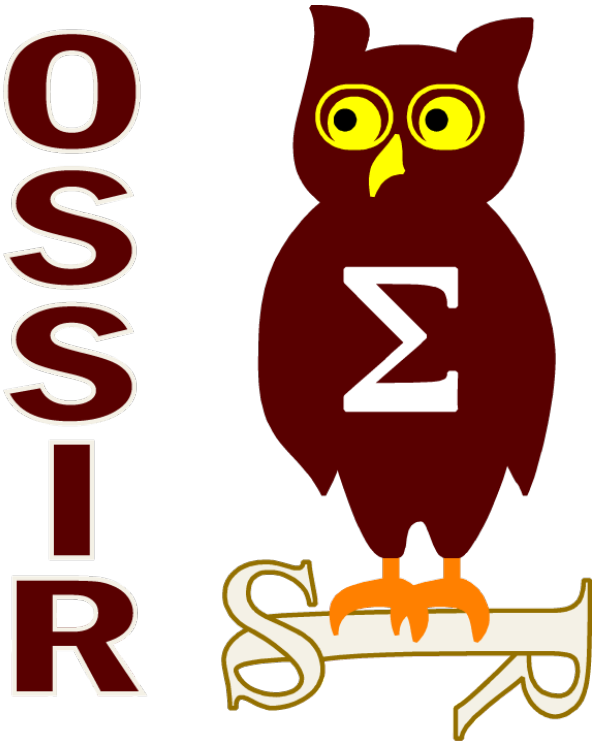


Groupe Paris

Réunion du 13/05/2014

Arnaud SOULLIE
Vladimir KOLLA
Jean-Philippe GAULIER
Ary KOKOS

Failles / Bulletins / Advisories
Microsoft - Avis Avril 2014

- **MS14-017 Vulnérabilité dans Microsoft Word et Office Web Apps** (3 CVE) [Exploitabilité 1]
  - Affecte:
    - Microsoft Office (toutes versions supportées)
    - Donc également Office 2013 RT et Office 2011 pour Mac
    - Word Viewer, donc Outlook utilisant cette visionneuse par défaut
    - SharePoint Server 2013 (Word Automation Services)
  - Exploit:
    - Exécution de code à l'ouverture d'un RTF spécialement formaté
    - Exploité publiquement dans la nature
      http://krebsonsecurity.com/2014/03/microsoft-warns-of-word-2010-exploit/
  - Crédits:
    - Will Dormann / CERT/CC (CVE-2014-1757)
    - Yuhong Bao (CVE-2014-1758)
    - Drew Hintz, Shane Huntley, and Matty Pellegrino / Google Security Team (CVE-2014-1761)

- **MS14-018 Vulnérabilités dans Internet Explorer** (6 CVE) [Exploitabilité 1]
  - Affecte: Internet Explorer (toutes versions supportées... et non supportées ^_^)
  - Exploit:
    - Corruption de mémoire aboutissant à une exécution de code à l'ouverture d'une page Web spécialement formatée
    - Nouveau "dernier" patch pour Windows XP ;-)
  - Crédits:
    - Anonymous par ZDI(CVE-2014-0235)
    - Dr. Bo Qu / Palo Alto Networks (CVE-2014-1751, CVE-2014-1752)
    - Yuki Chen / Trend Micro par ZDI (CVE-2014-1753)
    - 096dc2a463051c0ac4b7caaf233f7eff et AMol NAik par VeriSign iDefense Labs (CVE-2014-1755)
    - Abdul-Aziz Hariri / ZDI (CVE-2014-1760)

Failles / Bulletins / Advisories
Microsoft - Avis Avril 2014

- **MS14-019 Vulnérabilité dans Windows File Handling** (1 CVE) [Exploitabilité 1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - Exécutions de code à l'ouverture d'un .bat ou .com spécialement formaté
    - Nouveau "dernier" patch pour Windows XP ;-)
  - Crédits:
    - Stefan Kanthak par Microsoft (CVE-2014-0315)

- **MS14-020 Vulnérabilité dans Microsoft Publisher** (1 CVE) [Exploitabilité 1]
  - Affecte: Microsoft Publisher 2003 SP3 et 2007 SP3
  - Exploit: Exécutions de code à l'ouverture d'un fichier Publisher spécialement formaté
  - Crédits:
    - Anonymous par VeriSign iDefense Labs (CVE-2014-1759)

Failles / Bulletins / Advisories
Microsoft

Advisories

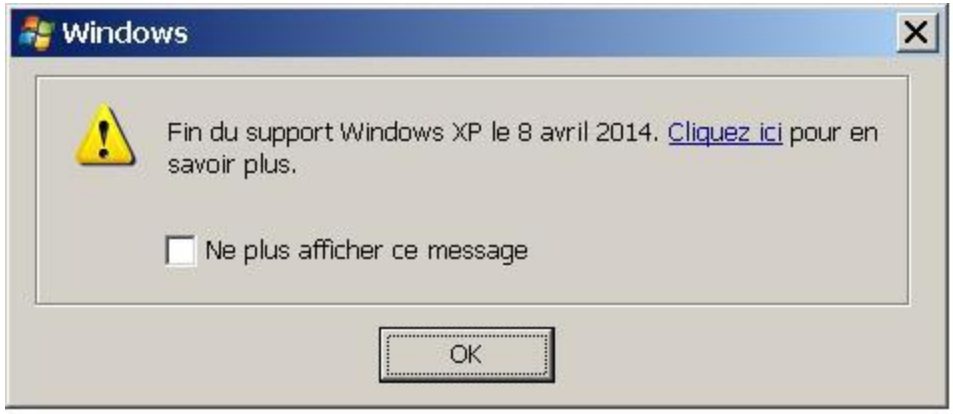
- **2962393**
  - v1.0 Mise à jour du client Juniper Pulse (VPN SSL) pour Windows 8.1 et 8.1 RT

Hors Bande

- **MS14-021 Vulnérabilités dans Internet Explorer** (1 CVE) [Exploitabilité 1]
  - Affecte: Internet Explorer (toutes versions supportées) sauf Server Core
  - Exploit : Exécutions de code à l'ouverture d'une page Web spécialement formaté
  - Crédits: FireEye, Inc. (CVE-2014-1776)

Microsoft OneDrive modifie vos fichiers de sauvegarde en secret

- http://thehackernews.com/2014/04/microsoft-onedrive-secretly-modifies.html



Failles / Bulletins / Advisories
Réseau

Cisco

Beaucoup de failles dont :

- XSS sur les caméras de surveillances « Dome », Cisco Unity Connection…
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0673
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2125
- Contournement des règles de sécurité sur les Firewalls ASA (Pas simple à exploiter)
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0738
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0739
- Déni de service sur les Firewalls ASA par des messages DHCPv6 et SIP
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2182
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2182
- Déni de service sur les Nexus-OS
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0739
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0677
- Déni de service sur les VPN monté par Cisco IOS, durant la phase d'échange des clefs (IKE)
  - http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143
- Et quelques-unes sur les switchs Huawei également
  - http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-334629.htm

Failles / Bulletins / Advisories
Réseau

Divers

- **Routeur Soho Linksys** (Mais aussi Cisco, Netgear et Diamond)
  - La backdoor TCP 32764 toujours présente -> une honte !
  - En janvier, découverte d'une backdoor avérée

    http://thehackernews.com/2014/01/hacking-wireless-dsl-routers-via.html

    https://github.com/elvanderb/TCP-32764
  - Correctif… avec la même backdoor mais cachée http://thehackernews.com/2014/04/router-manufacturers-secretly-added-tcp.html
  - Activable par du port knocking

Failles / Bulletins / Advisories
Divers

VMWare

- **VMSA-2014-0004.7**
  - Heartbleed

- **VMSA-2014-0003**
  - Exécution de code sur le client vSphere avec la possibilité de pousser une mise à jour sans vérification de la source
  - Man in the Middle SSL entre le client vSphere et ses seveurs, par une erreur de validation des certificats X509

Failles / Bulletins / Advisories
Open Source

Qemu

- **Toutes versions**
  - Déni de service (CVE-2014-0150, CVE-2014-0142, CVE-2014-0146, CVE-2014-0148)
  - Integer overflow avec exécution de code pouvant aller à la prise de contrôle totale
  - http://git.qemu.org/?p=qemu.git;a=commitdiff;h=edc243851279e3393000b28b6b69454cae1190ef;hp=21e2db72601c48fa593ef7187faf17f324d925c5

Ubuntu

- **Passer l'écran de vérouillage d'Ubuntu**
  - En laissant simplement la touche [Entrée] enfoncée
  - https://bugs.launchpad.net/ubuntu/+source/unity/+bug/1308572

OAuth et OpenID

- **Vulnérabilité**
  - Réécriture du paramètre redirect_uri permettant de rediriger vers un site malveillant.
    http://tetraph.com/covert_redirect/oauth2_openid_covert_redirect.html
    http://www.youtube.com/watch?v=HUE8VbbwUms#t=109

Failles / Bulletins / Advisories
Divers

Oracle

- **30 failles Oracle Java (Cloud Java d'Oracle)**
  - Oracle contacté sur ces failles par des chercheurs de la société Polonaises Security Explorations
  - 2 mois de mutisme côté Oracle
  - Publication de codes d'exploitations

    http://www.networkworld.com/news/2014/040214-researchers-publicly-disclose-vulnerabilities-in-280317.html

- **Java**
  - 37 failles corrigées
  - Dont 4 qui méritent le score CVSS parfait de 10 (Compromission totale à distance sans authent)
    http://krebsonsecurity.com/2014/04/critical-java-update-plugs-37-security-holes/

- **Google Chrome : 31 vulnérabilités, dont 19 critiques**

  http://threatpost.com/google-patches-31-flaws-in-chrome/105326

- **Un mot de passe par défaut laisse les usagers d'optus à découvert**

  http://www.smh.com.au/it-pro/security-it/default-password-leaves-tens-of-thousands-of-optus-cable-subscribers-at-risk-20140403-zqprz.html

Failles / Bulletins / Advisories
Divers

Terminaux de communication par satellite

- **Audit du code par IOActive**
  - Des failles trivialles :
    - Mot de passe en dur dans le binaire ;
    - Protocoles comprenant des failles ;
    - Portes dérobées / Backdoor

    http://magazine.qualys.fr/menaces-alertes/communications-satellite-vulnerables/
  - << on en viendrait presque à penser que toute industrie qui produit du code sans craindre l'audit applique par défaut l' ensemble du répertoire des mauvaises pratiques de sécurité !>>

Vendor	Product	Vulnerability Class	Service	Severity
Harris	 RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	 9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	 ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	 EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical

Failles / Bulletins / Advisories
Crypto

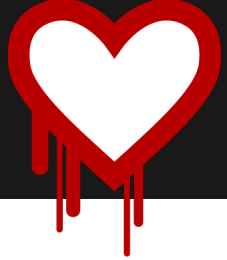
Stong Swan

- **Strong Swan = VPN IPSec de Linux, Android, FreeBSD et Mac OS X**
  - Renégociation
  - En visant un Strong Swan n'ayant pas encore monté son VPN
    http://www.strongswan.org/blog/2014/04/14/strongswan-authentication-bypass-vulnerability-%28cve-2014-2338%29.html

OpenSSL Rampage

- **Site référençant les pires commit d'OpenSSL ;-)**
  - Maintiennent du code pour Visual C++ 5
  - support de big-endian sur x86
  - ...
    http://opensslrampage.org/

Failles / Bulletins / Advisories
Crypto



Reparlons d'HeartBleed

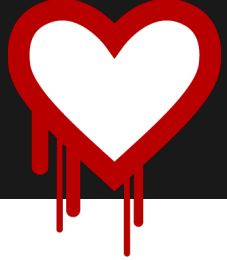
- Récupération de la clé privée : c'est possible, c'est prouvé et c'est outillé
- La révocation des certificats n'empêche pas l'interception des données
- Vous allez casser Internet en activant la vérification des certificats
  - Révocation massive des certificats (~ 50k chez Cloudfar) = croissance des tailles des CRL
    - Téléchargées régulièrements par les navigateurs
  - Certains prédisent que cela va ralentir Internet de manière importante
- Il n'y a pas que les serveurs web de touchés
  - Tout ce qui utilise OpenSSL, cf slide suivant
- Le site du FISC québécois a subi une attaque via heartbleed
  - L'auteur présumé a été arrêté
- la CNIL s'en mèle

  http://www.cnil.fr/linstitution/actualite/article/article/faille-de-securite-heartbleed-comment-reagir/

  "Tout responsable de traitement mettant en œuvre une version vulnérable d'OpenSSL doit donc :
  - mettre à jour les serveurs vulnérables, afin de ne plus utiliser de version affectée par la faille ;
  - révoquer les clés et certificats utilisés ;
  - renouveler les clés et mettre à jour les certificats correspondants ;
  - conseiller aux utilisateurs de renouveler leurs moyens d'authentification, notamment leurs mots de passe."

  "La CNIL vérifiera les mises à jour et correctifs de sécurité dans le cadre des contrôles qu'elle opère régulièrement auprès des responsables de traitement. Elle sera en mesure de procéder à une série de contrôles visant spécifiquement les sites les plus exposés qui ne se seraient pas mis en conformité. "

Failles / Bulletins / Advisories
Crypto



Reparlons d'HeartBleed

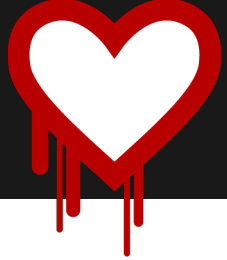
- Quelques avis d'éditeurs
  - BlackBerry delivre un correctif pour BBM Messenger
    http://www.zdnet.com/blackberry-to-release-heartbleed-fixes-for-bbm-messenger-secure-work-space-7000028390/#ftag=RSSf468ffe
  - Cisco, Juniper, OpenVPN, Checkpoint, Watchguard…
    https://isc.sans.edu/diary/Heartbleed+vendor+notifications/17929
  - IBM (Liste Trèèèèèèèès longue)
    https://www-304.ibm.com/connections/blogs/PSIRT/entry/openssl_heartbleed_cve_2014_0160?lang=en_us
  - VMWare (voir précédement)
  - Les relais TOR sont vulnérables à HeartBleed
    http://www.net-security.org/secworld.php?id=16708
  - Mais aussi des équipements réseau, des concentrateurs VPN, des imprimantes, des serveurs mails supportant TLS, certaines webcam, des logiciels...

- **Les navigateurs sont épargnés**
  - Car les librairies de chiffrements sont différentes
  - Sauf pour les téléphones Android en version 4.1.1 ;-)

- **Il n'y a pas QUE Heartbleed : autres bugs sur SSL**
  http://armoredbarista.blogspot.de/2014/04/easter-hack-even-more-critical-bugs-in.html

- **L'équipe d'OpenBSD forke OpenSSL pour créer LibreSSL**
  http://www.zdnet.fr/actualites/heartbleed-l-equipe-d-openbsd-forke-openssl-pour-creer-libressl-39800227.htm

Failles / Bulletins / Advisories
Crypto



Reparlons d'HeartBleed

- **La NSA aurait eu connaissance de la faille HeartBleed depuis… 2 ans et l'aurait exploité**
  http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html
  - Contre des criminels ?
    http://www.01net.com/editorial/618984/heartbleed-utilisee-contre-des-hackers-qui-font-le-commerce-de-donnees-volees/#?xtor=RSS-20
  - Le gouvernement US reconnait « publiquement et officiellement » utiliser des 0-days
    http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

- **Les contradictions de Heartbleed**
  http://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

- **Accès aux télévisions Smart TV de Philips**
  - Wifi ouvert avec une clef codée en dur et diffusée publiquement (« Miracast », du nom de la fonctionnalité de la télé)
    http://thehackernews.com/2014/03/philips-smart-tvs-vulnerable-to-screen_29.html

- **Target**
  - Démission de la vice-présidente exécutive en charge des technologies et de la direction des systèmes d'information
  - Un bel exemple, que les RSSI peuvent mettre dans leurs escarcelles face au COMEX et DSI ;-)
    http://www.silicon.fr/piratee-dsi-target-demissionne-93104.html

- **Casser les captcha avec des humains**
  http://skipinput.com/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

- **Exploitation d'une faille sur des machines à sous**
  - Les casinos se retournent contre le constructeur pour être rembourser des pertes
  - Les gens ayant exploité la faille ne seront pas poursuivi car ils n'ont pas vraiment piraté les machines à sous
    http://www.lefigaro.fr/international/2014/04/14/01003-20140414ARTFIG00272-une-faille-informatique-fait-sauter-la-banque-de-plusieurs-casinos.php

- **Déni de service sur un réseau GSM avec un simple appel**
  http://www.01net.com/editorial/618678/faire-planter-un-reseau-mobile-national-cest-simple-comme-un-coup-de-fil/

Piratages, Malwares, spam, fraudes et DDoS
Hack / sites piratés

- **La chaîne de magasins « Michaels » touchée par une attaque sur les PoS**
  - 3 millions de n° CB dérobés
    http://www.darkreading.com/attacks-breaches/michaels-retail-chain-reveals-details-of-breach-nearly-3m-affected/d/d-id/1204585

- **La boutique en ligne de Lacie piratée ?**
  http://nakedsecurity.sophos.com/2014/04/16/hardware-maker-lacie-admits-to-year-long-credit-card-breach
  http://krebsonsecurity.com/2014/04/hardware-giant-lacie-acknowledges-year-long-credit-card-breach/

- **Site web de l'ASECNA, utilisé pour du phishing**
  http://news.netcraft.com/archives/2014/04/04/aero-air-safety-site-hijacked.html

- **Accès en lecture sur les serveurs de Google**
  http://blog.detectify.com/post/82370846588/how-we-got-read-access-on-googles-production-servers

- **Service AOL mail piraté**
  http://blog.trendmicro.com/trendlabs-security-intelligence/aol-mail-service-hacked-compromised-emails-used-to-send-spam/

- **Fuite de données chez France Info**
  http://www.nextinpact.com/news/87308-fuite-donnees-personnelles-chez-france-info-adresse-ip-mail-navigateur.htm

- **Piratage de bit.ly**
  http://blog.bitly.com/#85169217199

Piratages, Malwares, spam, fraudes et DDoS
Malwares

- **Sauvons les petits Panda de la noyade**
  - Un malware iOS a récemment été identifié, infecte les terminaux jailbreakés
  - « hooke » les fonctions de chiffrement SSL
  - Récupére les identifiants et mots de passe Apple et les envoie vers deux adresses IP
    http://nakedsecurity.sophos.com/2014/04/21/new-ios-malware-with-a-funky-name-unflod-baby-panda/

- **Binaire Zeus signé par un certificat légitime**
  - Certificat d'Isonet AG, attribué par Verisign et surement volé
  - http://www.isonet.de/en/services : << isonet ag offers a wide range of complementary services on the topic of IT.>> ;-)
    https://blogs.comodo.com/e-commerce/comodo-av-labs-id-zeus-trojan/

Piratages, Malwares, spam, fraudes et DDoS
DDoS

- **Attaque par DDoS par injection d'un script dans le navigateur (XSS)**
  - Publication d'une « nouvelle » attaque DDoS par l'éditeur de solution anti-DDoS Incapsula
  - Faille XSS sur un site légitime
  - Couplée injecter une JavaScript requêtant sans cesse une cible
    http://www.incapsula.com/blog/world-largest-site-xss-ddos-zombies.html
  - Déjà présenté par XMCO en 2010 dans son « Actu Sécu 25 » ;-)
    http://www.xmco.fr/actusecu.html

- **DDoS avec Facebook**
  - Ajout de balises <img> dans Facebook Notes
  - Possibilité d'éviter que Facebook ne cache le résultat <img src="http://target.com/file?r=1"></img>
    http://thehackernews.com/2014/04/vulnerability-allows-anyone-to-ddos.html
    http://chr13.com/2014/04/20/using-facebook-notes-to-ddos-any-website/

Piratages, Malwares, spam, fraudes et DDoS
Darknet

- **Grams, nouveau moteur de recherche pour TOR**
  http://grams7enufi7jmdl.onion

Crypto

- **TrueCrypt 7.1a ne contiendrait pas de Backdoor**
  - mais des integer overflow, bypass de check au montage d'un volume, mélange d'entier signés et non signés... https://isecpartners.github.io/news/2014/04/14/iSEC-Completes-Truecrypt-Audit.html
  - Cela confirme la certification CSPN par l'ANSSI en 2009 www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/p_32_TrueCrypt_version_6.0a.html

- **Gmail s'intéresse au chiffrement point à point**
  - http://thehackernews.com/2014/04/End-to-End-Encryption-for-Gmail.html
  - Comme d'autres : http://www.ciphercloud.com/products/ciphercloud-for-gmail/

- **Yahoo mets les bouchées cryptographiques doubles**
  - Le support de TLS 1.2 et surtout de PFS
  - Chiffrement des flux entre ses datacenters mais sans détails (DWDM ? Niveau 2? Ipsec?)
  - HTTPS par défaut
  - HSTS, pour dire au navigateur « la prochaine fois que tu te connectes, viens en SSL/TLS »
  - Support du SMTPS http://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo
  - Mais les lois américaines restent ce qu'elles sont et donnent le droit au gouvernement d'avoir accès aux les données hébergées

Scada

<Autopromo>

- **Mise à jour du module « modbusclient » de Metasploit**

</Autopromo>

- **GE se paye Wurldtech**
  http://techcrunch.com/2014/05/09/ge-buys-wurldtech-to-beef-up-internet-of-things-industrial-infrastructure-security/

- **Un quart des systèmes critiques jamais audités …**
  http://www.controleng.com/single-article/control-engineering-2014-cyber-security-study/992cf83959f0b11837250236e375da48.html

- **La segmentation réseau, une protection insuffisante ?**
  Image employée : "*Préférez-vous un masque ou un vaccin ?*"
  http://www.ultra-3eti.com/ultratalk/PLC-Security/

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

- **Le gouvernement Anglais passerait sous Open Office**
  http://www.theguardian.com/technology/2014/jan/29/uk-government-plans-switch-to-open-source-from-microsoft-office-suite

- **Facebook, Google, Twitter, LinkedIn créer une nouvelle base de données : WebScaleSql**
  - Basé sur du MySQL
    http://webscalesql.org/

Nouveautés (logiciel, langage, protocole...)
Sécurité

- **Malware.lu lance son service de scan antivirus multi-agent**
  http://avcaesar.malware.lu/

- **Trustwave publie une mise à jour fonctionnelle de son WAF Mod_security 2.8.0**
  - Mises à jour fonctionelles (JSON, XSS, liste blanche sur les limites de connexion…)
    https://github.com/SpiderLabs/ModSecurity/releases/tag/v2.8.0

- **L'association Phishing Initiative dépasse les 100 000 urls**
  http://blog.phishing-initiative.com/2014/04/100-000.html

- **Utiliser Bitcoin pour détecter des malwares**
  http://hackaday.com/2014/04/11/using-bitcoin-to-detect-malware/
  https://www.bitcoinvigil.com/

- **Désassembleur asm x86 dans le navigateur**
  http://pasm.pis.to/

- **Une banque espagnole permet de s'authentifier via Facebook**
  http://www.nfcworld.com/2014/05/07/328941/caixabank-integrates-bank-accounts-facebook/

- **Un stagiare de Facebook analyse les certificats SSL forgés**
  - 0,2% d'interception
  - Principalement des équipements de sécurité

  https://www.linshunghuang.com/papers/mitm.pdf

Nouveautés (logiciel, langage, protocole...)
Sécurité

- **Internet Explorer, pas mauvais pour detecter les URL frauduleuses**
  - Selon le NSS Labs
    https://www.nsslabs.com/reports/browser-security-comparative-analysis-report-socially-engineered-malware

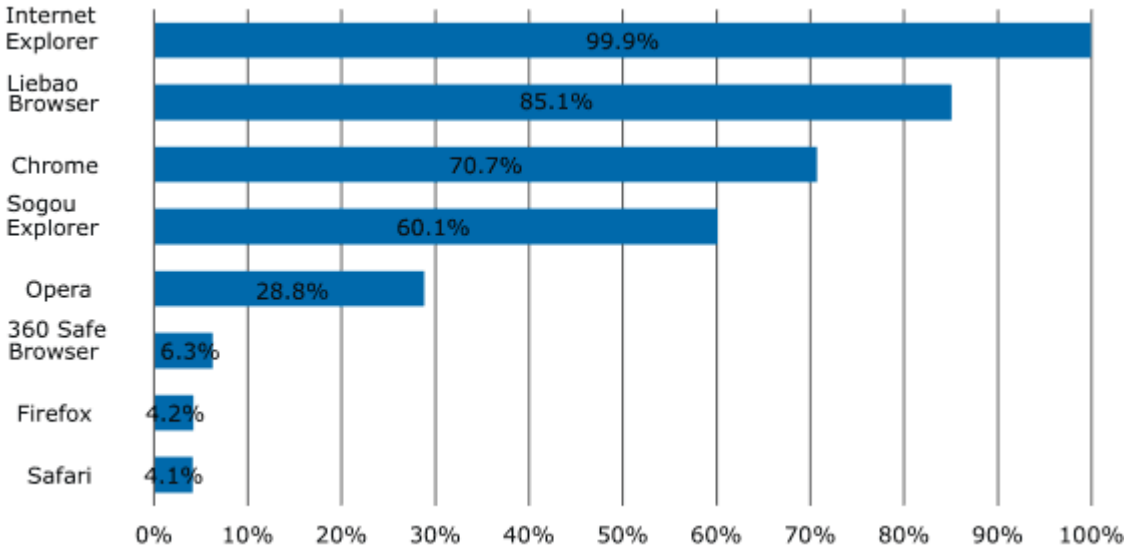


Figure 1 – Average Block Rate for SEM

Nouveautés (logiciel, langage, protocole...)
Réseau

- **Fin du cuivre pour les nouveaux logements à partir de 2016, pour Orange**
  https://lafibre.info/ftth-la-fibre-optique-gpon-ou-p2p/fin-cuivre-nouveaux-logements/

GNU Hacking (DIY)
Tools

- **Burp 1.6**
  - Copier une requête http directement en requête curl
  - Support de l'extension Firefox Plug-n-hack
  - Installation facile des extensions users
  - Accès à TOR
    http://releases.portswigger.net/2014/04/v16.html

- **OWASP ZAP 2.3.0**
  - Scan Policy
  - Plus d'API supportées
  - Nouvelles options UI
  - Plus de règles de scan
    https://code.google.com/p/zaproxy/wiki/Downloads?tm=2

- **Blackarch Linux, distribution pour audit de sécurité logique (pentest)**
  - 150 outils supplémentaires
    http://www.blackarch.org/

- **Tail 1.0**
    https://tails.boum.org/news/version_1.0/
  - La version 1.1 sera elle sur Wheezy (Debian 7)

GNU Hacking (DIY)
Tools

- **Un outil de test de charge http**
  https://github.com/tsenart/vegeta

- **Capstan pour gérer des machines virtuelles**
  http://osv.io/blog/blog/2014/04/03/capstan/

- **Un nouvel outil de trouble shooting**
  http://www.sysdig.org/

Bancaire

- **La BNP (UkrSibbank) stoppe ses activitées en Crimée**
  http://www.lesechos.fr/entreprises-secteurs/finance-marches/actu/0203455267492-bnp-paribas-et-credit-agricole-quittent-la-crimee-665944.php
  - Tout comme le Crédit Agricole

Droit / Politique
France

- **Le décret relatif à la création de la Direction générale de la sécurité intérieure a été publié**
  - La DGSI se substitue à la direction centrale du renseignement intérieur (DCRI) et constitue un service actif de la police nationale, relevant de l'autorité directe du ministre. Effective à partir du 15 mai 2014, elle sera ainsi chargée « de rechercher, de centraliser et d'exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation ».
  - L'article 2 du décret n° 2014-445 détaille les missions de la nouvelle direction qui seront de répondre avec efficacité aux exigences opérationnelles de l'analyse thématique, du contre-terrorisme, de la cyber-défense, de l'investigation judiciaire et du soutien technique et linguistique.
    http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000028887486&dateTexte=&oldAction=dernierJO&categorieLien=id
    http://www.gouvernement.fr/gouvernement/direction-generale-de-la-securite-interieure

- **La Réserve Citoyenne Cyberdéfense a enfin son site Internet**
  http://cyber.event-etrs.fr/
  http://www.defense.gouv.fr/reserves/presentation/cyberdefense/le-reseau-de-la-reserve-citoyenne-cyberdefense

- **Une salle « Secret Défense » à l'Assemblée Nationale pour se protéger de la NSA**
  http://www.journaldugeek.com/2014/04/17/salle-secret-defense-assemblee-nationale-nsa/

- **Le domaine public payant, le beurre et l'argent du labeur**
  http://www.nextinpact.com/news/87171-le-domaine-public-payant-beurre-et-argent-labeur.htm

- **Les CNIL réagissent à Prism**
  http://www.nextinpact.com/news/87012-les-cnil-europeennes-reagissent-enfin-a-prism-et-a-surveillance-masse.htm

Droit / Politique
Europe

- **Cyber Europe 2014**
  - L'union Européenne (ENISA) simule la cyberguerre à grande échelle
    http://www.01net.com/editorial/618888/l-union-europeenne-simule-la-cyberguerre-totale/
    http://www.zdnet.fr/actualites/cyber-europe-2014-l-enisa-lance-sa-campagne-de-tests-de-resistance-39800473.htm
    http://www.01net.com/editorial/618888/l-union-europeenne-simule-la-cyberguerre-totale/

- **La Cour Européenne de Justice règlemente le fait que les FAI auront peut-être à bloquer des sites pirates**
    http://www.engadget.com/2014/03/28/eu-rules-isps-may-have-to-block-pirates/

- **La Grande-Bretagne remplace 6 niveau de marquage de protection par 3**
    https://twitter.com/cyberguerre/status/451308563093520384

Droit / Politique
Monde

- **Une nouvelle loi sur la fuite de données au Canada**
  - "Digital Privacy Act", lourdes pénalités en cas de fuite de données
  - $100.000 par utilisateur non prévenu

    http://itsupportblog.tdcnet.ca/privacy-breach-could-cost-millions-under-new-digital-privacy-act

- **YouTube bloque un film sous licence libre sur demande de Sony**

  http://www.pcinpact.com/news/86893-youtube-bloque-film-sous-licence-libre-sur-demande-sony.htm

- **Les États-Unis enterrent-ils la neutralité du net ?**

  http://www.journaldugeek.com/2014/04/24/letats-unis-enterrent-neutralite-internet/

- **Apple, Google, Adobe et Intel versent 324 millions de dollars à leurs employés, pour mettre fin aux poursuites pour entente illégale**

  http://www.developpez.com/actu/70415/Apple-Google-Adobe-et-Intel-versent-324-millions-de-dollars-a-leurs-employes-pour-mettre-fin-aux-poursuites-pour-entente-illegale/

- **Snapchat s'attire les foudres des régulateurs américains**

  Les destinataires seraient en mesure de sauvegarder les images censées s'auto-détruire
  http://www.huffingtonpost.com/2014/05/08/snapchat-disappearing_n_5290101.html?&ncid=tweetlnkushpmg00000046

Conférences

- **Conférences Passées**
  - Hackito Ergo Sum

- **Conférences à venir**
  - SSTIC - 4 au 6 juin 2014 à Rennes
    - Qui a eu ses places ?
    - Compte-rendu à l'OSSIR le 10 juin
  - Hack in Paris - 23 au 27 juin 2014 chez Mickey
  - No Such Con - 19 au 21 novembre 2014 à Paris
  - Bot Conf - 3 au 5 Décembre 2014 à Nantes

Divers / Trolls velus

- **Amazon décompile les applications Android pour y trouver les clefs secrètes AWS**
  http://blog.rajbala.com/post/81038397871/amazon-is-downloading-apps-from-google-play-and

- **Malware chez GitHub ?**
  - Vérifiez-vous le code avant d'exécuter ? ;)
    http://magazine.qualys.fr/menaces-alertes/github-piege-binaire/

- **Bientôt la Fin de support Windows Server 2K3**
  http://www.theregister.co.uk/2014/04/20/next_windows_obsolescence_panic_is_450_days_from_now/

- **VirusTotal n'est plus si efficace**
  http://magazine.qualys.fr/menaces-alertes/antivirus-virustotal/

- **DynDNS ferme son service gratuit**
  http://dyn.com/blog/why-we-decided-to-stop-offering-free-accounts/

- **Le hacking serait-il addictif ?**
  https://docs.google.com/presentation/d/1Sv8IHkBtBEXjSW7WktEYg4EbAUHtVyXIZBrAGD3WR5Y/preview?sle=true#slide=id.g268c10cab_0343

- **IBM nie aider la NSA pour son espionnage industriel**
  http://www.zdnet.com/ibm-denies-assisting-nsa-in-customer-spying-7000027380/

Divers / Trolls velus

- **Contre l'espionnage, le gouvernement Russe jette ses iPad**
  http://www.01net.com/editorial/616824/espionnage-le-gouvernement-russe-se-debarrasse-de-ses-ipad/
  - Et remplace cela par son fork d'Android : RomOS (<<Российская мобильная операционная система>>)
    http://www.phonearena.com/news/RoMOS-is-a-hack-proof-Android-based-platform-Russian-government-nods-approvingly_id34045

- **Monoprix acceptera le Bitcoin d'ici fin 2014**
  http://www.journaldunet.com/ebusiness/expert/57210/monoprix-et-amazon--deux-visions-opposees-sur-les-bitcoins.shtml

- **Sauvez la planete, regardez du porno :)**
  http://www.pornhub.com/event/arborday

- **CAC40 et souveraineté des emails par newsoft**
  - 28 entreprises du CAC40 font appels à des prestataires étrangers pour leur email
    http://t.co/EOvx3NwdBU
  - Mais.. Google a vos emails de toute façon !
    http://mako.cc/copyrighteous/google-has-most-of-my-email-because-it-has-all-of-yours

Divers / Trolls velus

- Le Wifi par défaut en 2014…

Questions ?

- **Prochaine réunion**
  Mardi 10 juin 2014