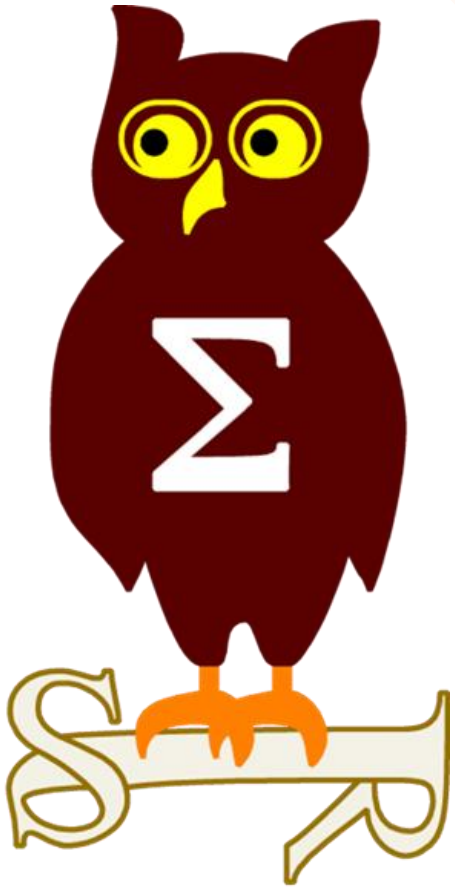
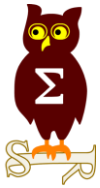


Revue d'actualité

10/05/2017

Préparée par

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



Failles / Bulletins / Advisories

Bulletin MSyy**-**000

A présent : autant de bulletins que de CVE !!!

Failles / Bulletins / Advisories

Microsoft - Avis

Office, exécution de code à l'ouverture d'un fichier RTF / CVE-2017-0199

- Exploité dans la nature
- Télécharge un fichier HTA
- L'exploitation en 140 caractères :

```
{\rt\object\objocx{\objdata
 01050000020000001600000004f6e654e6f74654d6f62696c652e53706e53796e6300000000000000000000010000004
 10105000000000000}}
```

https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

- Créer son propre fichier RTF

https://github.com/tfairane/cve-2017-0199

CVE-2017-0290

- Vulnérabilité dans MsMpEng, un composant de Miscrosoft Defender
- Mini-filter sur les accès au disque, donc toute activité est susceptible de déclencher ce composant
- Composant NScript pour analyser le JavaScript. Tourne en NT\Autorité système sans Sandbox
- Confusion de type permettant de faire crasher le composant (PoC) voir l'exécution de code
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5

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

Nouvelle solution anti-exploit pour le navigateur Microsoft Edge

- Ferme de VM chez Microsoft pour les URL “louches” ou non “white-listées”
  http://www.computerworld.com/article/3194666/microsoft-windows/microsoft-asks-windows-10-enterprise-customers-to-test-new-anti-exploit-tech.html

Compromettre un DC depuis DNSAdmin

- Compromettre un DC sans compte admin du domaine
- Injecter une DLL depuis le compte « DNSAdmin »
  https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83

Failles / Bulletins / Advisories

Système (principales failles)

Intel Management Engine (composant Active Management Technology / AMT)

- Management Engine = composants+logiciels contrôlant le CPU et la RAM
- AMT = gestion à distance dans besoin de l'OS
- Port en écoute à partir d'AMT (l'OS ne le sait pas)
- Prise de contrôle à distance (challenge à vide) CVE-2017-5689, présent depuis 2008
  https://www.tenable.com/blog/rediscovering-the-intel-amt-vulnerability
  https://communities.intel.com/docs/DOC-5693
  https://downloadcenter.intel.com/download/26754

Exploitation dans la nature d'une vulnérabilité sur GhostScript

- Dans la nature
  https://twitter.com/tqbf/status/856652492691488768
- Il semblerait que la vulnérabilité soit la 697748 citée ici et non encore corrigée
  https://bugs.ghostscript.com/buglist.cgi?quicksearch=security%20problem

Failles / Bulletins / Advisories

Système (principales failles)

Magento, exécution de code

- Une faille sur l'édition communautaire permet une exécution de code arbitraire
- Lors de l'ajout d'une vidéo Viméo sur un produit en vente, une image de prévisualisation est automatiquement récupérée et stockée sur le serveur. L'absence de vérification du type de fichier et de suppression en cas de mauvais format de fichier, c'est-à-dire lorsque le fichier n'est pas une image, permet l'upload de fichier arbitraire tel qu'une interpréteur de commande PHP et entraine ainsi la compromission de l'application.

http://www.defensecode.com/advisories/DC-2017-04-003_Magento_Arbitrary_File_Upload.pdf
http://www.veracode.com/blog/security-news/magento-zero-day-leaves-200000-online-retailers-vulnerable-attack

Vulnérabilités dans Netbackup 8

- Protocole propriétaire non-chiffré
- Exécution de code à distance
- Tourne évidemment en root

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

Failles / Bulletins / Advisories

Système (principales failles)

Fuite mémoire dans GCC

https://akrzemi1.wordpress.com/2017/04/27/a-serious-bug-in-gcc/

Buffer Overflow dans la librairie NSS / Network Security Services

- Lors du décodage Base64

  https://www.mozilla.org/en-US/security/advisories/mfsa2017-10/#CVE-2017-5461

Exécution de code dans NVIDIA GeForce Experience

- Pilotes et optimisation des jeux

  http://nvidia.custhelp.com/app/answers/detail/a_id/4459

Nvidia comme levier d'exécution de code

- Pour contourner AppLocker

```
echo require('child_process').exec("calc.exe") | "%ProgramFiles(x86)%\NVIDIA
 Corporation\NvNode\NVIDIA Web Helper.exe" -i
```

Failles / Bulletins / Advisories

Système (principales failles)

Vulnérabilité dans mbedTLS (ex Polar SSL)

- Exécution de code à la lecture d'un certificat X509

  http://blog.talosintelligence.com/2017/04/vulnerability-spotlight-arm-tls.html

Et dans WolfSSL

http://blog.talosintelligence.com/2017/05/wolfssl-x509-vuln.html

Failles / Bulletins / Advisories

Système (principales failles)

Qemu, évasion de la machine virtuelle

- Qube et Xen vulnérables
  http://www.phrack.org/papers/vm-escape-qemu-case-study.html

VirtualBox, communication entre plusieurs machine virtuelles

- A partir des répertoires partagés avec l'hôte (à base de ../../..)
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1037

Exécution de code à distance dans Linux kernel < 4.5 / CVE-2016-10229

- Si un port UDP est ouvert, un simple message MSG_PEEK suffit
- CVSSv3: **9.8 / 10**
- Systèmes vulnérables : OpenWRT, Debian, Android dont Nexus 5X, Nexus 6, Nexus 6P, Pixel, Pixel XL, Pixel C, Android One, Nexus Player ...
  https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=197c949e7798fbf28cfadc69d9ca0c2abbf93191

Android, des millions de smartphones vulnérables à cause d'app ouvrant "des ports"

- Ports en écoute peu ou pas sécurisés
  http://mashable.com/2017/04/28/smartphones-hack-android-open-ports-google-play/

Failles / Bulletins / Advisories

Réseau (principales failles)

Citrix NetScaler, dépassement de mémoire / CVE-2017-7219

- Exécution de code sans authentification avec la fonctionnalité de “ping” (sur https)
  https://blog.scrt.ch/2017/04/26/heap-overflow-vulnerability-in-citrix-netscaler-gateway-cve-2017-7219/
- Module Metasploit
  https://blog.scrt.ch/wp-content/uploads/2017/04/netscaler_heap_overflow.rb

Cisco ASA, Déni de service avec un simple paquet SSL/TLS / CVE-2017-6608

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-tls

Attaques sur le protocole de communication chiffré ZRTP

https://www.sufficientlysecure.org/2017/03/15/zrtp.html

Attaquer le SIEM

https://pentest.blog/unexpected-journey-3-visiting-another-siem-and-uncovering-pre-auth-privileged-remote-code-execution/
https://pentest.blog/unexpected-journey-4-escaping-from-restricted-shell-and-gaining-root-access-to-solarwinds-log-event-manager-siem-product/

Failles / Bulletins / Advisories

Réseau (principales failles)

StringBleed, contourner les communautés SNMP

- Affecte les modems Technicolo DPC3928SL
- Le PoC crée un github à chaque utilisation avec “i randomly run PoC exploits without checking them first”
  https://github.com/string-bleed/StringBleed-CVE-2017-5135
- Un autre PoC
  https://github.com/nixawk/labs/blob/master/CVE-2017-5135/StringBleed-CVE-2017-5135.py

Collecter des informations sur les utilisateurs Whatsapp

- Numéro de téléphone, statut et photo de profile peuvent être récupérés pour n’importe quel numéro de téléphone
- Utilisation d’une API non-documentée
  https://www.lorankloeze.nl/2017/05/07/collecting-huge-amounts-of-data-with-whatsapp/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

ShadowBrokers, publication de nouveaux outils de la NSA

- 6 000 fichiers, exploits, executables, codes en python…
- Framework proche de Metasploit nommé FuzzBunch
- Exploits « wormable » pour des vulnérabilités SMB **miraculeusement** corrigées en mars 
- Exploits pour RDP (pré-auth), Lotus Notes…
- Documents relatifs à des compromissions de Swift
- La liste des rebond pour exploiter des cibles

NAME	TYPE	TARGET	NOTES	SERVICE	AUTH	VERSIONS	NT	XP	VISTA	7	8	10	2000	2003	2008	2012
EARLYSHOVEL	EXPLOIT	REDHAT 7.0/7.1	SENDMAIL			8.11.x										
EASYBEE	EXPLOIT	MDAEMON	WEBADMIN	HTTP/HTTPS		9.5.2-10.1.2 (except 10.0.0)										
EASYPI	EXPLOIT	LOTUS MAIL	LOTUS MAIL	(TCP) 3264			y	y					y	y		
EBBISLAND/EBBSHAVE	EXPLOIT	SOLARIS 6-10	RPC XDR			6-10										
ECHOWRECKER	EXPLOIT	LINUX	SAMBA 3.0.x			3.0.x										
ECLIPSEDWING	EXPLOIT	SERVER SERVICE	MS08-067	(TCP 445) SMB/ (TCP 139) NBT			y	y					y	y		
EDUCATEDSCHOLAR	EXPLOIT	SMB	MS09-050	(TCP 445) SMB					y						y	
EMERALDTHREAD	EXPLOIT	SMB	MS10-061	(TCP 445) SMB/ (TCP 139) NBT	y?			y						y		
EMPHASISMINE	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP	y	6.5.4-6.5.5FP1, 7.0-8.5.2										
ENGLISHMANSDENTIST	EXPLOIT	OUTLOOK EXCHANGE WEBACCESS		(TCP 25) SMTP		< exchange 2010?										
EPICHERO	EXPLOIT	AVAYA CALL SERVER														
ERRATICGOPHER	EXPLOIT	SMBv1		(TCP 445) SMB				y						y		
ESKIMOROLL	EXPLOIT	KERBEROS SERVICE	MS14-068	(TCP 88) KERBEROS	y								y	y	y	
ESTEEMAUDIT	EXPLOIT	RDP		(TCP 3389) RDP				y						y		
ETERNALBLUE	EXPLOIT	SMBv2/NBT	MS17-010	(TCP 445) SMB				y	y	y	y	y	y	y	y	y
ETERNALCHAMPION	EXPLOIT	SMBv1/SMBv2?	MS17-010	(TCP 445) SMB												
ETERNALROMANCE	EXPLOIT	SMBv1	MS17-010	(TCP 445) SMB				y	y	y	y?	y?	y?	y	y	y?
ETERNALSYNERGY	EXPLOIT	SMBv3	MS17-010	(TCP 445) SMB							y					y
ETRE	EXPLOIT	IMAIL				8.10-8.22										
EWOKFRENZY	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP		6.5.4, 7.0.2										
EXPLODINGCAN	EXPLOIT	IIS5.0?/6.0 (WEBDAV)		(TCP 80) HTTP/HTTPS		5.0?,6.0								y		
FUZZBUNCH	TOOL		FRAMEWORK (PYTHON)													
ODDJOB	TOOL		IMPLANT BUILDER													
ZIPPYBEER	EXPLOIT	SMB	DCs	(TCP 445) SMB	y											

ShadowBrokers, publication de nouveaux outils de la NSA (suite)

- La NSA utilise(sait) TrueCrypt pour ses propres besoins
  https://twitter.com/musalbas/status/852860956396986370/photo/1

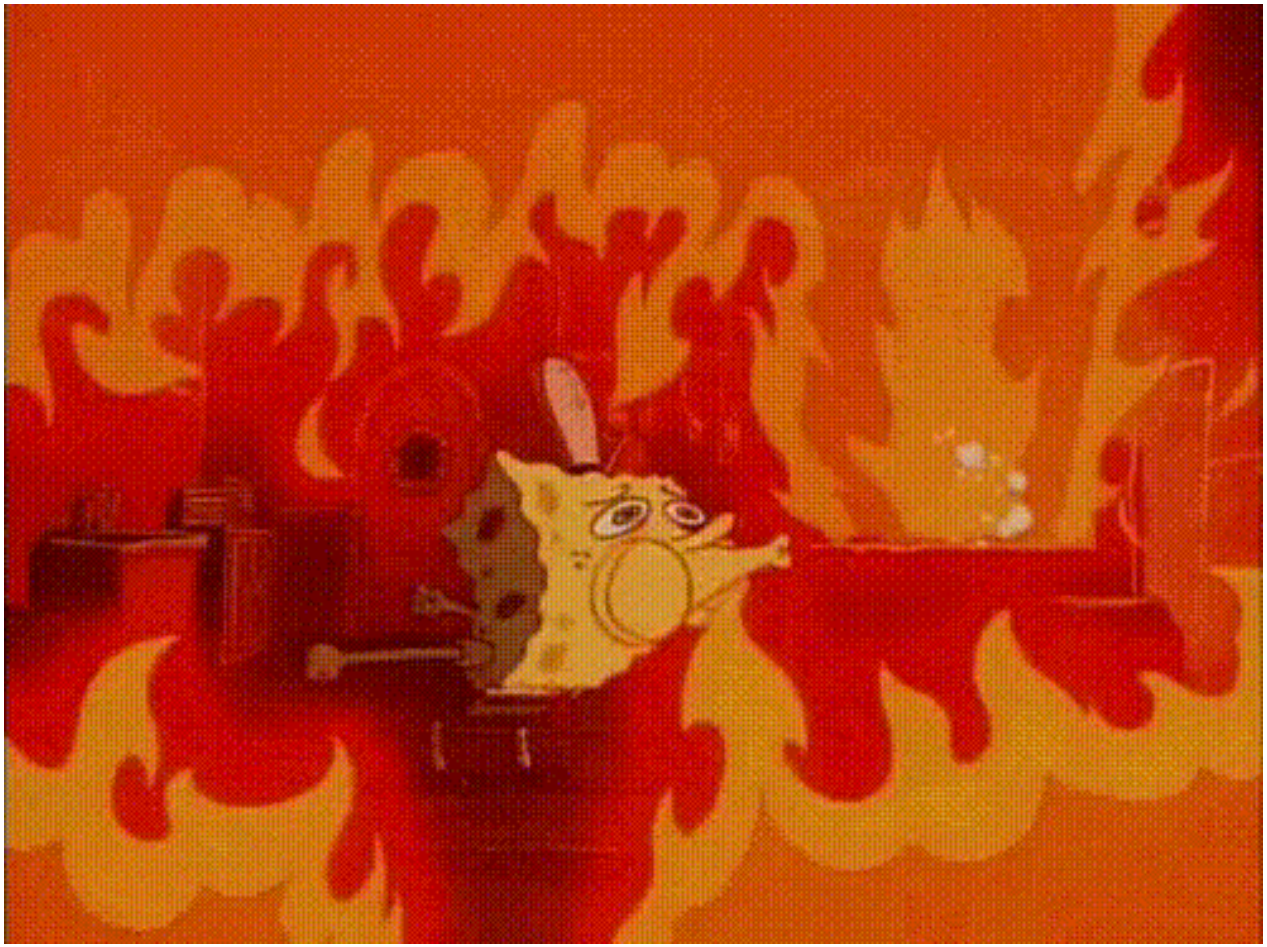
```
# UNMOUNT TRUECRYPT
#

promptToRun ("Unmount TrueCrypt", "c:\\progra~1\\TrueCrypt\\truecrypt.exe /l T /d /q /s /f /w");
```

- Selon Bruce Schneier, ce sont les Russes
  - Mais la China, Israel et la France en auraient les capacités

https://www.lawfareblog.com/who-publishing-nsa-and-cia-secrets-and-why

ShadowBrokers, publication de nouveaux outils de la NSA (suite)

- Chez Microsoft en Mars



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Les exploits publiés par ShadowBrokers sont utilisés activement sur Internet

- plus de 50 000 machines Windows exposées sur Internet présentent une installation de la backdoor DoublePulsar,
- Un script de détection d'infection ;disponible sur GitHub.

https://below0day.com/2017/04/23/doublepulsar-global-implants/
https://github.com/countercept/doublepulsar-detection-script/
https://threatpost.com/nsas-doublepulsar-kernel-exploit-in-use-internet-wide/125165/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Piratage de FlexiSpy et Retina-X, entreprises de vente de logiciels de surveillance

- La méthodologie est publiée
  https://pastebin.com/raw/Y1yf8kq0
- Code source de l'outil / trojan
  https://github.com/Te-k/flexidie

Noms de domaine internationalisés pour du phishing

- Exemple sur epic.com
  https://www.wordfence.com/blog/2017/04/chrome-firefox-unicode-phishing/

Ascii		Cyrillique	
Lettre	Hexadécimal	Lettre	Hexadécimal
e	0x0065	e	0xD0B5
p	0x0070	p	0xD180
i	0x0069	i	0xD196
c	0x0063	c	0xD181

- Fonctionnel sur Apple
  http://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html?m=1

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

10 000 routeurs ZyXel utilisés pour bruteforcer des blogs WordPress

- Appartenant au FAI algérien Telecom Algeria
- La vulnérabilité « Misfortune Cookie » dans le service de management à distance du protocole TR-069 est exploitée depuis Internet sur le port 7547 et permet d'obtenir un accès d'administration à l'interface Web.

https://www.tripwire.com/state-of-security/featured/hacked-home-routers-trying-brute-force-way-wordpress-websites/

http://mis.fortunecook.ie/

Transformer un KVM en keylogger à distance

- L'équipe de sécurité Talos de Cisco démontre comment il est possible de modifier un équipement d'accès à distance de type Keyboard Virtual Mouse (KVM) afin d'en faire un keylogger

https://labs.portcullis.co.uk/whitepapers/hacking-the-belkin-e-series-omniview-2-port-kvm-switch/

Une étude recense les failles applicatives des tutoriaux populaires de développement Web

https://www.helpnetsecurity.com/2017/04/21/programming-tutorials-vulnerabilities/

Vol de comptes bancaires allemands en interceptant les SMS de confirmation

- Exploitation de failles SS7 (en partie présentées en janvier 2015)

http://www.01net.com/actualites/des-pirates-vident-des-comptes-bancaires-en-detournant-des-sms-1156971.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

IBM fournit des clefs USB infectées par un malware

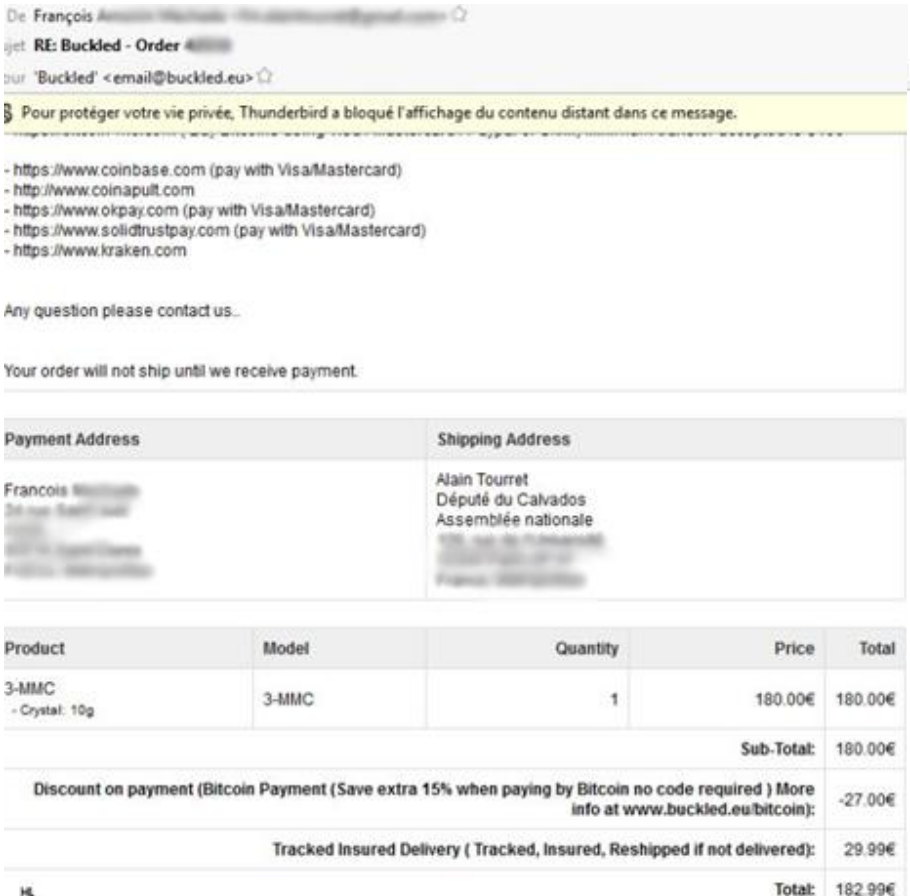
- Clef USB d'initialisation de leurs appliances de stockage
  https://www.grahamcluley.com/ibm-shipping-malware-infected-usb-sticks/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Macron Leak

- Publication de 15Go de données vendredi soir
  https://pastebin.com/bUJKFpH1
- Beaucoup de documents totalement inintéressants
  - Pleins de faux mal faits, comme une commande Méthamphétamine par Alain Tourret
    - Payé en Bitcoins



De François
jet RE: Buckled - Order
ur 'Buckled' <email@buckled.eu>

Pour protéger votre vie privée, Thunderbird a bloqué l'affichage du contenu distant dans ce message.

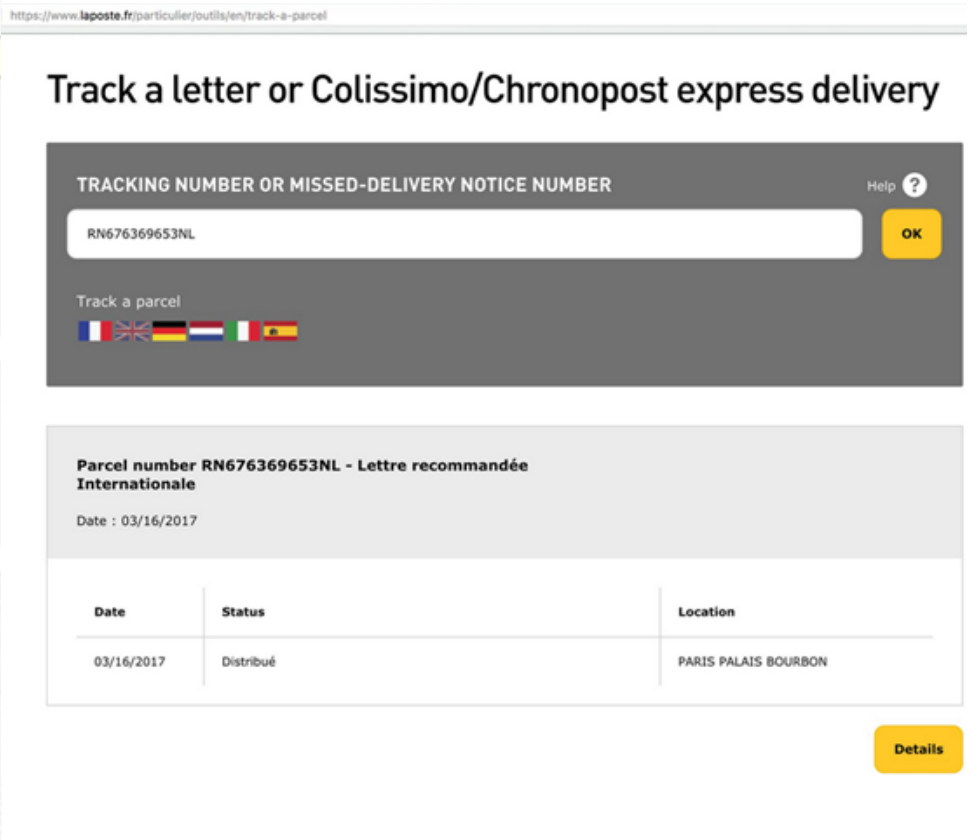
- https://www.coinbase.com (pay with Visa/Mastercard)
- http://www.coinapult.com
- https://www.okpay.com (pay with Visa/Mastercard)
- https://www.solidtrustpay.com (pay with Visa/Mastercard)
- https://www.kraken.com

Any question please contact us..

Your order will not ship until we receive payment.

Payment Address	Shipping Address
Francois	Alain Tourret Député du Calvados Assemblée nationale

Product	Model	Quantity	Price	Total
3-MMC - Crystal: 10g	3-MMC	1	180.00€	180.00€
			Sub-Total:	180.00€
			Discount on payment (Bitcoin Payment (Save extra 15% when paying by Bitcoin no code required) More info at www.buckled.eu/bitcoin):	-27.00€
			Tracked Insured Delivery (Tracked, Insured, Reshipped if not delivered):	29.99€
			Total:	182.99€



https://www.laposte.fr/particulier/outils/en/track-a-parcel

Track a letter or Colissimo/Chronopost express delivery

TRACKING NUMBER OR MISSED-DELIVERY NOTICE NUMBER

Help

RN676369653NL

OK

Track a parcel

Parcel number RN676369653NL - Lettre recommandée Internationale

Date : 03/16/2017

Date	Status	Location
03/16/2017	Distribué	PARIS PALAIS BOURBON

Details

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Macron Leak (suite)

- Mounir Mahjoubi (Président du Conseil national du numérique) explique comment ils se sont préparés
  http://resistancereport.com/news/frances-macron-defeated-russian-hackers-one-simple-trap/
- L'attaque ressemble aux méthodes des Russes
  http://lexpansion.lexpress.fr/high-tech/en-marche-cible-par-les-hackers-fancy-bear_1900835.html
- Des métadonnées en cyrillique ajoutée juste avant la publication
  https://twitter.com/msuiche/status/860762309299511296
- Le même domaine mail utilisé pour la fuite du parti démocrate américain (gmx.de)
  https://twitter.com/pwnallthethings/status/860670945974996992/photo/1

L'analyse de @thegrugq
https://medium.com/@thegrugq/a-list-minute-influence-op-by-data-ddos-3698906d8836

Piratages, Malwares, spam, fraudes et DDoS

Malwares

HandBrake pour macOS, Piratage du serveur de téléchargement

- Si téléchargé entre le 2 et le 6 mai, il est accompagné d'un vilain cadeau
  https://forum.handbrake.fr/viewtopic.php?f=33&t=36364

Piratages, Malwares, spam, fraudes et DDoS

Hardware / IoT

Une vulnérabilité dans l'application Hyundai Blue Link permet à un attaquant de géolocaliser, déverrouiller et démarrer la voiture de sa victime

- Fonctionnalité de log qui envoie aux serveurs des informations sensibles (user, password, etc) chiffrées avec une clé statique présente dans l'application
- Une écoute passive permet de récupérer les données et ensuite de déverrouiller les véhicules concernés

https://community.rapid7.com/community/infosec/blog/2017/04/25/r7-2017-02-hyundai-blue-link-potential-info-disclosure-fixed

Un framework pour évaluer la sécurité des véhicules via le bus CAN

- Permet de sniffer et d'injecter des données de plusieurs protocoles

  Liste des interfaces physiques compatibles sous Linux

  http://elinux.org/CAN_Bus#CAN_Support_in_Linux

  https://github.com/CaringCaribou/caringcaribou

Domotique IKEA : un premier coup d'oeil à la sécurité

- Fonctionne via ZigBee
- Une seule interface exposée, DTLS
- Secret propre à chaque objet

  http://mjg59.dreamwidth.org/47803.html

Piratages, Malwares, spam, fraudes et DDoS

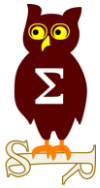
Hardware / IoT

Modification de firmware par I2C sur Google Nexus 9

- Bus I2C accessible par le FASTBOOT en USB ainsi qu'en UART sur le câble jack audio (cf. revue précédente)
  http://seclists.org/fulldisclosure/2017/May/19

Casque Bose, collecte des données personnelles

- A partir de l'application "Bose Connect"
- Fuite du nom, du numéro de téléphone, du mail…
- Le chercheur ayant découvert la fuite a attaqué Bose
  https://www.developpez.com/actu/131166/Les-casques-de-Bose-collectent-secretement-des-donnees-personnelles-des-utilisateurs-pour-les-livrer-a-des-parties-tierces-selon-une-plainte-aux-USA/



Nouveautés, outils et techniques

Pentest
Techniques & outils

Persistence via Office

- En ajoutant des “Add Ins” (dll, VBA, VBE, …)

https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/

Gagner un CTF par la compromission de l’infrastructure

- Google Kontainers Engine & Kubernetes utilisé lors du CTF des BSides SF
- Par défaut, le volume /var/run/secrets/kubernetes.io/serviceaccount est monté dans chaque nouveau conteneur et contient une clé API permettant d’exécuter du code sur le conteneur

https://hackernoon.com/capturing-all-the-flags-in-bsidessf-ctf-by-pwning-our-infrastructure-3570b99b4dd0

Malware-Hunter, le service permettant de lister les serveurs de C&C

- Le projet Malware-Hunter, né de la fusion entre Shodan et Recorded Future, permet de scanner Internet à la recherche des serveurs de Command and Control (C&C). Pour cela, l'outil prétend être un hôte infecté qui demande de nouveaux ordres en s'adressant à chaque adresse IP comme si elle était un serveur de C&C. Ainsi, lorsque l'application reçoit une réponse positive, le serveur est alors taggé en tant que C&C.
- Les résultats préliminaires indiquent déjà des centaines d'adresses IP répondant aux malwares tels que Gh0st RAT, Dark Comet ou encore njRAT. De plus, ils sont aussi accessibles sur le moteur de recherche Shodan.

https://malware-hunter.shodan.io/

https://go.recordedfuture.com/hubfs/reports/threat-identification.pdf

https://www.shodan.io/search?query=category%3Amalware

Récupérer le code source d'un script Python en cours d'exécution

https://pythontips.com/2017/03/12/recovering-lost-python-source-code-if-its-still-resident-in-memory/

Business et Politique

Droit / Politique
International

Sa montre Fitbit contredit ses dires

- Il assassine sa femme alors qu'elle est enceinte, qu'il a une liaison
  - Puis essaie de récupérer l'assurance vie de près de $500k
- Les données de sa montre connectées contredisent son alibi

http://www.numerama.com/politique/252876-le-meurtre-et-lobjet-connecte-quand-un-bracelet-fitbit-contredit-le-recit-du-suspect.html

Démantèlement d'un réseau pédophile utilisant Whatsapp

- Enquête débutée sur TOR
- 39 personnes arrêtées

http://www.lemonde.fr/pixels/article/2017/04/19/un-reseau-de-pedopornographie-sur-whatsapp-demantele_5113628_4408996.html

La Turquie bloque l'accès à Wikipédia

http://tempsreel.nouvelobs.com/en-direct/a-chaud/36405-turquie-internet-turquie-bloque-acces-wikipedia-toutes.html

Droit / Politique

International

Cout du déblocage de l'iPhone de San Bernardino

- Selon un sénateur américain, il s'élève à $900 000
  http://uk.businessinsider.com/dianne-feinstein-fbi-paid-900000-to-hack-into-san-bernardino-iphone-2017-5?r=US&IR=T

Conférences

Conférences

Passées

- Troopers
- Hack in the Box

A venir

- Nuit du Hack - 24-25 juin 2017 à Paris (Eurodisney)
- SSTIC - 7 au 9 juin 2017 à Rennes
- BeeRump - 22 juin à Paris (Epita)

Divers / Trolls velus

Divers / Trolls velus

Une tentative de lister tous les bypass UAC

https://www.peerlyst.com/posts/wiki-uac-bypasses-and-uac-bypass-research-nic-cancellari

WhatsApp : mise à jour en lien avec Siri et déchiffrement

- La nouvelle version de l'application permet de lire ses derniers messages, depuis Siri

Quand on vous dit de chiffrer…

- Un employé de Bercy s'est fait fracturer sa voiture
- Son PC ainsi que son smartphone et des documents confidentiels ont été volés.

http://www.lemondeinformatique.fr/actualites/lire-des-codes-sources-de-logiciels-gouvernementaux-dans-la-nature-67831.html

Divers / Trolls velus

FranceInfo, une requête SQL en Javascript…

- Depuis une requête GET
  https://twitter.com/Michel_Gaschet/status/861604301470408704/photo/1

Firefox Fichier Édition Affichage Historique Marque-pages Outils Fenêtre Aide — Lun. 17:20

CARTE. Présidentielle : décou

mobile.francetvinfo.fr/elections/presidentielle/infographie-election-presidentielle-decouvrez-la-participation-au-s

Rechercher

scrutin de 2002 (26,19% à midi).

Si cette carte ne s'affiche pas correctement sur votre téléphone, cliquez ici.

PARTICIPATION A 12H
19.54
37.56
//x

{{departement}}
La participation à 12h s'élève à {{abstention_percent}} % des inscrits.

//]]> //
{{departement}}
La participation à 12h s'élève à {{abstention_percent}} % des inscrits.
//]]> // 0)?[46.283840,3.370722]:[43.183840,1.370722], zoom: (document.location.href.indexOf('www.') > 0)?6:5, zoomControl:false, }); var layerSource = { type: 'cartodb', user_name: 'francetvinfo', sublayers: [{ sql: 'SELECT departements_presidentielle.cartodb_id as cartodb_id, departements_presidentielle.the_geom_webmercator as the_geom_webmercator, departements_presidentielle.insee as insee, participation_midi.departement as departement, participation_midi.participation_percent as participation_percent FROM departements_presidentielle, participation_midi WHERE participation_midi.insee = departements_presidentielle.insee', cartocss: 'Map{background-color: #fff;} #a{polygon-fill: ramp([participation_percent], (#fef7cc, #fcef99, #fbe666, #f9de33, #f8d600), quantiles);line-color: #fff;line-width: 1;line-opacity: 1;}', }] };cartodb.createLayer(map, layerSource) .addTo(map) .on('done', function(layer) { staticSubLayer=layer.getSubLayer(0); cdb.vis.Vis.addInfowindow(map, staticSubLayer,['departement','participation_percent'],{ infowindowTemplate: $('#infowindow_template').html(), sanitizeTemplate:false }); layer.leafletMap.viz.addOverlay({ type: 'tooltip', layer: staticSubLayer, template: $('#hover_template').html(), position: 'bottom|right', fields: [{ name: 'name' }] }); layer.setInteraction(true); map.dragging.disable(); map.touchZoom.disable(); map.doubleClickZoom.disable(); map.scrollWheelZoom.disable(); map.keyboard.disable(); }) .on('error', function() { //log the error }); } $(document).ready(function(){loadCartoDb();}); //]]>

Quels sont les bons et les mauvais élèves ?

Divers / Trolls velus

Les techniques du roi des hackers pour surfer sur le web anonymement

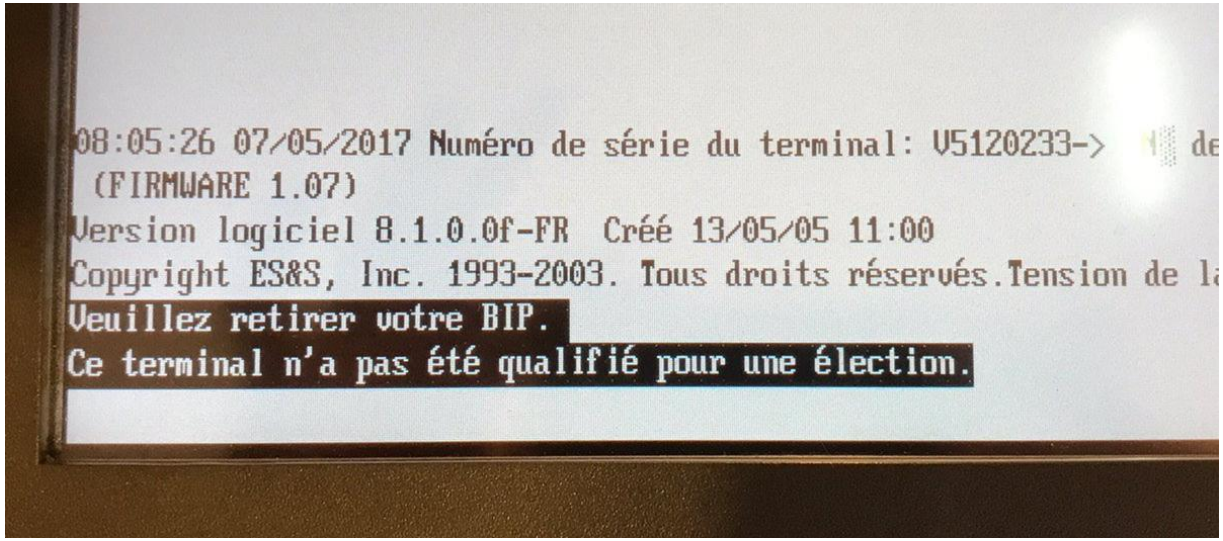
- Acheter un PC en liquide
- Installer Tails Linux
- Utiliser Tor Browser depuis un lieu autre que chez soi

http://www.01net.com/actualites/les-techniques-du-roi-des-hackers-pour-surfer-le-web-anonymement-1157929.html

- Et sinon la Virtualisation ? Les Snapshot ?

Les machines à voter…

https://twitter.com/iacovellixavier/status/861115791143575552/photo/1



Divers / Trolls velus

Le nouveau top10 de l'OWASP en pré-release

- Fusion de "A4: Insecure Direct Object References" et "A7: Missing Function Level Access"
- Ajout de "A7: Insufficient Attack Protection" et "A10: Underprotected APIs"
- Suppression de "A10: Unvalidated Redirects and Forwards"
- Par ailleurs et pour la première fois, les données statistiques provenant d'acteurs tiers (sociétés de conseil/audit, éditeurs etc.) ayant servi de base à cette nouvelle mouture sont publiquement accessibles.
  https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf

- Grosse polémique :
  - Pas de WAF ou RASP = vulnérabilité ?
  - Construit par une seule personne en conflit d'intérêt

  https://sakurity.com/blog/2017/04/24/owasp.html -> excellent article !

  http://www.skeletonscribe.net/2017/04/abusing-owasp.html

  https://twitter.com/sirdarckcat/status/856560661534564352 <<The 3 problems with OWASP A7 Fiasco: #1 Proposed by those with a clear conflict of interest. Severely damaging credibility of the project.>>

  https://twitter.com/sirdarckcat/status/855860484377063424

OWASP Top 10 – 2017 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities
A10 – Underprotected APIs (NEW)

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 13 juin 2017

After Work

- Mardi 23 mai 2017

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous