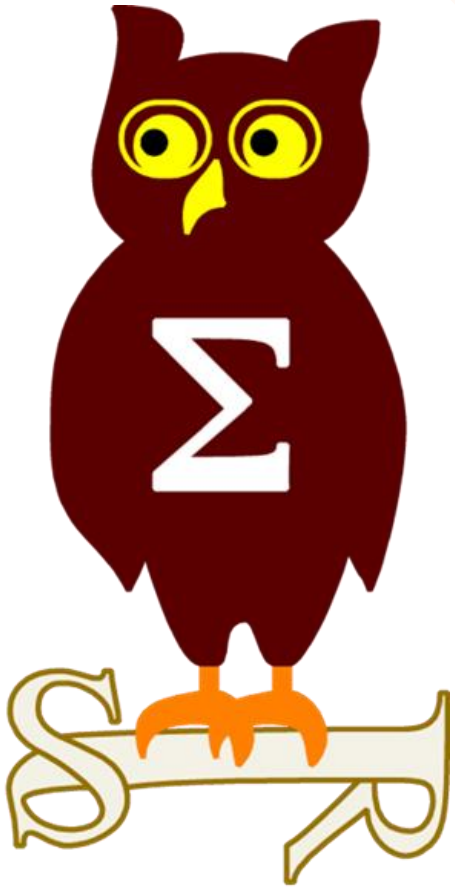
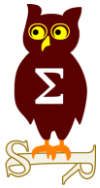


Revue d'actualité

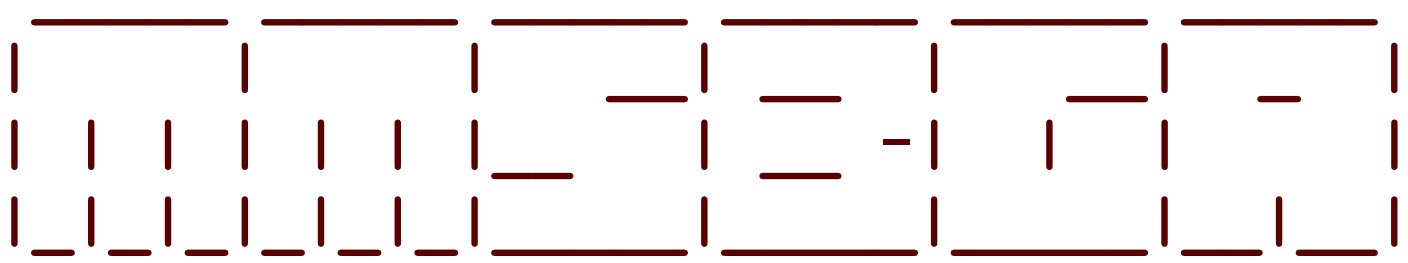
10/10/2017

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*



Failles / Bulletins / Advisories



Make MS Bulletin Great Again / MMSBGA

- Publication du code source sur Github
  https://github.com/mynameisv/MMSBGA

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-108 Vulnérabilités in Internet Explorer (7 CVE)

- Exploit:
  - 1 x Spoofing
  - 5 x Corruption de mémoire aboutissant à une exécution de code
  - 1 x Fuite d'information (contournement d'ASLR)
- Crédits:
  - likemeng de Baidu Security Lab par Trend Micro's Zero Day Initiative (CVE-2017-8750)
  - Hui Gao de Palo Alto Networks (CVE-2017-8749)
  - Microsoft ChakraCore Team (CVE-2017-8741)
  - Masato Kinugawa de Cure53 (CVE-2017-8733)
  - ? (CVE-2017-8748, CVE-2017-8747)
  - Jun Kokatsu (@shhnjk) (CVE-2017-8736)

MS17-109 Vulnérabilités in Edge (29 CVE)

- Exploit:
  - 2 x Security Feature Bypass
  - 20 x Corruption de mémoire aboutissant à une exécution de code
  - 5 x Fuite d'information (contournement d'ASLR)
  - 2 x Usurpations de site web
- Publiée: CVE-2017-8723
- Crédits:
  - Giwan Go de STEALIEN & HIT par Trend Micro's Zero Day Initiative (CVE-2017-8737, CVE-2017-8728)
  - Giorgi Maisuradze, CISPA (CVE-2017-8643)
  - Ivan Fratric de Google Project Zero (CVE-2017-8731, CVE-2017-8734)
  - likemeng de Baidu Security Lab par Trend Micro's Zero Day Initiative (CVE-2017-8750)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2017-8738)
  - Yuki Chen de Qihoo 360 Vulcan team (CVE-2017-8753)
  - Lokihart de Google Project Zero (CVE-2017-11764, CVE-2017-8755, CVE-2017-8729, CVE-2017-8740)
  - Liu Long de Qihoo 360Vulcan Team (CVE-2017-8597, CVE-2017-8757)
  - Microsoft ChakraCore Team (CVE-2017-8649, CVE-2017-8660, CVE-2017-8739, CVE-2017-8741)
  - Maksymilian Motyl from CERT Orange Poland, Zhong Zhaochen (@asnine) de Neusoft (CVE-2017-8648)
  - ? (CVE-2017-11766, CVE-2017-8751, CVE-2017-8752, CVE-2017-8756, CVE-2017-8735, CVE-2017-8748)
  - Jun Kokatsu (@shhnjk) (CVE-2017-8754, CVE-2017-8736, CVE-2017-8724, CVE-2017-8723)

Dont 4 communes avec IE:

- CVE-2017-8736
- CVE-2017-8741
- CVE-2017-8748
- CVE-2017-8750

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-110 Vulnérabilités dans Microsoft Graphics (GDI) (6 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
  - 5 x Fuite d'information (contournement d'ASLR)

    http://0day.today/exploit/28579

    http://0day.today/exploit/28578
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-8685, CVE-2017-8684)
  - Axel Souchet (@0vercl0k) de MSRC Vulnerabilités and Mitigations Team (CVE-2017-8695, CVE-2017-8696)
  - Weibo Wang (@ma1fan) de 360 Skyeye Labs (CVE-2017-8688, CVE-2017-8676)

MS17-111 Vulnérabilités dans Windows PDF Library (2 CVE)

- Affected:
  - Windows 8.1, RT 8.1, Server 2012, Server 2012 R2
- Exploit:
  - 2 x Corruption de mémoire aboutissant à une exécution de code
- Crédits:
  - Giwan Go de STEALIEN & HIT par Trend Micro's Zero Day Initiative (CVE-2017-8728, CVE-2017-8737)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-112 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (9 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
  - 6 x Fuite d'information (contournement d'ASLR)

    http://0day.today/exploit/28581 http://0day.today/exploit/28582 http://0day.today/exploit/28577
  - 2 x Elévation de privilèges
- Credits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-8683, CVE-2017-8682, CVE-2017-8681, CVE-2017-8680)
  - Mateusz Jurczyk, Google Project Zero (CVE-2017-8687)
  - WenQunWang de Tencent's Xuanwu LAB (CVE-2017-8675)
  - Mateusz Jurczyk, Google Project Zero, fanxiaocao and pjf de IceSword Lab, Qihoo 360 (CVE-2017-8678, CVE-2017-8677)
  - Jaanus Kp de Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-8720)

MS17-113 Vulnerability dans Windows NetBIOS (1 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-0161)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-114 Vulnérabilité dans Windows DHCP Server (1 CVE)

- Affected:
  - Windows Server 2012, 2012 R2, 2016
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - ? (CVE-2017-8686)

MS17-115 Vulnérabilité dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - ? (CVE-2017-11767)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-116 Vulnérabilités dans Office (8 CVE)

- Affected:
  - Office toutes versions supportées
  - SharePoint 2007, 2010, 2013, 2016
  - Microsoft Excel pour Mac 2011
- Exploit:
  - 8 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - Lucas Leong de Trend Micro par Trend Micro's Zero Day Initiative, MSRC Vulnérabilités and Mitigations Team (CVE-2017-8744)
  - Minh TranFortinet's FortiGuard Labs (CVE-2017-8742)
  - Steven Seeley (mr_me) de Offensive Security par Trend Micro's Zero Day Initiative (CVE-2017-8631)
  - Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-8743)
  - Jin Chen de Paloaltonetworks (CVE-2017-8567)
  - Debasish Mandal de McAfee IPS Vulnerability Research (CVE-2017-8630)
  - Phil BlankenshipCerberus Security (CVE-2017-8725)
  - Jaanus Clarified Security (CVE-2017-8632)

MS17-117 Vulnérabilités dans Hyper-V (6 CVE)

- Affected:
  - Windows 8.1, RT 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016
- Exploit:
  - 1 x Denial of Service
  - 5 x Fuite d'information (contournement d'ASLR)
- Credits:
  - Nicolas Joly de MSRC Vulnérabilités & Mitigations, ZhenhaoHong de Qihoo 360 Marvel Team (CVE-2017-8707)
  - Nicolas Joly de MSRC Vulnérabilités & Mitigations (CVE-2017-8706)
  - Joe Bialek, MSRC Vulnérabilités and Mitigations Team (CVE-2017-8713)
  - Jordan Rabet, Microsoft Offensive Security Research Team (CVE-2017-8704, CVE-2017-8711)
  - Windows & Devices Group - Operating System Security Team (CVE-2017-8712)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-118 Vulnérabilités dans Windows Kernel (4 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 4 x Fuite d'information (contournement de KASLR)
- Credits:
  - fanxiaocao and pjf de IceSword Lab , Qihoo 360 (CVE-2017-8709, CVE-2017-8719)
  - fanxiaocao and pjf de IceSword Lab, Qihoo 360 (CVE-2017-8679)
  - James Forshaw de Google Project Zero (CVE-2017-8708)

MS17-119 Vulnérabilités dans Windows (3 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Security Feature Bypass
  - 1 x Fuite d'information (contournement d'ASLR)
  - 1 x Elévation de privilèges
- Credits:
  - Zhang Yunhai de NSFOCUS (CVE-2017-8716)
  - Alex Ionescu, CrowdStrike Inc. (CVE-2017-8702)
  - SaifAllah benMassaoud (@benmassaou) (CVE-2017-8710)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-120 Vulnérabilités dans SharePoint (2 CVE)

- Affected:
  - Microsoft SharePoint Foundation 2013 Service Pack 1
  - Microsoft SharePoint Server 2013 Service Pack 1
- Exploit:
  - 2 x Elévation de privilèges
- Credits:
  - Jayson Grace Sandia National Laboratories (CVE-2017-8629)
  - ? (CVE-2017-8745)

MS17-121 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Affected:
  - Microsoft Exchange Server 2013, 2016
- Exploit:
  - 1 x Fuite d'information (contournement d'ASLR)
  - 1 x Elévation de privilèges
- Credits:
  - Zhongcheng Li (CK01) (CVE-2017-11761)
  - Cem Onat Karagun Kocaeli University (CVE-2017-8758)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-122 Vulnérabilité dans Device Guard (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Security Feature Bypass
- Publiée: CVE-2017-8746
- Credits:
  - ? (CVE-2017-8746)

MS17-123 Vulnérabilité dans Uniscribe (1 CVE)

- Affected:
  - Windows 8.1, RT 8.1, 10, server 2012, 2012 R2, 2016
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - Yong Chuan Koh (@yongchuank) de MWR Labs, Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-8692)

MS17-124 Vulnérabilité dans Bluetooth Driver (1 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Spoofing
- Credits:
  - Ben Seri and Gregory Vishnepolsky de Armis, Inc. (CVE-2017-8628)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-125 Vulnérabilité dans .Net (1 CVE)

- Affected:
  - Microsoft .NET toutes version supportées
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Exploitée dans une attaque gouvernementale (FinSPy) dans un RTF piégé

  https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
- Credits:
  - Genwei Jiang and Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2017-8759)

MS17-126 Vulnérabilité dans Windows Shell (1 CVE)

- Affected:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - Pedro Gallegos de Microsoft Office Security Team (CVE-2017-8699)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-127 Vulnérabilité dans Chipset Broadcom BCM43xx (1 CVE)

- Affected:
  - Windows 10
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code

    Explications https://blog.exodusintel.com/2017/07/26/broadpwn/

    Exploit (pour Android et iOS) https://github.com/mailinneberg/Broadpwn
- Credits:
  - ? (CVE-2017-9417)

MS17-128 Vulnérabilité dans Windows RDP (1 CVE)

- Affected:
  - Windows 8.1, 10, Server 2012, 2012 R2, 2016
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
- Credits:
  - Jared S. Candelaria (CVE-2017-8714)

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**

Failles / Bulletins / Advisories

Microsoft - Autre

Un bug dans l'affichage des icônes permets d'usurper celle-ci

- Bug au niveau du cache des icones
- Utilisé par des malwares pour se dissimuler

https://www.cybereason.com/labs-a-zebra-in-sheeps-clothing-how-a-microsoft-icon-display-bug-in-windows-allows-attackers-to-masquerade-pe-files-with-special-icons/

Les différences entre Windows 7/8.1 et 10 permettent de trouver des vulnérabilités

- Technique déjà utilisée sur les correctifs pour trouver les vulnérabilités

https://googleprojectzero.blogspot.fr/2017/10/using-binary-diffing-to-discover.html

La couche Linux de Windows 10 échappe aux antivirus

- Il est possible d'y cacher un malware
- Avec Wine (émulateur) il est même possible d'y cacher un exécutable Windows

http://www.01net.com/actualites/la-couche-linux-integree-a-windows-10-permet-de-cacher-des-malwares-1253998.html

Failles / Bulletins / Advisories

Système (principales failles)

Linux Redhat et CentOS, élévation locale de privilèges, CVE-2017-1000253

- Corruption de la pile à partir de execve()
- Corrigé en 2015 mais non marqué comme sécurité

  https://www.qualys.com/2017/09/26/linux-pie-cve-2017-1000253/cve-2017-1000253.txt

Linux, déni de service sur BlueTooth (exécution de code probable), CVE-2017-1000251

- Après la CVE-2017-8628 sur Windows...
- Un nom de code : BlueBorne
- Un joli logo
- Touche : Windows, Linux, Android, iOS et des IoT (???)

  http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf

  https://gitlab.com/marcinguy/blueborne-CVE-2017-1000251/blob/master/blueborne.txt

OpenVPN, exécution de code à distance

- Sur la fonctionnalité de génération de clef “key-method 1”
- Ancienne fonctionnalité, par défaut dans OpenVPN 2.0 mais remplacé depuis

  https://community.openvpn.net/openvpn/wiki/CVE-2017-12166

Failles / Bulletins / Advisories

Système (principales failles)

Apache Tomcat, exécution de code à distance CVE-2017-12617

- Contournement de la CVE-2017-12615
- Si la méthode PUT est activée (pas par défaut, option “readonly=false”)
- Upload d’un JSP

https://www.alphabot.com/security/blog/2017/java/Apache-Tomcat-RCE-CVE-2017-12617.html

Apache httpd, fuite de mémoire CVE-2017-9798

- Fuite mémoire à partir de la méthode OPTIONS (use after free)
- Si un .htaccess est présent avec l’option “Limit”

http://0day.today/exploits/28573

Vulnérabilité dans dnsmasq

- Serveur DNS et DHCP présent dans de nombreux systèmes Linux et embarqués
- Les correctifs existent, seront-ils déployés sur les objets finaux ?

https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

Failles / Bulletins / Advisories

Système (principales failles)

De très nombreux Mac ont des EFI (Bios) anciens et vulnérables

- Anciens Mac n'ayant pas reçu de mises à jour
- Nouveau Mac vendu non à jour

https://duo.com/blog/the-apple-of-your-efi-mac-firmware-security-research

Une faille au sein de la nouvelle mouture "High Sierra" de Mac OS

- Affichage du mot de passe de chiffrement de volume au sein via la fonctionnalité de définition d'un indice de mot de passe

https://nakedsecurity.sophos.com/2017/10/05/urgent-update-your-mac-again-right-now/

Microsoft trouve une exécution de code dans Chrome

- Chaîne de 3 vulnérabilités

https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-desktop_21.html

Failles / Bulletins / Advisories

Réseau (principales failles)

Etat des lieux de la sécurité des applications mobiles de trading

- IOActive a analysé la sécurité de 21 applications mobiles de bourse
- Les résultats s'avèrent être plus catastrophiques que pour les applications bancaires

http://blog.ioactive.com/2017/09/are-you-trading-securely-insights-into.html

Des failles critiques dans le pare-feu applicatif DenyAll

- De multiples failles critiques découvertes pour le pare-feu applicatif DenyAll
- Ces vulnérabilités sont présentes dans l'API PHP et permettent d'exécuter des commandes arbitraires sans authentification

https://pentest.blog/advisory-denyall-web-application-firewall-unauthenticated-remote-code-execution/

Failles / Bulletins / Advisories

Hardware / IoT

CLKSCREW

- Attaque physique sur les régulateurs de tension (Differential Fault Attack)
- Le principe est de comparer l'exécution entre des conditons normales et des conditions aux limites
- Démontré sur ARM TrustZone, mais possible également sur Intel SGX

https://blog.acolyer.org/2017/09/21/clkscrew-exposing-the-perils-of-security-oblivious-energy-management/

HP iLo, exécution de code à distance, CVE-2017-12542

- Service web "maison" vulnérable à un dépassement de tampon

https://www.synacktiv.com//posts/exploit/rce-vulnerability-in-hp-ilo.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

L’évolution du piratage des distributeurs de billets

- Espionnage des banques
- Intrusion dans leur réseau (phishing…)
- Compromission des distributeurs

http://www.01net.com/actualites/les-nouvelles-techniques-des-pirates-pour-piller-les-distributeurs-de-billets-1267014.html

Carte d’identité numérique en Estonie

- Le générateur de nombres pseudos aléatoire peut être cassé avec 80k€ d’équipement

https://geenius.ee/eksklusiiv/mis-id-kaardiga-ilmselt-tegelikult-juhtus-ja-kui-ohtlik-see-eestile/

Flickr, envoie de photos sur le compte de n’importe qui

- Fonctionnalité d’upload par envoie de mail (non activée par défaut)
- Mail : [mot<=6char][0-100][mot<=6char]@photos.flickr.com
- Mot provenant d’un dictionnaire de moins de 1000 mots

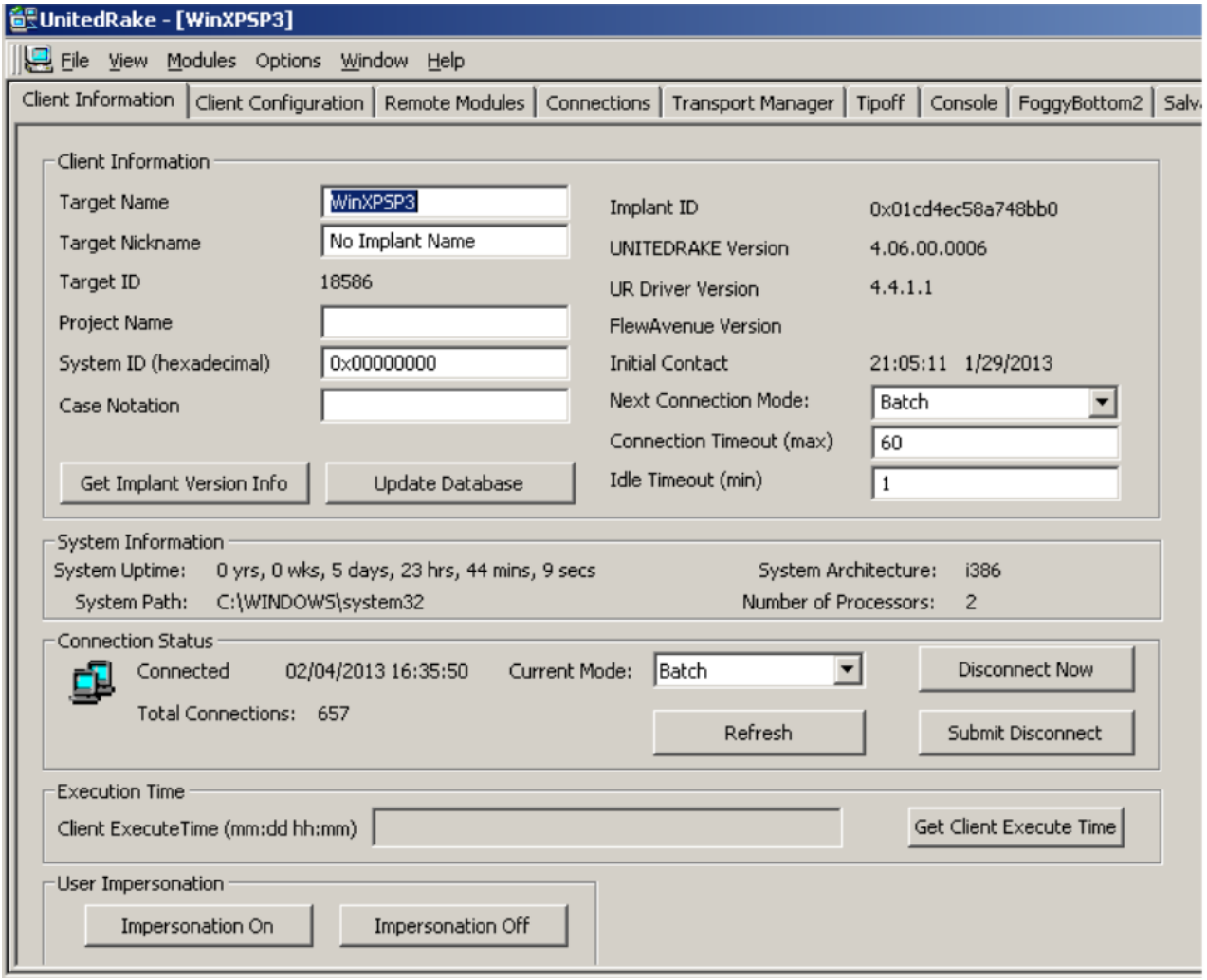
https://ret2got.wordpress.com/2017/10/05/how-i-could-have-mass-uploaded-from-every-flickr-account/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

UnitedRake, le guide de l'opérateur de la NSA

https://assets.documentcloud.org/documents/3987443/The-Shaow-Brokers-UNITEDRAKE-Manual.pdf



Piratages, Malwares, spam, fraudes et DDoS
Espionnage

NSA, encore une fuite ?

- Un sous traitant emporte les outils de la NSA chez lui
- Sur son PC connecté à Internet
- Avec l'antivirus Kaspersky d'installé
- En version "Cloud" qui envoie les hash sur internet

https://assets.documentcloud.org/documents/3987443/The-Shaow-Brokers-UNITEDRAKE-Manual.pdf

APT33, une campagne qui vise les secteurs aéronautique et énergie

- Cibles américaines, sud-coréennes et saoudiennes

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage de Forrester.com

- A priori, pas de fuite de documents confidentiels

  http://securityaffairs.co/wordpress/64016/data-breach/forrester-data-breach.html

Piratage SmartBillions

- “Smart contract” de loterie sur Ethereum
- Hackaton avec 1 500 Ethers ou $450 000, avant le lancement
- Pari sur “0”, après 256 blocks, appel à won(), retour à “0” et gain !
- Mais gain uniquement de 400 Ethers ou $120 000

  https://www.reddit.com/r/ethereum/comments/74d3dc/smartbillions_lottery_contract_just_got_hacked/

CCleaner v5.33.6162, présence d'un malware

- Compromission de Piriform
- Ajout d'un malware dans le package signé
- Distribution entre le 15 août et le 12 septembre
- 3 niveaux d'infection, en cas de cible qualifiée (Intel, Samsung, HTC, VMware, Microsoft, Sony, MSI et Akamai)

  https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-013

  http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Piratages, Malwares, spam, fraudes et DDoS

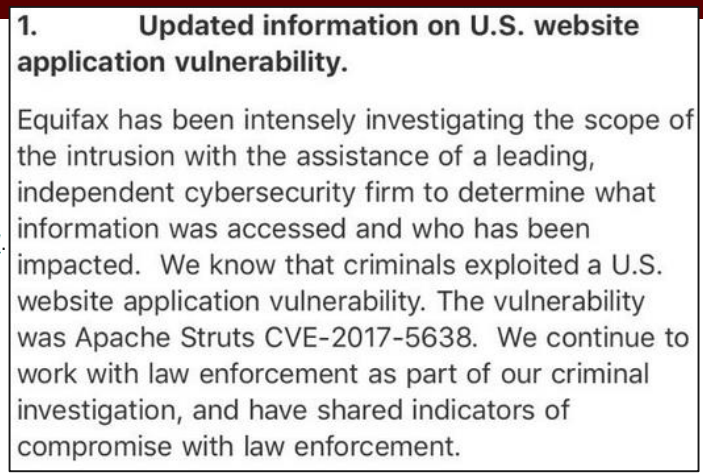
Sites Piratés

Equifax, la suite

- La faille utilisée serait la Struts CVE-2017-5638 de mars
- Equifax n'aurait pas mis à jour..

  http://www.zdnet.com/article/equifax-confirms-apache-struts-flaw-it-failed-to-patch-was-to-blame-for-data-breach/.
- Les 4 autorités de certification d'Equifax ont été révoquées

  https://www.geotrust.com/resources/repository/crls/



1. Updated information on U.S. website application vulnerability.

Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

Deloitte victime d'une attaque sur son infrastructure de messagerie

- Attaque initiée en 2016 mais personne ne sait vraiment
- Des serveurs accessibles en RDP, du NetBIOS sur Internet
- Des comptes VPN publiés sur un GitHub (fermé depuis)

  https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

  https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Kaspersky publie un état des lieux des menaces sur les SI industriels

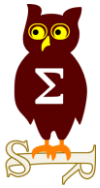
- ~2500 familles de malwares ciblant les SI industriels observés durant le 1er semestre 2017

https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2017/82660/

https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/10/KL-ICS-CERT-H1-2017-report-en.pdf

Vulnérabilité OPC publiée par Siemens…

- ...Mails la vulnérabilité provient de l'implémentation de référence fournie par la fondation OPC



Nouveautés, outils et techniques

Crypto et Divers

Divers

TLS 1.3 a du mal à prendre

- A cause d'équipements intermédiaires buggés

  https://www.ietf.org/mail-archive/web/tls/current/msg24517.html

security.txt le cousin de robots.txt

- Pour décrire la politique de sécurité d'un site web (contacts, chiffrement…)

  https://it.slashdot.org/story/17/09/16/1541219/securitytxt-standard-proposed-similar-to-robotstxt

Pentest
Techniques & outils

Un smartphone Android impossible à surveiller

- Projet en préparation chez Kaspersky
- Ajout d'options pour limiter les informations récupérées par les applications
- Destiné aux employés sensibles d'entreprises liée à l'état Russe

http://www.phonandroid.com/kaspersky-cree-smartphone-android-impossible-surveiller.html

L'arroseur arrosé : faille de sécurité dans Mimikatz

- Lors du parsing d'un fichier LSASS
- Exploitation possible : laisser traîner un faux dump LSASS et attendre qu'un attaquant vienne le récupérer
- Où sont les références CVE ??? 😆

https://www.sec-consult.com/en/blog/2017/09/hack-the-hacker-fuzzing-mimikatz-on-windows-with-winafl-heatmaps-0day/index.html

Un "decoder" amélioré pour Burp

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2017/september/decoder-improved-burp-suite-plugin-release-part-1/

https://www.nccgroup.trust/au/about-us/newsroom-and-events/blogs/2017/october/decoder-improved-burp-suite-plugin-release-part-2/

Identifier l'IP réelle d'un service protégé par un CDN

http://www.chokepoint.net/2017/10/exposing-server-ips-behind-cloudflare.html

Pentest
Techniques & outils

Méthodologie d'audit des "buckets" Amazon S3
https://labs.detectify.com/2017/07/13/a-deep-dive-into-aws-s3-access-controls-taking-full-control-over-your-assets/

Contourner un WAF en changeant l'encodage dans le "Content-type"
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/request-encoding-to-bypass-web-application-firewalls/

Ressources sur la sécurité des BIOS/UEFI
https://github.com/advanced-threat-research/firmware-security-training

Limiter la détéction AV en volant une signature et les méta-données
- D'un exécutable légitime
- Même invalide, une signature vaut mieux que pas de signature
  http://threatexpress.com/2017/10/metatwin-borrowing-microsoft-metadata-and-digital-signatures-to-hide-binaries/

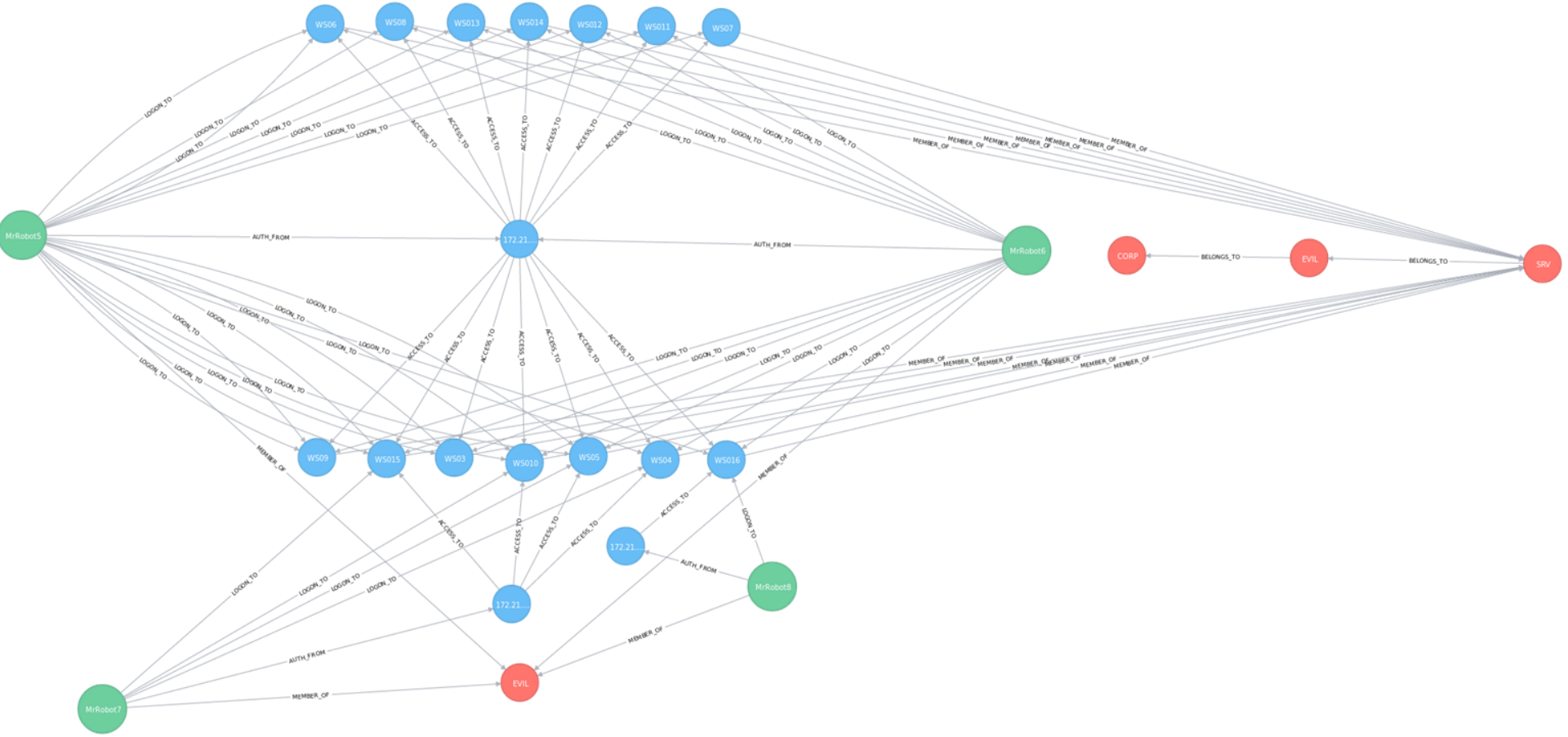
WebUSB
- Nouveau standard permettant d'accéder aux périphériques USB directement depuis le navigateur, avec des implications sur la sécurité
  https://labs.mwrinfosecurity.com/blog/webusb/

Pentest

Défense

Créer un graph de relations utilisateurs/machines à partir des événements Windows

https://github.com/THIBER-ORG/userline/



Business et Politique

Droit / Politique

France

France, ne pas donner ses comptes de réseau sociaux = prison

- Pour 3 ans maximum avec une amende de 45 000€
- Si vous présentez une

  `<<une menace d'une particulière gravité pour la sécurité et l'ordre publics>>`

  https://www.nextinpact.com/news/105265-les-deputes-adoptent-lobligation-declarer-tous-ses-identifiants-electroniques.htm
- Finalement retiré du projet de loi !

ACCReD, l'autre base de données qui fait peur (après TES)

- Concerne les postes « sensibles » : lien avec des grands évènements sportifs ou musicaux, transport… donc beaucoup de monde

  http://www.europe1.fr/societe/accred-ce-mega-fichier-passe-inapercu-et-qui-crible-des-milliers-de-francais-3427637

Droit / Politique
International

USA, ne pas déchiffrer = prison

- Sans limite de durée

  https://www.theregister.co.uk/2017/08/30/ex_cop_jailed_for_not_decrypting_data/?mt=1507555800636

Google abandonne le combat contre le gouvernement US

- Concernant la récupération de données sur un serveur à l'étranger

  https://www.nextinpact.com/news/105203-aux-etats-unis-google-renonce-a-contester-mandats-recherche.htm

4 ans sur Tinder = 800 pages de données collectées

- Une journaliste fait appliquer Directive 95/46/CE et demande ses données à Tinder

  http://mashable.france24.com/medias-sociaux/20170926-tinder-data-vie-privee-internet-reseaux-sociaux-protection

Droit / Politique

International

Chine, 9 mois de prison pour la vente de VPN

- Sanction sur la vente
  http://www.numerama.com/politique/286456-la-chine-condamne-un-internaute-a-9-mois-de-prison-pour-vente-de-vpn.html

Conférences

Conférences

Passées

- n/a

A venir

- Hack.lu - 17-19 October 2017 à Luxembourg
- BlackHat Europe : 6-7 décembre 2017 à Londres
- Botconf - 6 au 8 décembre 2017 à Montpellier
- 34C3 - 27-30 décembre à Leipzig

Divers / Trolls velus

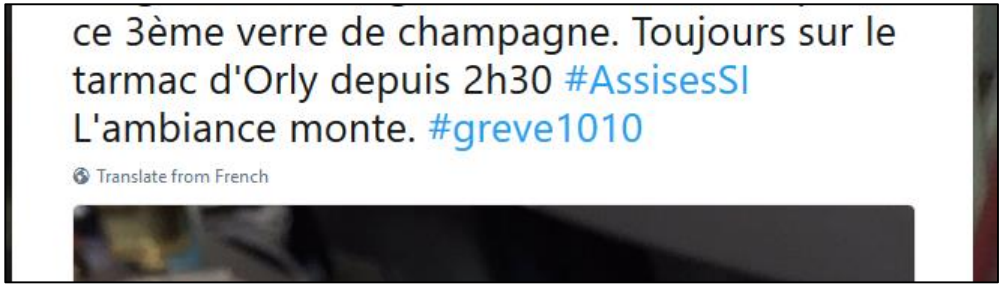
Divers / Trolls velus

Les Assises vs Les Grèves

- Vols annulés

  https://twitter.com/StephaneRou/status/917669755489832960

  https://twitter.com/gbillois/status/916973622719320065



- Site web inaccessible dans la matinée

Divers / Trolls velus

Orange va bloquer les vieux téléphones ne supportant que la 2G

- Pour bloquer les attaques d'interception
- Remonté par l'ANSSI en… 2011

https://www.nextinpact.com/news/105316-orange-mise-a-jour-securite-sur-reseau-2g-bloquera-certains-telephones.htm

La valse des traductions

- data scientist -> expert en mégadonnées
- darknet -> internet clandestin
- deep web -> toile profonde ou abysse

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035638782&dateTexte=&categorieLien=id

Blouson connectée Google et Levis, lavable seulement 10 fois

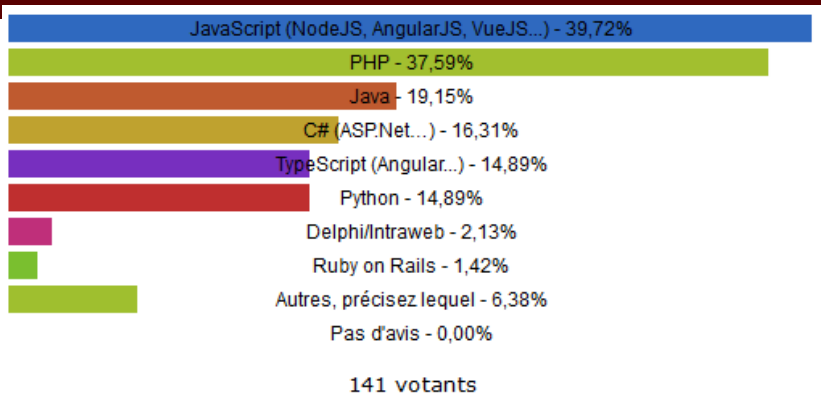
- Et c'est largement suffisant selon Google et Levis 
- Mais qui lave son blouson régulièrement...

https://thenextweb.com/opinion/2017/09/26/google-levis-smart-jacket-wash/

Divers / Trolls velus

PHP reste l'un des langages les plus utilisé

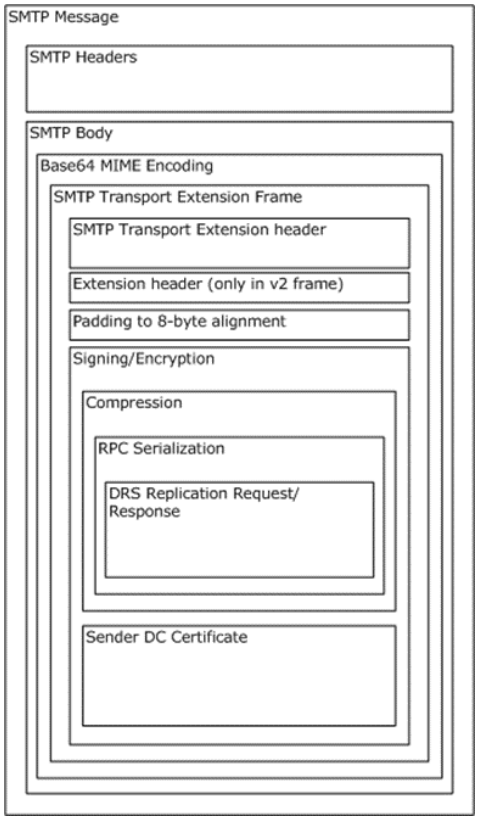
https://web.developpez.com/actu/163267/Quels-sont-vos-langages-de-programmation-preferes-pour-le-Web-en-2017-Et-pourquoi-Vous-etes-invites-a-partager-votre-experience/



RPC et Réplication AD sur SMTP

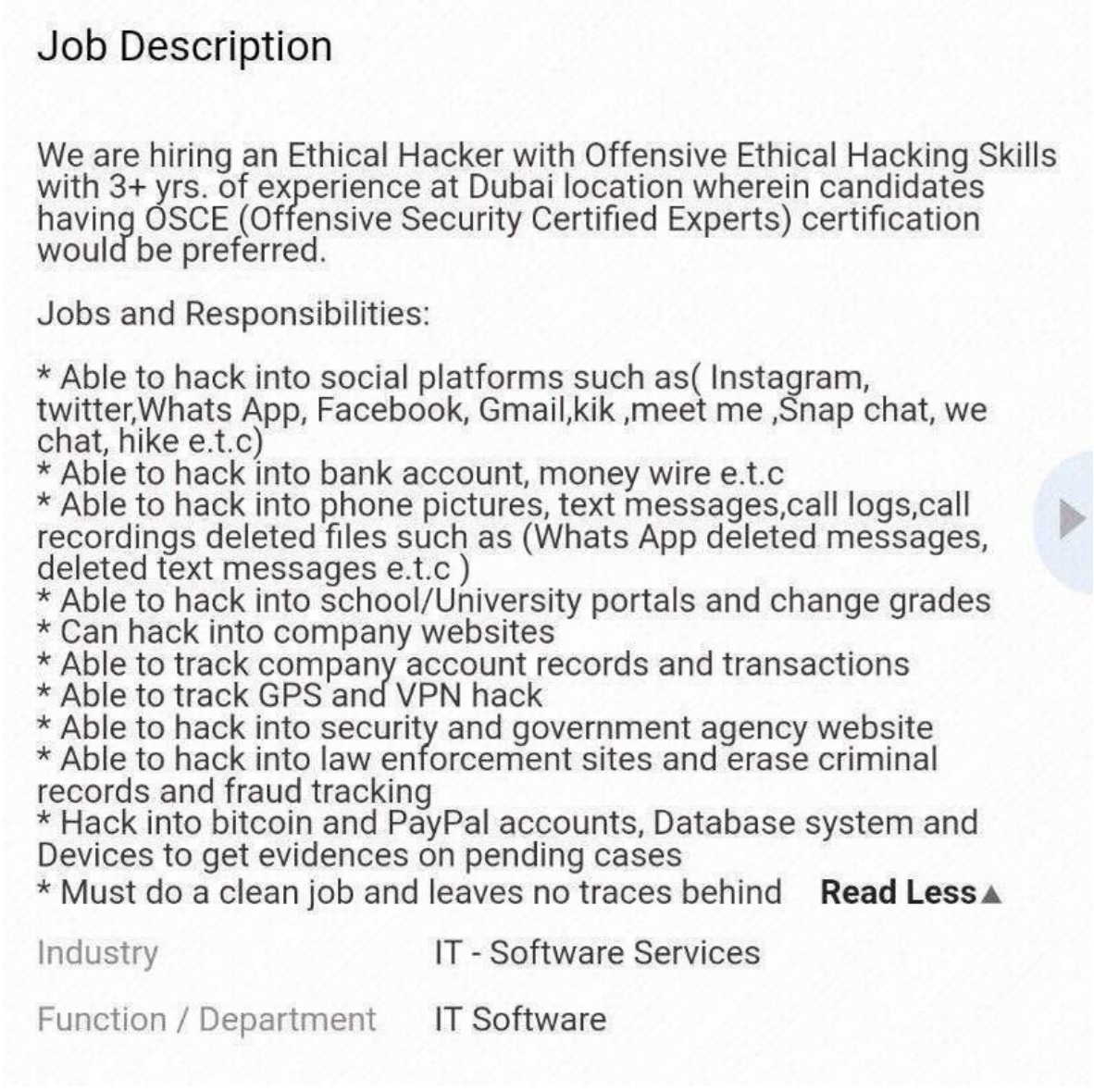
- Mais quelle est cette folie !!?

  https://msdn.microsoft.com/en-us/library/dd358469.aspx



Divers / Trolls velus

Recherche “Ethical Hacker” pour…



Job Description

We are hiring an Ethical Hacker with Offensive Ethical Hacking Skills with 3+ yrs. of experience at Dubai location wherein candidates having OSCE (Offensive Security Certified Experts) certification would be preferred.

Jobs and Responsibilities:

* Able to hack into social platforms such as(Instagram, twitter,Whats App, Facebook, Gmail,kik ,meet me ,Snap chat, we chat, hike e.t.c)
* Able to hack into bank account, money wire e.t.c
* Able to hack into phone pictures, text messages,call logs,call recordings deleted files such as (Whats App deleted messages, deleted text messages e.t.c)
* Able to hack into school/University portals and change grades
* Can hack into company websites
* Able to track company account records and transactions
* Able to track GPS and VPN hack
* Able to hack into security and government agency website
* Able to hack into law enforcement sites and erase criminal records and fraud tracking
* Hack into bitcoin and PayPal accounts, Database system and Devices to get evidences on pending cases
* Must do a clean job and leaves no traces behind **Read Less▲**

Industry IT - Software Services

Function / Department IT Software

Divers / Trolls velus

Quand Abobe publie sa clef privée sur son Blog

- Clef changée depuis

  https://blogs.adobe.com/psirt/?page_id=1498

- Mais archive.org est passé par là

  https://archive.is/BAq9n

Adobe Product Security Incident Response Team (PSIRT) Blog

Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT(at)adobe(dot)com.

PSIRT PGP Key (0x33E9E596)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5iv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcvp335
```

...

```
=QOc7
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
```

CATEGORIES

Alert
Security Bulletins and Advisories
Uncategorized

ARCHIVES

September 2017
August 2017
July 2017
June 2017
May 2017
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
June 2012
May 2012
April 2012
March 2012
February 2012

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 14 novembre 2017

After Work

- Mardi 24 octobre 2017
- Au bar “la Kolok”

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous