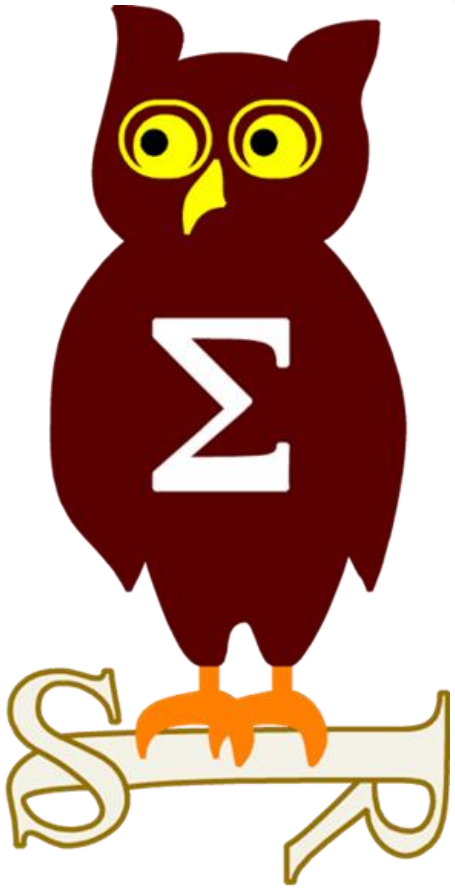
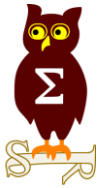


Revue d'actualité

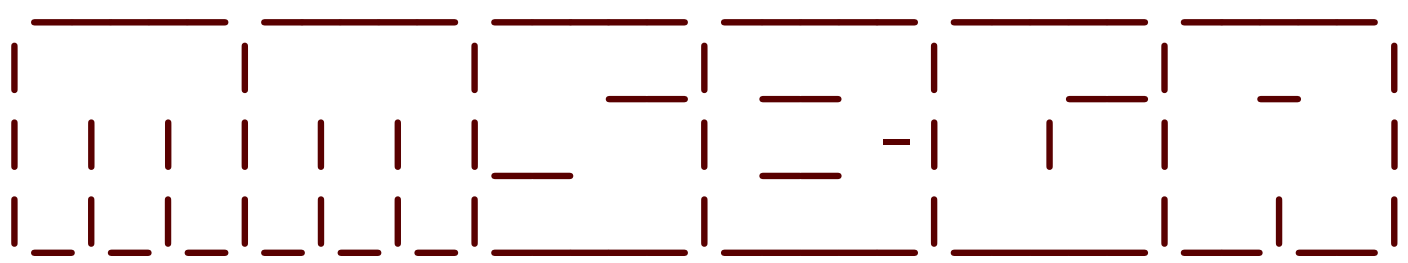
12/09/2017

Préparée par

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



Failles / Bulletins / Advisories



Make MS Bulletin Great Again / MMSBGA

- Contenu des bulletins auto-générés, identiques à ceux du passé
- **Ordre** assez **proches** des bulletins passés
  - Pas de formule magique pour retrouver le bon ordre
- Plus de 100 correctifs manuels pour coller au “style” de Microsoft
  - style = les bulletins ont été construits par des ingénieurs défoncés au crack !

Les Bulletins Microsoft sont de retour !

(code source bientôt sur github)

Failles / Bulletins / Advisories

*Microsoft - Avis - **Anciennes vulnérabilités remarquables***

MS17-055 Vulnérabilités in Windows (9 CVE)

- CVE-2017-8464 : Exécution de code à partir des raccourcis Windows
- Fonctionne avec la propriété **SpecialFolderDataBlock** et **KnownFolderDataBlock**
  - Combiné à du téléchargement automatique des navigateurs, c'est fatal !

CVE-2017-7269

- Exécution de code à distance sur Windows 2003 IIS 6.0
- Tous les détails sont ici :

  https://0patch.blogspot.fr/2017/03/0patching-immortal-cve-2017-7269.html
- Plus de 300 000 IIS sur Shodan

  https://www.shodan.io/search?query=Microsoft-IIS%2F6.0

Failles / Bulletins / Advisories

*Microsoft - Avis - **Anciennes vulnérabilités remarquables***

MS17-072 Vulnérabilités dans Windows (7 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 2 x Remote Code Execution => dans PowerShell 
  - 2 x Information Disclosure
  - 2 x Elevation of Privilege
- Credits:
  - Tencent Security Sword Team par Trend Micro s Zero Day Initiative (ZDI) (CVE-2017-8463)
  - SaifAllah benMassaoud (@benmassaou) (CVE-2017-8557)
  - David Fernandez de Sidertia Solutions (CVE-2017-0170)
  - Yaron Zinar, Eyal Karni, Roman Blachman Preempt (CVE-2017-8563)
  - Oleksandr Mirosh and Alvaro Mu oz (@pwntester) from Hewlett-Packard Enterprise Security (**CVE-2017-8565**)
  - Pedro Gallegos de Microsoft Office Security Team (CVE-2017-8566)
  - ? (CVE-2017-8587)

MS17-074 Vulnérabilité dans HoloLens (1 CVE) 

- Affecte:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Remote Code Execution
- Credits:
  - ? (CVE-2017-8584)

Failles / Bulletins / Advisories

*Microsoft - Avis - **Anciennes vulnérabilités remarquables***

MS17-075 Vulnérabilités dans Office (7 CVE)

- Out of Band, publié 10j. après les autres CVE
  https://nakedsecurity.sophos.com/2017/08/08/microsoft-issues-out-of-band-security-updates-for-outlook-office/amp/
- Affected:
  - Offices toutes versions supportées, SharePoint Enterprise Server 2013
- Exploit:
  - 5 x Remote Code Execution
  - 1 x Security Feature Bypass
  - 1 x Information Disclosure
- Credits:
  - @j00sean (CVE-2017-0243)
  - Haifei Li de McAfee Security Team (CVE-2017-8570)
  - Nicolas Joly de MSRCE UK (CVE-2017-8571)
  - Microsoft Office Security Team (CVE-2017-8663)
  - Aaron Grattafiori de Facebook, RedTeam, Soroush Dalili from NCC Group (CVE-2017-8572)
  - Yangkang (@dnpushme) & Liyadong & Wanglu de Qihoo 360 Qex Team (CVE-2017-8501)
  - Yong Chuan Koh (@yongchuank de MWR Infosecurity (CVE-2017-8502)

MS17-084 Vulnérabilité dans WordPad (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution 
- Credits:
  - Pedro Gallegos and Willson David de Microsoft Office Security Team (CVE-2017-8588)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-088 Vulnérabilités dans Internet Explorer (7 CVE)

- Affecte:
  - Internet Explorer 9, 10, 11
- Exploit:
  - 6 x Remote Code Execution
  - 1 x Security Feature Bypass, Contournement de Device Guard et UMCI

  https://posts.specterops.io/umci-vs-internet-explorer-exploring-cve-2017-8625-3946536c6442
- Crédits:
  - wh1ant par Trend Micro's Zero Day Initiative, Huang Anwen, He Xiaoxiao ichunqiu Ker Team (CVE-2017-8641)
  - 62600BCA031B9EB5CB4A74ADDDD6771E par Trend Micro's Zero Day Initiative (CVE-2017-8653)
  - Lokihart de Google Project Zero (CVE-2017-8635)

  Matt Nelson (@enigma0x3) de SpecterOps, Oddvar Moe (@oddvarmoe) working for Advania AS (CVE-2017-8625)
  Hui Gao de Palo Alto Networks (CVE-2017-8651)
  Lokihart de Google Project Zero, Huang Anwen, He Xiaoxiao ichunqiu Ker Team (CVE-2017-8636)
  MSRC Vulnerabilities and Mitigations Team (CVE-2017-8669)

MS17-089 Vulnérabilités dans Edge (28 CVE)

- Affecte:
  - Edge
- Exploit:
  - 2 x Security Feature Bypass
  - 20 x Remote Code Execution

    https://dl.packetstormsecurity.net/1708-exploits/msedgechakraint-overflow.txt
  - 4 x Information Disclosure
  - 2 x Elevation of Privilege
- Crédits:
  - Ivan Fratric de Google Project Zero (CVE-2017-8644, CVE-2017-8637, CVE-2017-8652, CVE-2017-8659)
  - wh1ant par Trend Micro's Zero Day Initiative, Huang Anwen, He Xiaoxiao ichunqiu Ker Team (CVE-2017-8641)
  - Natalie Silvanovich de Google Project Zero (CVE-2017-8657)
  - 62600BCA031B9EB5CB4A74ADDDD6771E par Trend Micro's Zero Day Initiative (CVE-2017-8653)
  - Hao Linan de Qihoo 360 Vulcan Team, HyungSeok Han, @daramg de KAIST SoftSec (CVE-2017-8634)
  - Lokihart de Google Project Zero (CVE-2017-8635, CVE-2017-8640, CVE-2017-8646, CVE-2017-8645, CVE-2017-8656, CVE-2017-8670, CVE-2017-8671)
  - ? (CVE-2017-8661, CVE-2017-8674)
  - Liu Long de Qihoo 360Vulcan Team (CVE-2017-8662)
  - Microsoft ChakraCore Team (CVE-2017-8647, CVE-2017-8655, CVE-2017-8638, CVE-2017-8639, CVE-2017-8672)
  - Thomas Vanhoutte par Trend Micro's Zero Day Initiative (CVE-2017-8503)
  - Lokihart de Google Project Zero, Huang Anwen, He Xiaoxiao ichunqiu Ker Team (CVE-2017-8636)
  - MSRC Vulnerabilities and Mitigations Team (CVE-2017-8669)
  - Jun Kokatsu (@shhnjk) (CVE-2017-8642, CVE-2017-8650)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-090 Vulnérabilités dans Windows Subsystem for Linux (2 CVE)

- Affecte:
  - Windows 10 Version 1703
- Exploit:
  - 1 x Denial of Service
  - 1 x Elevation of Privilege
- Credits:
  - ? (CVE-2017-8627)
  - Alex Ionescu de Winsider Seminars & Solutions, Inc. (CVE-2017-8622)

MS17-091 Vulnerabilities in Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 1 x Remote Code Execution
- Credits:
  - Microsoft ChakraCore Team (CVE-2017-8658)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-092 Vulnérabilité dans Windows (1 CVE)

- Affecte:
  - Windows 10, 8.1, 8.1 RT, 2012, 2016
- Exploit:
  - 1 x Remote Code Execution
- Credits:
  - Microsoft Office Security Team (CVE-2017-8591)

MS17-093 Vulnérabilité dans Windows PDF Library (1 CVE)

- Affecte:
  - Windows 10, 8.1, 8.1 RT, 2008 R2, 2012, 2012 R2 , 2016
- Exploit:
  - 1 x Remote Code Execution
- Credits:
  - Ke Liu (winsonliu) de Tencent's Xuanwu LAB par Trend Micro's Zero Day Initiative (CVE-2017-0293)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-094 Vulnérabilité dans Windows Search / WSearch (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution, exploitable à distance par SMB pour prendre le contrôle d'un système
    - Vulnérabilité "**wormable**"
- Credits:
  - Nicolas Joly de MSRC Vulnerabilities & Mitigations (CVE-2017-8620)

MS17-095 Vulnérabilité dans JET Database Engine (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Remote Code Execution
- Credits:
  - Zhou Yu par Trend Micro's Zero Day Initiative (CVE-2017-0250)

MS17-096 Vulnérabilité dans Hyper-V (2 CVE)

- Affecte:
  - Windows 8.1, 10, 2012, 2012 R2, 2016
- Exploit:
  - 1 x Denial of Service
  - 1 x Remote Code Execution => évasion de la machine virtuelle
- Credits:
  - Azure Security Reliance Team (CVE-2017-8623)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2017-8664)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-097 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (2 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
- Credits:
  - fanxiaocao and pjf de IceSword Lab , Qihoo 360 (CVE-2017-8666)
  - WenQunWang de Tencent's Xuanwu LAB (CVE-2017-8593)

MS17-098 Vulnérabilité dans Adobe Font Driver (1 CVE)

- Affecte:
  - Windows 7, 2008, 2008 R2
- Exploit:
  - 1 x Remote Code Execution
    - Exploitable depuis une page web, un PDF...
- Credits:
  - Wayne Low de Fortinet FortiGuard Labs (CVE-2017-8691)

MS17-099 Vulnérabilité dans Office (1 CVE)

- Affecte:
  - Microsoft SharePoint Server 2010 Service Pack 2
- Exploit:
  - 1 x Spoofing
- Credits:
  - Microsoft Office Security Team, Andrew Watts & Adam Awan, eShare Ltd Company (CVE-2017-8654)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-100 Vulnérabilité dans SQL Server (1 CVE)

- Affecte:
  - SQL Server 2012, 2014, 2016
- Exploit:
  - 1 x Information Disclosure
- Credits:
  - ? (CVE-2017-8516)

MS17-101 Vulnérabilité dans Windows RDP (1 CVE)

- Affecte:
  - Windows 10
- Exploit:
  - 1 x Denial of Service
- Credits:
  - Tripwire VERT (CVE-2017-8673)

MS17-102 Vulnérabilité dans Volume Manager (1 CVE)

- Affecte:
  - Windows 7, 8.1, RT 8.1, 2008, 2008 R2, 2012, 2012 R2
- Exploit:
  - 1 x Information Disclosure
- Credits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2017-8668)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-103 Vulnérabilité dans Windows Error Reporting (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
- Credits:
  - Thomas Vanhoutte par Trend Micro's Zero Day Initiative (CVE-2017-8633)

MS17-104 Vulnérabilité dans Windows Common Log File System Driver (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
- Credits:
  - Jaanus Kp Clarified Security par Trend Micro's Zero Day Initiative (CVE-2017-8624)

MS17-105 Vulnérabilité dans Xamarin (iOS) (1 CVE)

- Affecte:
  - Xamarin.iOS
- Exploit:
  - 1 x Elevation of Privilege (Xamarin est une plateforme de développement)
- Credits:
  - Yorick Koster Securify B.V. (CVE-2017-8665)

Failles / Bulletins / Advisories

Microsoft - Avis

MS17-106 Vulnérabilité dans Windows NetBIOS (1 CVE)

- Affecte:
  - Toutes versions supportées
- Exploit:
  - 1 x Denial of Service
- Credits:
  - Huichen Lin and Prof. Neil Bergmann de School de Information Technology and Electrical Engineering - The University de Queensland (CVE-2017-0174)

MS17-107 Vulnérabilités dans Adobe Flash (2 CVE)

- Affecte:
  - Adobe Flash Player
- Exploit:
  - 2 x Remote Code Execution
    - Contournement du correctif (liste noire de chemins) en démarrant par une requête web avec côté serveur un redirect vers smb

    https://blog.bjornweb.nl/2017/02/flash-bypassing-local-sandbox-data-exfiltration-credentials-leak/#smb-at-play-leaking-windows-user-credentials
- Credits:
  - ? (CVE-2017-3085, CVE-2017-3106)

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

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

Failles / Bulletins / Advisories

Microsoft - Autre

Edge, contournement du filtre anti-XSS

```
1,class extends[]/alert(1){}//
```

Windows 10 intègre à présent EMET

```
c:\windows\system32/syswow64\PayloadRestrictions.dll
```

- Tous les détails du chargement des processus :

  https://github.com/deroko/payloadrestrictions

SMBv1 est désactivé sur les images de machine virtuelle dans Azure

- Il était temps !

  https://twitter.com/GossiTheDog/status/902267729457160193/photo/1

Failles / Bulletins / Advisories

Système (principales failles)

Rufus, mise à jour en HTTP

- Réponse du développeur : <<dans la crypto depuis 15 ans, tu va pas m'apprendre la vie>>

https://github.com/pbatard/rufus/issues/1009#issuecomment-325415199

Chrome

- Plusieurs exécutions de code à distance
  - Les plus critiques viennent du Bug Bounty

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

Extension de navigateur Cisco Webex, de nouvelles exécutions de code à distance

- Injection d'objet JSON, contournement de la liste de blanche de site...

https://bugs.chromium.org/p/project-zero/issues/detail?id=1324&desc=2

Race condition dans Linux vieille de 7 ans / CVE-2017-2636

https://www.youtube.com/watch?v=-EIlFhcOvTs

Failles / Bulletins / Advisories

Système (principales failles)

Apache Struts2 “encore” des exécutions de code à distance

- CVE-2017-9791 code d'exploitation contre les “Object Graph Navigation Language “
  https://github.com/nixawk/labs/tree/master/CVE-2017-9791
- CVE-2017-9805 présent depuis 2008, code pour tester sa présence
  https://github.com/mazen160/struts-pwn_CVE-2017-9805

Nginx 1.12.1 et 1.13.3, dépassement d’entier / CVE-2017-7529

- Avec l’entête “Range:”
  http://nginx.org/en/security_advisories.html

Git, exécution de code à partir d'un lien ssh:// CVE-2017-9800, CVE-2017-1000116 et CVE-2017-1000117

- En précédant le nom de domaine d'un tiret '-'
- Aboutissant à méprise, prenant cela pour un paramètre
  `ssh://-oProxyCommand=sh...`
- Cela fonctionne aussi avec un dépôt dont le nom est précédé d'un tiret
  https://www.mail-archive.com/linux-kernel@vger.kernel.org/msg1466490.html
  https://gitlab.com/joernchen/CVE-2017-1000117

Thunderbird, exécution de code lors du redimensionnement d’une fenêtre

https://www.mozilla.org/en-US/security/advisories/mfsa2017-20/

Failles / Bulletins / Advisories

Système (principales failles)

Antivirus F-Secure, exécution de code à distance

- A la reception d'un mail au format Microsoft TNEF
- Antivirus sans sandbox, tournant en SYSTEM

https://landave.io/2017/08/f-secure-anti-virus-arbitrary-free-vulnerability-via-tnef/

Kaspersky Privacy Cleaner

- Retiré du marché
- Nombreuses vulnérabilités : téléchargement en HTTP, chargement arbitraire de dll, …

http://seclists.org/fulldisclosure/2017/Sep/25?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed%3A+seclists%2FFullDisclosure+%28Full+Disclosure%29

SMBLoris

- Déni de service à distance, sans authentification,
  - Surconsommation des ressources (CPU/RAM)

https://smbloris.com/

Failles / Bulletins / Advisories

Système (principales failles)

VirtualBox 5.1.22

- Elévation de privilège par injection de DLL en trichant sur le chemin de la librairie avec un lien symbolique \\localhost\c$\poc\dummy\vboxc.dll

  https://www.exploit-db.com/exploits/42426/

- Contournement de la signature des DLL

  https://www.exploit-db.com/exploits/42425/

Hyper-V (cf. Microsoft)

- Evasion de la machine virtuelle

VMware NSX-V, déni de service sur OSPF

https://www.vmware.com/security/advisories/VMSA-2017-0014.html

Failles / Bulletins / Advisories

Réseau (principales failles)

Bind TKEY

- Encore un déni de service sur Bind (CVE-2016-2776)
- Avec un plugin pour Metasploit

  https://github.com/rapid7/metasploit-framework/pull/7382

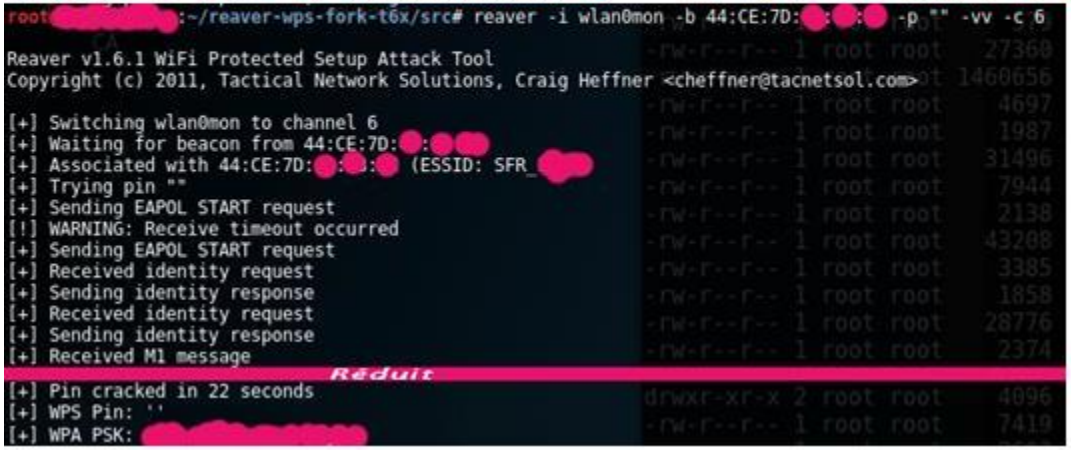
Vulnérabilité WPS sur les box ADSL françaises

- Authentification réussie avec une clef vide !

  http://www.crack-wifi.com/forum/topic-12127-0-day-crack-wps-vs-zte-avec-reaver-16b-et-un-pin-null.html

- Il est plus long de télécharger les bons paquets que d'exploiter la vulnérabilité 😂

```
git clone https://github.com/t6x/reaver-wps-fork-t6x
cd reaver-wps-fork-t6x*/
cd src/
./configure
make
./reaver -i wlan0 -b XX:XX:XX:XX:XX -p "" -vv -c 6  --> avec à la place des X l'adresse MAC de la borne/box ciblée
```



Failles / Bulletins / Advisories

Hardware / IoT

Alarme iSmartAlarm, contournement de l'authentification et exécution de commande

- MitM: interception de la clef secrète chiffrée avec une mauvaise implémentation de XXTEA

  http://seclists.org/fulldisclosure/2017/Jul/27

Smartphone OnePlus 2, contournement du secureboot / CVE-2017-11105

- Réponse du constructeur "won't patch"

  https://alephsecurity.com/vulns/aleph-2017026

Chipset WiFi Broadcom, dépassement de tampon / CVE-2017-9417

- A partir de messages Wireless Multimedia Extensions (WME) de gestion de la qualité de service
- Exploitable sans que l'équipement se connecte à un point d'accès
- Exécution de code possible à condition de connaitre l'équipement et le firmware

  http://boosterok.com/blog/broadpwn/

  http://boosterok.com/blog/broadpwn2/

WiFi Direct sur les télévision Samgung

- WiFi sans point d'accès avec liste blanche sans authentification par adresse MAC

`<<Samsung replied ... this is not a security threat>>`

http://seclists.org/fulldisclosure/2017/Apr/101

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Un robot qui ouvre les coffre-fort

- 15min pour ouvrir un coffre avec 3 rotors de 100 positions

  https://www.wired.com/story/watch-robot-crack-safe/

Rétro-ingénierie de microcode x86

- Micro-code : traduit les instructions assembleur en langage processeur
- Peut se mettre à jour
- Possible de l'exploiter pour introduire une porte dérobée cryptographique
- Sources :

  http://syssec.rub.de/media/emma/veroeffentlichungen/2017/08/16/usenix17-microcode.pdf

Fuite de données par canal auxiliaire USB

- Récupération des frappes d'un clavier par un autre périphérique
- Fonctionne même avec un port "charge seulement / pas de données"

  https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-su.pdf

Commande des assistants personnels avec des fréquences inaudibles par l'homme

- Siri, Amazon Echo, Okay Google...

  https://apple.slashdot.org/story/17/09/06/2026247/hackers-can-take-control-of-siri-and-alexa-by-whispering-to-them-in-frequencies-humans-cant-hear

RawHammer sur des disques SSD

- Modifier le contenu ou les propriétés d'un fichier (SUID)

  https://www.usenix.org/system/files/conference/woot17/woot17-paper-kurmus.pdf

- Permet par exemple une élévation de privilèges

  https://www.youtube.com/watch?v=Mnzp1p9Nvw0

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

ShadowPad

- Attaque révélée par Kaspersky
- Compromission d'un éditeur de logiciel de gestion de serveur
- Distribution d'un malware par une mise à jour signée

https://securelist.com/shadowpad-in-corporate-networks/81432/

https://www.symantec.com/security_response/writeup.jsp?docid=2017-081607-0105-99

https://usa.kaspersky.com/about/press-releases/2017_shadowpad-attackers-hid-backdoor-in-software-used-by-hundreds-of-large-companies-worldwide

Express Lane, l'espionnage par le CIA de ses alliés

- Fourniture d'une solution de prise d'empreintes biométriques
- Solution "backdoorée" avec récupération des données par clef USB lors des mises à jour

https://wikileaks.org/vault7/#ExpressLane

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage d'un employé de Mandiant

https://pastebin.com/raw/6HugrWH4

Leak des épisodes de Game of Thrones

- Des indiens arrêtés

  https://www.wired.com/story/game-of-thrones-leak-hbo-hack/

Les données personnelles de 200 millions de votants américains exposées

- Mauvaise configuration d'un service cloud (bucket S3)

  https://www.darkreading.com/cloud/cloud-security-lessons-from-the-voter-data-leak-/d/d-id/1329197

  http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html

Piratage de WikiLeaks ?

- Non, juste du compte de gestion des DNS
- Redirection vers http://181.215.237.148/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

EquiFax, fuite des données de 143 millions de personnes

- Entreprise de “credit ranking” existant depuis 1899
- Fuite de 143 millions de données
  - Nom, prénom, adresse
  - Numéros de sécurité social
  - Numéros de permis de conduire
  - Environ 200 000 n° CC
- Déjà en vente sur internet

  https://twitter.com/real_1x0123/status/906145402025598977/photo/1

- Exploitation d’une faille Apache Struts
- Débat sur la faille : 0day ou pas ?

  https://www.theregister.co.uk/2017/09/11/apache_rebuts_equifax_allegation/
- Juste avant l’annonce, le top management vend ses actions

  https://www.democracynow.org/2017/9/8/headlines/equifax_executives_sold_18m_in_stock_before_disclosing_massive_data_breach
- La communication changeante et déplorable est fortement critiquée

  https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

Le kit d'exploitation Angler contourne EMET 5.5

- En particulier DEP et EAF avec des exploits Flash et Silverlight

  https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html

Piratages, Malwares, spam, fraudes et DDoS

SCADA

Attaque sur le protocole S7CommPlus de Siemens

- Protocole sécurisé pour la communication avec les automates
- Chiffre les échanges
- Apparemment, utilisation de secrets hardcodés dans l'application pour le chiffrement

  https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/Cheng%20Lei/DEFCON-25-Cheng-Lei-The-Spear-to-Break-the-Security-Wall-of-S7CommPlus-WP.pdf

Vulnérabilités sur des pompes à insulines

- MedFusion 4000
- Buffer Overflow, secrets codés en dur, contrôle d'accès défaillant, ...

  https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02

Vulnérabilité XXE dans les SCADA Siemens

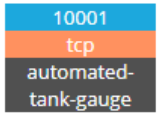
- Dans le service de découverte OPC UA

  https://ics-cert.us-cert.gov/advisories/ICSA-17-243-01

Les pompes à essence aussi vulnérables

- Injection SQL, contrôle d'accès insuffisant

  https://ics-cert.us-cert.gov/advisories/ICSA-17-243-04




```
r
I20100
SEP 7, 2017    06:26 PM
   OPW-FMS SiteSentinel iSite

   EXXON ID: 1
   800 South Cobb Drive
   Marietta, GA 30008
   770-499-0899

INVENTORY REPORT

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  Unleaded               8008      7917     1516    71.50    -0.00    76.23
  2  Premium
  3  Diesel                  344       341     9156     7.23    -0.00    79.10
```

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

Faille sur le bus CAN

- Utilisé depuis plusieurs décennies dans l'automobile
- Fonctionnalité pour isoler un périphérique sur le bus s'il envoie trop de messages d'erreur
- Peut être exploité par des attaquants pour désactiver certaines fonctions de sécurité

  https://www.schneier.com/blog/archives/2017/08/unfixable_autom.html

  http://blog.trendmicro.com/trendlabs-security-intelligence/connected-car-hack/

Vulnérabilités sur les pacemakers

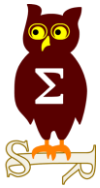
- Produits de la société Abbot
- Possibilité de contourner l'authentification, de vider la batterie, ...
- Environ 500 000 patients sont appelés à venir faire une mise à jour

  https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01

Etat des lieux de la sécurité des boxes et accès Internet en Corée du Sud

- Par Pierre Kim
- Trop long à détailler...

  https://pierrekim.github.io/advisories/z0-Owning_embedded_devices_and_network_protocols-redacted.pdf



Nouveautés, outils et techniques

Crypto
Divers

GnuPG, évolutions importantes

- Fin des 3 versions en parallèle
- Protocole de distribution des clefs simplifié (WKS)

  https://lists.gnupg.org/pipermail/gnupg-announce/2016q3/000393.html

VeraCrypt 1.21

- ASLR + NX
- Meilleures performances
- Support des puces TPM 2.0 (encore en développement)
- SecureDesktop, intéressant contre un malware userland

  https://www.veracrypt.fr/en/Downloads.html

Framework de pentest pour ZigBee

http://pentestit.com/z3sec-zigbee-penetration-testing-framework/

Modules GNU radio pour décoder les signaux de certaines clés de voiture

https://github.com/bastibl/gr-keyfob

BlueFlower

- Outil pour chercher des secrets dans des fichiers

  https://github.com/veorq/blueflower

Portes dérobées Active Directory dans les DACL

- Présenté par wald0,harmj0y, …, créateurs d'Empire, Empyre et Bloodhound
- Vue d'ensemble de techniques de portes dérobées Active Directory se basant sur les DACL
- Exemple : On définit un utilisateur comme étant son propre propriétaire, on supprime les droit de lister le contenu sur l'OU qui le contient
- Résultat : Même un administrateur du domaine ne peut pas voir l'utilisateur via des requêtes LDAP ou dans l'interface graphique !

https://www.blackhat.com/docs/us-17/wednesday/us-17-Robbins-An-ACE-Up-The-Sleeve-Designing-Active-Directory-DACL-Backdoors.pdf

Recherche de compromission via les données de réplication

https://posts.specterops.io/hunting-with-active-directory-replication-metadata-1dab2f681b19

Koadic C3

- Post-exploitation reposant sur DCOM
- Support de toutes les versions de Windows depuis 2000
- Cependant de nombreuses limitations dues à l'utilisation de VBS

https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-zerosum0x0-alephnaught-Koadic-C3.pdf

Recherche d'agents Empire persistants

- Script pour chercher sur un système Windows les méthodes de persistance Windows employée par Empire (par défaut)

  https://github.com/n00py/NorkNork

Business et Politique

Droit / Politique

France

Les boites mails professionnelles ne peuvent être surveillées sans prévenir l'employé

- Jurisprudence de la Cour européenne des droits de l'homme
- Suite au licenciement d'un employé roumain ayant utilisé sa boîte pro en perso

  http://www.lemonde.fr/pixels/article/2017/09/05/les-communications-d-entreprise-ne-peuvent-etre-surveillees-que-si-le-salarie-est-prevenu_5181151_4408996.html

Droit / Politique

International

La commission éthique de l'Allemagne publie un rapport sur les véhicules connectés et automatiques

- En anglais

"the systems must be programmed to accept damage to animals or property in a conflict if this means that personal injury can be prevented."

"any distinction based on personal features (age, gender, physical or mental constitution) is strictly prohibited"

https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile

Lire les conditions générales… ou nettoyer les toilettes

- Conditions générales d'accès à un Wifi ouvert, que 22 000 ont accepté
- Avec une clause originale :
  - Nettoyer des cabines de toilettes mobiles
  - Faire des câlins à des chats errants
  - Peindre des coquilles d'escargots

http://mashable.france24.com/mashallow/20170713-nettoyer-toilette-conditions-generales-wifi

Droit / Politique

International

Arrestation de MalwareTech (Marcus Hutchins) au retour de la BlackHat

- Chercheur connu pour avoir déposé le 1er nom de domaine bloquant WannaCry
- Accusé d'être l'auteur et vendeur du malware Kronos
  - Division de la communauté sur le sujet
- Enquête de Brian KREBS sur des données publiques

  https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/
- L'émission NoLimitSecu sur le sujet

  https://www.nolimitsecu.fr/malwaretech/

Droit / Politique
International

Manifestation du 20 janvier, la justice américaine veut TOUTES les logs de DisruptJ20.org

- Log web, FTP, SSH, informations sur les administrateurs du site...
- Opposition ferme des intéressés, soutenus par l'EFF

  https://www.dreamhost.com/blog/we-fight-for-the-users/

La Chine (janv-17) et la Russie (nov-2017) interdisent les VPN et les Proxy

https://www.undernews.fr/anonymat-cryptographie/la-chine-et-la-russie-interdisent-les-vpn.html

- Apple supprime des applications VPN de ses stores locaux

  https://techcrunch.com/2017/07/30/apple-issues-statement-regarding-removal-of-unlicensed-vpn-apps-in-china/
- Est-ce contraire aux droits de l'homme ?
  - tl;dr : oui

  http://www.thierryvallatavocat.com/2017/08/les-lois-anti-vpn-sont-elles-contraires-aux-droits-de-l-homme.html
- Si c'est appliqué aux entreprises, cela va être problématique
  - Mais quelle est la différence entre HTTPS et un VPN SSL/TLS ? 😉

Business
International

Lenovo et les adware pré-installés

- Qui injectent des publicités dans les pages web consultées par les utilisateurs
  - Accord entre Lenovo et la FTC
- 3,5 millions de dollars d'amende

http://www.zdnet.com/article/lenovo-receives-3-5m-fine-for-pre-installing-adware-that-hijacks-https-connections/

Samsung, lancement d'un BugBounty

- Primes allant de $200 à $200 000

https://security.samsungmobile.com/rewardsProgram.smsb

Maersk annonce $200m à 300m de perte à cause de NotPetya

- Au même moment du rachat par Total pour $7,45 milliards

http://investor.maersk.com/releasedetail.cfm?ReleaseID=1037421

Google vs Symantec, suite et fin ?

- Google voulait faire le ménage des les vieilles AC
- Echanges houleux entre Google et Symantec

  https://groups.google.com/a/chromium.org/forum/m/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ
- Finalement Google accorde un délais avant de ne plus supporter ces AC
- Symantec vend sa branche certificats à DigiCert
  - elle-même rachetée par le fond d'investissement Thoma Bravo LLC

  https://www.digicert.com/news/2015-08-26-thoma-bravo-majority-stake-in-digicert/
- Débat similaire chez Mozilla

  https://wiki.mozilla.org/CA:Symantec_Issues

Conférences

Conférences

Passées

- BSides Las Vegas + BlackHat + DEFCON - 26 au 30 juillet 2017 à Las Vegas

A venir

- BruCon - 5 and 6 October 2017 à Gent
- Hack.lu - 17-19 October 2017 à Luxembourg
- Botconf - 6 au 8 décembre 2017 à Montpellier

Divers / Trolls velus

Divers / Trolls velus

Pancarte réelle ou fausse ?

- Dans tous les cas, c'est très drôle

  https://twitter.com/dalmoz_/status/889530871870390272

Due to the DEFCON Hacking convention, we will be accepting email print jobs with attachments only. We will not accept USB prints or any links.

We apologize for the inconvenience.

Divers / Trolls velus

Aspirateur iRobot Roomba

- Revue du 13/12/2016 : envoie les plans de la maison sur AWS
- A présent, iRobot prévoir de vendre ces plans

  https://www.lesechos.fr/amp/98/2104198.php

Intel Management Engine, enfin désassemblé

- Des chercheurs ont reconstruit les tables Huffman

  https://github.com/ptresearch/unME11
- Basé sur Minix

  http://blog.ptsecurity.com/2017/08/disabling-intel-me.html
- Fonctionnalité HAP : High Assurance Platform, liée à la NSA
  - Possibilité de désactiver “partiellement” Intel Management Engine

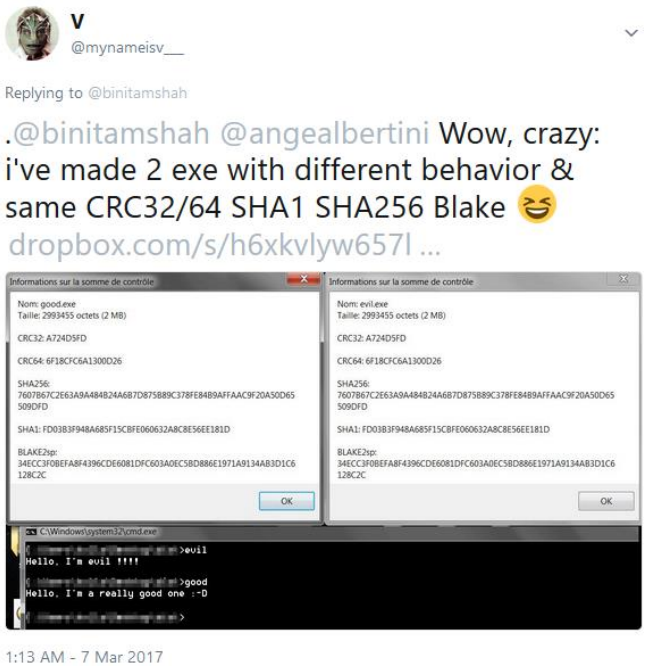
Divers / Trolls velus

2 exécutables avec même MD5 et SHA1 mais comportement différents

- Quand l'idée de ton tweet rigolo est reprise pour un challenge et un article complet
- Le tweet :

  https://twitter.com/mynameisv___/status/839041392823394304
- L'article

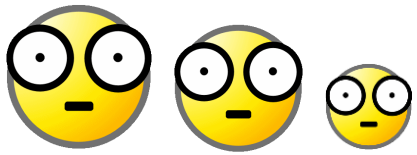
  https://hackernoon.com/a-collision-too-perfect-279a47fb5d42



Les mails publiés par WikiLeaks révèlent (révèleraient) que…

- Sony, Obama, Seth Rogen et la CIA ont secrètement planifié un changement du régime de la Corée du Nord

  http://archive.is/3GhRc

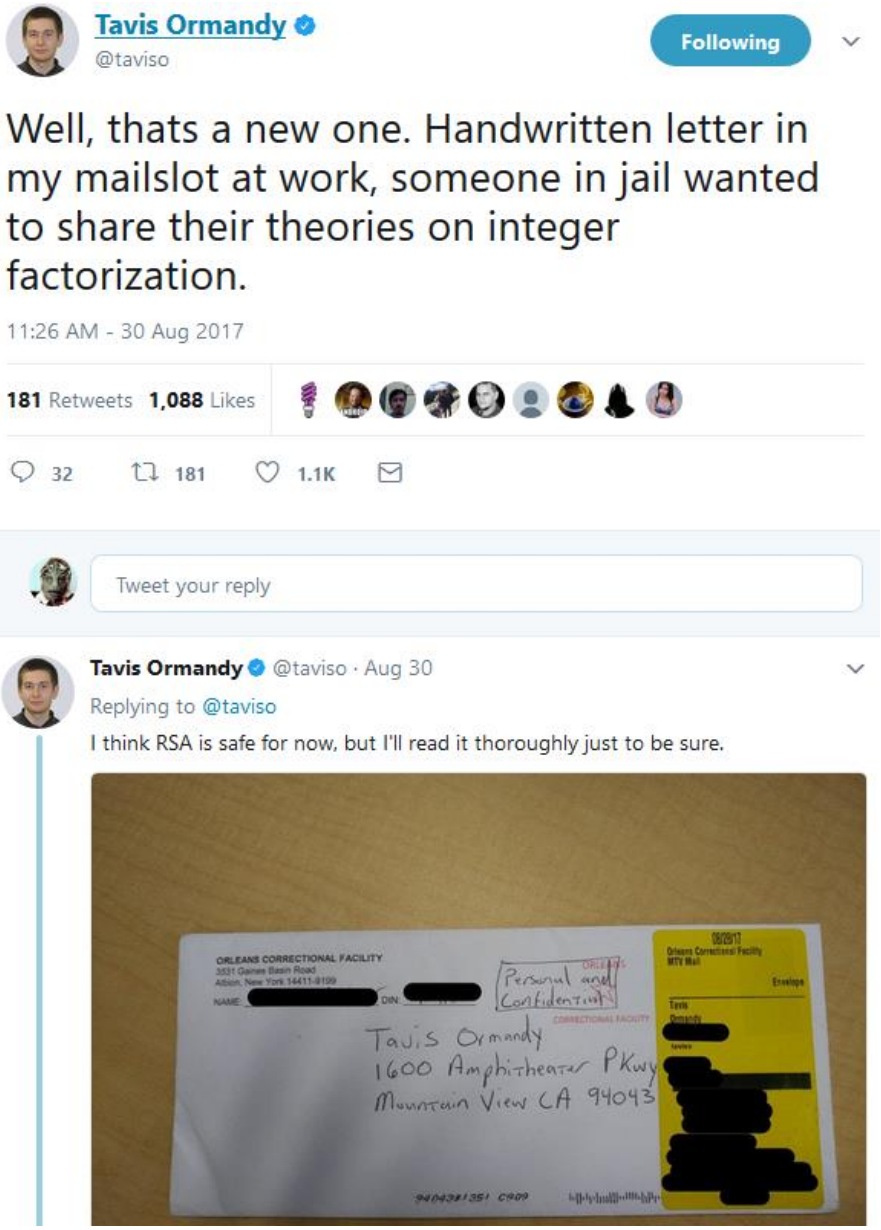


Divers / Trolls velus

RSA est cassé, enfin… d'après un taulard

- Courrier reçu par Tavis O.

  https://twitter.com/taviso/status/902960795977318400?refsrc=email&s=11



Divers / Trolls velus

Have I been pwned? Ne choisissez pas un de ces 306 millions de mots de passe

- Vérification **en ligne**… mais qui ira y tester son mot de passe !!?
- Vérification **hors ligne** avec la publication de 306 millions de mots de passe ✌🏽

  https://haveibeenpwned.com/Passwords

Have I been pwned? > MAX_INT32

- 4,729,225,727 mots de passe > 2^32 = 4,294,967,295

Une base de 711 millions de comptes

- benkow_ trouve par hasard une base publiquement accessible sur un C&C

  https://www.troyhunt.com/inside-the-massive-711-million-record-onliner-spambot-dump/

Les rançongiciels ont fait plus pour la sécurité que les 10 dernières conférences RSA

- TheGrugq : <<ransomware (authors and criminals) are doing more to advance the state of cyber security readiness than the last 10 RSA conferences.>>

  https://twitter.com/thegrugq/status/738234940437856257

Divers / Trolls velus

Un auteur de malware utilise le même identifiant Skype

- Pour son Botnet et… pour chercher du travail

https://www.bleepingcomputer.com/news/security/malware-author-uses-same-skype-id-to-run-iot-botnet-and-apply-for-jobs/

Thread Rating: New Reply

Scanning Help (CNC) - live: [redacted]pro69 Thread Options

06-30-2017, 10:25 PM Post: #1

DaddyPvP
Peasant

Prestige: 0
Posts: 9
Joined: Jun 2017
Reputation: -3

I need help scanning to a qBot botnet :P

HMU on skype - live: [redacted]pro69

PM Find TS Quote Q+ Report

My name is [redacted]nd i am interested in this. I am very experienced at getting servers started and managing them. I may not me as experienced as the people listed above, but I can code PHP and make a website. I also have tons of premium plugins that i would be happy to donate to the server. If i was chosen for this task I would go for a more normal/semi-op factions server. I prefer factions becau it gets a good player base for servers who are just starting out. If you would like to contact me for more information you can reach me a one of the following:

Skype: live:[redacted]pro69

Email: [redacted]pro69@gmail.com

Skype: live:[redacted]pro69

Email: [redacted]pro69@gmail.com

or just pm me on here!

I'm online for 15-18 hours each day. Meaning I will be able to spend most of my time working on this server. I'm currently out of school f 2~3 weeks. I believe I would be able to get the server up and running by the time school is back in session.

Prochains rendez-vous de l’OSSIR

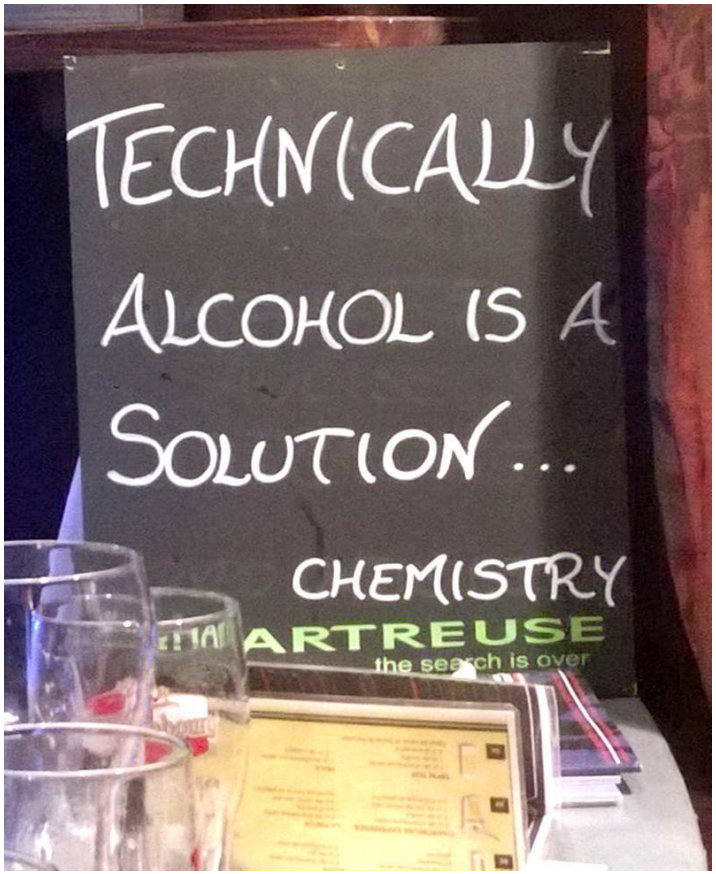
Prochaines réunions

Prochaine réunion

- Mardi 10 octobre 2017
  (Juste avant les assises)

After Work

- Mardi 19 septembre 2017
- Au bar “la Kolok”



Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous