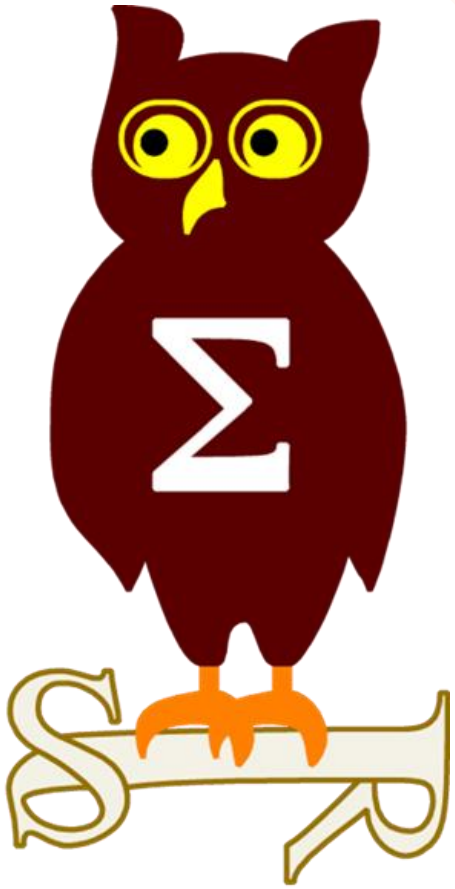
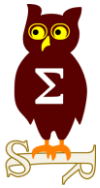


Revue d'actualité

11/07/2017

Préparée par

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



Failles / Bulletins / Advisories

Bulletin MSyy**-**000

Pas de bulletin ce mois-ci
(manque de temps…)

Mais nous espérons une bonne surprise pour septembre avec
MMBGA / **M**ake **M**S **B**ulletin **G**reat **A**gain

Failles / Bulletins / Advisories

Système (principales failles)

Systemd, double combo

- Un utilisateur dont le nom début par un chiffre... est root
  - C'est facile de critiquer, mais si vous ne suivez pas les instructions...

```
<<Usernames must start with a lower case letter or an underscore, followed by lower case
  letters, digits, underscores, or dashes...>>
```

https://github.com/systemd/systemd/issues/6237

  - Corrections des outils de création d'utilisateur

https://gist.github.com/bloerwald/a482791395114fa82636e2ab207cdb11

- Exécution de code à distance à partir d'une simple réponse DNS CVE-2017-9445

http://thehackernews.com/2017/06/linux-buffer-overflow-code.html

Libgcrypt, récupération des clefs RSA 1024bits

- Canal auxiliaire local, fonctionne entre processus, entre dockers, entre machines virtuelles
  - "serait" fonctionnel sur les clefs 2048bits

https://eprint.iacr.org/2017/627.pdf

https://www.debian.org/security/2017/dsa-3901

Failles / Bulletins / Advisories

Système (principales failles)

Antivirus BitDefender, exécution de code à la lecture d'un fichier RAR

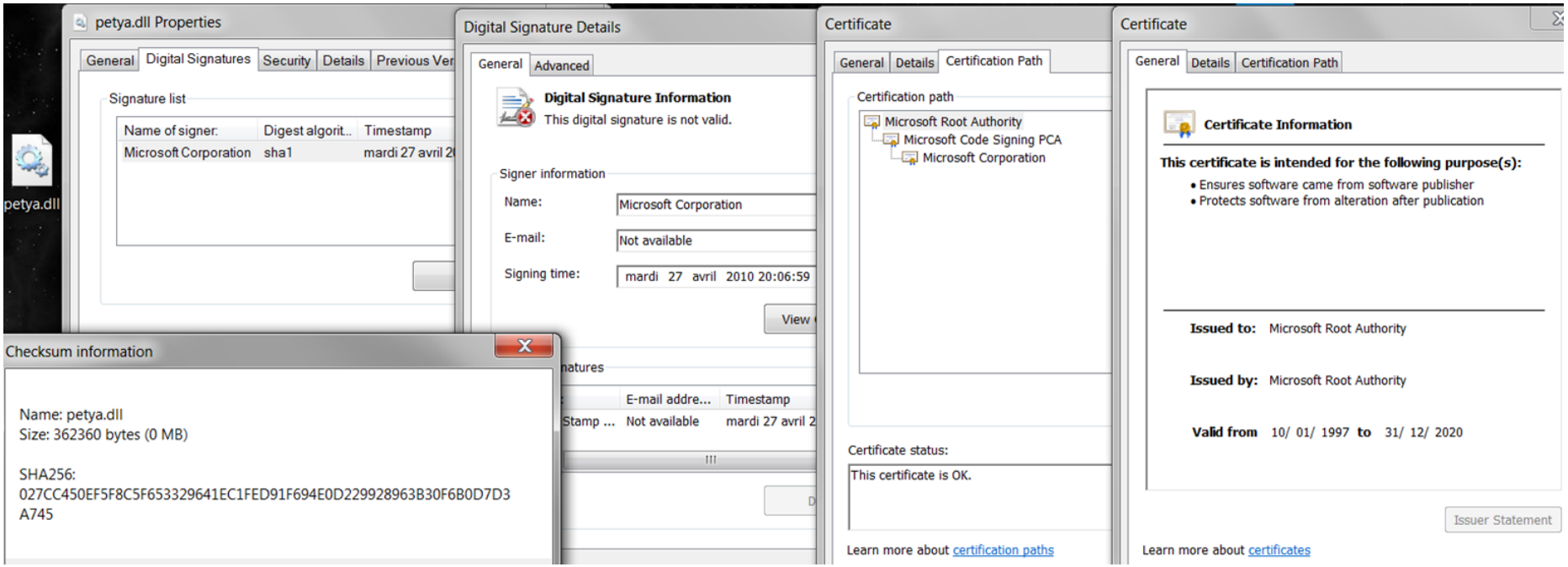
- Depuis 2013…

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1278&desc=6

Contourner TrendMicro, Webroot, Malwarebytes, Arcabit, Zonealarm, Kaspersky

- Simplement en générant une fausse signature Microsoft

  https://github.com/HackerFantastic/Public/blob/master/tools/bypassavp.sh



Failles / Bulletins / Advisories

Système (principales failles)

Elévation de privilèges dans Ocaml (CVE-2017-9772)

- Élévation à partir du binaire setuid

  http://www.openwall.com/lists/oss-security/2017/06/23/6

Xen, écriture dans la mémoire de l'hyperviseur

https://bugs.chromium.org/p/project-zero/issues/detail?id=1231

- Et beaucoup d'autres vulnérabilités

  http://xenbits.xen.org/xsa/

VirtualBox, évasion de la machine virtuelle

- Depuis un processus en Ring3

  https://bugs.chromium.org/p/project-zero/issues/detail?id=1227

VMWare, tous les détails de l'évasion de la machine virtuelle présentée à Pwn2Own

http://acez.re/the-weak-bug-exploiting-a-heap-overflow-in-vmware/

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco exécution de code à distance sur SNMP

http://securityaffairs.co/wordpress/60570/hacking/cisco-ios-software-flaws.html

Cisco, clef privée de drmlocal.cisco.com dans un exécutable

https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/T6emeoE-lCU

Cisco ASA, exécution de code à distance sur IKE

- Code d'exploitation de la vulnérabilité de 2016

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/june/a-warcon-2017-presentation-cisco-asa-exploiting-the-ikev1-heap-overflow-cve-2016-1287/

Juniper JunOs, déni de service avec un packet IPv6

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10749&cat=SIRT_1&actp=LIST

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Ransomware, everywhere

- MySQL

  https://www.bleepingcomputer.com/news/security/database-ransom-attacks-have-now-hit-mysql-servers/

- UEFI

  https://twitter.com/ericevenchick/status/847642569924202496/photo/1

Augmentation de la fraude au piratage des cartes bancaires sans contact (NFC)

- £2.8m en 2015 et £7m en 2016
- Principalement du fait de pertes des cartes et non blocage par les banques

  http://www.bbc.com/news/uk-england-devon-39942246

Vault7, outil de la CIA pour voler les identifiants et mots de passe SSH

- Ciblant Windows et Linux

  https://www.nextinpact.com/news/104742-vault-7-wikileaks-devoile-deux-techniques-cia-pour-derober-identifiants-ssh.htm

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Exploitation dans la nature de la vulnérabilité Samba (CVE-2017-7494)

- Exécution de code “en cas de possibilité d’écrire sur le partage

  https://www.undernews.fr/reseau-securite/sambacry-la-vulnerabilite-samba-sous-linux-activement-exploitee.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Un document confidentiel de la NSA concernant le piratage des élections américaines

- Les services de renseignement militaires Russes “seraient” impliqués
- A base de phishing ciblant les employés des logiciels de vote électronique

https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

Microsoft, fuite du code source de Windows 10 ?

- 32To partagé sur le site BetaArchive
- Ancienne ISO, Kit de dev ARM, pilotes WiFi, USB, Bluetooth...

https://arstechnica.com/information-technology/2017/06/32tb-of-windows-10-beta-builds-driver-source-code-leaked/

- Liste des fichiers

https://pastebin.com/VGEbWVSM

Fuite des données de 198 millions de citoyens américains

- Base servant aux analyses des électeurs du parti républicain
- Données stockées chez Amazon librement accessibles

http://www.numerama.com/politique/268580-les-etats-unis-subissent-la-plus-grosse-fuite-de-donnees-delecteurs-de-lhistoire.html

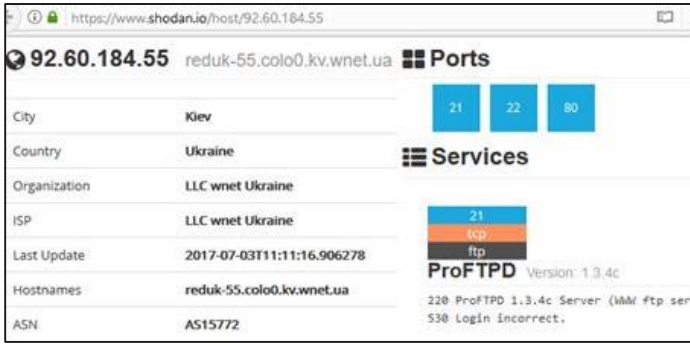
Piratages, Malwares, spam, fraudes et DDoS

Malwares

Ver Petya/NotPetya 1/4

- Inspiré de WannaCry
- Compromission du serveur de mise à jour d'un éditeur tiers

  https://www.shodan.io/host/92.60.184.55

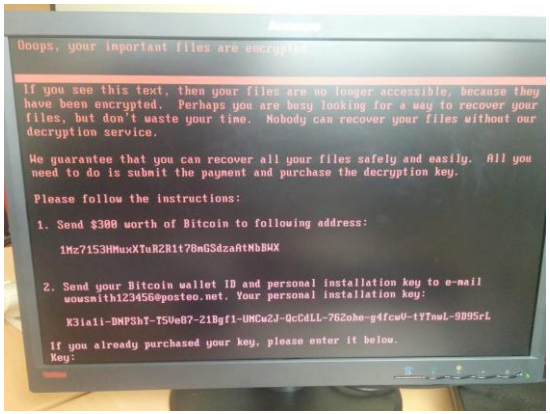


- Récupération d'identifiants en mémoire
  - Avec du code de Mimikatz

  https://twitter.com/gentilkiwi/status/879865891558752257/photo/1

- Propagation par WMI, PsExec et EternalBlue
- ~~Chiffrement~~ Destruction des disques

  http://thehackernews.com/2017/06/petya-ransomware-wiper-malware.html



- Course au buzz et beaucoup d'articles bourrés de n'importe quoi

  http://www.slate.fr/story/147876/cyberattaque-mondiale

- Il "semblerait" qu'il soit possible de déchiffrer

  http://blog.ptsecurity.com/2017/07/recovering-data-from-disk-encrypted-by.html

- De peur d'être mêlé à une cyberguerre, l'auteur de Petya publie ses clefs

  https://blog.malwarebytes.com/cybercrime/2017/07/the-key-to-the-old-petya-has-been-published-by-the-malware-author/

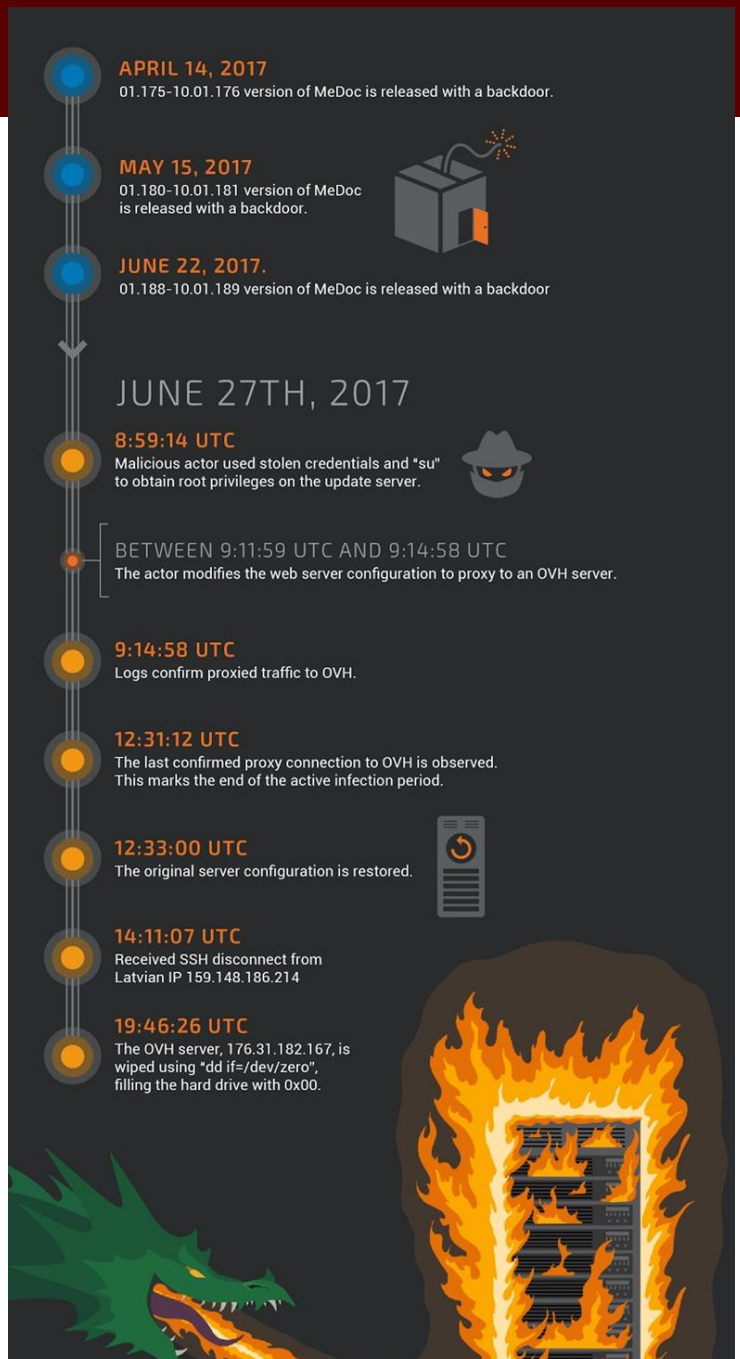
Piratages, Malwares, spam, fraudes et DDoS

Malwares

Ver Petya/NotPetya 2/4

- Un article et une timeline sur le sujet

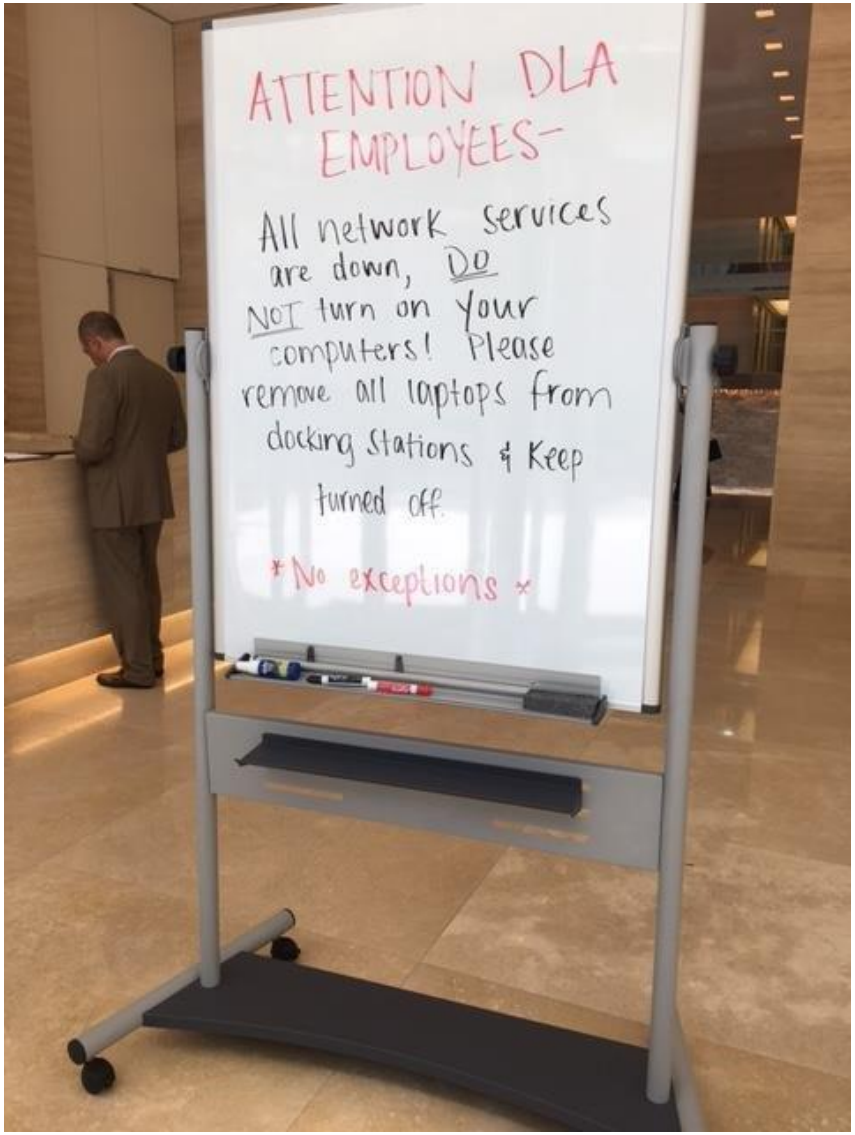
  http://blog.talosintelligence.com/2017/07/the-medoc-connection.html



Piratages, Malwares, spam, fraudes et DDoS

Malwares

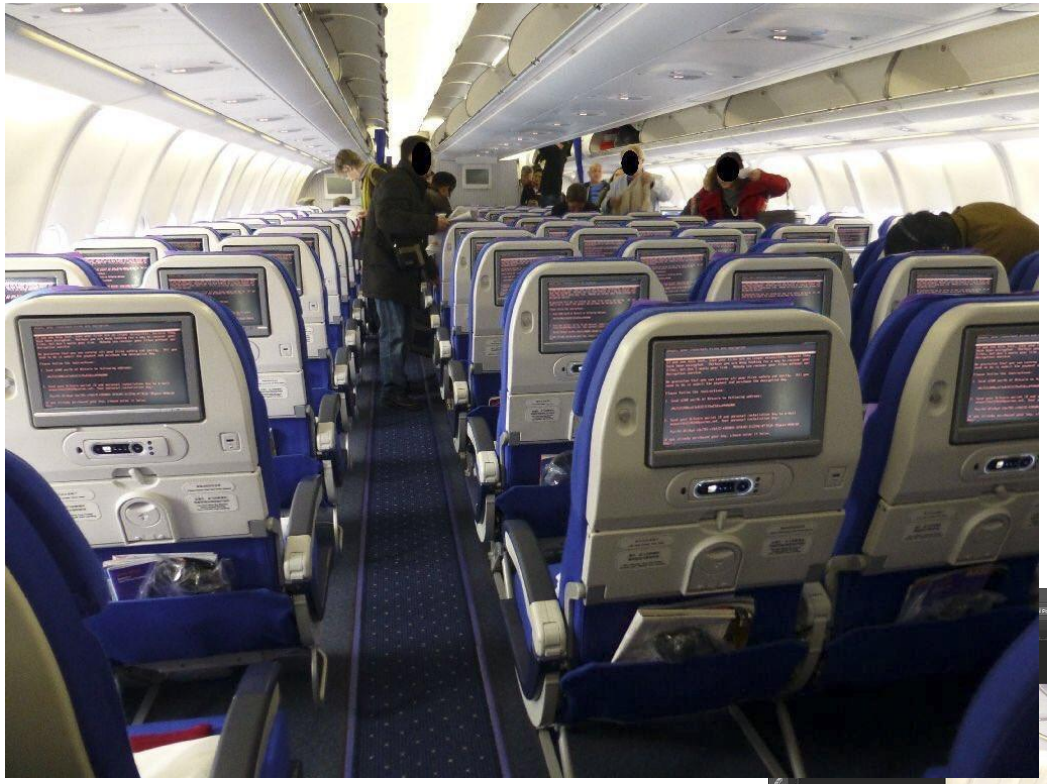
Ver Petya/NotPetya 3/4

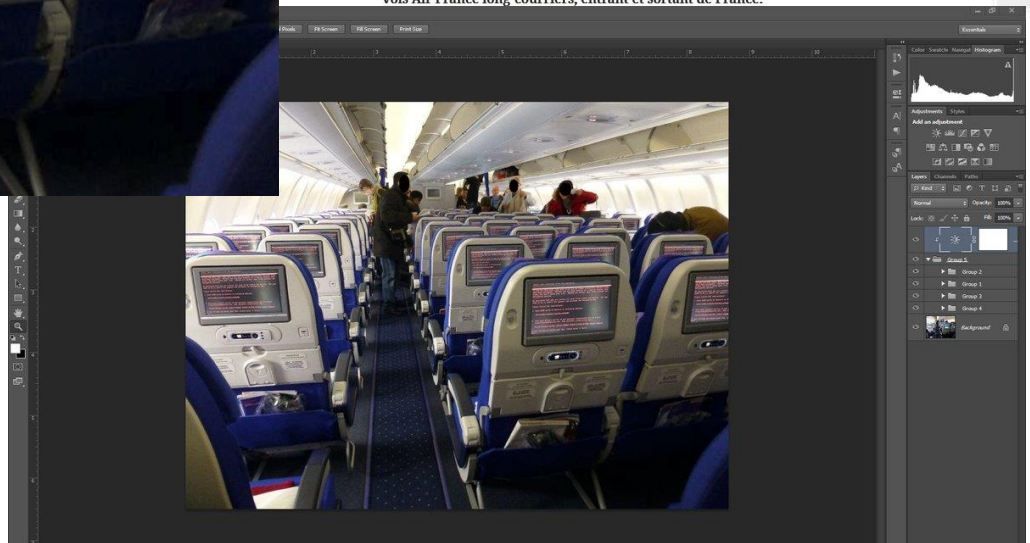


Piratages, Malwares, spam, fraudes et DDoS

Malwares

Ver Petya/NotPetya 4/4





Piratages, Malwares, spam, fraudes et DDoS

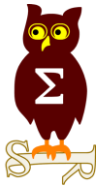
Panne

OVH, panne pour 50 000 sites

- Fuite d'un liquide de refroidissement sur des baies de disques
- + nouveau système d'alarme qui a mal fonctionné
- + baies en fin de vie
- + mise à jour des bases MySQL en 5.5a récemment
- = restauration et pannes multiples

https://www.nextinpact.com/news/104700-mutualise-dovh-importante-panne-communication-floue-clients-dans-expectative.htm

http://www.silicon.fr/baie-emc-noyee-ovh-pris-eau-179983.html



Nouveautés, outils et techniques

La révocation des certificats, c'est compliqué !

- CRL trop grosses (ce qui posent des problèmes sur certains équipements)
- OCSP n'est pas proposé par tous le monde

https://arstechnica.com/security/2017/07/https-certificate-revocation-is-broken-and-its-time-for-some-new-tools/

Tiens, la courbe de l'ANSSI n'est plus considérée comme sûre

http://safecurves.cr.yp.to/

		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False	False	False
M-221	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
E-222	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
NIST P-224	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False	False
Curve1174	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
Curve25519	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
BN(2,254)	False	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False	False	False
brainpoolP256t1	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False
ANSSI FRP256v1	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	False	False	False
NIST P-256	False	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	False	False	True ✓	False	False
secp256k1	False	True ✓	True ✓	True ✓	True ✓	True ✓	False	True ✓	False	True ✓	False	False
E-382	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
M-383	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓
Curve383187	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓	True ✓

EMET is Back ! (dans Windows 10)

- Et va être renommé "Windows Exploit Guard

  http://www.silicon.fr/windows-10-va-renforcer-sa-securite-avec-emet-179099.html

OpenBSD met en place KARL (Kernel Virtual Address Space)

- Sorte de ASL pour le noyau
- Complexifie les exécutions de code combinées avec une fuite d'information mémoire
- ROP beaucoup plus compliqué à réaliser

https://www.bleepingcomputer.com/news/security/openbsd-will-get-unique-kernels-on-each-reboot-do-you-hear-that-linux-windows/

Business et Politique

Droit / Politique
International

T411 arrêté 😭

- Un préjudice d'1 milliards d'euros... ce qui ne fait pas très sérieux
  - C'est ce que dirait un enfant de 4 ans quand sa sœur lui demande de rendre sa Barbie

https://www.nextinpact.com/news/104672-t411-quatre-personnes-arretees-en-france-lalpa-evoque-milliard-deuros-prejudice.htm

Les Five Eyes contre le chiffrement

- Influence directement au niveau des éditeurs, constructeurs et FAI
- L'excuse ? Contre l'extrémisme violent

http://www.lemondeinformatique.fr/actualites/lire-5-pays-anglo-saxons-veulent-casser-sur-le-chiffrement-internet-68713.html

Google arrête de lire vos mails

- Mais continue le tracking des internautes

https://www.generation-nt.com/goolge-arrete-lecture-emails-ciblage-publicitaire-actualite-1943851.html

Les banques européennes vont devoir déclarer les incidents significatifs

- Qu'est ce qu'un incident significatif ?

http://www.lemagit.fr/actualites/450421113/Les-banques-europeennes-devront-signaler-les-incidents-significatifs

Business
International

En Russie il faut:

- Héberger les données localement : ok
- Fournir son code au FSB : Telegram refuse !

  https://www.nextinpact.com/news/104665-en-russie-telegram-et-dautres-societes-sommees-devoiler-leur-code-source-par-securite.htm

Conférences

Conférences

Passées

- Nuit du Hack - 24-25 juin à Paris (Eurodisney)
- SSTIC - 7 au 9 juin à Rennes
- BeeRump - 22 juin à Paris (Epita)
- Hack in Paris - 19 au 23 juin

A venir

- BlackHat USA - 22 au 26 juillet
- Defcon - 27 au 30 juillet

Divers / Trolls velus

Divers / Trolls velus

Hack In Paris, doxing BNPP

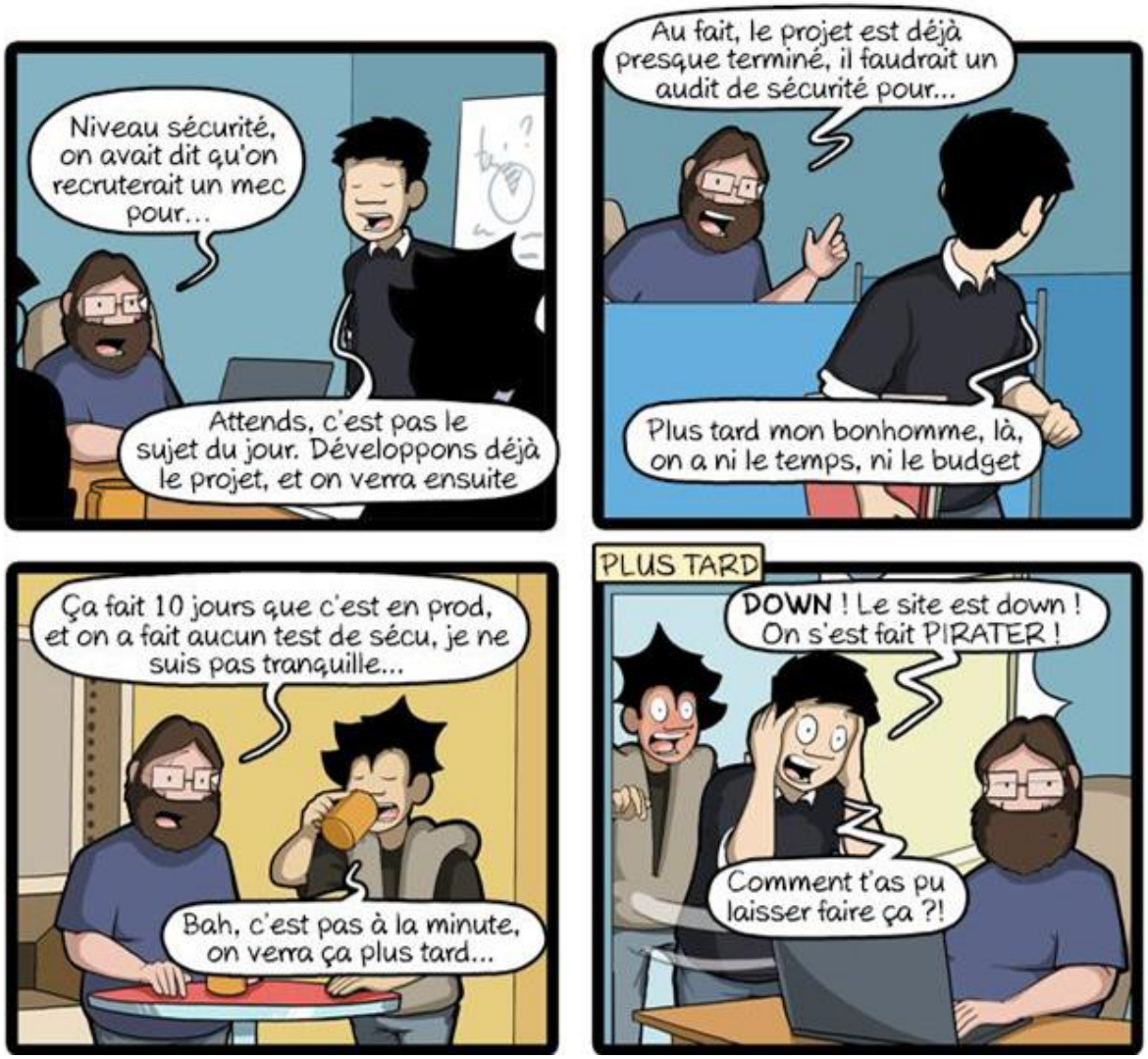
- Recherche d’information sur les gens de la sécurité chez BNPP
- Affichage non flouté/censuré des visages des personnes

  https://twitter.com/Creased_/status/877798313105530881/photo/1

Divers / Trolls velus

La sécurité…

http://www.commitstrip.com/fr/2017/06/19/security-too-expensive-try-a-hack/



Divers / Trolls velus

Atos, le SOC prescriptif

- `<<permet aux clients de` **`prédire`** `les cybermenaces avant même qu'elles ne se produisent>>`

  https://atos.net/fr/2017/communiques-de-presse/communiques-generaux_2017_07_04/atos-lance-le-premier-security-operations-center-soc-prescriptif-au-monde-avec-reponse-automatisee

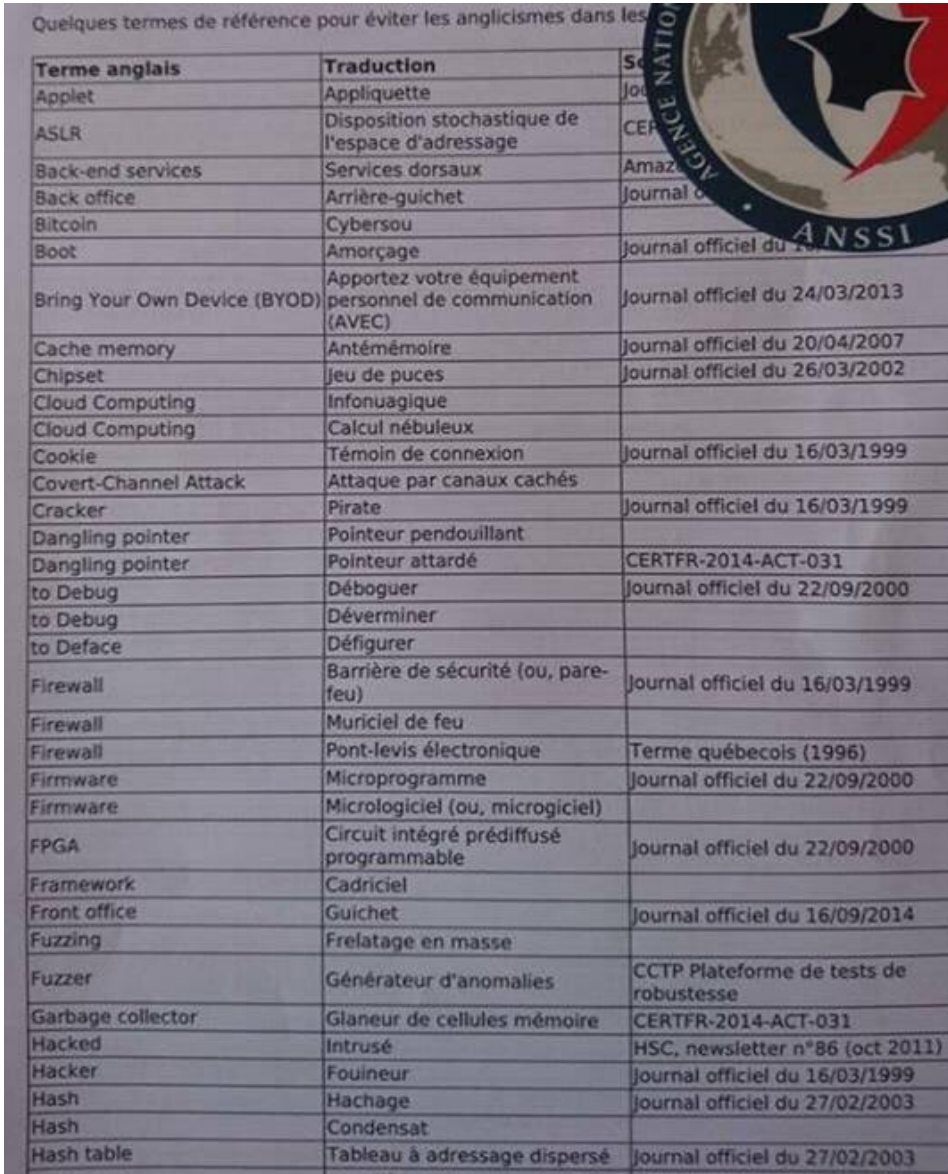
- Pendant ce temps-là, dans la vraie vie
  - **Atos** oublie de renouveler le nom de domaine 3D Secure -> panne des paiements

  http://www.zdnet.fr/blogs/infra-net/panne-du-systeme-de-paiement-3d-secure-a-cause-du-nom-de-domaine-39853696.htm

Divers / Trolls velus

Termes francisés de l'ANSSI, blague ou réalité ?

- Si c'est vrai, il faut tout mettre sur Bitoduc
  https://twitter.com/TaciteFood/status/881239750463586304



Quelques termes de référence pour éviter les anglicismes dans les

Terme anglais	Traduction	Sc
Applet	Appliquette	Jo
ASLR	Disposition stochastique de l'espace d'adressage	CE
Back-end services	Services dorsaux	Amaz
Back office	Arrière-guichet	Journal
Bitcoin	Cybersou	
Boot	Amorçage	Journal officiel du
Bring Your Own Device (BYOD)	Apportez votre équipement personnel de communication (AVEC)	Journal officiel du 24/03/2013
Cache memory	Antémémoire	Journal officiel du 20/04/2007
Chipset	Jeu de puces	Journal officiel du 26/03/2002
Cloud Computing	Infonuagique	
Cloud Computing	Calcul nébuleux	
Cookie	Témoin de connexion	Journal officiel du 16/03/1999
Covert-Channel Attack	Attaque par canaux cachés	
Cracker	Pirate	Journal officiel du 16/03/1999
Dangling pointer	Pointeur pendouillant	
Dangling pointer	Pointeur attardé	CERTFR-2014-ACT-031
to Debug	Déboguer	Journal officiel du 22/09/2000
to Debug	Déverminer	
to Deface	Défigurer	
Firewall	Barrière de sécurité (ou, pare-feu)	Journal officiel du 16/03/1999
Firewall	Muriciel de feu	
Firewall	Pont-levis électronique	Terme québecois (1996)
Firmware	Microprogramme	Journal officiel du 22/09/2000
Firmware	Micrologiciel (ou, microgiciel)	
FPGA	Circuit intégré prédiffusé programmable	Journal officiel du 22/09/2000
Framework	Cadriciel	
Front office	Guichet	Journal officiel du 16/09/2014
Fuzzing	Frelatage en masse	
Fuzzer	Générateur d'anomalies	CCTP Plateforme de tests de robustesse
Garbage collector	Glaneur de cellules mémoire	CERTFR-2014-ACT-031
Hacked	Intrusé	HSC, newsletter n°86 (oct 2011)
Hacker	Fouineur	Journal officiel du 16/03/1999
Hash	Hachage	Journal officiel du 27/02/2003
Hash	Condensat	
Hash table	Tableau à adressage dispersé	Journal officiel du 27/02/2003

Divers / Trolls velus

Une idée qui devrait devenir une loi, une obligation !

<<If you hack someone with IT certs you should automatically absorb their credentials & acronyms.>>

https://twitter.com/FuxNet/status/877663218482786304

Linux vs GRSecurity / Torvald vs Spengler

- T:<<Quite frankly, I'd much rather see *you* actually send in patches that are acceptable for inclusion, something you've never done.>>
- T:<<Wouldn't it be nice if you actually tried to make the baseline actually better?>>
- B:<<Are you delusional? Sorry, you don't get to weasel your way out of calling us clowns, that our code is garbage…>>

http://www.openwall.com/lists/oss-security/2017/06/24/2

La NSA est sur GitHub

https://nationalsecurityagency.github.io/

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 12 septembre 2017

After Work

- Fin septembre

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

Bonnes vacances