 Technology Co. Ltd. (CVE-2019-0864)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilité dans Microsoft Dynamics (1 CVE)

- Affectés
  - Microsoft Dynamics
- Exploit:
  - 1 x Contournement de restrictions de sécurité
- Crédits:
  - Adam Willard (CVE-2019-1008)

MS19-058 Vulnérabilités dans Microsoft Graphics Component (5 CVE)

- Affectés
  - Toutes versions de Windows
- Exploit:
  - 3 x Vol d'informations
  - 1 x Élévation de privilèges
  - 1 x Exécution de code à distance
- Crédits:
  - Axel Souchet (@0vercl0k) of MSRC Vulnerabilities and Mitigations Team (CVE-2019-0882)
  - Zhang Yunhai of NSFOCUS (CVE-2019-0892)
  - kdot working Trend Micro's Zero Day Initiative (CVE-2019-0903, CVE-2019-0758)
  - Kamlapati Choubey of Trend Micro Security Research working Trend Micro's Zero Day Initiative (CVE-2019-0961)

MS19-058 Vulnérabilité dans NuGet (1 CVE)

- Affectés
  - Nuget 5.0.2
- Exploit:
  - 1 x Manipulation de données
- Crédits:
  - ? (CVE-2019-0976)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-058 Vulnérabilité dans Skype for Android (1 CVE)

- Affectés
  - Skype 8.35 (Android)
- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - ? (CVE-2019-0932)

Failles / Bulletins / Advisories

Microsoft - Autre

1 vulnérabilité découverte dans RDP

- Contournement du mécanisme NLA sur RDP (limité à Windows 10 et Server 2019)

https://www.kb.cert.org/vuls/id/576688/

Codes d'exploitation publiés pour des 0day publiés par SandboxEscaper

- Microsoft Windows :
  - permettant de contourner des restrictions de sécurité et élever ses privilèges
    - un attaquant est en mesure de récupérer tous les droits sur un fichier. (2x contournement du patch)
    - un attaquant est en mesure d'écrire une DLL (bibliothèque de code dynamique) arbitraire dans C:\Windows\System32.
    - un attaquant est en mesure de récupérer tous les droits d'édition sur un fichier. Correctif disponible
- IE 11
  - injection de code dans le processus

https://github.com/SandboxEscaper/polarbearrepo/tree/5fd3a1e3652bba36ee95186945c5cc1c5f006143/CVE-2019-0841-BYPASS

https://github.com/SandboxEscaper/polarbearrepo/tree/5fd3a1e3652bba36ee95186945c5cc1c5f006143/InstallerBypass

https://github.com/SandboxEscaper/polarbearrepo/tree/5fd3a1e3652bba36ee95186945c5cc1c5f006143/angrypolarbearbug2

https://github.com/SandboxEscaper/polarbearrepo/sandboxescape

https://github.com/SandboxEscaper/polarbearrepo/tree/master/bearlpe

Failles / Bulletins / Advisories

Microsoft - Autre

Une vulnérabilité critique sur Microsoft Sharepoint exploitée sur Internet

- pour délivrer un malware
- patchs publiés en février et mars pour la vulnérabilité CVE-2019-0604
- RCE sans authentification via un défaut de vérification d'un paquet applicatif

https://www.securityweek.com/microsoft-sharepoint-vulnerability-exploited-wild

Une ancienne vulnérabilité affectant Office exploitée sur Internet par email (RTF)

- liée à l'éditeur d'équation, elle cible les utilisateurs européens
- corrigée en 2017

https://www.helpnetsecurity.com/2019/06/10/office-equation-editor-exploit/

La mise à jour KB4497936 pour les systèmes faisant partie du programme Insider rend la sandbox Windows inutilisable

- dû à une erreur de gestion de la langue du système

https://www.bleepingcomputer.com/news/microsoft/windows-update-kb4497936-for-insiders-breaks-windows-sandbox/

Distribution du ransomware GrandCrab lors d'une vague d'attaque ciblant des instances MySQL sur Windows

- détecté par Sophos, téléchargé 800 fois en quelques jours

https://nakedsecurity.sophos.com/2019/05/25/serious-security-dont-let-your-sql-server-attack-you-with-ransomware/
https://securityaffairs.co/wordpress/86110/hacking/mysql-databases-gandcrab-ransomware.html
https://news.sophos.com/en-us/2019/05/24/gandcrab-spreading-via-directed-attacks-against-mysql-servers/

Failles / Bulletins / Advisories

Microsoft - Autre

Un bruteforce RDP observé sur 1,5 millions de serveurs

- Chine (876 000 serveurs) et USA (434 000) ciblés

https://nakedsecurity.sophos.com/2019/06/10/the-goldbrute-botnet-is-trying-to-crack-open-1-5-million-rdp-servers/

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle du système via une vulnérabilité au sein d'Adobe Flash Player (APSB19-26)

- 1x use-after-free

https://helpx.adobe.com/security/products/flash-player/apsb19-26.html

Prise de contrôle du système et divulgation d'informations via 84 vulnérabilités au sein des produits Adobe Reader et Adobe DC (APSB19-18)

- Lecture hors-limite
- Écriture hors-limite
- Confusion de type
- Réutilisation de mémoire désallouée
- Dépassement de tas
- Corruption de tampon
- Double free
- Contournement de sécurité

https://helpx.adobe.com/security/products/acrobat/apsb19-18.html

Failles / Bulletins / Advisories

Système (principales failles)

Manipulation de données via une vulnérabilité dans Spring Framework

- erreur au sein du module OAuth2 de Spring Security.
- Un attaquant pouvait être en mesure de rediriger un utilisateur vers un site malveillant.

https://pivotal.io//security/cve-2019-11269

Élévation de privilèges et manipulation de données via 13 vulnérabilités au sein des produits SAP

- 13 bulletins publiés, 1 en criticité élevé pour SAP Identity Management
  - via une erreur au sein de l'API REST permettant une modification de rôle ou privilège

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=520259032

Prise de contrôle du système via une vulnérabilité au sein d'Exim

- code d'exploitation partagé
- provient d'un manque de contrôle sur l'adresse destinatrice
- nécessite une configuration spécifique
- ${run{\x2F**bin**\x2F**sh**\t**-c**\t\x22**id**\x3E\x3E\x2F**tmp**\x2F**id**\x22}}@localhost

https://seclists.org/oss-sec/2019/q2/153
http://www.exim.org/static/doc/security/CVE-2019-10149.txt
https://bugzilla.redhat.com/show_bug.cgi?id=1715237

Failles / Bulletins / Advisories

Système (principales failles)

Exploit : Élévation de privilèges via une vulnérabilité au sein de Docker

- permet d'obtenir un accès root en lecture et en écriture sur l'ensemble du disque
- image docker et de deux scripts bash permettant d'exploiter l'accès concurrent pour lire et écrire un fichier préalablement défini (via la commande docker cp)

https://bugzilla.suse.com/attachment.cgi?id=773218

Exploit : Divulgation d'informations via une vulnérabilité au sein d'Oracle Enterprise Manager Products Suite

- intégré à Metasploit
- permet de lire des fichiers arbitraires depuis le serveur

https://github.com/rapid7/metasploit-framework/commit/527658dfbc04253d2059e5f5a6b9bba20727a5da

Exploit : Élévation de privilèges via une vulnérabilité au sein d'Oracle Solaris

- permet de devenir root

https://www.exploit-db.com/exploits/46877

Élévation de privilèges via une vulnérabilité dans VMware Workstation

- exploit disponible
- chargement incorrect de certains fichiers DLL

https://www.vmware.com/security/advisories/VMSA-2019-0007.html

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle du système et manipulation de données via 3 vulnérabilités au sein de HPE Integrated Lights-Out

- 2 XSS et 1 dépassement de tampon

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03917en_us

Prise de contrôle du système et contournement de restrictions de sécurité via 24 vulnérabilités au sein de Firefox ESR et Firefox

- associés aux composants Skia library, Windows Sandbox, Libpng library, WebGL
- et liés à des corruptions mémoires

=> ajout de protection contre le pistage dans la version 67.0.1

https://www.mozilla.org/en-US/security/advisories/mfsa2019-14/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-13/

Prise de contrôle du système et contournement de restrictions de sécurité via 12 vulnérabilités au sein de Google Chrome

- associés aux composants Skia library, Windows Sandbox, Libpng library, WebGL
- et liés à des corruptions mémoires

=> Google va limiter le blocage/tracking des utilisateurs aux entreprises

https://www.mozilla.org/en-US/security/advisories/mfsa2019-14/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-13/

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle du système et contournement de mesures de sécurité via 44 vulnérabilités au sein de macOS

- composants affectés : Accessibility Framework, AMD, Application Firewall, CoreAudio, DesktopServices, Disk Images, EFI, Intel Graphics Driver, IOAcceleratorFamily, IOKit, Kernel, Security, SQLite, StreamingZip, sysdiagnose, Touch Bar Support, WebKit

https://support.apple.com/en-gb/HT210119

Exploit : Prise de contrôle du système via une vulnérabilité au sein de macOS

- permet de contourner le composant Gatekeeper

https://www.fcvl.net/vulnerabilities/macosx-gatekeeper-bypass

Prise de contrôle du système via 13 vulnérabilités au sein de Gitlab

- dont une exécution de commandes arbitraires via le mécanisme de téléchargement d'un dépôt

https://about.gitlab.com/2019/06/03/security-release-gitlab-11-dot-11-dot-1-released/

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco

- 54 vulnérabilités pour 21 produits
- 1 vulnérabilité critique pour :
  - Cisco Prime Infrastructure (PI)
    et Cisco Evolved Programmable Network (EPN)
    - exécution de code arbitraire avec privilèges *root*

- Produits vulnérables
  - Cisco AnyConnect Secure Mobility Client
  - Cisco Enterprise
  - Cisco Evolved Programmable Network Manager
  - Cisco Expressway Series
  - Cisco Firepower Threat Defense Software
  - Cisco FXOS
  - Cisco Identity Services
  - Cisco Industrial Network Director
  - Cisco IOS XR
  - Cisco MDS 9700 Series Multilayer Directors
  - Cisco Nexus 3000/7000/7700/9000 Switches
  - Cisco NX-OS
  - Cisco Prime Infrastructure
  - Cisco Small Business Series Switches
  - Cisco TelePresence VCS
  - Cisco Expressway Series
  - Cisco Unified Communications
  - Cisco Unified Computing System
  - Cisco Unified Intelligence Center
  - Cisco Video Surveillance Manager
  - Cisco Webex

https://tools.cisco.com/security/center/Search.x?publicationTypeIDs=1&firstPublishedStartDate=2019%2F05%2F14&firstPublishedEndDate=2019%2F06%2F06&limit=100

Failles / Bulletins / Advisories

Hardware / IoT

Découverte de 4 vulnérabilités "MDS" affectant les processeurs Intel permettant d'accéder à des données sensibles

- liées encore une fois à l'exécution spéculative
- CVE-2018-12126 (baptisée MSBDS pour Microarchitectural Store Buffer Data Sampling par Intel, Fallout par les chercheurs) ;
- CVE-2018-12127 (baptisée MLPDS pour Microarchitectural Load Port Data Sampling par Intel) ;
- CVE-2018-12130 (baptisée MFBDS pour Microarchitectural Fill Buffer Data Sampling par Intel, RIDL ou ZombieLoad par les chercheurs) ;
- CVE-2019-11091 (baptisée MDSUM pour Microarchitectural Data Sampling Uncacheable Memory par Intel).

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html
https://cpu.fail/
https://mdsattacks.com

Failles / Bulletins / Advisories

Android / iOS

Prise de contrôle du système et contournement de mesures de sécurité via 40 vulnérabilités au sein d'iOS

- corruption de la mémoire, validation d'entrées incorrecte, lecture en dehors des limites, use-after-free, problème d'accès, etc.

https://seclists.org/fulldisclosure/2019/May/19

Prise de contrôle du système via 22 vulnérabilités au sein d'Android

https://source.android.com/security/bulletin/2019-06-01.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

460 000 comptes en ligne de Uniqlo dérobés par des attaquants

- nom, adresse, contact et information bancair

https://www.cnbc.com/2019/05/14/japans-uniqlo-says-hackers-access-data-from-460000-online-accounts.html

Un ransomware chiffre 80% des données d'un négociant pétrolier français

- plusieurs stations bloqués pendant plusieurs jours
- 80% des données chiffrés, 500 000€ demandés

https://www.lemondeinformatique.fr/actualites/lire-un-ransomware-chiffre-80-des-donnees-du-negociant-petrolier-picoty-75277.html

Le magazine Forbes infecté par le groupe de cybercriminels Magecart

- ajout d'un code Javascript malveillant pour dérober des informations bancaires

https://twitter.com/bad_packets/status/1128517905765683201
https://urlscan.io/result/86305615-624b-4500-a573-fad538b0b93d/dom/
https://pastebin.com/3AR7wQ70

Les systèmes de production du site Stack Overflow ont été compromis

- pas de détail disponible hormis la date de l'incident : 11 mai

https://stackoverflow.blog/2019/05/16/security-update/
https://www.zdnet.com/article/stack-overflow-says-hackers-breached-production-systems/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

TeamViewer confirme le fait d'avoir subi une attaque en 2016

- originaire de Chine, elle n'aurait pas entrainé de fuite de données

https://www.bleepingcomputer.com/news/security/teamviewer-confirms-undisclosed-breach-from-2016/

Plus de 885 millions de documents sensibles étaient exposés sur le site de First American Financial Corporation

- **accessible sans authentification depuis 2017**
- numéro de compte bancaire ;
- relevé de compte bancaire ;
- taux du prêt immobilier ;
- numéro de sécurité sociale ;
- reçus d'opérations financières ;
- photo du permis de conduire.

https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des skimmers Magecart découverts sur le CDN Amazon CloudFront

- bibliothèques infectées par un skimmer
- données envoyées en Chine

https://blog.malwarebytes.com/threat-analysis/2019/06/magecart-skimmers-found-on-amazon-cloudfront-cdn/

Une faille dans un plugin WordPress est exploitée par des attaquants pour rediriger les visiteurs vers des sites malveillants

- plugin nommée WP Live Chat Support, vulnérabilité XSS
- 47 sites affectés

https://arstechnica.com/information-technology/2019/05/hackers-actively-exploit-wordpress-plugin-flaw-to-send-visitors-to-bad-sites/

Les informations personnelles de 1 400 000 de Français sont en vente dans un black market

- données mises en vente sur la plateforme HookShop :
  - le nom
  - l'adresse mail
  - l'adresse physique
  - le numéro de téléphone
- probablement issues de credential stuffing / phishing

https://www.zataz.com/francais-a-vendre-cyberboutiques/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Un groupe de cybercriminels arrêté pour le vol de l'équivalent de 19 millions de dollars de téléphones

- via le programme d'upgrade annuel en s'ajoutant en tant qu'utilisateur autorisé après avoir compromis un compte
- une mule activait le programme et récupérait le smartphone en optant pour le prélèvement mensuel
- méthode appliqué dans 34 états
- identifiés par les échanges réguliers de colis par la société de transport

https://nakedsecurity.sophos.com/2019/06/06/gang-charged-with-19-million-iphone-scam/

Flipboard réinitialise les mots de passe de ses utilisateurs suite à la découverte d'un incident de sécurité

- données dérobées :
  - nom ;
  - nom d'utilisateur ;
  - empreinte du mot de passe (la majorité des mots de passe étaient hachés avec l'algorithme bcrypt, d'autres étaient hachés avec l'algorithme SHA-1) ;
  - adresse email ;
  - jetons d'accès (pour les utilisateurs ayant lié leur compte Flipboard à un réseau social).

https://fr-fr.about.flipboard.com/support-information-incident-may-2019/?noredirect=fr_FR

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Trend Micro confirme une intrusion et Symantec nie l'attaque du groupe "Fxmsp"

- Pour Trend Micro, il s'agirait d'un environnement de test local, aucune donnée dérobée identifiée
- Pour Symantec, il n'y a pas assez de preuves
- Pour McAfee, ils n'ont pas identifié d'incident de sécurité lié à cette attaque

https://www.bleepingcomputer.com/news/security/fxmsp-chat-logs-reveal-the-hacked-antivirus-vendors-avs-respond/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Retour sur l'arrestation des espions chinois ayant ciblé Safran

- la DGSI prévenue par le FBI car Safran apparaissait dans la liste des domaines ciblés pour de l'espionnage industriel
- les ordinateurs infectés lors de déplacement en Chine par les employés associés au Ministère chinois de la Sécurité de l'Etat
- employés licenciés et politique de sécurité revue entièrement

https://www.challenges.fr/entreprise/aeronautique/comment-le-fbi-et-la-dgsi-ont-traque-les-espions-de-safran_655004

Google suspend ses activités avec Huawei suite à l'annonce de Donald Trump

- plus d'accès à Android, Gmail, Youtube, Google Play, etc.
- plus d'accès aux fournisseurs Intel Corp, Qualcomm, Xilinx et Broadcom
- En Europe le cout pour les opérateurs Telecom estimé à 55 milliards d'euros

https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive-idUSKCN1SP0NB
https://www.latribune.fr/technos-medias/telecoms/bannir-huawei-couterait-55-milliards-d-euros-aux-operateurs-europeens-819744.html

Nouveautés, outils et techniques

Crypto et Divers

Divers

Google stocke en clair des mots de passe de certains de ses clients depuis plus de 10 ans

- dû à une erreur dans l'ancienne implémentation des fonctions de mise en place et de récupération des mots de passe.

https://www.bleepingcomputer.com/news/security/google-stored-unhashed-g-suite-passwords-for-over-a-decade/

Les fonctionnalités de sécurité pour le moteur de recherche Elasticsearch sont désormais gratuites

- TLS pour des communications chiffrées ;
- authentification native et basée sur des fichiers pour la création et la gestion d'utilisateurs ;
- contrôle d'accès basé sur les rôles pour contrôler l'accès utilisateur aux API du cluster et aux index

https://www.elastic.co/fr/blog/security-for-elasticsearch-is-now-free

Regrippy

- RegRipper en python

https://github.com/airbus-cert/regrippy

OSSIR

Business et Politique

Business

France

Citalid lève 1,2 million d’euros

https://www.globalsecuritymag.fr/Levee-de-fonds-d-amorcage-de-1-2,20190604,87716.html

Business

International

Dashlane lève 110 millions de dollars

https://www.linformaticien.com/actualites/id/52150/dashlane-leve-110-millions-de-dollars.aspx

FireEye achète Verodin

http://www.reseaux-telecoms.net/actualites/lire-verodin-passe-dans-le-giron-de-fireeye-27761.html

Droit / Politique

France

La société SERGIC condamnée à une amende de 400 000€ pour insuffisance dans la protection des données personnelles de ses clients

- données accessibles sans authentification :
  - carte d'identité ;
  - carte Vitale ;
  - avis d'imposition ;
  - attestations délivrées par la Caisse d'allocations familiales ;
  - jugements de divorce ;
  - relevés de compte ;
  - relevés d'identité bancaire.
- données de candidats non retenus conservés en base sans limitation de durée

https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de

478 incidents déclarés par les structures de santé depuis 18 mois

- selon l'ASIP santé (Agence des systèmes d'information partagés de santé)
- 5 cas de mise en danger avérée du patient

https://www.techopital.com/cybersecurite--478-incidents-declares-par-les-structures-de-sante-depuis-18-mois-NS_4278.html

Droit / Politique
International

Trois utilisateurs d'iTunes attaquent Apple en justice pour l'utilisation abusive de leurs données

- D'après eux, Apple revendait les informations suivantes :
  - les noms et prénoms ;
  - l'adresse ;
  - le niveau d'éducation ;
  - une estimation des revenus du foyer ;
  - les goûts musicaux.

https://www.cnet.com/news/apple-sued-by-itunes-customers-over-alleged-data-misuse/
https://www.bloomberg.com/news/articles/2019-05-24/apple-sued-for-selling-customers-itunes-information

L'irlande fait le point sur le RGPD

- 6624 plaintes reçues en 2018 (contre 2500 en 2017)
- 54 enquêtes ouvertes, 11 visent Facebook, WhatsApp et Instagram.
- Twitter, LinkedIn et Google également ciblés

https://www.linformaticien.com/actualites/id/52095/un-an-de-rgpd-vu-d-irlande.aspx

Conférences

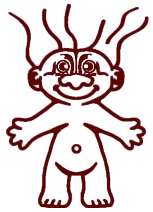
Conférences

Passées

- SSTIC - 5 au 7 juin 2019

A venir

- Pass the Salt - 1 au 3 juillet 2019
- Le Hack - 6 et 7 juillet 2019
- BlackHat - 7 au 9 août 2019
- BSides LasVegas - 6 & 7 août 2019
- DEFCON - 8 au 11 août 2019



Divers / Trolls velus

Divers / Trolls velus

Facebook...

- dévoile qu'il n'y a pas d'attente en matière de vie privée sur les réseaux sociaux
- en cherchant à déjouer une plainte suite à Cambridge Analytica

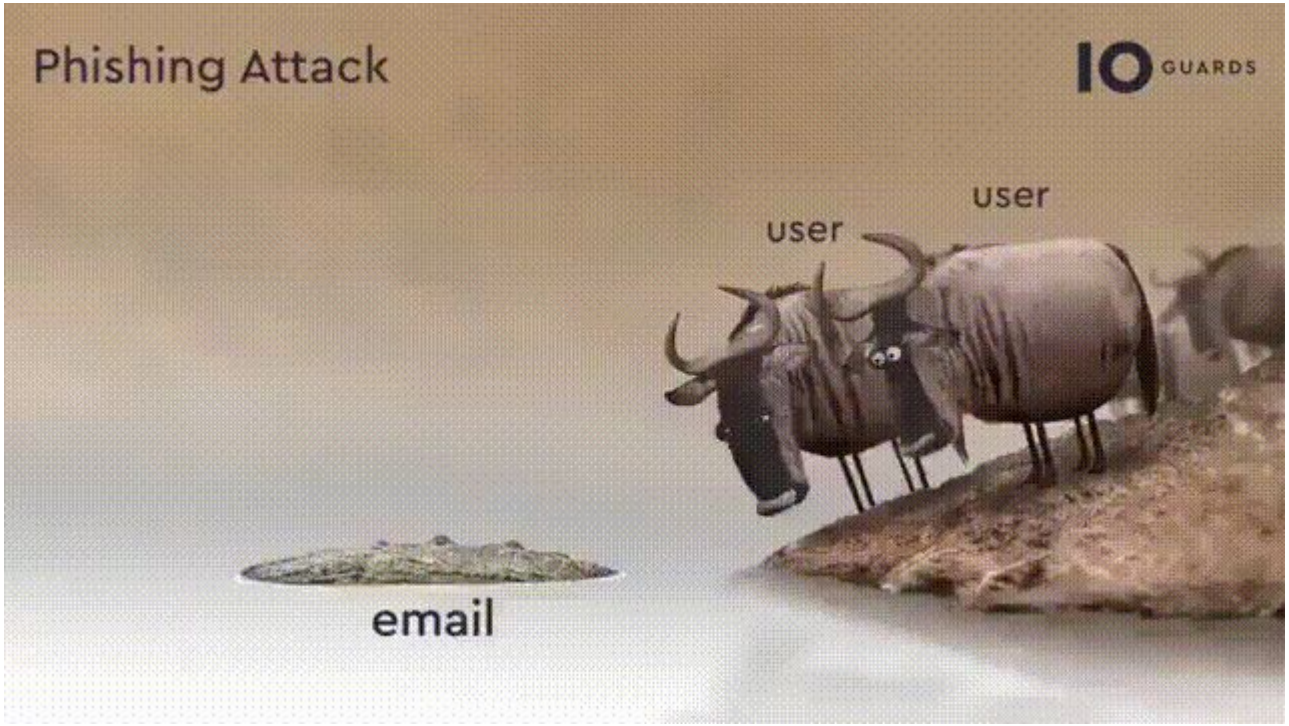
https://www.cnet.com/news/facebook-reportedly-thinks-theres-no-expectation-of-privacy-on-social-media/

- Mark survit au vote de défiance

https://www.bbc.com/news/technology-48472408

"There is no invasion of privacy at all, because there is no privacy"

Divers / Trolls velus



Divers / Trolls velus

Att: All Staff & Al Substations,

Impersonation of persons, living, dead or fictional, is against company policy. Please refer to the Employee Handbook on this and many more rules you should be abiding by during your employ here.

As such, we were very disappointed to learn that someone started a process running under the username "mimikatz" on the domain controller.

As we do not have an employee here named Mimi Katz, nor any employees with the first name "Mimi" nor the last name "Katz", we consider this a violation of aforesaid policy and ask that the person responsible please see H.R. for retraining by the end of business today.

Thank you,

The Management

P.S. Tara, please stop spraying members of the Finance dept with silly string and telling them they are 3-D printed ethernet cables. Your cooperation is appreciated!

Divers / Trolls velus

Do you hate your Competitor?

We'll help you send them a GDPR Data Access Request designed to waste as much of their time as possible. They are legally required to respond to your request within 30 days! 🔥

Divers / Trolls velus

To Whom It May Concern,

I am writing to you in your capacity as data protection officer for your company and I am making this request for access to my personal data pursuant to Article 15 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "GDPR"). I am including a copy of documentation necessary to verify my identity. Please advise as to the following:

1. Please confirm whether or not any of my personal data is being processed. If any of my personal data is being processed, please provide me with the information of which categories of personal data are being processed.
    - 1.a. In particular, please tell me what you know about me in your information systems, whether or not contained in databases, and including e-mail, documents on your networks, or voice or other media that you may store.
    - 2.b. Additionally, please advise me in which countries my personal data is stored, or accessible from. In case you make use of cloud services to store or process my data, please include the countries in which the servers are located where my data are or were (in the past 12 months) stored. Should the personal data be stored on servers outside the EEA, please provide such information.
    - 3.c. Please provide me with a copy of, or access to, my personal data that you have or are processing and if possible with information regarding the exact date you obtained that particular data.
2. Please provide me with a detailed list of the specific purposes of processing of my personal data.
3. Please provide a list of all third parties with whom you have (or may have) shared my personal data. Should these third parties further provided my personal data to another subject, please provide who these subjects are/were.
    - 1.a. If you cannot identify with certainty the specific third parties to whom you have disclosed my personal data, please provide a list of third parties to whom you may have disclosed my personal data.
    - 2.b. Please also identify in which jurisdictions do the third parties that you have identified in 1(a) above that these third parties with whom you have or may have shared my personal data, from which these third parties have store or can access my personal data or from which jurisdictions are my personal data accessed. Please also provide insight in the legal grounds for transferring my personal data to these jurisdictions. Where you have done so, or are doing so, on the basis of appropriate safeguards, please provide a copy.
    - 3.c. Additionally, I would like to know what appropriate safeguards pursuant to article 46 of GDPR that have been put in place in relation to these third parties that you have identified in relation to the transfer of my personal data.
4. Please advise how long you store my personal data, and if retention is based upon the category of personal data, please identify how long each category is retained.
5. If you are additionally collecting personal data about me from any source other than myself, please provide me with all information about their source, as referred to in Article 14 of the GDPR.
6. If you are making any automated decisions about me, including profiling, whether or not on the basis of Article 22 of the GDPR, please provide me with information concerning the basis for the logic in making such automated decisions, and the significance and consequences of such processing.
7. I would like to know whether or not my personal data has been disclosed inadvertently by your company in the past, or as a result of a security or privacy breach.
    - 1.a. If so, please advise as to the following details of each and any such breach:
        - 1.i. a general description of what occurred;
        - 2.ii. the date and time of the breach (or the best possible estimate);
        - 3.iii. the date and time the breach was discovered;
        - 4.iv. the source of the breach (either your own organization, or a third party to whom you have transferred my personal data);
        - 5.v. details of my personal data that was disclosed;
        - 6.vi. your company's assessment of the risk of harm to myself, as a result of the breach;
        - 7.vii. a description of the measures taken or that will be taken to prevent further unauthorized access to my personal data;
        - 8.viii. contact information so that I can obtain more information and assistance in relation to such a breach, and
        - 9.ix. information and advice on what I can do to protect myself against any harms, including identity theft and fraud.
    - 2.b. If you are not able to state with any certainty whether such an exposure has taken place, through the use of appropriate technologies, please advise what mitigating steps you have taken, such as
        - 1.i. Encryption of my personal data;
        - 2.ii. Data minimization strategies; or,
        - 3.iii. Anonymization or pseudonymization;
        - 4.iv. Any other means
8. I would like to know your information policies and standards that you follow in relation to the safeguarding of my personal data, such as whether you adhere to ISO27001 for information security, and more particularly, your practices in relation to the following:
    - 1.a. Please inform me whether you have backed up my personal data to tape, disk or other media, and where it is stored and how it is secured, including what steps you have taken to protect my personal data from loss or theft, and whether this includes encryption.
    - 2.b. Please also advise whether you have in place any technology which allows you with reasonable certainty to know whether or not my personal data has been disclosed, including but not limited to the following:
        - 1.i. Intrusion detection systems;
        - 2.ii. Firewall technologies;
        - 3.iii. Access and identity management technologies;
        - 4.iv. Database audit and/or security tools; or,
        - 5.v. Behavioural analysis tools, log analysis tools, or audit tools;
9. In regards to employees and contractors, please advise as to the following:
    - 1.a. What technologies or business procedures do you have to ensure that individuals within your organization will be monitored to ensure that they do not deliberately or inadvertently disclose personal data outside your company, through e-mail, web-mail or instant messaging, or otherwise.
    - 2.b. Have you had had any circumstances in which employees or contractors have been dismissed, and/or been charged under criminal laws for accessing my personal data inappropriately, or if you are unable to determine this, of any customers, in the past twelve months.
    - 3.c. Please advise as to what training and awareness measures you have taken in order to ensure that employees and contractors are accessing and processing my personal data in conformity with the General Data Protection Regulation.

Finally, I would like you to be aware at the outset, that I anticipate reply to my request within one month as required under Article 12 GDPR, failing which I will be forwarding my inquiry with a letter of complaint to the relevant data protection authorities. In case you will not be able to respond to my request within specified date and will, under the GDPR provided measures, be aiming to prolong such term because of the complexity of my request, please respond to my questions in the maximum possible extent during the original one month term. Should you require any additional information from myself in order to identify me as the subject of data being processed by you, please contact me immediately.

Yours Sincerely,

Your Name

Prochains rendez-vous de l’OSSIR

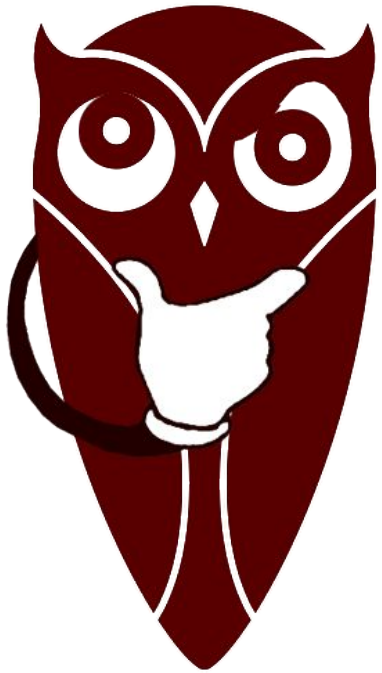
Prochaines réunions

Prochaine réunion

- Mardi 9 juillet 2019

After Work

- ?



Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

OSSIR