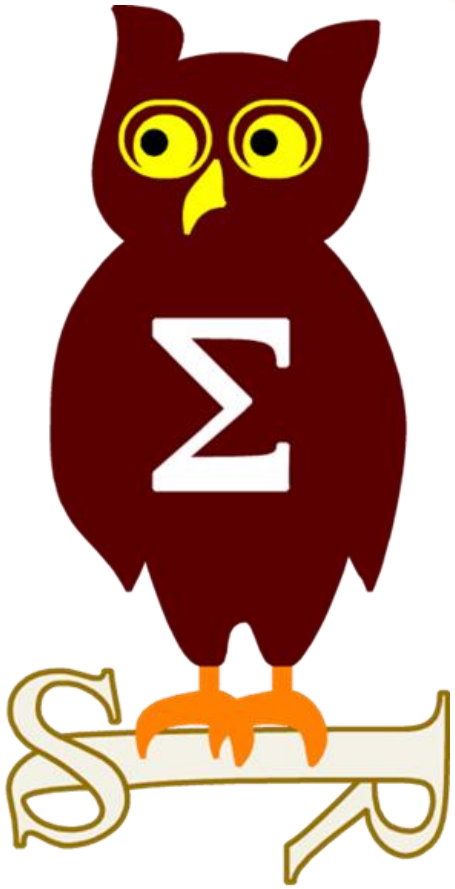
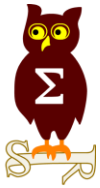


Revue d'actualité

09/02/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-001 Vulnérabilités dans Internet Explorer (2 CVE) [Exploitabilité 1,2]

- Affecte:
  - Windows (toutes versions supportes), Remplace MS15-124
- Exploit:
  - Élévation de privilèges
  - Exécution de code à l'affichage d'une page web contenant un ActiveX (CVE-2016-0002)
- Crédits:
  - Anonymous contributor par VeriSign iDefense Labs (CVE-2016-0002)
  - Heige (a.k.a. SuperHei) de Knownsec 404 Security Team (?)

MS16-002 Vulnérabilités dans Edge (2 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 10, Remplace MS15-125
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code
  - Exécution de code à l'affichage d'une page web contenant un ActiveX (CVE-2016-0024)
- Crédits:
  - 003 par ZDI (CVE-2016-0003)
  - CESG (CVE-2016-0024)
  - Wenbin Zheng de Qihoo 360Vulcan Team (?)

MS16-003 Vulnérabilités dans VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
  - JScript 5.7 et 5.8 (Windows Vista, 2003, 2008, 2008 Core)
  - Remplace MS15-126
- Exploit:
  - Exécution de code à l'affichage d'une page web contenant un ActiveX
- Crédits:
  - Anonymous contributor par VeriSign iDefense Labs (CVE-2016-0002)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-004 Vulnérabilités dans Office (5 CVE) [Exploitabilité 3,2,2,1,1]

- Affecte:
  - Microsoft Office toutes versions supportées (Windows et Mac)
  - Microsoft SharePoint 2013
  - Remplace MS14-024, MS15-131, MS15-116, MS15-110, MS12-060
- Exploit:
  - 2 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
  - 1 x Contournement ASLR (fuite d'information)
  - 2 x XSS dans SharePoint
- Crédits:
  - Tom Kahana et Elad Menahem de IBM X-Forcer (CVE-2016-0012)
  - Jack Tang de Trend Micro (?)
  - Jonas Nilsson de Disruptive Innovations AB (CVE-2015-6117)
  - Kai Lu de Fortinet's FortiGuard Labs (CVE-2016-0010)
  - Steven Seeley de Source Incite par ZDI (CVE-2016-0035)

MS16-005 Vulnérabilités noyau Win32k et GDI32 (2 CVE) [Exploitabilité 2,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS15-072, MS15-073
- Exploit:
  - 1 x Exécutions de code
  - 1 x Contournement ASLR (fuite d'information)
- Crédits:
  - Kerem Gümrükcü (CVE-2016-0009)
  - Steven Seeley de Source Incite par VeriSign iDefense Labs (CVE-2016-0008)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-006 Vulnérabilités dans Silverlight (1 CVE) [Exploitabilité 1]

- Affecte:
  - Silverlight 5
  - Remplace MS15-129
- Exploit:
  - 1 x Exécutions de code
- Crédits:
  - Anton Ivanov et Costin Raiu de Kaspersky Lab (CVE-2016-0034)

MS16-007 Vulnérabilités diverses (6 CVE) [Exploitabilité 1,2,1,1,2,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS13-062, MS14-041, MS13-101, MS13-011, MS12-004, MS14-071
- Exploit:
  - 2 x Elevations de privilèges lors du chargement d'une librairie (DLL)
  - 1 x Exécutions de code depuis DirectShow
  - 2 x Exécutions de code lors du chargement d'une librairie (DLL)
  - 1 x Possibilité d'ouvrir une session RDP avec un compte sans mot de passe (normalement interdit)
- Crédits:
  - Ashutosh Mehra par ZDI (CVE-2016-0020)
  - Gal Goldshtein et Viktor Minin de Citadel (CVE-2016-0019)
  - Stefan Kanthak (CVE-2016-0014, CVE-2016-0014)
  - Steven Vittitoe de Google Project Zero (CVE-2016-0015, CVE-2016-0016)
  - parvez@greyhathacker.net (CVE-2016-0018)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-008 Vulnérabilités noyau (2 CVE) [Exploitabilité 1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS15-111, MS15-122, MS15-115
- Exploit:
  - 2 x Élévations de privilèges locale depuis des points de montage
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-0006, CVE-2016-0007)

MS16-009 ??? (? CVE) [Exploitabilité ?]

- Retardé pour réaliser plus de tests

MS16-010 Vulnérabilité dans Microsoft Exchange (4 CVE) [Exploitabilité 2,1,2,1]

- Affecte:
  - Exchange 2013 et 2016
  - Remplace MS15-103
- Exploit:
  - 4 x usurpations de contenu et redirections depuis Microsoft Outlook Web Access
- Crédits:
  - Abdulrahman Alqabandi (CVE-2016-0029)
  - Alexandru Coltuneac (CVE-2016-0030)
  - Nirmal Kirubakaran, Individual (CVE-2016-0031)
  - israelg@bugsec.com (CVE-2016-0032)

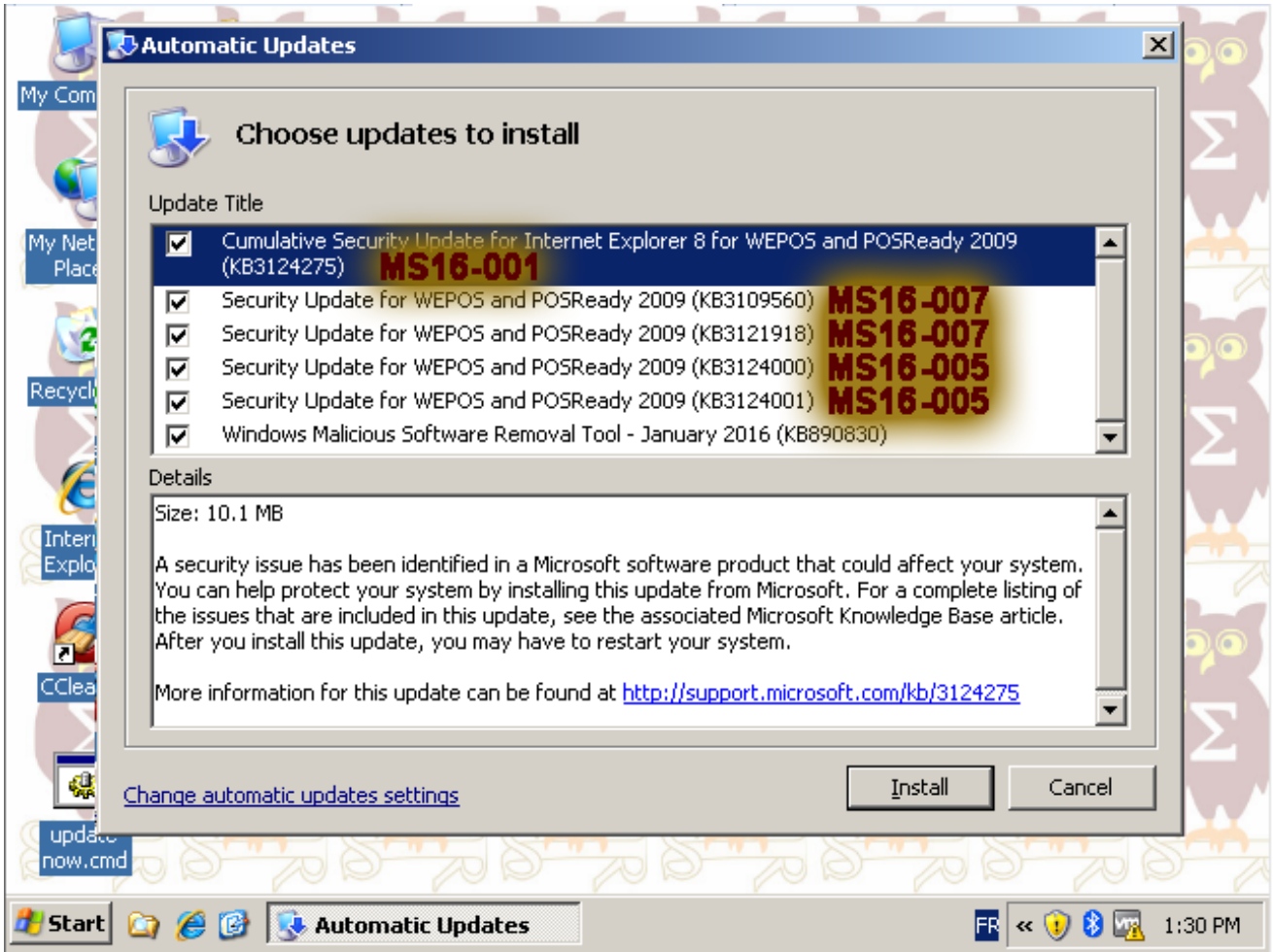
Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…
  - Contrairement à ce qui était annoncé en janvier ?

http://betanews.com/2016/01/11/windows-xp-embedded-service-pack-3-dies-tomorrow/



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

2755801 Mise à jour de Flash Player

- V53.0 Nouvelle mise à jour de Flash Player

3123479 Fin du support de SHA-1

- V1.0 Fin du support de SHA-1 160bits pour les Autorité de Certification racine de Microsoft

3109853 Meilleur support de la RFC 5077 sur TLS avec SChanel

- V1.0 Meilleur support de la reprise de session TLS (sans état sur le serveur) et empechant de rétrograder dans une version TLS/SSL inférieure

3118753 Mise à jour de la liste noire d'ActiveX (kill bits)

- V1.0 Ajout dans la liste noire de : IBM Endpoint Manager for Remote Control (>=9.0.1) et IBM Assist On-site 4.0.0

Failles / Bulletins / Advisories

Microsoft - Autre

Charka, le moteur Javascript d'Edge en Open Source sur Github

https://github.com/Microsoft/ChakraCore

Windows 10 aurait dépassé Windows 8.1

http://www.zdnet.fr/actualites/windows-10-serait-passe-devant-windows-81-39831400.htm

Windows 8, c'est fini pour les mises à jour de sécurité

- Il faut passer à 8.1 (ou revenir à 7)

https://support.microsoft.com/en-us/lifecycle#gp/LifeWinFAQ

Policy Analyzer

- Auditez vos GPO

http://microsoft-news.com/microsoft-releases-new-tool-policy-analyzer/

Failles / Bulletins / Advisories

Système (principales failles)

cPanel, exécution de code

http://news.cpanel.com/cpanel-tsr-2016-0001-full-disclosure/

PayPal, exécution de code

- Encore un un problème de désérialisation Java

  http://artsploit.blogspot.com.au/2016/01/paypal-rce.html

- Redirection web permettant d'usurper le site de PayPal (et d'autres)

  http://seclists.org/fulldisclosure/2015/Sep/52

AngularJS, XSS par injection de modèle (template)

- Grâce à l'injection de doubles d'accolades, même si bien encodé par htmlspecialchars()

  http://blog.portswigger.net/2016/01/xss-without-html-client-side-template.html

Failles / Bulletins / Advisories

Système (principales failles)

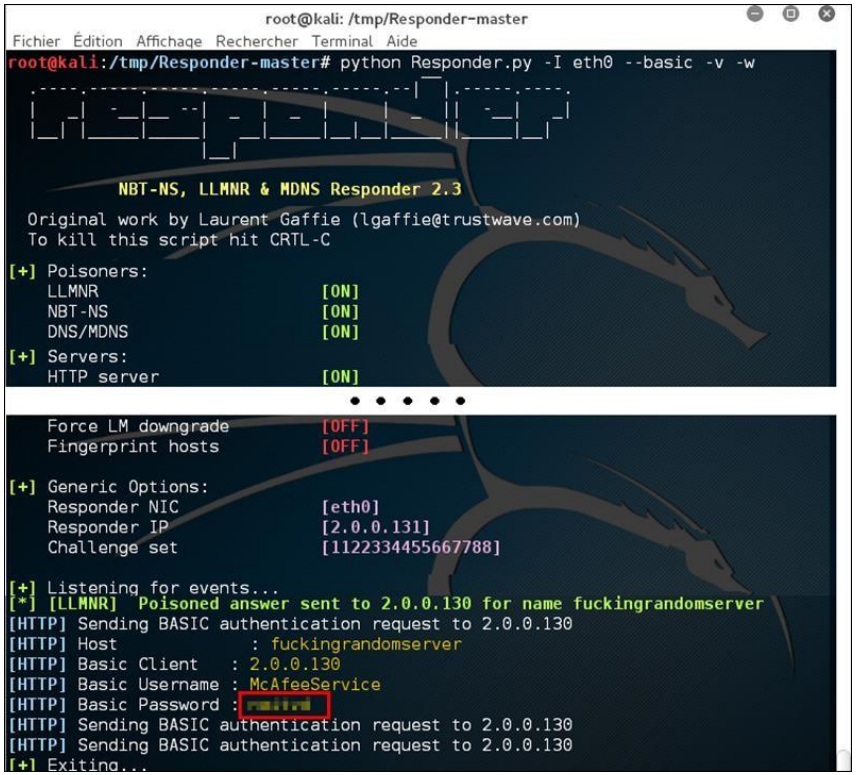
TrendMicro, XSRF sur Direct Pass permettant l'exécution de Javascript chez les clients

http://seclists.org/fulldisclosure/2016/Jan/97

McAfee, récupération du mot de passe du compte de service

- Présent chiffré dans C:\ProgramData\McAfee\Common Framework\SiteList.xml
- Un outil pour déchiffrer existe mais non public

https://github.com/tfairane/HackStory/blob/master/McAfeePrivesc.md



Failles / Bulletins / Advisories

Système (principales failles)

Antivirus Comodo, élévation de privilège

https://twitter.com/Laughing_Mantis/status/650198599507181568/photo/1

Comodo, navigateur Chromodo

- Désactivation des fonctionnalités de sécurité de Chrome

  https://code.google.com/p/google-security-research/issues/detail?id=704

Avast, navigateur Avastium : pas mieux

https://code.google.com/p/google-security-research/issues/detail?id=679

Socat, utilisation d'un nombre premier "non premier" pour Diffie-Hellman

- Nombre fixé arbitrairement et non premier

  http://www.theregister.co.uk/2016/02/03/socat_backdoor_fix/

- Le diff

  https://fossies.org/diffs/socat/1.7.3.0_vs_1.7.3.1/xio-openssl.c-diff.html

Failles / Bulletins / Advisories

Système (principales failles)

OpenSSH Roaming

- Fonctionnalité non documentée mais présente dans le code pour “reconnecter” une session après une coupure réseau
- Buffer Overflow dans cette fonctionnalité sur le client OpenSSH (5.4 à 7.1)
- Peut permettre l’extraction de clé privée

http://seclists.org/fulldisclosure/2016/Jan/44

MITM sur les mises à jour de driver Intel

- Les fichiers sont récupérés en HTTP

http://seclists.org/fulldisclosure/2016/Jan/56

Injection SQL dans Symfony

- Lors de l’ajout d’un utilisateur…

http://seclists.org/fulldisclosure/2016/Feb/13

Failles / Bulletins / Advisories

Réseau (principales failles)

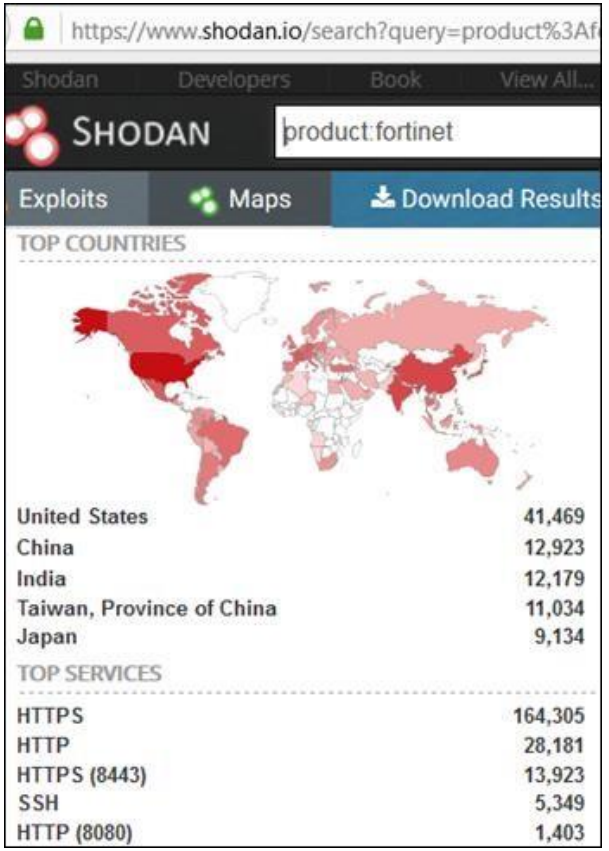
Fortinet / Fortigate, porte dérobée

- Large gamme de produits vulnérables
  - FortiAnalyzer: 5.0.5 à 5.0.11 et 5.2.0 à 5.2.4
  - FortiSwitch: 3.3.0 à 3.3.2
  - FortiCache: 3.0.0 à 3.0.7
  - FortiOS 4.1.0 à 4.1.10, 4.2.0 à 4.2.15, 4.3.0 à 4.3.16 et 5.0.0 à 5.0.7
- Compte **Fortimanager_Access** / FGTAbc11*xy+Qqz27 (SHA-1 du pass).

  http://seclists.org/fulldisclosure/2016/Jan/26
- 5 349 firewalls accessibles en SSH dont 260 en France
- Selon Fortinet, ce n'est pas une backdoor

  <<This was not a "backdoor" vulnerability issue but rather a management authentication issue. >>

  http://blog.fortinet.com/post/brief-statement-regarding-issues-found-with-fortios



Failles / Bulletins / Advisories

Réseau (principales failles)

Visioconférence AMX / Harman, porte dérobée

- Compte caché **BlackWidow**
- Alerte de chercheurs
- 7 mois après, correction… en renommant le compte **1MB@aMaN**

http://blog.sec-consult.com/2016/01/deliberately-hidden-backdoor-account-in.html

Failles / Bulletins / Advisories

Routeurs SOHO

Netgear, commutateur GS105Ev2

- Contournement de l'authentification du protocole de configuration
- XSS, CSRF, récupération du mot de passe, prédiction de cookie

  http://seclists.org/fulldisclosure/2016/Jan/77

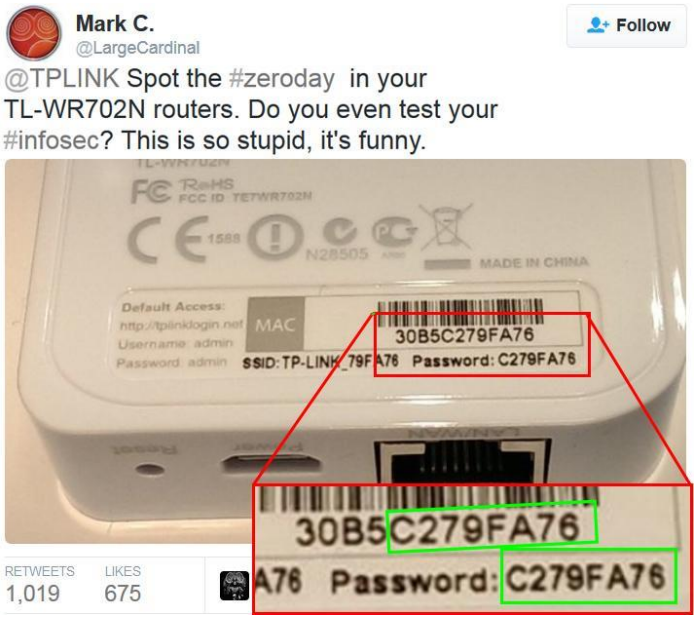
Netgear, outil de gestion réseau NMS300

- Téléchargement arbitraire de fichier et Exécution de code à distance

  http://seclists.org/fulldisclosure/2016/Feb/30

TPLink, le mot de passe est la fin de la MAC

https://twitter.com/LargeCardinal/status/682591420969029632/photo/1



Failles / Bulletins / Advisories

Apple

Apple Software Update 2.1.3, exécution de code à distance

- Flux non chiffré, MitM et injection d'un champ contenant un paramètre de ligne de commande

  http://seclists.org/fulldisclosure/2016/Feb/28

Failles / Bulletins / Advisories

Google

Android, correction de vulnérabilités critiques

- Exécution de code sur le pilote WiFi Broadcom
- Exécution de code depuis la librairie multimédia StageFright

http://thehackernews.com/2016/02/update-android-security.html

Android à base de CPU Mediatek MT6582 (ARM Quad-core)

- Porte dérobée permettant une élévation de privilège (propriété système ro.secure)

https://twitter.com/jcase/status/687151870255755264

https://twitter.com/AeoliaZHANG/status/687487611263270912

Failles / Bulletins / Advisories

Crypto

Blackberry PGP cassé par la police néerlandaise ?

https://translate.google.com/translate?sl=nl&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Fwww.misdaadnieuws.com%2Famsterdam-00053.html&edit-text=

OpenSSL 1.0.2

- Exposant Diffie-Helman unique par process, permettant

http://arstechnica.com/security/2016/01/high-severity-bug-in-openssl-allows-attackers-to-decrypt-https-traffic/

PGP fait fuiter plus d'informations que vous l'imaginez

- Le PGP Key ID peut-être considéré comme une métadonnées et être collecté pour désanonymiser des utilisateurs

https://www.youtube.com/watch?v=zqnKdGnzoh0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Malware

Dridex piraté

- “Quelqu’un” a piraté le botnet Dridex (le serveur central de C&C?)
- Et remplace le loader Dridex par une installation de l’antivirus Avira

https://blog.avira.com/dridex_serves_avira/

3 mois de Honeypot POS

http://cybermashup.com/2016/02/04/honey-where-is-my-pos/

Piratage massif de sites Wordpress

- Utilisés ensuite pour infecter les visiteurs avec des rançongiciels

http://arstechnica.com/security/2016/02/mysterious-spike-in-wordpress-hacks-silently-delivers-ransomware-to-visitors/

Bilan du piratage de TalkTalk

- 100 000 clients perdus
- Cout total : 65 millions de livres

http://www.zdnet.fr/actualites/l-operateur-talktalk-tire-le-bilan-de-son-piratage-100000-clients-perdus-39832288.htm

Piratages, Malwares, spam, fraudes et DDoS

Portes dérobées / Backdoor

AMX / Harman : systèmes de Visioconférence

- Fonction setUpSubtleUserAccount() ajoutant **subtilement** le compte BlackWidow
  - Utilisateur avec des fonctionnalités supplémentaires comme la capture de paquets réseau
- Remontée de l'information à l'éditeur et … correction 7 mois après
  - En renommant la backdoor 1MB@aMaN

http://blog.sec-consult.com/2016/01/deliberately-hidden-backdoor-account-in.html

Lucky7Coin

- Fonctions popen() et pclose() dissimulée et accessible par un canal de contrôle sur IRC

https://github.com/alerj78/lucky7coin/blob/master/src/irc.cpp

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS sur le site d'HSBC

- Revendiqué par New World Hacktivists (???)

  http://www.net-security.org/secworld.php?id=19392

Étude de Kaspersky sur le DDoS (datant de 6 mois)

- 50% des DDoS sont effectifs
- 35% ne durent que quelques heures
  - Mais **7%** durent **plusieurs semaines**
- Principales cibles : Telecom (24%), Finance (22%), IT (21%), gouvernements (18%)
- Ressources ciblées : Sites web (47%), Portail client (38%), communications (37%), serveurs de fichiers (27%), transactionnel (24%)
- 32% masquent des intrusions
- **12%** viennent des **concurrents**

  https://press.kaspersky.com/files/2015/09/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf

Piratages, Malwares, spam, fraudes et DDoS

Scada

Advantech, porte dérobée dans les passerelles GSM/Ethernet ou GSM/Série EKI-1322

- Clef SSH en dur (corrigé avec la dénomination "Fixed security issues within SSH login")
- Heartbleed (non corrigé)
- Shellshock (non corrigé)

https://threatpost.com/advantech-eki-vulnerable-to-bypass-possible-backdoor/115900/

Advantech toujours, nombreuses vulnérabilités dans les IHM web

https://ics-cert.us-cert.gov/advisories/ICSA-16-014-01

Injection de commande via SNMP sur les UPS GE

- Via l'interface SNMP/Web

http://seclists.org/fulldisclosure/2016/Feb/21

http://apps.geindustrial.com/publibrary/checkout/GEIS_SNMP?TNR=Application%20and%20Technical%7CGEIS_SNMP%7CPDF&filename=GEIS_SNMP.pdf

https://ics-cert.us-cert.gov/advisories/ICSA-16-033-02

Rejeu de paquets sur les Siemens S7-1500

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2201

Piratages, Malwares, spam, fraudes et DDoS

Scada

Buffer Overflow dans les pompes à insuline Hospira

https://ics-cert.us-cert.gov/advisories/ICSA-15-337-02

Buffer Overflow dans les automates Rockwell MicroLogix

https://ics-cert.us-cert.gov/advisories/ICSA-16-026-02

S4xEurope les 9 & 10 juin à Vienne

- Le CFP est ouvert

https://www.digitalbond.com/s4/s4xeurope-june-9-10-in-vienna/

Impacts d'un MITM sur Ethernet/IP

http://fr.slideshare.net/gilsinnj/mechanics-of-an-icsscada-maninthemiddle-attack

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Vulnérabilités dans les jouets connectés

- Possibilité d'accéder :
  - aux profils des enfants pour une peluche connectée
  - aux coordonnées GPS pour une montre qui géo-localise

https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform

Sonnette connectée, facile à démonter (2 vis), elle permet de récupérer la clef WiFi

- Un bouton la transforme en point d'accès
- Et un service web vous donne sa configuration, dont la clef WiFi

https://www.pentestpartners.com/blog/steal-your-wi-fi-key-from-your-doorbell-iot-wtf/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

GPS Spoofing

- Où : comment l'Iran a dérouté un bateau américain

  http://sofrep.com/46818/gps-spoofing-how-iran-tricked-us-patrol-boats-into-capture/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage du compte mail et téléphone du directeur de la CIA

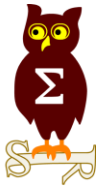
- Ainsi que le mail de sa femme
- Il a redirigé les appels vers une organisation de défense de la Palestine

http://motherboard.vice.com/read/teen-who-hacked-cia-email-is-back-to-prank-us-spy-chief

La NASA piratée par Anonymous

- Récupération (achat?) d'une porte d'entrée à un hackeur
- Prise d'empreinte du réseau pendant des mois
- Exfiltration de 250Go de donnéees : données personnelles, plans de vol, vidéos…
- Prise de contrôle de systèmes dont des NAS
  - Contenant les futurs plans de vol, qu'ils ont modifié

http://www.ibtimes.co.uk/nasa-hack-anonsec-attempts-crash-222m-drone-releases-secret-flight-videos-employee-data-1541254



Nouveautés, outils et techniques

Crypto
Divers

Le point sur SSL/TLS et SHA-1 160 bits

- SHA-1, Firefox fait retour en arrière

  https://blog.mozilla.org/security/2016/01/06/man-in-the-middle-interfering-with-increased-security/

- SHA-1, Edge ne fait plus confiance au certificats développeur au 1er janvier 2016 et serveur au 1er janvier 2017
- Pas d'HTTPS, Chrome = 

  http://www.zdnet.com/article/google-chrome-gets-ready-to-mark-all-http-sites-as-bad/

La NSA augmente ses niveaux de chiffrement

- AES 256, SHA-2 384, RSA 3072
- Et prépare l'ère quantique

  https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

OVH rejoint la liste des sponsors de Let's Encrypt

http://www.linformaticien.com/actualites/id/38941/ovh-rejoint-la-liste-des-sponsors-de-let-s-encrypt.aspx

Récupérer les certificats en PowerShell (comme avec openssl connect)

https://isc.sans.edu/diary/Assessing+Remote+Certificates+with+Powershell/20645

Pentest
Techniques & outils

SMOD 1.0.2, un framework pour auditer ModBus

http://seclist.us/smod-v1-0-2-modbus-penetration-testing-framework.html

Outil d'entraînement à l'injection SQL

https://github.com/himadriganguly/sqlilabs

Contourner les mécanismes à "rolling code"

- Utilisé dans les voitures, portails et portes de garages

http://andrewmohawk.com/2016/02/05/bypassing-rolling-code-systems/

AuthMatrix v0.4

- Plugin Burp pour tester le cloisonnement entre utilisateurs

https://github.com/SecurityInnovation/AuthMatrix

Inveigh

- Responder-like en PS

https://github.com/Kevin-Robertson/Inveigh

Pentest
Techniques & outils

Outil d'extraction de base de données à partir de Blind SQLi

https://github.com/nbshelton/bitdump

Keylogger pour Keepass

- Contourne les protections du presse-papier

http://www.sinfocol.org/2016/02/keepasslogger-keepass-two-channel-auto-type-obfuscation-bypass/

Framework de phishing open-source

https://getgophish.com/

Télécharger Mimikatz depuis Github et l'exécuter en mémoire

https://gist.github.com/subTee/7e3f8979eafbe65d63e2

Les AV n'aiment pas Office 2003

- Une attaque via intégration de document XML détectée sous Office 2007+
- Passe inaperçu (0/57) en enregistrant au format 2003

http://randorisec.fr/word-2003-xml-another-trick-to-bypass-anti-virus/

Crowbar, brute force sur openvpn, rdp, sshkey, vnckey

http://seclist.us/crowbar-v3-4-is-a-brute-force-tool-which-is-support-openvpn-rdp-sshkey-vnckey.html

Nouveautés (logiciel, langage, protocole...)
Open Source

Mimikatz ne laisse plus d'artefact lors de la création d'un Golden Ticket

- Précédemment : "eo.oe.kiwi :)" puis "<3 eo.oe ~ ANSSI E>"

  https://github.com/gentilkiwi/mimikatz/blob/master/mimikatz/modules/kerberos/kuhl_m_kerberos.c

```
@@ -586,7 +599,7 @@ PDIRTY_ASN1_SEQUENCE_EASY kuhl_m_kerberos_golden_data(LPCWSTR username, LPCWSTR
586 599         KIWI_NEVERTIME(&validationInfo.PasswordLastSet);
587 600         KIWI_NEVERTIME(&validationInfo.PasswordCanChange);
588 601         KIWI_NEVERTIME(&validationInfo.PasswordMustChange);
589     -       RtlInitUnicodeString(&validationInfo.LogonDomainName, L"<3 eo.oe ~ ANSSI E>");
    602 +       RtlInitUnicodeString(&validationInfo.LogonDomainName, LogonDomainName);
```

- amélioration de l'extraction des données du "vault"
- Possibilité de "compresser" Mimikatz pour occuper moins d'espace disque

Qubes Windows Tools en OpenSource

https://www.qubes-os.org/news/2016/01/27/windows-tools-open-source/

Mac OS X, auditez et durcissez votre configuration

https://github.com/SummitRoute/osxlockdown

PowerSCCM

- Module PS pour intéragir avec une base de données SCCM

  http://seclist.us/powersccm-powershell-module-to-interact-with-sccm-databases-for-both-offensive-defensive-applications.html

Nouveautés (logiciel, langage, protocole...)

Divers

EMET 5.5 Final

- Support de Windows 10, meilleures performances, amélioration des GPO

  https://www.microsoft.com/en-us/download/details.aspx?id=50766

- Mettez vite à jour, on trouve des .doc avec contournement de la version précédente d'EMET

  http://casual-scrutiny.blogspot.in/2016/02/cve-2015-2545-itw-emet-evasion.html

Journaliser la sortie console de PowerShell via GPO

https://4sysops.com/archives/log-powershell-command-outputs-with-group-policy/

VirusTotal supporte le scan de firmware

http://blog.virustotal.com/2016/01/putting-spotlight-on-firmware-malware_27.html

Suricata 3.0 !

https://redmine.openinfosecfoundation.org/versions/80

Cuckoo sandbox 2.0 RC1

https://cuckoosandbox.org/2016-01-21-cuckoo-sandbox-20-rc1.html

Nouveautés (logiciel, langage, protocole...)

Divers

Kit d'inforensique pour Android

http://blog.elcomsoft.com/2016/01/forensic-acquisition-android/

Forensic en PowerShell

https://github.com/davidhowell-tx/PS-WindowsForensics

Forensic en Powershell 2

https://github.com/Invoke-IR

Outil de visualisation des Prefetch Windows, supportant Windows 8 et 10

http://binaryforay.blogspot.fr/2016/01/windows-prefetch-parser-in-c.html

Comment se protéger des exploitations en PowerShell ?

- Activer et superviser certains évènements Windows spécifiques

  http://www.redblue.team/2016/01/powershell-traceless-threat-and-how-to.html

Une autre façon d'enregistrer les frappes clavier sous Windows

- Avec des callback, car les keylogger classiques avec boucle consomment beaucoup de CPU

  http://www.patch-tuesday.net/2016/01/scripting-windows-key-logger.html

Business et Politique

Business
France

Oceanet acquière NBS

- Oceanet, spécialiste de l'hébergement Windows, acquière NBS / No Blue Screen System

  http://www.oceanet-technology.com/blog/post/29-rapprochement-groupe-oceanet-technology-nbs-system

Orange et Bouygues Telecom discutent d'un rapprochement

http://www.lemonde.fr/economie/article/2016/01/04/orange-bouygues-telecom-la-fusion-avance_4841254_3234.html

http://www.begeek.fr/confessions-patron-dorange-rachat-de-bouygues-telecom-190949

http://live.lesechos.fr/57/021597005057.php

Carrefour arrête son site marchant

http://www.journaldunet.com/ebusiness/commerce/1170394-carrefour-s-apprete-a-debrancher-son-site-marchand-carrefour-online/

Les managers français sont parmi les plus mauvais

- Mou, pas d'objectif ou pas clair, pas d'autorité, petits-chefs...

  http://www.lemonde.fr/economie/article/2007/12/10/les-managers-francais-sont-parmi-les-plus-mauvais_987814_3234.html

Business
France

Le Privacy Shield remplacerait le Safe Harbor

- Accord de principe sur le transfert de données personnelles

  http://www.zdnet.fr/actualites/du-safe-harbor-au-privacy-shield-de-reels-progres-ou-blanc-bonnet-bonnet-blanc-39832094.htm

Business
International

Patent Troll, Apple paiera $625 millions à VirnetX

http://pro.clubic.com/legislation-loi-internet/propriete-intellectuelle/actualite-794696-brevets-apple-devra-payer-virnetx-625-dollars.html

Google a payé $1 milliard à Apple pour garder sa barre de recherche

- En 2014

  http://www.bloomberg.com/news/articles/2016-01-22/google-paid-apple-1-billion-to-keep-search-bar-on-iphone

Licenciements

- STMicro suppression de 1400 emplois (430 en france)
- VMware (5% des effectifs)
- VCE (12%)
- Toshiba (entre 6000 et 7000)
- GoPro (7% des effectifs)

Droit / Politique

France

Décret n° 2015-1912 du 29/12/2015 sur les agents contractuels de la fonction publique territoriale (Donc ANSSI)

- Non titulaires de droit public -> contractuels de droit public
- Entretien professionnel annuel
- Indemnité compensatrice en cas de congés non pris en fin de CDD ou licenciement
- Licenciement possible

https://priscillafontainerh.wordpress.com/2016/01/18/analyse-detaillee-du-decret-2015-1912-concernant-les-contractuels-de-la-fpt/

Un système d'exploitation souverain ?

http://www.nextinpact.com/news/98243-un-systeme-d-exploitation-souverain-il-y-a-comme-os.htm

- L'ANSSI n'est pas forcement pour

http://mobile.lemonde.fr/pixels/article/2016/01/25/le-responsable-de-la-securite-informatique-de-l-etat-fustige-le-projet-d-os-souverain_4853380_4408996.html

Un clavier souverain ?

- Basé sur le BEPO ?

http://www.nextinpact.com/news/98108-le-ministere-culture-veut-clavier-azerty-french-touches.htm

Amendement (souverain) **pour interdire les liens hypertexte dans consentement de l'auteur**

http://www.journaldugeek.com/2016/01/20/deputes-ps-interdiction-liens-hypertextes/

Droit / Politique

France

CNIL, plafond des amendes passé à 20 millions d'euros

http://www.nextinpact.com/news/98192-loi-numerique-cnil-pourra-infliger-amendes-20-millions-d-euros.htm

Pour lutter contre la fraude, les logiciels de caisse devront être certifiés

- A partir de 2018, allant d'une simple mise à jour à un changement complet

https://www.service-public.fr/professionnels-entreprises/actualites/A10279

Rapport parlementaire sur la CyberSécurité

- Enfin une prise de conscience ?

http://www.publicsenat.fr/lcp/politique/un-rapport-parlementaire-se-penche-cybersecurite-des-entreprises-1198420

Négociations entre l'ANSSI et les OIV

http://www.silicon.fr/cybersecurite-grandes-entreprises-trouvent-modus-vivendi-anssi-136930.html?PageSpeed=noscript

Droit / Politique
International

USA : le premier système d'arme numérique certifié pleinement opérationnel (FOC)

http://www.afspc.af.mil/news1/story.asp?id=123467152

L'employeur peut regarder les communications de ses employés

- Usage des moyens de l'entreprise à titre personnel toléré tant que raisonnable

  http://www.lesechos.fr/politique-societe/societe/021616561145-lemployeur-peut-surveiller-les-communications-de-ses-employes-1192222.php

Conférences

Conférences

Texte en gris = déjà traité précédemment

Passées

- FIC - 25 et 26 janvier 2016 à Lille
- CORI&IN - 27 janvier 2016 à Lille

A venir

- JSSI - 8 mars 2016 à Paris
- Insomni’hack - 17 et 18 mars 2016 en Suisse
- GSDays - 7 avril 2016 à Paris
- Conférence du Clusif - 13 avril à Paris

Divers / Trolls velus

Divers / Trolls velus

Spécial FIC 2016

Quand Cyril Bruder tente d'aller au FIC

à	"cyrilbruder@orange.fr" <cyrilbruder@orange.fr>
date	19/01/16 19:59
objet	[FIC2016]

créer une alerte SMS

Bonsoir,

Je me permets de vous contacter au sujet de votre inscription. Nous serons ravis de vous accueillir au FIC2016 mais nous ne pouvons pas laisser l'intitulé que vous avez renseigné - LICENCIE DU CREDIT AGRICOLE CARDS & PAYMENTS (POUR COUVRIR LES MAGOUILLES DU CERT CREDITAGRICOLE) / Lanceur d'alertes - sur votre badge.

Nous sommes à votre disposition pour tout changement.

Cordialement,

ceis

Hugo Lemarchand
Consultant en Cybersécurité et Management des risques
+33 6 09 78 41 01 / +33 1 45 55 92 47
Notes stratégiques : L'entrainement cyber : un élément clé pour améliorer la resilience – Monnaies virtuelles et cybercriminalité
Actualités : secuinsight.fr - forum-fic.com
Suivez-nous : LinkedIn and Twitter

FIC 2016 — 8e FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ — DATA SECURITY & PRIVACY — 25 & 26 JANVIER 2016 — LILLE GRAND PALAIS

Forensics Slut Retweeted

FIC 2016 @FIC_fr · 19h

View translation

@cyrilbruder Nous avons proposé de discuter. Vous avez décidé de nous afficher. Au #FIC2016, vous êtes refusé.
#PasDeBrasPasDeChocolat

7 6

View conversation

Divers / Trolls velus

Spécial FIC 2016

Quand 2 jeunes découvrent une vulnérabilité sur le site du FIC

- Et finissent au poste pour avoir été un peu trop pressé à communiquer publiquement

  http://www.01net.com/actualites/ils-notifient-une-faille-sur-un-site-web-puis-recoivent-la-visite-des-gendarmes-945669.html

Nouveautés au CES

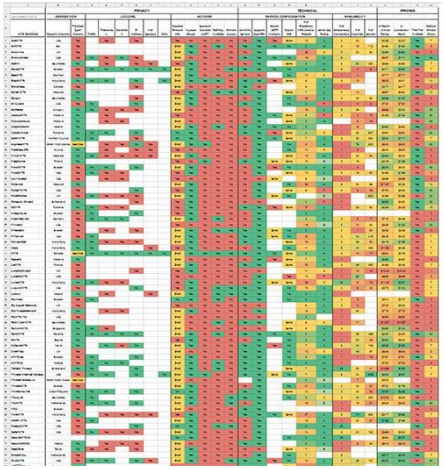
Craintes au FIC

Divers / Trolls velus

Quel VPN choisir ?

- Comparaison de 115 services de VPN

  https://docs.google.com/spreadsheets/d/1FJTvWT5RHFSYuEoFVpAeQjuQPU4BVzbOigT0xebxTOw/htmlview?usp=sharing&sle=true



iOS, encore plusieurs clefs de déchiffrement

- iOS 9.2.1 pour iPhone 5, 5C, 5S

  https://www.theiphonewiki.com/wiki/Firmware_Keys

Connaissez-vous tous les modes de traitement des algorithmes de chiffrement par bloc ?

- ECB, CBC, CFB… c'est pour les looser !
- Essayez plutôt LSD (Layered Subset Difference) 😇

Oracle, fin du plugin Java

https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free

Divers / Trolls velus

Et voici arriver le “transpileur”, convertissant du Python non typé en C++ 14

https://github.com/lukasmartinelli/py14/blob/master/README.md

Cellebrite, une offre d’emploi limpide

- [...] looking for a talented Security Researcher and Reverse Engineer
- [...] mobile phones, [...] Seek and exploit vulnerabilities;
- 1337 skills – must
- Military intelligence elite courses (you know and we know)

http://www.cellebrite.com/Careers/security-researcher-reverse-engineer-jb-256

Wikipedia bloque une IP du ministère de l’Intérieur pour cause de vandalisme

http://rue89.nouvelobs.com/blog/les-coulisses-de-wikipedia/2016/01/13/non-wikipedia-na-pas-banni-le-ministere-de-linterieur-235177

L'intelligence artificielle de Google, DeepMind, bat l’humain au jeu de GO

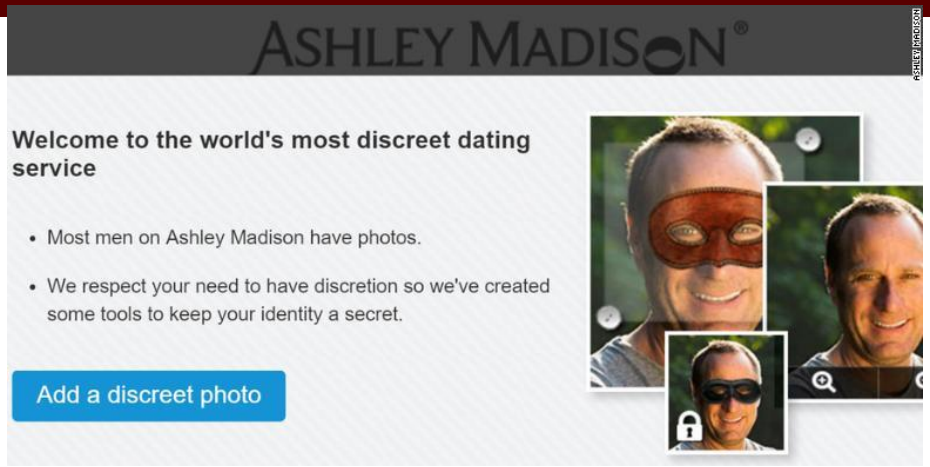
- Après les échecs, le GO… que nous reste-t-il ?

https://xcorr.net/2016/02/03/5-easy-pieces-how-deepmind-mastered-go/

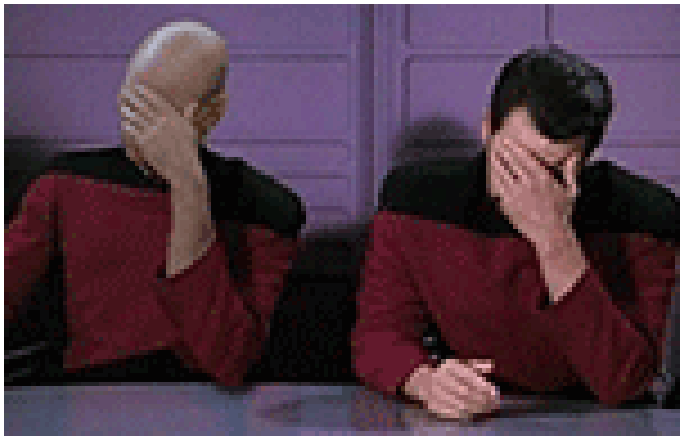
Divers / Trolls velus

Ashley Madison est de retour

- Avec une option d'anonymisation
- Et oui : ils existent toujours !!?



Domaine de premier niveau .Security / TLD



Divers / Trolls velus

La NSA explique comment se protéger... de la NSA

- Intervention du directeur de la TAO
  1. Prise d'empreintes
  2. Exploitation
  3. Persistance
  4. Installation d'outils
  5. Mouvements latéraux
  6. Collecte, exfiltration de données

  https://www.youtube.com/watch?v=bDJb8WOJYdA

Follow the White rabbit…

- Enchaînement de recherches exotiques et leet sur Google = test de recrutement !

  http://www.01net.com/actualites/comment-un-ingenieur-s-est-fait-drague-par-google-via-son-moteur-de-recherche-910133.html

Améliorer le temps de chargement des pages web

- En chargeant Jquery depuis l'interface web des routeurs :)

  https://twitter.com/dbloom/status/695477117576843264/photo/1

Divers / Trolls velus

RoundCube Mail : Pensez-vous que quelqu'un a changé la clef ?

https://github.com/roundcube/roundcubemail/blob/master/config/config.inc.php.sample#L73-L77

```
73  // this key is used to encrypt the users imap password which is stored
74  // in the session record (and the client cookie if remember password is enabled).
75  // please provide a string of exactly 24 chars.
76  // YOUR KEY MUST BE DIFFERENT THAN THE SAMPLE VALUE FOR SECURITY REASONS
77  $config['des_key'] = 'rcmail-!24ByteDESkey*Str';
```

Blizzard ajoute des watermark dans les screenshot fait sur World of Warcraft

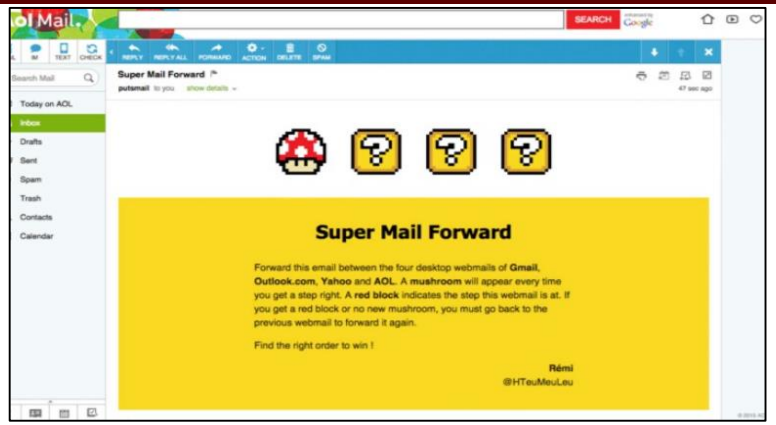
http://www.ownedcore.com/forums/world-of-warcraft/world-of-warcraft-general/375573-looking-inside-your-screenshots.html

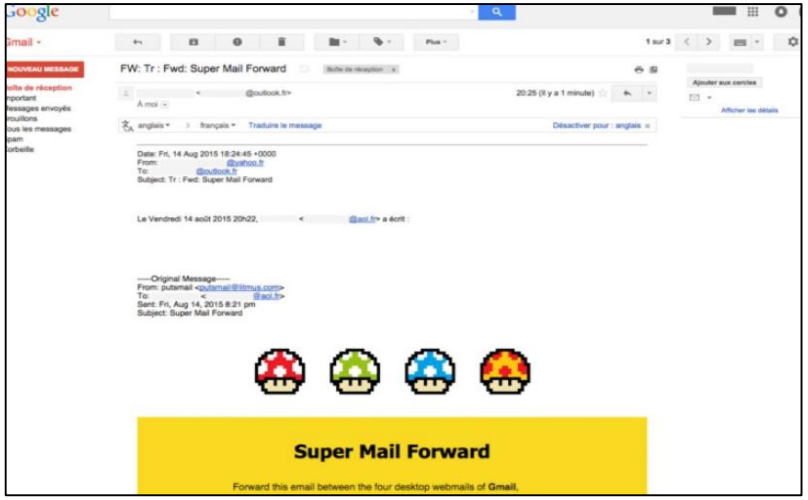
Divers / Trolls velus

Un email qui évolue au rythme de ses transferts

- Avec du CSS

  https://medium.com/@hteumeuleu/super-mail-forward-an-email-that-evolves-as-you-forward-it-84466596f30d#.ycikr9k4f





Prochains rendez-vous de l’OSSIR

Prochaines réunions

- Mardi 12 Avril 2016

After Work

- Mardi 31 Mai 2016

JSSI 2016

- Mardi 8 Mars 2016
- Programme en ligne

JSSI 2016

- Mardi 8 Mars 2016
- Programme en ligne
- Inscriptions ouvertes

http://www.ossir.org/jssi/index/jssi-2016.shtml

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous