Brèves 2015 S22, s23, s24 & S25 – La mare du Gof

Actus Sécurité Grand public

=> **The Teenage Mutant Malvertiser Network**. 26/05/2015. «*Bedep's network activity has been documented in other security blogs here and here; this blog's focus is more on the scope of malvertising and redirection activity involving the particular networks that lead to the Exploit Kits (...).*»
Source : www.fireeye.com/blog/threat-research/2015/05/the_teenage_mutantm.html

=> **Angler EK Exploiting Adobe Flash CVE-2015-3090**. 26/05/2015. «*FireEye has detected a new attack by the Angler Exploit Kit (EK) that exploits CVE-2015-3090 in Adobe Flash Player. Angler began exploiting CVE-2015-3090 about two weeks after Adobe released a patch (Patch: May 11, 2015, Exploit: approx. May 26, 2015) (...).*»
Source : www.fireeye.com/blog/threat-research/2015/05/angler_ek_exploiting.html
Billets en relation :
26/05/2015. *CVE-2015-3090 (Flash up to 17.0.0.169) and Exploit Kits* : malware.dontneedcoffee.com/2015/05/cve-2015-3090-flash-up-to-1700169-and.html

=> **How to Spot Frauds on Professional Networks**. 28/05/2015. «*Here are a number of practical ways to detect if someone is trying to trick you into divulging sensitive company information (...).*»
Source : www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-to-spot-frauds-on-professional-networks
Billets en relation :
02/06/2015. *Reconnaissance via Professional Social Networks* : blog.trendmicro.com/trendlabs-security-intelligence/reconnaissance-via-professional-social-networks/

=> **Lessons learned from Flame, three years later**. 29/05/2015. «*Three years ago, on May 28th 2012, we announced the discovery of a malware known as Flame. At the same time we published our FAQ, CrySyS Lab posted their thorough analysis of sKyWIper. A few days earlier, Maher CERT published IOCs for Flamer. In short, Flame, sKyWIper and Flamer are different names for the same threat, which took the world by surprise as the first major discovery after Stuxnet and Duqu (...).*»
Source : securelist.com/blog/opinions/70149/lessons-learned-from-flame-three-years-later/

=> **"Troldesh" – New Ransomware from Russia** . 01/06/2015. «*"Troldesh", aka Encoder.858 or Shade, is a Trojan and a crypto-ransomware variant created in Russia and spread all over the world. Troldesh is based on so-called encryptors that encrypt all of the user's personal data and extort money to decrypt the files. Troldesh encrypts a user's files with an ".xtbl" extension. Troldesh is spread initially via e-mail spam (...).*»
Source : blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/

=> **Multiple Malwares used to Target an Asian Financial Institution**. 02/06/2015. «*Recently, Cyphort Labs received multiple malware samples that were used to target a financial institution in Asia. Due to an ongoing investigation, we will keep the company name anonymous (...).*»
Source : www.cyphort.com/multiple-malwares-used-to-target-an-asian-financial-institution/

=> **Crypto remorse?**. 02/06/2015. «*Crypto ransomware author appears to regret encrypting victims' computers and automatically decrypts their files (...).*»
Source : www.symantec.com/connect/blogs/crypto-remorse-author-new-locker-crypto-ransomware-repents-after-earning-just-us169
Billets en relation :
30/05/2015. *Locker database release* : pastebin.com/1WZGqrUH
31/05/2015. *"Locker" Ransomware Author Allegedly Releases Database of Private Keys* :
www.bleepingcomputer.com/forums/t/577861/locker-ransomware-author-allegedly-releases-database-of-private-keys/
02/06/2015. *V Locker (variante de Cryptolocker) – La fin du cauchemar ?* : korben.info/cryptolocker-la-fin-du-cauchemar.html

=> **(More) Confessions of a Support Scammer**. 03/06/2015. «*Marek Lelovic, my colleague at ESET, drew my attention to a fascinating Reddit thread. It was initiated by someone who stated that: "I worked at a phone scam for 6 months. I had just recently quit because I hated the job. So literally ask me anything." (...).*»
Source : www.welivesecurity.com/2015/06/03/confessions-support-scammer/
Billets en relation :
25/05/2015. *I worked at a tech support scam phone room AMA* :
www.reddit.com/r/AMA/comments/3766m1/i_worked_at_a_tech_support_scam_phone_room_ama/

=> **Les choses ne sont pas toujours ce qu'elles paraissent** . 03/06/2015. «*Cette expertise est délicate : je dois accompagner un huissier de justice pour faire un constat sur un ordinateur d'entreprise. Encore une fois, je connais peu le contexte technique avant l'intervention. Vais-je trouver un terminal relié à un AS/400, un magnifique Macintosh, un classique ordinateur sous Windows, un surprenant poste sous GNU/Linux ou un client léger très tendance ? (...).*»
Source : zythom.blogspot.fr/2015/06/les-choses-ne-sont-pas-toujours-ce.html

=> **Kaspersky Lab inaugure un nouveau centre de recherche européen à Londres**. 03/06/2015. «*Kaspersky Lab, l'entreprise russe spécialisée en sécurité informatique, a annoncé qu'elle inaugurerait prochainement son premier centre de recherche en Europe. Celui-ci sera intégré au siège européen de l'entreprise à Londres (...).*»
Source : www.observatoire-fic.com/kaspersky-lab-inaugure-un-nouveau-centre-de-recherche-europeen-a-londres/

=> **LuminosityLink – Extracting The Config of 1.0 and 1.1**. 04/06/2015. «*I decided to look at a emerging "stable" RAT that was released early April. It's called LuminosityLink, the developer has previous experience in malware with being the author of the malware named "PLASMA HTTP". I found a XSS vulnerability in this certain strand of malware and was able to takeover some panels and kill some botnets (...).*»
Source : itsjack.cc/blog/2015/06/luminositylink-extracting-the-config-of-1-0-and-1-1/

=> **Malware Persistence With HKEY_CURRENT_USER Shell Extension Handlers, No Admin Required**. 04/06/2015. «*I was recently exposed to a new (to me anyway) method of persistence that the Bedep malware is using. The novel aspect of this persistence method is that it doesn't require administrator rights and it evades my two favourite persistence detection tools: Autoruns, and RegRipper. The persistence method requires the creation of a per-user shell extension handler where the shell handler DLL is the malware that requires persistence (...).*»
Source : herrcore.blogspot.fr/2015/06/malware-persistence-with.html
Billets en relation :
07/06/2015. *Problem with RegRipper* : windowsir.blogspot.ca/2015/06/links.html

=> **Angler EK: More Obfuscation, Fake Extensions, and Other Nonsense**. 05/06/2015. «*This exploit kit evolves on an almost constant basis. However, the recent activity caught our attention due to a change to the URL structure of the landing pages. This type of change doesn't occur often and was coupled with some other interesting tidbits including how the HTTP 302 cushioning has evolved and the payload of another ransomware has changed (...).*»
Source : blogs.cisco.com/security/talos/angler-update
Billets en relation :
16/06/2015. *Domain Shadowing Goes Nuclear: A Story in Failed Sophistication* : blogs.cisco.com/security/talos/nuclear-sophistication

=> **Vawtrak Uses Tor2Web**. 05/06/2015. «*Vawtrak, also known as Neverquest, is a banking trojan that is capable of bypassing 2FA (two factor authentication) on some financial institutions. It is also one of your typical information stealer. One of the main strengths of Vawtrak is its use of layering techniques within its code (...).*»
Source : blog.fortinet.com/post/vawtrak-uses-tor2web
Billets en relation :
11/06/2015. *Vawtrak uses Tor2Web to connect to Tor hidden C&C servers* : www.virusbtn.com/blog/2015/06_11a.xml

=> **Adwares/PUPs: des améliorations….**. 05/06/2015. «*Un petit billet pour faire le point sur les adwares et PUPs (Programmes parasites). Ces derniers sont devenus la première menace depuis quelques années, sur les forums de désinfections, j'estime les demandes à 80%. Aujourd'hui, nous assistons à une chute significative (...).*»
Source : www.malekal.com/2015/06/05/adwarespups-des-ameliorations/

=> **Veille Cyber NUMERO 28**. 08/06/2015. «*Une actualité toujours plus fournie, toujours plus diversifiée, les métiers de l'Information numérique connectée et de sa Sécurité, le retour sur l'établi de la loi sur le renseignement, en même temps un Freedom Act aux États-Unis, pas si freedom que cela, et puis des rapports, des études, des sujets techniques et managériaux, pour une bonne lecture de cette veille qui n'est qu'un simple survol de l'actualité de la semaine dans le monde cyber, pour vous donner envie d'aller plus loin … (...).*»
Diverses veille à thématique 'sécu', de différentes difficultés.
Source : veillecyberland.wordpress.com/2015/06/08/veille-cyber-n28-8-juin-2015/
Billets en relation :
26/05/2015. *Bulletin d'actualité CERTFR-2015-ACT-021* : www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-021/index.html
26/05/2015. *[Newsletter HSC] N°129 - Mai 2015* : www.hsc-news.com/archives/2015/000130.html
26/05/2015. *Links and Stuff* : windowsir.blogspot.fr/2015/05/links-and-stuff.html
28/05/2015. *Labs: Blog Digest Mai 2015* : www.scip.ch/?labs.20150528
29/05/2015. *Cyber Scoop* : www.threatgeek.com/2015/05/cyber-scoop-may-29-2015.html
30/05/2015. *Wawa Security Links 74* : www.wawaseb.com/lutile/wsl74.php
31/05/2015. *Downclimb: Summit Route's Weekly Cyber News Recap* : summitroute.com/blog/2015/05/31/downclimb/
01/06/2015. *Veille Cyber NUMERO 27* : veillecyberland.wordpress.com/2015/06/01/veille-cyber-n27-01-juin-2015/

01/06/2015. *Newsletter Sécurité N°119* : us5.campaign-archive2.com/?u=7984711c6610214deca369bee&id=a16127f5b4
01/06/2015. *The Brief* : blog.opendns.com/2015/06/08/the-brief-june-1st-2015/
01/06/2015. *Bulletin d'actualité CERTFR-2015-ACT-022* : www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-022/index.html
01/06/2015. *Security News #0x88* : cyberoperations.wordpress.com/2015/06/01/security-news-0x88/
01/06/2015. *May 2015 Global Threat Intelligence Report* : krypt3ia.wordpress.com/2015/06/01/may-2015-global-threat-intelligence-report/
05/06/2015. *Cyber Scoop* : www.threatgeek.com/2015/06/this-week-in-cybersecurity-news-chinese-breach-data-of-4-million-federal-workers-by-ellen-nakashima-washington-post-hacke.html
05/06/2015. *Wawa Security Links 75* : www.wawaseb.com/lutile/wsl75.php
05/06/2015. *[Newsletter HSC] N°130 - juin 2015* : www.hsc-news.com/archives/2015/000131.html
07/06/2015. *Crimes de cyber* : informatiques-orphelines.fr//index.php?post/2015/06/07/Crimes-de-cyber
07/06/2015. *Downclimb: Summit Route's Weekly Cyber News Recap* : summitroute.com/blog/2015/06/07/downclimb/
08/06/2015. *The Brief* : blog.opendns.com/2015/06/15/the-brief-june-8th-2015/
08/06/2015. *Bulletin d'actualité CERTFR-2015-ACT-023* : www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-023/index.html
08/06/2015. *Veille - Une approche par les risques.....* : pseudonyme.over-blog.net/2015/06/veille-une-approche-par-les-risques.html
12/06/2015. *Cyber Scoop* : www.threatgeek.com/2015/06/cyber-scoop-june-12-2015.html
14/06/2015. *Veille Sécurité* : www.ledecodeur.ch/2015/06/14/veille-securite-14-juin-2015/
14/06/2015. *Wawa Security Links 76* : www.wawaseb.com/lutile/wsl76.php
15/06/2015. *Bulletin d'actualité CERTFR-2015-ACT-024* : www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/index.html
15/06/2015. *Veille Cyber du 15 juin 2015* : veillecyberland.wordpress.com/2015/06/14/veille-cyber-n29-14-juin-2015/
15/06/2015. *Veille - Encore DUQU ?? Mais c'était déjà le sujet de l'article précédent.....* : pseudonyme.over-blog.net/2015/06/veille-encore-duqu-mais-c-etait-deja-le-sujet-de-l-article-precedent.html
19/06/2015. *Cyber Scoop* : www.threatgeek.com/2015/06/cyber-scoop-june-19-2015.html
21/06/2015. *Veille Sécurité* : www.ledecodeur.ch/2015/06/21/veille-securite-21-juin-2015/

=> **May 2015 Cyber Attacks Statistics**. 08/06/2015. «*It's time to aggregate the two timelines of May 2015 (Part I and Part II) into statistics (...).*»
Source : hackmageddon.com/2015/06/08/may-2015-cyber-attacks-statistics/
Billets en relation :
26/05/2015. *New Web Site and Updated Page for the 2015 Master Index* : hackmageddon.com/2015/05/26/new-web-site-and-updated-page-for-the-2015-master-index/
28/05/2015. *Company That Lets Parents Spy On Their Kids' Computer Usage... Has Database Hacked And Leaked* : www.techdirt.com/articles/20150522/12444731087/company-that-lets-parents-spy-their-kids-computer-usage-has-database-hacked-leaked.shtml
29/05/2015. *Chine - OceanLotus* : econflicts.blogspot.fr/2015/05/chine-oceanlotus.html
03/06/2015. *16-31 May 2015 Cyber Attacks Timeline* : hackmageddon.com/2015/06/03/16-31-may-2015-cyber-attacks-timeline/
04/06/2015. *OPM to Notify Employees of Cybersecurity Incident* : www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/
05/06/2015. *4 million government employees' personal data stolen in OPM hack* : www.welivesecurity.com/2015/06/05/4-million-government-employees-personal-data-stolen-opm-hack/
09/06/2015. *Continuous Diagnostic Monitoring Does Not Detect Hackers* : taosecurity.blogspot.fr/2015/06/continuous-diagnostic-monitoring-does.html
13/06/2015. *OPM Breach Discovered During a Product Demo* : hackmageddon.com/2015/06/13/opm-breach-discovered-during-a-product-demo-and-undetected-for-over-a-year/
15/06/2015. *Etats-Unis : un vol de données de fonctionnaires pire qu'estimé* : www.lemagit.fr/actualites/4500248150/Etats-Unis-un-vol-de-donnees-de-fonctionnaires-pire-questime
15/06/2015. *Banking Trojan has targeted Bundestag* : blog.gdatasoftware.com/blog/article/banking-trojan-has-targeted-bundestag.html
15/06/2015. *LastPass notification de sécurité* : blog.lastpass.com/fr/2015/06/lastpass-security-notice.html/
16/06/2015. *Le Bundestag victime d'une cyberattaque* : www.lemonde.fr/pixels/article/2015/06/16/le-bundestag-victime-d-une-cyberattaque_4654692_4408996.html
17/06/2015. *Des sites gouvernementaux canadiens paralysés par une cyberattaque* : www.lemonde.fr/ameriques/article/2015/06/17/des-sites-gouvernementaux-canadiens-paralyses-par-une-cyberattaque_4656421_3222.html
18/06/2015. *U.S. cyber hack unsettles, frustrates U.S. defense industry* : venturebeat.com/2015/06/18/u-s-cyber-hack-unsettles-frustrates-u-s-defense-industry/
18/06/2015. *OPM: WHO? WHY? WHAT? ERMEGERD CHINA!* : krypt3ia.wordpress.com/2015/06/18/opm-who-why-what-ermegerd-china/
18/06/2015. *The Importance of Data (Part I)* : www.hackmageddon.com/2015/06/18/the-importance-of-data-part-i/
19/06/2015. *Lastpass, quand trépasse le « pass », hélas* : www.cnis-mag.com/lastpass-quand-trepasse-le-pass-helas.html

=> **TV5 Monde, Russia and the CyberCaliphate**. 10/06/2015. «*Yesterday evening French magazine L'Express published a report linking an attack against TV5 Monde very firmly to the Russian state. The attack, which knocked 11 of its global channels off air for a period of time and resulted in a compromised website and Facebook page, took place back in April (...).*»
Source : countermeasures.trendmicro.eu/tv5-monde-russia-and-the-cybercaliphate/
Billets en relation :
09/06/2015. *Cyberattaque de TV5MONDE : des pirates informatiques russes aux commandes ?* : information.tv5monde.com/info/cyberattaque-de-tv5monde-s-agirait-il-de-pirates-informatiques-russes-37691
09/06/2015. *Piratage de TV5 Monde: l'enquête s'oriente vers la piste russe* : www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html
10/06/2015. *Le retour de la revanche de l'Affaire TV5Monde : cette fois ce sont les russes!* : fr.intstrat.org/article/le_retour_de_la_revanche_de_laffaire_tv5monde__cette_fois_ce_sont_les_russes/
10/06/2015. *TV5 Monde : un pirate peut en cacher un autre* : www.lemonde.fr/pixels/article/2015/06/10/tv5-monde-un-pirate-peut-en-cacher-un-autre_4651349_4408996.html

=> **Rencontre avec les chasseurs de pirates de Trend Micro**. 12/06/2015. «*Chasser les virus, les codes malveillants, les attaques informatiques d'aujourd'hui et de demain, telle est la mission des laboratoires de recherche de Trend Micro. L'éditeur de Solution de Sécurité informatique a ouvert quelques-uns des secrets du Trend Labs à la rédaction de ZATAZ.com lors d'un voyage de presse au Philippines (...).*» Opération de relations publiques de l'éditeur. Les titres ne sont pas toujours 'heureux', comme d'habitude (cf. ci-dessous).
Source : www.zataz.com/rencontre-avec-les-chasseurs-de-pirates-de-trend-micro/
Billets en relation :
26/05/2015. *«Attaques ciblées : le jeu» de Trend Micro* : targetedattacks.trendmicro.com/fra/index.html
12/06/2015. *Sécurité : comment les nouvelles menaces sont décortiquées* : www.silicon.fr/securite-comment-nouvelles-menaces-decortiquees-118779.html
15/06/2015. *TrendLabs : les têtes chercheuses de Trend Micro prêtes pour passer à "l'offensif"* : cyberisques.com/mots-cles-1/446-trendlabs-les-tetes-chercheuses-de-trend-micro-pretes-pour-passer-a-l-offensif
18/06/2015. *Profession : chasseur de hackers* : www.silicon.fr/profession-chasseur-hackers-119529.html

=> **Oh look – JavaScript Droppers**. 12/06/2015. «*Recently we found a couple of curious specimen that does not follow this fashion. These cases are not new, but we thought they're worth mentioning because we've been seeing quite a few of those lately. One of them is the shellcode from an Internet Explorer exploit, which instead of downloading a binary executes the following CMD command (...).*»
Source : labs.bromium.com/2015/06/12/oh-look-javascript-droppers/

=> **Y a-t-il un pirate dans l'avion ?**. 15/06/2015. «*Un pirate informatique peut-il vraiment prendre les commandes d'un avion ou d'une voiture à distance ? Enquête auprès des chercheurs qui développent les systèmes anti-intrusion qui équiperont les transports de demain (...).*»
Source : lejournal.cnrs.fr/articles/y-a-t-il-un-pirate-dans-lavion
Billets en relation :
12/06/2015. *"Avions, trains : aucune raison que les cyberattaques se limitent aux entreprises" (Patrice Caine, PDG de Thales) »* : www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/aeronautique-le-modele-economique-est-aligne-avec-l-interet-ecologique-patrice-caine-pdg-de-thales-483355.html
12/06/2015. *Cybersécurité: les hackers mèneront-ils toujours le jeu ?* : www.ssi.gouv.fr/actualite/cybersecurite-les-hackers-meneront-ils-toujours-le-jeu/
16/06/2015. *Spécial Bourget 2015 : pirater un avion, simple comme un clic de souris ?* : www.zataz.com/piratage-hacking-avion-aeroport/

=> **Digital Security, filiale du groupe Econocom, lance le premier CERT européen dédié à la sécurité des objets connectés**. 17/06/2015. «*« Le CERT-UBIK rassemble des profils issus du monde des télécoms, de l'informatique et de l'électronique: analyseurs de spectre, récepteurs radio et plates-formes de rétro-ingénierie font partie de la panoplie nécessaire à l'évaluation de la sécurité des objets connectés » rapporte Thomas Gayet, Directeur du CERT-UBIK. (...).*»
Source : www.econocom.com/fr/actus/communiques-de-presse/digital-security-filiale-du-groupe-econocom-lance-le-premier-cert

=> **Campagne Dridex - documents Microsoft Word & Excel piégés**. 18/06/2015. «*Depuis plusieurs jours, la France comme d'autres pays est sévèrement arrosée de pourriels qui contiennent en pièce jointe des documents Microsoft Word & Excel piégés par des macros malveillantes qui font télécharger et exécuter silencieusement Dridex, un programme spécialisé dans le vol d'identifiants et de données bancaires. Ce n'est pas la première fois et ce ne sera pas la dernière ; déjà en février 2015, j'abordais le sujet "Documents malveillants : macros-commandes VBA + PowerShell" ; les mois suivants plusieurs alertes avaient été émises (...).*»
Source : forum.malekal.com/campagne-dridex-documents-microsoft-word-excel-pieges-t52049.html
Billets en relation :
15/06/2015. *Campagne DRIDEX, outils de détection et désinfection* : www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

15/06/2015. *Campagne de pourriels avec documents Microsoft Office malveillants* : cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/
17/06/2015. *Analyst's Handbook - Analyzing Weaponized Documents* : dfir.it/blog/2015/06/17/analysts-handbook-analyzing-weaponized-documents/
17/06/2015. *DRIDEX : la cyber-attaque qui mitraille l'Internet* : wearesecure.blogspot.fr/2015/06/dridex-la-cyber-attaque-qui-mitraille.html
18/06/2015. *In-depth analysis of a Dridex malware dropper* : christophe.rieunier.name/securite/Dridex/20150608_dropper/Dridex_dropper_analysis.php
18/06/2015. *Evolution of Dridex* : www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html
18/06/2015. *Analyse détaillée d'un dropper du malware Dridex* : christophe.rieunier.name/securite/Dridex/20150608_dropper/Dridex_dropper_analysis_fr.php
18/06/2015. *Xylibox - Having a look on Dridex config* : www.youtube.com/watch?v=rj2DVRN5UyU

=> **Unmasked: How Police Beat Shakespearean Cyber Thieves**. 18/06/2015. «*Shakespeare-quoting hackers targeted British banks. Police led a global operation to stop the heist, but can they catch the Shylock gang? (...).*»
Source : www.bloomberg.com/news/features/2015-06-18/cyber-thieves-used-shakespeare-to-steal-millions-then-police-hit-back

=> **The POS Malware Epidemic: The Most Dangerous Vulnerabilities and Malware**. 19/06/2015. «*Point-of-sale (POS) malware is an information security ailment that, within less than seven years, reached colossal proportions and became more damaging to organizations than almost any other threat. Although this threat is less sophisticated than malware like banking Trojans, it can be hugely destructive due to the following (...).*»
Source : securityintelligence.com/the-pos-malware-epidemic-the-most-dangerous-vulnerabilities-and-malware/
Billets en relation :
10/06/2015. *'Evoltin' POS Malware Attacks via Macro* : blogs.mcafee.com/mcafee-labs/evoltin-pos-malware-attacks-via-macro

Actus Sécurité Confirmé(s)

=> **The Latest Flash UAF Vulnerabilities in Exploit Kits**. 28/05/2015. «*We analyzed the code found in the exploit kits to determine which vulnerabilities are present and how they are exploited (...).*»
Source : researchcenter.paloaltonetworks.com/2015/05/the-latest-flash-uaf-vulnerabilities-in-exploit-kits/
Billets en relation :
01/06/2015. *Understanding Flash Exploitation and the Alleged CVE-2015-0359 Exploit* : researchcenter.paloaltonetworks.com/2015/06/understanding-flash-exploitation-and-the-alleged-cve-2015-0359-exploit/
08/06/2015. *Base91 & Angler SWFs* : hooked-on-mnemonics.blogspot.fr/2015/06/base91-angler-swfs.html
10/06/2015. *Large Malvertising Campaign Leads to Angler EK & Bunitu Malware* : community.websense.com/blogs/securitylabs/archive/2015/06/10/large-malvertizing-campaign-leads-to-angler-ek-amp-bunitu-malware.aspx

=> **Unusual Exploit Kit Targets Chinese Users (Part 1)** . 28/05/2015. «*We are very accustomed to seeing the same exploit kits over and over. Angler EK, Nuclear EK or Fiesta EK all have become familiar faces on this blog. Today, we are looking at an exploit kit that we have not seen before. Contrary to its counterparts, it is not used on mainstream websites or via malvertising attacks but rather it specifically targets Chinese websites and users (...).*»
Source : blog.malwarebytes.org/exploits-2/2015/05/unusual-exploit-kit-targets-chinese-users-part-1/
Billets en relation :
12/06/2015. *Unusual Exploit Kit Targets Chinese Users (Part 2)* : blog.malwarebytes.org/intelligence/2015/06/unusual-exploit-kit-targets-chinese-users-part-2/

=> **When Hackers Get Hacked: the Malware Servers of a Data-Stealing Campaign**. 29/05/2015. «*Selling stolen data is an easy way for cybercriminals to make some quick money on cyber black markets. The following flowchart shows a generic credential-stealing campaign in action. In the last step, the flow is bidirectional. The malware makes a two-way authentication-free connection between the victim and the attacke (...).*»
Source : blogs.mcafee.com/mcafee-labs/when-hackers-get-hacked-the-malware-servers-of-a-data-stealing-campaign

=> **Fast look at Sundown EK**. 08/06/2015. «*Disclaimer : There is nothing worth a post there...except mentionning this EK is around. I would put that "kit" in the same sad basket than Archie (same level, same kind of traffic source). The exploit kit is out there since middle of April. I first heard about it by Will Metcalf from Emerging Threats. (...).*»
Source : malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html

=> **Stegoloader: A Stealthy Information Stealer**. 15/06/2015. «*The Stegoloader malware family (also known as Win32/Gatak.DR and TSPY_GATAK.GTK despite not sharing any similarities with the Gataka banking trojan) was first identified at the end of 2013 and has attracted little public attention. Dell SecureWorks Counter Threat Unit(TM) (CTU) researchers have analyzed multiple variants of this*

malware, which stealthily steals information from compromised systems (...).»
Source : www.secureworks.com/cyber-threat-intelligence/threats/stegoloader-a-stealthy-information-stealer/
Billets en relation :
16/06/2015. *New Malware Found Hiding Inside Image Files* : www.darkreading.com/endpoint/new-malware-found-hiding-inside-image-files/d/d-id/1320895

=> **Magnitude Exploit Kit Uses Newly Patched Adobe Vulnerability; US, Canada, and UK are Most At Risk**. 15/06/2015. «*Adobe may have already patched a Flash Player vulnerability last week, but several users—especially those in the US, Canada, and the UK —are still currently exposed and are at risk of getting infected with CryptoWall 3.0. The Magnitude Exploit Kit included an exploit, detected as SWF_EXPLOIT.MJTE, for the said vulnerability, allowing attackers to spread crypto-ransomware into their target systems. We first saw signs of this activity yesterday (...).*»
Source : blog.trendmicro.com/trendlabs-security-intelligence/magnitude-exploit-kit-uses-newly-patched-adobe-vulnerability-us-canada-and-uk-are-most-at-risk/
Billets en relation :
16/06/2015. *CVE-2015-3104/3105 (Flash up to 17.0.0.188) and Exploit Kits* : malware.dontneedcoffee.com/2015/06/cve-2015-3105-flash-up-to-1700188-and.html

=> **The ELF ChinaZ "reloaded"** . 19/06/2015. «*MalwareMustDie (MMD) group found new ELF malware called ChinaZ reported in the previous post in?January 2015 while it was riding the Shellshock for infecting Linux boxes in the internet. And the new version of ChinaZ was accidentally spotted while our team was gathered to scan internet for more ELF bad stuff, and we were all in sleepy mode after our day work in weekend... (...).*»
Source : blog.malwaremustdie.org/2015/06/the-elf-chinaz-reloaded.html

Rapports, études, slides et publications

=> **2015 curl user poll analysis**. 26/05/2015. «*My full 30 page document with all details and analyses of the curl user poll 2015 is now available. It shows details of all the questions, most of them with a comparison with last year's survey. The write-ins are also full of good advice, wisdom and some signs of ignorance or unawareness (...).*»
Source : daniel.haxx.se/blog/2015/05/26/2015-curl-user-poll-analysis/
Billets en relation :
26/05/2015. *2015 curl user poll analysis* : daniel.haxx.se/media/curl%20user%20poll%202015%20analysis.pdf

=> **Moose – the router worm with an appetite for social networks**. 26/05/2015. «*ESET researchers have issued a technical paper today, analyzing a new worm that is infecting routers in order to commit social networking fraud, hijacking victims' internet connections in order to "like" posts and pages, "view" videos and "follow" other accounts (...).*»
Source : www.welivesecurity.com/2015/05/26/moose-router-worm/
Billets en relation :
26/05/2015. *Dissecting Linux/Moose: a Linux Router-based Worm Hungry for Social Networks* : www.welivesecurity.com/2015/05/26/dissecting-linuxmoose/
26/05/2015. *Dissecting Linux/Moose* : www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf

=> **Conclusion for the European Public-Private Partnership (PPP) for Resilience scheme** . 27/05/2015. «*This report analyses the opportunities and challenges of the first European public-private partnerships in the field of network and information security and resilience in Europe: the European Public-Private Partnership for Resilience (EP3R), in which mainly participated stakeholders belonging to the Telecom and Information Technology sectors (...).*»
Source : www.enisa.europa.eu/media/news-items/conclusion-for-the-european-public-private-partnership-ppp-for-resilience-scheme
Billets en relation :
15/04/2015. *EP3R 2009-2013 Future of NIS Public Private Cooperation* : www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013

=> **Does CCTV put the public at risk of cyberattack?**. 27/05/2015. «*How insecure surveillance technology is working against you (...).*»
Source : securelist.com/blog/research/70008/does-cctv-put-the-public-at-risk-of-cyberattack/
Billets en relation :
26/05/2015. *Security Researchers Start Effort to Protect 'Smart' Cities* : bits.blogs.nytimes.com/2015/05/26/security-researchers-start-effort-to-protect-smart-cities/
27/05/2015. *Does CCTV put the public at risk of cyberattack?* : securingsmartcities.org/wp-content/uploads/2015/05/CCTV_research_final.pdf
27/05/2015. *CCTV surveillance security issues: almost a year later* : securingsmartcities.org/?p=301
27/05/2015. *La vidéosurveillance présente-t-elle un risque pour le public en cas de cyberattaque?* : www.viruslist.com/fr/analysis?pubid=200676391

=> **APWG Releasese Global Phishing Survey for Second Half of 2014**. 27/05/2015. «*APWG released its latest Domain Name Use and Trends report on May 27, 2014 (...).*»
Source : apwg.org/apwg-news-center/
Billets en relation :
27/05/2015. *APWG Cybercrime Report: Phishers Try to Catch Consumers by Attacking New Targets* : www.businesswire.com/news/home/20150527005745/en/APWG-Cybercrime-Report-Phishers-Catch-Consumers-Attacking
27/05/2015. *APWG Releasese Global Phishing Survey for Second Half of 2014* : apwg.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf
01/06/2015. *APWG présente son rapport sur les domaines et les sites de phishing au 2e semestre* : www.viruslist.com/fr/news?id=197471302

=> **Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne**. 28/05/2015. «*Droit a la vie privée et protection des données personnelles (Assemblée Parlementaire du Conseil de l'Europe) (...).*»
Source : revdh.revues.org/1300#tocto1n2
Billets en relation :
28/05/2015. *Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne* : revdh.revues.org/pdf/1300
29/05/2015. *Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne* : combatsdroitshomme.blog.lemonde.fr/2015/05/29/quand-la-realite-de-la-surveillance-massive-tend-a-depasser-la-fiction-orwellienne/

=> **Statistics on botnet-assisted DDoS attacks in Q1 2015**. 29/05/2015. «*This report presents DDoS Intelligence statistics collected from 1 January to 31 March 2015 (or Q1 2015), which is analyzed in comparison with the equivalent data collected within the previous 3-month period (1 October to 31 December 2014, or Q4 2014) (...).*»
Source : securelist.com/blog/research/70071/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/
Billets en relation :
29/05/2015. *Statistics on botnet-assisted DDoS attacks in Q1 2015* : www.slideshare.net/KasperskyLabGlobal/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015
29/05/2015. *Statistiques sur les attaques DDoS organisees a l'aide de reseaux de zombies au T1 2015* : www.viruslist.com/fr/analysis?pubid=200676392

=> **The Effect of Piracy Website Blocking on Consumer Behavior**. 29/05/2015. «*Understanding the relationship between copyright policy and consumer behavior is an increasingly important topic for participants in digital media markets. In this paper we seek to study how consumer behavior changes when Internet Service Providers are required to block access to major piracy websites. We do this in the context of two court-ordered events affecting consumers in the UK: The blocking order directed at The Pirate Bay in May 2012, and blocking orders directed at 19 major piracy sites in October and November 2013 (...).*»
Source : papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063
Billets en relation :
08/06/2015. *Piratage : bloquer un site ne suffit pas à changer les pratiques* : www.lemonde.fr/pixels/article/2015/06/08/piratage-bloquer-un-site-ne-suffit-pas-a-changer-les-pratiques_4649654_4408996.html

=> **CA Privilege Identity Manager Security Research Whitepaper**. 31/05/2015. «*Today we are announcing the release of our latest whitepaper that includes the results of a research project performed for CA Technologies earlier this year. The focus of the research was to determine the effectiveness of the security controls provided by the CA Privilege Identity Manager (CA PIM) solution against attacks that target privileged identities (...).*»
Source : blog.gdssecurity.com/labs/2015/5/31/ca-privilege-identity-manager-security-research-whitepaper.html
Billets en relation :
31/05/2015. *CA Privilege Identity Manager Security Research Whitepaper* : github.com/GDSSecurity/Whitepapers/raw/master/GDS%20Labs%20-%20CA%20Technologies%20CA%20PIM%20Security%20Research%20White%20Paper.pdf

=> **Which Malware Lures Work Best?**. 31/05/2015. «*Last week at the APWG eCrime Conference in Barcelona I presented some new results about an old Instant Messaging (IM) worm from a paper written by Tyler Moore and myself. In late April 2010 users of the Yahoo and Microsoft IM systems started to get messages from their buddies which said, for example (...).*»
Source : www.lightbluetouchpaper.org/2015/05/31/which-malware-lures-work-best/
Billets en relation :
31/05/2015. *Which Malware Lures Work Best? (slides)* : www.cl.cam.ac.uk/~rnc1/talks/150520-malware-lures.pdf
31/05/2015. *Which Malware Lures Work Best?* : www.cl.cam.ac.uk/~rnc1/malware-lures.pdf

=> **SBK - A Bootkit Capable of Surviving Reformat**. 01/06/2015. «*Since i got into firmware hacking, I've been working on a little project behind the scenes: A hard disk firmware based rootkit which allows malware to survive an operating system re-install or full disk format. Unfortunately I can't post a proof of concept for many reasons (...).*»

Source : www.malwaretech.com/2015/06/hard-disk-firmware-rootkit-surviving.html
Billets en relation :
01/06/2015. *Hard Disk Firmare Hacking - MBR spoofing* : www.youtube.com/watch?v=0gc-VF6bi3g
01/06/2015. *SBK - A Bootkit Capable of Surviving Reformat* : malwaretech.net/MTSBK.pdf
12/06/2015. *Le bootkit qui ne voulait pas mourir* : www.cnis-mag.com/le-bootkit-qui-ne-voulait-pas-mourir.html

=> **Check Point's annual security report**. 02/06/2015. «*Check Point Research Reveals a Rise in Zero-Day Attacks on Mobile Devices and Networks are the Biggest Threats for Today's Enterprises (...).*»
Source : www.checkpoint.com/press/2015/2015-secuirty-report-pressing-security-challenges-todays-enterprises/
Billets en relation :
02/06/2015. *Check Point's annual security report* : www.checkpoint.com/resources/2015securityreport/
09/06/2015. *Security Report 2015 de Check Point* : www.intrusio.fr/non-classe/security-report-2015-de-check-point-les-attaques-zero-day-ciblant-les-terminaux-mobiles-et-les-reseaux-sont-la-menace-la-plus-importante-pour-les-entreprises/

=> **Le Spiil publie un panorama complet des aides à la presse**. 02/06/2015. «*Le Spiil a agrégé l'ensemble des aides dédiées à la presse, pour mieux comprendre la réalité du soutien au secteur (...).*»
Source : www.spiil.org/20150602/spiil-publie-un-panorama-complet-aides-presse

=> **Maccarthysme 5 - Ennemis intérieurs** . 02/06/2015. «*Il n'y a pas de maccarthysme sans volonté de répression, pas forcément sous sa forme carcérale (encore que l'on ait récemment vu condamner à des peines fermes des ivrognes qui évoquaient les frères Kouachi avant la cellule de dégrisement ou des imbéciles qui écrivaient "Vive la Kalach" sur Facebook). Mais la répression est surtout devenue réprobation médiatique et sociale : elle exclut le coupable (...).*» Une série d'articles de F.B.Huyghe.
Source : www.huyghe.fr/actu_1291.htm
Billets en relation :
22/05/2015. *Maccarthysme version 1 - le macarthysme de guerre froide* : www.huyghe.fr/actu_1287.htm
26/05/2015. *Maccarthysme 2 - Nouvelle peur et nouvelles sorcières* : www.huyghe.fr/actu_1288.htm
27/05/2015. *Maccarthysme 3 - Ministères de la vérité* : www.huyghe.fr/actu_1289.htm
29/05/2015. *The Information War Part 2 : Fighting jihadist online propaganda* : hestia.hypotheses.org/452
30/05/2015. *Maccarthysme 4 - Contre-discours et contre-complot* : www.huyghe.fr/actu_1290.htm
02/06/2015. *Djihadisme : les géants du Web et le gouvernement vantent le « contre-discours »* : www.lemonde.fr/pixels/article/2015/06/02/djihadisme-les-geants-du-web-et-le-gouvernement-vantent-le-contre-discours_4645709_4408996.html
04/06/2015. *ISIS Dumps 40,000 Tweets a Day on France* : www.breitbart.com/national-security/2015/06/04/isis-dumps-40000-tweets-a-day-on-france/

=> **Internet. Géopolitique de la donnée**. 03/06/2015. «*Pourquoi la donnée peut-elle être considérée comme une ressource qui, une fois exploitée, créé de la valeur et de la puissance ? L'auteur répond clairement en présentant successivement comment les moteurs de recherche sont des vecteurs de puissance, mais aussi les défis du web profond et la dépendance excessive de l'Union européenne (...).*»
Source : www.diploweb.com/Internet-Geopolitique-de-la-donnee.html
Billets en relation :
03/06/2015. *Internet. Géopolitique de la donnée (pdf)* : bit.ly/1T4vZdX
13/06/2015. *L'Écho du mois : regards croisés – Après le colloque « la donnée n'est pas donnée »* : echoradar.eu/2015/06/13/lecho-du-mois-regards-croises-apres-le-colloque-la-donnee-nest-pas-donnee/

=> **A New Look at APT – China as Victim**. 04/06/2015. «*Much of this information has been taken from an English translation of Qihoo 360's SkyEye Labs report, and has been interpreted accordingly. The original report in Chinese can be found (...).*»
Source : www.threatgeek.com/2015/06/a-new-look-at-apt-china-as-victim.html

=> **Internet Attacks Against Nuclear Power Plants**. 05/06/2015. «*We presented "Internet Attacks Against Nuclear Power Plants" at the IAEA International Conference on Computer Security in a Nuclear World in Vienna, Austria on June 3, 2015 (...).*»
Source : blog.kleissner.org/?p=781
Billets en relation :
05/06/2015. *Slides - Internet Attacks Against Nuclear Power Plants* : kleissner.org/download/Internet%20Attacks%20Against%20NPP%20Presentation.pdf
05/06/2015. *Ppaer - Internet Attacks Against Nuclear Power Plants* : kleissner.org/download/Internet%20Attacks%20Against%20Nuclear%20Power%20Plants.pdf
15/06/2015. *Stuxnet : il reste des machines infectées et connectées* : www.lemagit.fr/actualites/4500248140/Stuxnet-il-reste-des-machines-infectees-et-connectees

=> **Explorer la dynamique humaine grâce aux smartphones**. 05/06/2015. «*A l'occasion de la journée Jeunes Chercheurs 2015, lundi 1er juin, Dingqi Yang a reçu le prix « doctorant Samovar/Télécom SudParis » pour ses travaux sur les réseaux sociaux de géolocalisation. Il a*

étudié les méthodes de collecte et d'analyse des données pour étudier les comportements individuels et collectifs des utilisateurs, ainsi que leurs applications (...).»
Source : blogrecherche.wp.mines-telecom.fr/2015/06/05/explorer-la-dynamique-humaine-grace-aux-smartphones/
Billets en relation :
10/02/2015. *Understanding Human Dynamics from Large-Scale Location-Centric Social Media Data: Analysis and Applications* : hal.archives-ouvertes.fr/tel-01115101/document

=> **La surveillance démocratique et effective des services de sécurité nationale**. 05/06/2015. «*Document thématique publié par le Commissaire aux droits de l'homme du Conseil de l'Europe. Résumé et recommandations du Commissaire (...).*»
Source : wcd.coe.int/ViewDoc.jsp?id=2328359&Site=COE
Billets en relation :
05/06/2015. *La surveillance démocratique et effective des services de sécurité nationale* : wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2758318&SecMode=1&DocId=2276488&Usage=2
08/06/2015. *Quel contrôle démocratique des services de sécurité ?* : securitedessystemesjuridiques.blogspot.fr/2015/06/quel-controle-democratique-des-services.html

=> **Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks**. 05/06/2015. «*In this paper, we present the results of a long-term study of ransomware attacks that have been observed in the wild between 2006 and 2014. We also provide a holistic view on how ransomware attacks have evolved during this period by analyzing 1,359 samples that belong to 15 different ransomware families (...).*»
Source : seclab.ccs.neu.edu/static/publications/dimva2015ransomware.pdf

=> **Le droit pénal de la fraude informatique, nouvel ami des censeurs ?**. 05/06/2015. «*Plusieurs décisions de justice rendues ces derniers mois en France – dont une décision de rejet de la Cour de cassation en date du 20 mai 2015 – s'appuient sur le droit de la criminalité informatique pour limiter les formes innovantes d'expression politique qui se déploient sur Internet. Or, ce mouvement jurisprudentiel qui s'inscrit dans un contexte d'abaissement tendanciel des garanties entourant la liberté d'expression risque encore de s'aggraver compte tenu des récentes évolutions législatives dans le domaine de la cybercriminalité (...).*»
Source : revdh.revues.org/1328
Billets en relation :
05/06/2015. *Source* : combatsdroitshomme.blog.lemonde.fr/2015/06/05/le-droit-penal-de-la-fraude-informatique-nouvel-ami-des-censeurs/
05/06/2015. *Le droit pénal de la fraude informatique, nouvel ami des censeurs ?* : revdh.revues.org/pdf/1328

=> **Temps terroriste et efficacité symbolique**. 07/06/2015. «*Au-delà de la question du contenu, et des facilités offertes pour émettre ou trouver de l'information, les liens qu'ils créent comptent. Les réseaux - on l'a assez répété - créent des communautés d'abord unies par de simples affinités et des rapports superficiels en quelques clics, mais qui, dans le cas des réseaux Web 2.0 poussent rapidement à des engagements plus profonds ou plus passionnels (...).*»
Source : www.huyghe.fr/actu_1292.htm

=> **McAfee Labs Threats Report Highlights Surge in Ransomware, Flash Exploits, Firmware Attacks**. 08/06/2015. «*Intel Security today released the McAfee Labs Threats Report: May 2015. Along with the usual compilation of threats statistics, it focuses on three key topics (...).*»
Source : blogs.mcafee.com/mcafee-labs/mcafee-labs-threats-report-highlights-surge-in-ransomware-flash-exploits-firmware-attacks
Billets en relation :
08/06/2015. *McAfee Labs Threats Report: May 2015* : www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf

=> **Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools**. 08/06/2015. «*Recorded Future has collected threat intelligence on the hacking activities of Cyber Berkut for over a year, aligning with the first month of ground fighting in Ukraine, at which time the group began coordinated cyber attacks. This article presents temporal and technical analysis of these activities, based on open source intelligence (OSINT) from the Web (...).*»
Source : www.recordedfuture.com/cyber-berkut-analysis/

=> **New Data: Volatile Cedar Malware Campaign** . 09/06/2015. «*At the end of March, we published a blog post and a whitepaper about a cyber-espionage campaign dubbed "Volatile Cedar." (...) After going public with our findings, we were provided with a new configuration belonging to a newly discovered sample we have never seen before (...).*»
Source :
Billets en relation :
31/03/2015. *Volatile Cedar – Analysis of a Global Cyber Espionage Campaign* : www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf
31/03/2015. *Volatile Cedar – Analysis of a Global Cyber Espionage Campaign* : blog.checkpoint.com/2015/03/31/volatilecedar/

=> **Q2 2015 Global DDoS Threat Landscape: Assaults Resemble Advanced Persistent Threats**. 09/06/2015. «*In our Q2 2015 DDoS Global Threat Landscape Report we share unique research data, collected in the course of mitigating thousands of DDoS assaults against Imperva Incapsula-protected domains and network infrastructures (...).*»
Source : www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html

=> **Étude G DATA Software : 50 $ le prix de votre compte en banque sur le blackmarket** . 09/06/2015. «*Attaques virales, escroqueries, hameçonnages, etc., la cyberdélinquance n'est jamais à court d'idées pour s'attaquer aux particuliers et aux entreprises. Le but de ces attaques : voler les données personnelles et professionnelles, et les revendre sur les marchés parallèles à d'autres cybercriminels (...).*»
Source : www.gdata.fr/security-labs/news/articles/article/etude-g-data-software-50-le-prix-de-votre-compte-en-banque-sur-le-blackmarket
Billets en relation :
09/06/2015. *Incursion dans le blackmarket* : public.gdatasoftware.com/_download/WP_GDATA_BLACKMARKET_2015.pdf
09/06/2015. *Numéros de CB, drogue, malwares : les prix des produits interdits* : www.01net.com/editorial/657126/numeros-de-cb-drogue-malwares-les-prix-des-produits-interdits-sur-le-dark-web/
10/06/2015. *G Data software : les malwares toujours plus présents sur la toile* : www.intrusio.fr/non-classe/g-data-software-les-malwares-toujours-plus-presents-sur-la-toile/

=> **Poweliks click-fraud malware goes fileless in attempt to prevent removal**. 09/06/2015. «*Prolific click-fraud bot, Trojan.Poweliks, resides only in the Windows registry and uses several tricks to make it difficult to evict (...).*»
Source : www.symantec.com/connect/blogs/poweliks-click-fraud-malware-goes-fileless-attempt-prevent-removal
Billets en relation :
09/06/2015. *The evolution of the fileless click-fraud malware Poweliks* :
www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/evolution-of-poweliks.pdf

=> **Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness**. 09/06/2015. «*A failure to sufficiently reform U.S. surveillance policies is hurting U.S. technology companies, costing American jobs, and weakening the U.S. trade balance (...).*»
Source : www.itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness
Billets en relation :
09/06/2015. *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness* : www2.itif.org/2015-beyond-usa-freedom-act.pdf
10/06/2015. *Prism/NSA : un impact finalement plus grand que prévu ?* : www.lemagit.fr/actualites/4500247908/Prism-NSA-un-impact-finalement-plus-grand-que-prevu

=> **2015 Trustwave Global Security Report**. 09/06/2015. «*Trustwave® today released the 2015 Trustwave Global Security Report which reveals the top cybercrime, data breach and security threat trends from 2014. The report discloses how much criminals can profit from malware attacks, which data they target, how they get inside, how long it takes for businesses to detect and contain data breaches, what types of businesses criminals are targeting and where the majority of victims are located. It also reveals the most commonly used exploits, most prevalent malware families and more (...).*»
Source : www.trustwave.com/Company/Newsroom/News/New-Trustwave-Report-Reveals-Criminals-Receive-1,425-Percent-Return-on-Investment-from-Malware-Attacks/
Billets en relation :
09/06/2015. *2015 Trustwave Global Security Report* :
www2.trustwave.com/rs/trustwave/images/Trustwave_2015SecurityPressuresReport-FINAL.pdf

=> **Fidelis Threat Advisory #1017: Phishing in Plain Sight**. 09/06/2015. «*Notably, some of this recent activity demonstrated actors implementing a technique that bypassed antivirus detection by saving a PowerPoint document in which malware executed once the document was opened in Slide Show presentation format. (...).*»
Source : www.threatgeek.com/2015/06/fidelis-threat-advisory-1017-phishing-in-plain-sight.html
Billets en relation :
09/06/2015. *Fidelis Threat Advisory #1017 Appendix* : www.fidelissecurity.com/sites/default/files/FTA_1017_Phishing_in_Plain_Sight-Appendix-FINAL.pdf
09/06/2015. *Fidelis Threat Advisory #1017* : www.fidelissecurity.com/sites/default/files/FTA_1017_Phishing_in_Plain_Sight-Body-FINAL.pdf

=> **Escaping VMware Workstation through COM1**. 09/06/2015. «*VMware Workstation offers printer "virtualization", allowing a Guest OS to access and print documents on printers available to the Host OS. On VMware Workstation 11.1, the virtual printer device is added by default to new VMs, and on recent Windows Hosts, the Microsoft XPS Document Writer is available as a default printer. Even if the VMware Tools are not installed in the Guest, the COM1 port can be used to talk to the Host printing Proxy (...).*»
Source : docs.google.com/document/d/1sIYgqrytPK-CFWfqDntraA_Fwi2Ov-YBgMtl5hdrYd4/edit?pli=1#

Billets en relation :
09/06/2015. *Source* : twitter.com/crypt0ad/status/608323169225711616
09/06/2015. *Vidéo* : drive.google.com/file/d/0B6P-iHujNOX2NVFMazBQY0kyUXM/view?pli=1
12/06/2015. *Escaping VMware Workstation through COM1* : www.exploit-db.com/docs/37276.pdf

=> **RAND study: Cyber-defense must change course, or else**. 10/06/2015. «*RAND today released the results of its multiphased study on cybersecurity's future, The Defender's Dilemma, delivering a frightening snapshot of defenders lost at sea (...).*»
Source : www.zdnet.com/article/rand-study-cyber-defense-must-change-course-or-else/
Billets en relation :
10/06/2015. *The Defender's Dilemma: Charting a Course Toward Cybersecurity* : www.rand.org/pubs/research_reports/RR1024.html
10/06/2015. *The Defender's Dilemma: Charting a Course Toward Cybersecurity* : www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf
10/06/2015. *RAND delivers a model for analyzing the economic drivers and challenges of cyber defense* : www.juniper.net/us/en/insights/rand2015/
11/06/2015. *Iterative Defense and The Intruder's Dilemma* : summitroute.com/blog/2015/06/11/iterative_defense_and_the_intruders_dilemma/
11/06/2015. *My 2015 Personal Security Guiding Principles and the New Rand Report* : securosis.com/blog/my-2015-personal-security-guiding-principles-and-the-new-rand-report
12/06/2015. *THE DEFENDER'S DILEMMA: CISO's and Execs to the right of me… APT's and Hackers to the left… Here I am stuck in the middle with you* : krypt3ia.wordpress.com/2015/06/12/the-defenders-dilemma-cisos-and-execs-to-the-right-of-me-apts-and-hackers-to-the-left-here-i-am-stuck-in-the-middle-with-you/

=> **The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns**. 10/06/2015. «*New zero-day used for effective kernel memory injection and stealth (...).*»
Source : securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/
Billets en relation :
10/06/2015. *Kaspersky Finds New Nation-State Attack—In Its Own Network* : www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/
10/06/2015. *Espionnage des négociations sur le nucléaire iranien : la Suisse et l'Autriche enquêtent* : www.lemonde.fr/pixels/article/2015/06/10/les-negociations-sur-le-nucleaire-iranien-espionnees-par-un-programme-informatique_4651449_4408996.html
10/06/2015. *Duqu is back: Kaspersky Lab reveals cyberattack on its corporate network* : www.kaspersky.com/about/news/virus/2015/Duqu-is-back
10/06/2015. *Kaspersky dévoile Duqu 2.0* : www.intrusio.fr/non-classe/kaspersky-devoile-duqu-2-0/
10/06/2015. *Stepson of Stuxnet stalked Kaspersky for months, tapped Iran nuke talks* : arstechnica.com/security/2015/06/stepson-of-stuxnet-stalked-kaspersky-for-months-tapped-iran-nuke-talks/
10/06/2015. *Duqu 2.0 found to target security company* : www.virusbtn.com/blog/2015/06_10.xml
10/06/2015. *Duqu 2.0: Reemergence of an aggressive cyberespionage threat* : www.symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat
11/06/2015. *The Mystery of Duqu 2.0 - 2.1* : securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf
11/06/2015. *Kaspersky being hacked is a lesson for us all* : grahamcluley.com/2015/06/kaspersky-hacked/
12/06/2015. *Hack Kaspersky, une leçon pour l'Anses et l'Anssi* : www.cnis-mag.com/hack-kaspersky-une-lecon-pour-lanses-et-lanssi.html
15/06/2015. *Stuxnet spawn infected Kaspersky using stolen Foxconn digital certificates* : arstechnica.com/security/2015/06/stuxnet-spawn-infected-kaspersky-using-stolen-foxconn-digital-certificates/
15/06/2015. *The Duqu 2.0 persistence module* : securelist.com/blog/research/70641/the-duqu-2-0-persistence-module/
16/06/2015. *Duqu APT malware 'undermines trust' in digital certificates* : www.scmagazineuk.com/duqu-apt-malware-undermines-trust-in-digital-certificates/article/420898/
17/06/2015. *Analysis of CVE-2015-2360 – Duqu 2.0 Zero Day Vulnerability* : blog.trendmicro.com/trendlabs-security-intelligence/analysis-of-cve-2015-2360-duqu-2-0-zero-day-vulnerability/

=> **Etudes Prospectives et Stratégiques**. 10/06/2015. «*Une grande partie de ces études, commandées et pilotées par les différents organismes du ministère (Direction générale des relations internationales et de la stratégie, Etat-major des armées, Etats-majors d'armée, Délégation générale pour l'armement, etc.) sont rendues publiques et mises à disposition sur le site de la DGRIS (...).*» Il me semble que suite au changement de désignation (DGRIS à la place de DAS), une actualisation des ressources en ligne a été faite. Des articles, de quelques mois à quelques années, ont été mis en ligne il me semble (alors que je ne crois pas qu'ils l'étaient). Bref, à fouiller. J'ai mis quelques éléments pour montrer ce qu'on peut y trouver d'intéressant, pour les lecteurs intéressés.
Source : www.defense.gouv.fr/das/reflexion-strategique/etudes-prospectives-et-strategiques
Billets en relation :
21/06/2013. *Description de la vulnérabilité´ des sociétés, des organisations ou des régimes politiques, selon leur nature, face aux*

possibilités offertes par les moyens de communication : www.defense.gouv.fr/content/download/327810/4516061/file/EPS2013-VulnerabilitesSocietesMoyensCommunication.pdf
21/09/2014. *La dualité dans les entreprises de défense* : www.defense.gouv.fr/content/download/339060/4749475/file/EPS2013-La%20dualit%C3%A9%20dans%20les%20entreprise%20de%20d%C3%A9fense.pdf
06/01/2015. *Réseau Internet et sécurité : Quel impact du progrès des Technologies de l'information et de la communication (TIC) sur la capacité de l'Etat français, de maîtrise du réseau et de sa sécurité d'ici 15 à 20 ans ?* : www.defense.gouv.fr/content/download/363921/5272321/file/EPS2013-R%C3%A9seau%20internet%20et%20s%C3%A9curit%C3%A9.pdf
15/03/2015. *CEIS - Description de la maniere dont la cybercriminalité et la lutte informatique sont abordées par les acteurs pouvant influencer le domaine* : www.defense.gouv.fr/content/download/375371/5509889/file/EPS2013-Cybercriminalite.pdf

=> **VoIP attacks are on the rise, particularly in the UK, according to new research by Nettitude** . 10/06/2015. «*During the first quarter of 2015, our security researchers have observed a large amount of VoIP attacks worldwide; however, the majority were against UK servers (...).*»
Source : www.nettitude.co.uk/voip-attacks-are-on-the-rise-particularly-in-the-uk-according-to-new-research-by-nettitude/
Billets en relation :
10/06/2015. *VoIP attacks are on the rise* : www.nettitude.co.uk/wp-content/uploads/2015/06/VoIP-attacks-on-the-rise-Jules-Pagna-Disso.pdf

=> **Symantec Intelligence Report: May 2015**. 11/06/2015. «*Welcome to the May edition of the Symantec Intelligence report. Symantec Intelligence aims to provide the latest analysis of cyber security threats, trends, and insights concerning malware, spam, and other potentially harmful business risks (...).*»
Source : www.symantec.com/connect/blogs/symantec-intelligence-report-may-2015
Billets en relation :
11/06/2015. *Symantec Intelligence Report: May 2015* : www.symantec.com/content/en/us/enterprise/other_resources/intelligence_report_05-2015.en-us.pdf

=> **Throwback Thursday: Virus Writers**. 11/06/2015. «*This Throwback Thursday, we bring you a series of articles from the archives that looked at virus writers, asking 'who are they?', 'why do they do it?', and other pertinent questions. (...).*» Relecture de vieux articles de 99.
Source : www.virusbtn.com/blog/2015/06_11.xml
Billets en relation :
11/06/2015. *3-why do they do it?* : www.virusbtn.com/virusbulletin/archive/2015/06/vb201506-throwback-thursday-virus-writers-3
11/06/2015. *2-How have they changed?* : www.virusbtn.com/virusbulletin/archive/2015/06/vb201506-throwback-thursday-virus-writers-2
11/06/2015. *1-Explain the inexplicable* : www.virusbtn.com/virusbulletin/archive/2015/06/vb201506-throwback-thursday-virus-writers-1

=> **How Many Million BIOSes Would you Like to infect ?**. 11/06/2015. «*In this paper, we are also providing evidence about the feasibility of widespread BIOS infection. For a Long time it has been assumed that BIOS malware was a theoretical possibility, but that in practice it was too Difficult to implement. One reason for this belief was the general notion that there was too much obscurity To overcome, and too much customization necessary to make infections widespread. This was perhaps true In legacy BIOSes. We don't know, because we started our research as legacy BIOS was being phased out, And UEFI BIOSes were coming to prominence. But we show here that it is demonstrably false on UEFI BIOSes (...).*»
Source : legbacore.com/Research_files/HowManyMillionBIOSesWouldYouLikeToInfect_Whitepaper_v1.pdf
Billets en relation :
11/06/2015. *Reearch* : legbacore.com/Research.html
16/06/2015. *Encore un super-virus immortel* : www.cnis-mag.com/encore-un-super-virus-immortel.html

=> **Amazon's bi-annual information request report**. 12/06/2015. «*Amazon's bi-annual information request report, available here, provides additional information on the types and volume of information requests we receive (...).*»
Source : blogs.aws.amazon.com/security/post/Tx35449P4T7DJIA/Privacy-and-Data-Security
Billets en relation :
12/06/2015. *Amazon's bi-annual information request report* : d0.awsstatic.com/certifications/Information_Request_Report.pdf
16/06/2015. *Amazon : un premier rapport de transparence trop léger* : www.nextinpact.com/news/95423-amazon-premier-rapport-transparence-trop-leger.htm

=> **Rapport d'activité Afnic 2014 : ouverture, compétitivité & responsabilité**. 12/06/2015. «*L'assemblée générale annuelle de l'Afnic s'est tenue le 12 juin 2015 et a adopté le rapport d'activité 2014. Découvrez-le ici (...).*»
Source : www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/9123/show/rapport-d-activite-afnic-2014-ouverture-competitivite-responsabilite-1.html

Billets en relation :
12/06/2015. *Rapport d'activité Afnic 2014 : ouverture, compétitivité & responsabilité* : www.afnic.fr/medias/documents/afnic-rapport-activite-2014.pdf

=> **Reuters Institute - Digital News Report 2015**. 15/06/2015. «*This year's report reveals new insights about digital news consumption based on a YouGov survey of over 20,000 online news consumers in the US, UK, Ireland, Germany, France, Italy, Spain, Denmark, Finland, Brazil, Japan and Australia. This year's data shows a quickening of the pace towards social media platforms as routes to audiences, together with a surge in the use of mobile for news, a decline in the desktop internet and significant growth in video news consumption online (...).*»
Source : www.digitalnewsreport.org/
Billets en relation :
15/06/2015. *Top findings from Reuters Institute Digital News Report 2015 in 100 seconds* : reutersinstitute.politics.ox.ac.uk/resource/top-findings-reuters-institute-digital-news-report-2015-100-seconds
16/06/2015. *Du téléspectateur à l'internaute : s'informer en ligne n'est pas (encore) une évidence* : www.rslnmag.fr/post/2015/06/16/information-usages-journalisme-internaute-reuters.aspx
16/06/2015. *Les médias face au pouvoir des réseaux sociaux* : www.lemonde.fr/actualite-medias/article/2015/06/16/les-medias-face-au-pouvoir-des-reseaux-sociaux_4655143_3236.html

=> **DD4BC DDoS Extortion Threat Activity**. 15/06/2015. «*Last week, ASERT provided Arbor customers with Situational Threat Brief 2015-04 DD4BC DDoS Extortion Threat Activity. This threat intelligence report profiles at least thirty-seven distinct attacks and/or attack campaigns launched by the DD4BC actor(s) between early 2014 and late May 2014. It includes sample extortion emails, related Bitcoin-based financial transactions, and references to several resources on how to easily mitigate attacks by this actor or by copycat attackers (...).*»
Source : asert.arbornetworks.com/dd4bc-ddos-extortion-threat-activity/
Billets en relation :
15/06/2015. *Situational Threat Brief 2015-04 DD4BC DDoS Extortion Threat Activity* : pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf

=> **Note d'information - DNS Rebinding - CERTFR-2015-INF-001**. 15/06/2015. «*Le DNS Rebinding vise à permettre à un attaquant situé dans un réseau d'accéder à une application web située dans un autre réseau. Le cas typique est la tentative d'accès à une application web du réseau interne d'un organisme par un attaquant situé sur Internet. Pour ce faire, l'attaquant contourne certains mécanismes de cloisonnement des navigateurs web en employant des réponses DNS fluctuantes. (...).*»
Source : www.cert.ssi.gouv.fr/site/CERTFR-2015-INF-001/CERTFR-2015-INF-001.html

=> **Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114**. 15/06/2015. «*This post analyzes targeted malware attacks against groups in the Tibetan diaspora and pro-democracy groups in Hong Kong. All of these attacks leveraged CVE-2014-4114 and were delivered via malicious Microsoft PowerPoint Slideshow files (*.pps). These attacks are highly targeted, appear to re-purpose legitimate content in decoy documents, and had very low antivirus (AV) detection rates at the time they were deployed (...).*»
Source : citizenlab.org/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/
Billets en relation :
15/06/2015. *Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114* : citizenlab.org/wp-content/uploads/2015/06/Targeted-Attacks-against-Tibetan-and-Hong-Kong-Groups-Exploiting-CVE-2014-4114.pdf
16/06/2015. *CVE-2014-4114: Tracing the Link* : www.threatgeek.com/2015/06/cve-2014-4114-tracing-the-link.html

=> **Le DoD vient de diffuser son "Law of War Manuel"**. 15/06/2015. «*C'est une première pour le ministère américain de la Défense (le doD): il vient de publier son "manuel de droit de la guerre" (1204 pages à télécharger ici) (...) On notera aussi le chapitre XVI sur les cyber-operations. (...).*»
Source : lignesdedefense.blogs.ouest-france.fr/archive/2015/06/15/le-dod-vient-de-diffuse-son-law-of-war-manuel-version-de-jui-14262.html
Billets en relation :
12/06/2015. *Law of War Manuel* : www.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf

=> **Using windows crash dumps for remote incident identification**. 16/06/2015. «*With the proliferation of defense mechanisms built into Windows Operating System,, such as ASLR, DEP, and SEHOP, it is getting more difficult for malware to successfully exploit it. (...).*»
Source : www.sans.org/reading-room/whitepapers/forensics/windows-crash-dumps-remote-incident-identification-36012

=> **Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependence On Apps, Software**. 16/06/2015. «*Encrypted Messaging With Fighters In Syria Or Iraq, Or Lone Wolf Jihadis In The West – One Click Away (...).*»
Source : www.memri.org/report/en/0/0/0/0/0/0/8610.htm
Billets en relation :
15/06/2015. *Darknet Jihad: These Aren't The Sites You Are Looking For* : krypt3ia.wordpress.com/2015/06/15/darknet-jihad-these-

arent-the-sites-you-are-looking-for/
19/06/2015. *Sophistication accrue de la technologie du cryptage adoptée par l'EI, Al-Qaïda et d'autres djihadistes* : www.memri.fr/2015/06/19/sophistication-accrue-de-la-technologie-du-cryptage-adoptee-par-lei-al-qaida-et-dautres-djihadistes-atteint-un-niveau-superieur/

=> **Operation Lotus Blossom: A New Nation-State Cyberthreat?**. 16/06/2015. «*Today Unit 42 published new research identifying a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia. The adversary group responsible for the campaign, which we named "Lotus Blossom," is well organized and likely state-sponsored, with support from a country that has interests in Southeast Asia. The campaign has been in operation for some time; we have identified over 50 different attacks taking place over the past three years (...).*»
Source : researchcenter.paloaltonetworks.com/2015/06/operation-lotus-blossom/
Billets en relation :
16/06/2015. *Operation Lotus Blossom* : www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html
17/06/2015. *'Lotus Blossom' cyberattacks hit military, gov't targets in Southeast Asia* : www.scmagazine.com/researchers-discover-50-cyber-attacks-in-lotus-blossom-campaign/article/421279/
17/06/2015. *Operation Lotus Blossom Sets Sights on Asian Military* : www.infosecurity-magazine.com/news/operation-lotus-blossom-sets/
17/06/2015. *The Spring Dragon APT* : securelist.com/blog/research/70726/the-spring-dragon-apt/

=> **National Cyber Security Structures Mapped and Compared** . 17/06/2015. «*The NATO Cooperative Cyber Defence Centre of Excellence is proud to announce that a selection of reports resulting from our National Cyber Security Organisation project is already available on our website. The aim of the project is to offer a comprehensive overview of existing national cyber security organisation models (...).*»
Source : ccdcoe.org/national-cyber-security-structures-mapped-and-compared.html
Billets en relation :
03/06/2015. *US Air Force Targets and Destroys ISIS HQ Building Using Social Media* : defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/
04/06/2015. *The War on Terror Is Now the War on Cyber* : motherboard.vice.com/read/the-war-on-terror-is-now-the-war-on-cyber
08/06/2015. *Inventer une cyberstratégie* : www.huyghe.fr/actu_1293.htm
11/06/2015. *US DNI - Cyber War, Netwar, and the Future of Cyberdefense* : www.dni.gov/index.php/newsroom/ic-in-the-news/211-ic-n-the-news-2015/1205-cyber-war,-netwar,-and-the-future-of-cyberdefense
11/06/2015. *Entretien sur les cybermenaces et la cyberstratégie russe* : harrel-yannick.blogspot.fr/2015/06/entretien-sur-les-cybermenaces-et-la.html
16/06/2015. *Le cyber en opérations* : www.egeablog.net/index.php?post/2015/06/14/Le-cyber-en-op%C3%A9rations
17/06/2015. *National Cyber Security Organisation* : ccdcoe.org/national-cyber-security-organisation.html
19/06/2015. *IDF to unify cyber warfare units* : www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war-future.html

=> **From ASM.JS to WebAssembly**. 17/06/2015. «*I'm burying the lede with context and catch-up material first, so impatient or already-clued-in readers should skip to below the videos for today's big news. Or just read Luke Wagner's blog post right now (...).*»
Source : brendaneich.com/2015/06/from-asm-js-to-webassembly/
Billets en relation :
18/06/2015. *WebAssembly* : www.developpez.com/actu/86605/Mozilla-Microsoft-et-Google-veulent-booster-le-Web-avec-un-nouveau-format-binaire-WebAssembly-represente-t-il-une-menace-pour-JavaScript/
19/06/2015. *WebAssembly* : sebsauvage.net/links/?6wF6ng

=> **Etudes marines n° 8 - Aspect stratégique des réseaux sous-marins**. 17/06/2015. «*Études Marines est une publication scientifique faisant intervenir des auteurs compétents et reconnus sur des sujets transversaux. Une multitude de points de vue réunis dans un seul ouvrage ! Cette revue prend la succession du Bulletin d'études de la Marine (...).*»
Source : cesm.marine.defense.gouv.fr/publications/etudes-marines/etudes-marines

=> **Critical Flaws in Apple, Samsung Devices**. 17/06/2015. «*Normally, I don't cover vulnerabilities about which the user can do little or nothing to prevent, but two newly detailed flaws affecting hundreds of millions of Android, iOS and Apple products probably deserve special exceptions (...) Separately, researchers at mobile security firm NowSecure disclosed they'd found a serious vulnerability in a third-party keyboard app that is pre-installed on more than 600 million Samsung mobile devices — including the recently released Galaxy S6 (...).*»
Source : krebsonsecurity.com/2015/06/critical-flaws-in-apple-samsung-devices/
Billets en relation :
16/06/2015. *Remote Code Execution as System User on Samsung Phones* : www.nowsecure.com/blog/2015/06/16/remote-code-execution-as-system-user-on-samsung-phones/
17/06/2015. *Apple CORED: Boffins reveal password-killer 0-days for iOS and OS X* :

www.theregister.co.uk/2015/06/17/apple_hosed_boffins_drop_0day_mac_ios_research_blitzkrieg/
17/06/2015. *Major zero-day security flaws in iOS & OS X allow theft of both Keychain and app passwords* : 9to5mac.com/2015/06/17/major-zero-day-security-flaws-in-ios-os-x-allow-theft-of-both-keychain-and-app-passwords/
17/06/2015. *Unauthorized Cross-App Resource Access on MAC OS X and iOS* : drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view?pli=1
17/06/2015. *Critical Flaws in Apple, Samsung Devices* : krebsonsecurity.com/2015/06/critical-flaws-in-apple-samsung-devices/

=> **Numéro 5 de DéfIS**. 17/06/2015. «*Le département Intelligence et sécurité économiques de l'INHESJ a le plaisir de vous adresser le numéro 5 de DéfIS, l'Intelligence stratégique au service de la compétitivité. Ce numéro intitulé Crime pharmaceutique, une épidémie silencieuse rassemble des analyses d'experts et une série d'entretiens conduits auprès de praticiens du privé et de la sphère publique concernés par la lutte contre les faux médicaments (...) Entretien avec : Jean-Claude COUSSERAN, directeur général de la DGSE de 2000 à 2003 et Philippe HAYEZ, magistrat à la Cour des comptes, co-responsables de l'enseignement sur le renseignement à Sciences-Po Paris et co-auteurs de l'ouvrage Renseigner les démocraties, renseigner en démocratie. Etienne DROUARD, chargé d'enseignement à l'INHESJ, avocat à la Cour - Cabinet K&L Gates : Loi sur le renseignement : un texte d'urgence attendu depuis 25 ans (...).*»
Source : www.inhesj.fr/mailling/defis/defis5.html
Billets en relation :
17/06/2015. *DéfIS n°5* : www.inhesj.fr/mailling/defis/defis5.pdf

=> **Stratégie numérique du Gouvernement**. 18/06/2015. «*Le Conseil national du numérique a remis, jeudi 18 juin, une synthèse de la grande concertation citoyenne lancée en octobre 2014. Sur cette base, le Gouvernement a présenté sa stratégie numérique et son plan d'actions, auquel chaque ministère a contribué. D'ici quelques semaines, un projet de loi numérique sera présenté pour mettre en œuvre les mesures législatives de ce plan d'actions (...).*»
Source : www.gouvernement.fr/la-republique-numerique-en-actes
Billets en relation :
18/06/2015. *L'AFDEL mécontente du rapport "Ambition Numérique" du CNNum* : www.numerama.com/magazine/33443-l-afdel-mecontente-du-rapport-34ambition-numerique34-du-cnnum.html
18/06/2015. *Rapport CCNUM - Ambition numérique* : contribuez.cnnumerique.fr/sites/default/files/media/CNNum--rapport-ambition-numerique.pdf
18/06/2015. *CP - Stratégie numérique du Gouvernement* : www.gouvernement.fr/sites/default/files/liseuse/4492/master/index.htm
18/06/2015. *Le gouvernement présente sa stratégie numérique pour la France* : www.lemonde.fr/pixels/article/2015/06/18/le-gouvernement-presente-sa-strategie-numerique-pour-la-france_4657207_4408996.html
18/06/2015. *« La révolution numérique pourrait saper les fondements de l'Etat »* : rue89.nouvelobs.com/2015/06/18/revolution-numerique-pourrait-saper-les-fondements-letat-259732
18/06/2015. *Loi Numérique : toutes les propositions du CNNum* : www.nextinpact.com/news/95462-loi-numerique-toutes-propositions-cnnum.htm
18/06/2015. *L'échec consommé de la gauche sur le numérique* : electronlibre.info/lechec-consomme-de-la-gauche-sur-le-numerique/
19/06/2015. *Rapport Ambition Numérique du CNNum* : standblog.org/blog/post/2015/06/19/Rapport-Ambition-numerique-CNNum
19/06/2015. *Un plan numérique incomplet* : www.lemonde.fr/idees/article/2015/06/19/un-plan-numerique-incomplet_4658034_3232.html
19/06/2015. *Le Premier ministre a présenté le 18 juin la stratégie numérique du Gouvernement* : www.ssi.gouv.fr/actualite/lanssi-acteur-de-la-strategie-numerique-de-la-france/

=> **Carte bancaire - 9 réflexes sécurité**. 18/06/2015. «*Même si l'amélioration de la sécurité des paiements par carte est constante, un certain nombre de précautions s'impose pour contribuer à éviter les fraudes : garder son code secret, être vigilant quand on communique les données de sa carte, faire rapidement opposition si besoin, porter plainte en cas de vol ou d'utilisation frauduleuse... Ce guide propose 9 réflexes sécurité (...).*» Des documents de bon sens de la fédération bancaire française.
Source : www.fbf.fr/Web/Internet2010/Content.nsf/DocumentsByIDWeb/B84417A439E1CA2DC1257E680051DDD7?OpenDocument
Billets en relation :
30/01/2015. *Ordres de virement des entreprises - 9 réflexes sécurité* : www.fbf.fr/Web/Internet2010/Content.nsf/DocumentsByIDWeb/AB701DDAD6DB0335C1257DDD0045162D?OpenDocument
20/02/2015. *Achats en ligne - 10 réflexes sécurité* : www.fbf.fr/Web/Internet2010/Content.nsf/DocumentsByIDWeb/375633B0EB8B512BC1257DF200330C33?OpenDocument
08/06/2015. *Veille - Avec ou sans contact..... à savoir* : pseudonyme.over-blog.net/2015/06/veille-avec-ou-sans-contact-a-savoir.html

=> **Who Has Your Back? 2015: Protecting Your Data From Government Requests report**. 18/06/2015. «*In this, our fifth annual Who Has Your Back report, we took the main principles of the prior reports and rolled them into a single category: Industry-Accepted Best Practices. We've also refined our expectations around providing users notice and added new categories to highlight other important transparency and user rights issues (...).*»
Source : www.eff.org/who-has-your-back-government-data-requests-2015
Billets en relation :
18/06/2015. *Le palmarès de l'EFF des services qui protègent vos données personnelles du gouvernement* :

www.lemonde.fr/pixels/article/2015/06/18/le-palmares-de-l-eff-des-services-qui-protegent-vos-donnees-personnelles-du-gouvernement_4657381_4408996.html
18/06/2015. *Who Has Your Back? 2015: Protecting Your Data From Government Requests report* : www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf
19/06/2015. *Vie privée : l'EFF encense Adobe, Apple et Dropbox, mais fustige WhatsApp* : www.nextinpact.com/news/95480-vie-privee-eff-encense-adobe-apple-et-dropbox-mais-fustige-whatsapp.htm

=> **Parution en ligne de « TIC & handicap », un numéro de la revue terminal**. 18/06/2015. «*Quelles contributions les technologies de l'information et de la communication peuvent-elles apporter à une meilleure insertion des personnes en situation de handicap ? Les articles et témoignages de ce numéro de la revue terminal, apportent chacun une réponse à cette question. (...).*»
Source : blogrecherche.wp.mines-telecom.fr/2015/06/18/parution-en-ligne-de-tic-handicap-le-dernier-numero-de-la-revue-terminal/
Billets en relation :
18/06/2015. *TIC & handicap* : terminal.revues.org/609

=> **Paper: Beta exploit pack: one more piece of crimeware for the infection road**. 19/06/2015. «*Today, we publish an article by researchers Aditya K. Sood and Rohit Bansal, in which they look at a new exploit kit, 'Beta'. Though it is still in a testing phase, Aditya and Rohit managed to gain access to one of its command-and-control servers and were thus able to learn details of the exploit kit, including its price, the structure of the URLs it uses, and the exploits that are being used (...).*»
Source : www.virusbtn.com/blog/2015/06_19.xml
Billets en relation :
15/06/2015. *Fast look at Sundown EK* : malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html
18/06/2015. *Beta exploit pack: one more piece of crimeware for the infection road* : www.virusbtn.com/pdf/magazine/2015/vb201506-Beta-BEP.pdf
18/06/2015. *Beta exploit pack: one more piece of crimeware for the infection road* : www.virusbtn.com/virusbulletin/archive/2015/06/vb201506-Beta-BEP

Conférences & Forums

=> **HITB Amsterdam Wrap-Up Day #1**. 28/05/2015. «*The HITB crew is back in the beautiful city of Amsterdam for a new edition of their security conference. Here is my wrap-up for the first day (...).*»
Source : blog.rootshell.be/2015/05/28/hitb-amsterdam-wrap-up-day-1-2/
Billets en relation :
28/05/2015. *HITB Amsterdam WhitePapers* : conference.hitb.org/hitbsecconf2015ams/materials/Whitepapers/
28/05/2015. *HITBSecConf2015 Amsterdam* : conference.hitb.org/hitbsecconf2015ams/
28/05/2015. *HITB Amsterdam Matérials* : conference.hitb.org/hitbsecconf2015ams/materials/
29/05/2015. *HITB Amsterdam Wrap-Up Day #2* : blog.rootshell.be/2015/05/29/hitb-amsterdam-wrap-up-day-2-2/
03/06/2015. *ERNW@HAXPO/HITB 2015* : www.insinuator.net/2015/06/ernwhaxpohitb-2015/
10/06/2015. *Retour sur la Hack In The Box Amsterdam 2015* : blog.xmco.fr/index.php?post/2015/06/09/Retour-sur-la-Hack-In-The-Box-Amsterdam-2015
18/06/2015. *Stegosploit : l'attaque par l'image* : cyberland.centerblog.net/239-Stegosploit-attaque-par-image

=> **Sud Web 2015**. 29/05/2015. «*Sud Web est la conférence itinérante à taille humaine qui privilégie le bien-être et les valeurs d'échanges. Deux journées dédiées à l'amélioration continue pour mieux travailler ensemble (...).*»
Source : sudweb.fr/2015/
Billets en relation :
29/05/2015. *Programme* : sudweb.fr/2015/programme.html
30/05/2015. *Sud Web 2015 - Vidéos* : vimeo.com/sudweb
03/06/2015. *Micro @HalluFMR #37 : Conférence, avec Nathalie Rosenberg et Frank Taillandier* : dascritch.net/post/2015/06/03/micro-%40HalluFMR-37-%3A-Conf%C3%A9rence%2C-avec-Nathalie-Rosenberg-et-Frank-Taillandier

=> **CARO 2015 – wrap up** . 29/05/2015. «*In May, I've visited the CARO workshop for the first time, representing Panda Security (not as a speaker, simply as an attendee) (...).*» Trop de ressources (slides) à indiquer, je mets juste le lien en direction des différentes présentations.
Source : bartblaze.blogspot.fr/2015/05/caro-2015-wrap-up.html
Billets en relation :
29/05/2015. *CARO 2015 - Presentations* : 2015.caro.org/presentations

=> **Blog 5: Beyond the Thunderdome: A Review of TROOPERS15**. 03/06/2015. «*The final blog in our series "Beyond the Thunderdome: A Review of TROOPERS15" focuses Exploitation & Attacking. With the last of this series we hope we you are already fired up and inspired for what lays a head during our upcoming TROOPERS16 (...).*» Un peu tardivement suite à l'évènement. Les ressources dédiées à cette

manifestation avait déjà été évoquée dans les précédentes brèves.
Source : www.insinuator.net/2015/06/blog-5-beyond-the-thunderdome-a-review-of-troopers15/
Billets en relation :
27/03/2015. *TROOPERS15 - Talks* : www.youtube.com/playlist?list=PL1eoQr97VfJkfckz9nZFR7tZoBkjij23f
25/05/2015. *Blog 1: Beyond the Thunderdome: A Review of TROOPERS15* : www.insinuator.net/2015/05/beyond-the-thunderdomea-review-of-troopers15/
27/05/2015. *Blog 2: Beyond the Thunderdome: A Review of TROOPERS15* : www.insinuator.net/2015/05/blog-2-beyond-the-thunderdomea-review-of-troopers15/
29/05/2015. *Blog 3: Beyond the Thunderdome: A Review of TROOPERS15* : www.insinuator.net/2015/05/blog-3-beyond-the-thunderdomea-review-of-troopers15/
31/05/2015. *Troopers15 Keynote: The hard thing about hard things* : blog.thinkst.com/2015/05/troopers15-keynote-hard-thing-about.html
01/06/2015. *Blog 4: Beyond the Thunderdome: A Review of TROOPERS15* : www.insinuator.net/2015/06/blog-4-beyond-the-thunderdome-a-review-of-troopers15/

=> **SSTIC 2015 - Jour 1**. 03/06/2015. «*Bon, c'est repartis pour un nouveau SSTIC. Cette année, les actes sont très réussis, et Très épais... ça pèse lourd dans le sac. Le ton est donné, cette année il y aura du lourd ;) (...).*»
Source : www.n0secure.org/2015/06/sstic-2015-jour-1.html
Billets en relation :
04/06/2015. *SSTIC 2015 - Jour 2* : www.n0secure.org/2015/06/sstic-jour-2.html
05/06/2015. *Vidéos et slides des présentations SSTIC 2015* : www.sstic.org/2015/programme/
05/06/2015. *Actes #sstic disponibles en ebooks* : static.sstic.org/ebooks/2015/
05/06/2015. *SSTIC 2015 - Jour 3* : www.n0secure.org/2015/06/sstic-2015-jour-1.html
07/06/2015. *No Limit Sécu [podcast] - SSTIC - feedback de Nicolas Ruff, Stéphane Sciacco et Christophe Chasseboeuf* : www.nolimitsecu.fr/sstic-2015/
07/06/2015. *Challenge 2015 SSTIC - Présentation et solutions* : communaute.sstic.org/ChallengeSSTIC2015
12/06/2015. *Présentations de l'ANSSI au SSTIC 2015* : www.ssi.gouv.fr/actualite/retrouvez-les-presentations-de-lanssi-au-sstic-2015/
17/06/2015. *Retour sur l'édition 2015 du SSTIC* : blog.xmco.fr/index.php?post/2015/06/17/Retour-sur-%C3%A9dition-2015-SSTIC

=> **Web2day**. 03/06/2015. «*Le Web2day offre, en 3 jours, un condensé des dernières tendances et des meilleures pratiques en matière d'innovation. Conférences, workshops, showroom, concours de startups, soirées, les professionnels du numérique viennent faire le plein de nouveautés, d'inspiration et de rencontres. Le festival s'adresse à l'ensemble des acteurs du numérique (...).*»
Source : web2day.co/programme/
Billets en relation :
03/06/2015. *Web2day : UX mobile et innovation : luxe ou obsession ?* : blog.gaborit-d.com/web2day-ux-mobile-et-innovation-luxe-ou-obsession/
04/06/2015. *Médias en ligne : quel avenir pour leur monétisation ?* : www.blogdumoderateur.com/conference-monetisation-media/
05/06/2015. *Le #web2day en chiffres* : www.blogdumoderateur.com/web2day-2015-chiffres/
05/06/2015. *Vidéos Web2day* : www.youtube.com/channel/UCCzfEV7NDD5OvkE3Ua7pcxQ/videos
10/06/2015. *Nos 25 mn de conférence sur les droits et libertés sur Internet en France* : www.numerama.com/magazine/33350-nos-25-mn-de-conference-sur-les-droits-et-libertes-sur-internet-en-france.html
19/06/2015. *Décryptage : l'intérêt du storytelling pour les marques* : www.blogdumoderateur.com/decryptage-storytelling-marques/

=> **Infosecurity Europe - Nouvelles pressions sur le chiffrement**. 04/06/2015. «*C'est donc sans surprise que le sujet du chiffrement s'est invité à Infosecurity Europe, cette semaine, à Londres (...).*»
Source : www.lemagit.fr/actualites/4500247524/Nouvelles-pressions-sur-le-chiffrement
Billets en relation :
02/06/2015. *L'ANSSI présente aux côtés des entreprises françaises sur le pavillon France du salon Infosecurity Europe* : www.ssi.gouv.fr/actualite/lanssi-presente-aux-cotes-des-entreprises-francaises-sur-le-pavillon-france-du-salon-infosecurity-europe/
04/06/2015. *Cazeneuve : 'Le développement de la cryptologie sur internet nous pose aujourd'hui un problème'* : www.assemblee-nationale.fr/14/cr-cloi/14-15/c1415072.asp
04/06/2015. *Infosecurity Europe - Media centre* : www.infosecurityeurope.com/media-centre/
18/06/2015. *Le chiffrement et l'anonymat : indispensables à la liberté de l'information* : fr.rsf.org/le-chiffrement-et-l-anonymat-18-06-2015,48010.html

=> **Le Futur en Seine, c'est maintenant** . 04/06/2015. «*150 innovations numériques françaises et internationales, 1 programme de conférence par des visionnaires du monde entier, 2 soirées pour faire l'expérience de la création numérique à 360°, 4 jours de networking, plus de 20 ateliers pour toute la famille et 160 événements partenaires dans toute la région Ile-de-France (...).*»
Source : www.inriality.fr/culture-loisirs/fens2015/le-futur-en-seine/
Billets en relation :
10/06/2015. *L'Institut Mines-Télécom à Futur en Seine* : blogrecherche.wp.mines-telecom.fr/2015/06/10/linstitut-mines-telecom-a-

futur-en-seine/
11/06/2015. *Futur en Seine - Programme* : www.futur-en-seine.paris/programme/
13/06/2015. *Futur en Seine, le meilleur des innovations numériques* : www.lemonde.fr/pixels/visuel/2015/06/13/festival-futur-en-seine-le-best-of-des-innovations-numeriques_4653285_4408996.html
17/06/2015. *Mobilis in mobile* : www.strategies.fr/blogs-opinions/idees-tribunes/1018286W/j-y-etais.html

=> **BSidesLondon 2015 Wrap-Up**. 04/06/2015. «*Here is a quick wrap-up of the just finished BSidesLondon. It was already the 5th edition (and my 5th participation!) (...).*» Pas vu les ressources accessibles.
Source : blog.rootshell.be/2015/06/04/bsideslondon-2015-wrap-up/
Billets en relation :
04/06/2015. *BSidesLondon 2015* : www.securitybsides.org.uk/schedule.html
08/06/2015. *Advanced Security Evaluation of Network Protocols* : www.insinuator.net/2015/06/advanced-security-evaluation-of-network-protocols/

=> **Hack in Paris 2015**. 15/06/2015. «*It is this gap that Hack In Paris aims to fill. After the success of last year, with more than 400 attendees, this 5 days corporate event will be held for the fifth time in France, at the Academie Fratellini Paris. Hack In Paris will let its attendees discovering the concrete reality of hacking, and its consequences for companies. The program includes the state of the art of IT security, industrial espionage, penetration testing, physical security, forensics, malware analysis and countermeasures. (...).*» A surveiller pour les archives vidéo et présentations qui ne sont pas encore en ligne.
Source : www.hackinparis.com/home
Billets en relation :
18/05/2015. *Hack In Paris 2015* : korben.info/hack-in-paris-2015.html
01/06/2015. *Hack in Paris, NDH, nécessaire partage de savoir* : www.cnis-mag.com/hack-in-paris-ndh-necessaire-partage-de-savoir.html
20/06/2015. *(slides) Axelle Apvrille - Fitness Tracker: Hack In Progress* : www.mediafire.com/view/djdr5sw25dqrr3y/fitbit-hackinparis.pdf

=> **Retour en vidéos sur le Toulouse Cyberdefense Workshop**. 17/06/2015. «*Le 29 Avril 2015, la CCI de Toulouse et ToulÉco organisaient au palais consulaire de la CCI de Toulouse le Toulouse Cyberdefense Workshop, premier workshop toulousain sur la cyberdéfense des PME en Midi-Pyrénées. Soutenu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), son objectif était de sensibiliser les PME aux attaques informatiques et à informer sur les enjeux de la cybersécurité. A cette occasion, une série d'interview vidéos ont été réalisées par ToulÉco.tv . Compilatio (...).*»
Source : www.vedocci.fr/retour-en-videos-sur-le-toulouse-cyberdefense-workshop/

=> **Pas sage en seine 2015**. 17/06/2015. «*PSES mêle conférences et ateliers, l'entrée y est toujours libre, gratuite et ouverte à tous et à toutes. Les sujets abordés y sont vastes et ne sont pas forcément techniques (du hack au partage, en passant par l'art, l'électronique ou la presse, jusqu'à la vie de tous les jours) (...).*»
Source : www.passageenseine.org/fr/accueil
Billets en relation :
17/06/2015. *Archives des précédentes éditions* : www.passageenseine.org/fr/archives-et-videos/
17/06/2015. *Programme PSES 2015* : www.passageenseine.org/fr/programme/
20/06/2015. *Vidéos et présentations PSES 2015* : numaparis.ubicast.tv/channels/#pas-sage-en-seine-2015

=> **Octopus 2015**. 17/06/2015. «*17-19 June 2015, Council of Europe, Strasbourg, France . Cooperation against Cybercrime (...).*»
Source : Http://www.coe.int/en/web/cybercrime/octopus2015
Billets en relation :
17/06/2015. *Secretary General: Cybercrime is reaching epic proportions* : www.coe.int/en/web/portal/-/secretary-general-cybercrime-is-reaching-epic-proportions
17/06/2015. *Octopus Presentations* : www.coe.int/en/web/cybercrime/presentations2015
17/06/2015. *Conference videos* : www.coe.int/en/web/cybercrime/conference-videos
17/06/2015. *UE-La lutte contre la cybercriminalité se perd dans les nuages* : www.challenges.fr/economie/20150617.REU8935/ue-la-lutte-contre-la-cybercriminalite-se-perd-dans-les-nuages.html
17/06/2015. *Current challenges in fighting cybercrime [EN] - Interview with Alexander Seger* : www.coe.int/en/web/portal/-/interview-the-current-challenges-in-fighting-cybercrime-en-
18/06/2015. *Le Conseil de l'Europe et sa convention de Budapest luttent contre un cybercrime difficile à contrer* : geopolis.francetvinfo.fr/une-convention-internationale-pour-lutter-contre-le-cybercrime-65027

=> **Recon Montreal 2015**. 19/06/2015. «*REcon is a computer security conference with a focus on reverse engineering and advanced exploitation techniques. It is held annually in Montreal, Canada (...).*» Archives des présentations pas encore en ligne. Mais celles-ci et les vidéos le sont normalement à terme.
Source : www.recon.cx/
Billets en relation :

19/06/2015. *Abusing Silent Mitigations* : h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/599/1/WP-Hariri-Zuckerbraun-Gorenc-Abusing_Silent_Mitigations.pdf
19/06/2015. *Abusing-silent-mitigations* : github.com/thezdi/abusing-silent-mitigations
19/06/2015. *There and back again: a journey through bounty award and disclosure* : h30499.www3.hp.com/t5/HP-Security-Research-Blog/There-and-back-again-a-journey-through-bounty-award-and/ba-p/6756465

=> **Nuit du Hack** . 20/06/2015. «*Initiée en 2003 par l'équipe Hackerz Voice, et inspiré par la célèbre DEF CON de Las Vegas, la "Nuit du Hack" est l'une des plus anciennes conférence de hacking underground francophone. (...).*»
Source : nuitduhack.com/fr/
Billets en relation :
20/06/2015. *Talks NDH* : nuitduhack.com/fr/talks.html
20/06/2015. *Live Streaming - Conférences - Nuit du Hack 2K15* : www.youtube.com/watch?v=8l8Ttf3PDVI
20/06/2015. *"Notre rôle est d'éviter les actes de sabotage. Ns avons besoin de la nouvelle génération"* : twitter.com/qwantcom/status/612173893495824384/photo/1
21/06/2015. *No Limit Sécu - Pourquoi es-tu venu à NDH15 ?* : www.nolimitsecu.fr/nuit-du-hack-2015/
21/06/2015. *How the ndh2k15 reward was made* : blog.electrolab.fr/2015/06/21/how-the-ndh2k5-reward-was-made/

Actus Généralistes

=> **Les douanes ont acheté des appareils de surveillance des mobiles dont l'utilisation est illégale**. 26/05/2015. «*Alors que les services de l'Etat ne semblent pas avoir voulu cacher ces marchés publics – les documents les recensant sont librement accessibles sur Internet – la direction des douanes n'a pas été en mesure d'expliquer leur achat alors que la loi interdit, jusqu'à présent, leur utilisation (...).*» Actu déjà évoquée dans les précédentes brèves.
Source : www.laquadrature.net/fr/lemonde-les-douanes-ont-achete-des-appareils-de-surveillance-des-mobiles-dont-l-utilisation-est-ille
Billets en relation :
02/06/2015. *Etat français et Amesys : business as usual (bis repetita)* : reflets.info/etat-francais-et-amesys-business-as-usual-bis-repetita/
03/06/2015. *L'Etat, ce bon client de la société Elexo* : reflets.info/letat-ce-bon-client-de-la-societe-elexo/
21/06/2015. *Le business des écoutes et des données personnelles* : moreas.blog.lemonde.fr/2015/06/21/le-business-des-ecoutes-et-des-donnees-personnelles/

=> **World Wide Push : l'internet des objets me file des boutons**. 28/05/2015. «*Ils s'appellent Dash ou Flic. Et ce sont des boutons. Mais des boutons "connectés". Et il paraît que c'est l'avenir (...).*»
Source : affordance.typepad.com//mon_weblog/2015/05/world-wide-push-internet-objets-boutons.html
Billets en relation :
02/06/2015. *Schizo-haptie : l'interface du faux-mouvement et la schizophrénie du geste-contrôle* : affordance.typepad.com//mon_weblog/2015/06/schizohaptie-faux-mouvement-interface-schizophrenie-geste-controle.html

=> **Plaidoyer pour un blog**. 31/05/2015. «*Récemment le petit monde de la sécurité informatique francophone s'est ému de la déroute judiciaire vécu par l'auteur du blog krach.in (...).*»
Source : cryptobourrin.wordpress.com/2015/05/31/plaidoyer-pour-un-blog/

=> **Des chercheurs français planchent sur le stockage du futur**. 04/06/2015. «*Une équipe du CNRS est parvenue à stocker et lire un message de plusieurs bits à l'échelle moléculaire sur un polymère. Une première mondiale qui devrait permettre à terme de conserver des quantités phénoménales de données sur de tous petits volumes (...).*»
Source : www.01net.com/editorial/656732/des-chercheurs-francais-planchent-sur-le-stockage-du-futur/
Billets en relation :
28/05/2015. *Communiqué de presse national du CNRS : "Des polymères inscriptibles, lisibles et effaçables"* : www.ics-cnrs.unistra.fr/spip.php?article1466

=> **Facebook et Intel sous le charme des mathématiciens français**. 05/06/2015. «*Deux géants du numérique viennent de succomber à l'une des beautés cachées de la France : son école de mathématique. Intel, monstre historique des semi-conducteurs et Facebook, le plus jeune des Gafa, viennent tous les deux d'annoncer l'ouverture de laboratoire de recherche avancé en France. Le premier sur les big data, le second sur l'intelligence artificielle (...).*»
Source : www.usine-digitale.fr/article/facebook-et-intel-sous-le-charme-des-mathematiciens-francais.N333726
Billets en relation :
05/06/2015. *Inria partenaire du nouveau labo d'IA de Facebook à Paris* : www.inria.fr/actualite/actualites-inria/inria-partenaire-du-labo-d-ia-de-facebook

=> **Microsoft ouvre son centre de transparence européen**. 08/06/2015. «*Microsoft vient d'ouvrir son centre de transparence européen,*

à Bruxelles, annoncé en février 2014. après des mois de révélations sur les activités de renseignement de la NSA. Dans ce centre, les clients gouvernementaux de l'éditeur pourront analyser le code source de ses produits, afin « de s'assurer eux-mêmes de son intégrité et confirmer l'absence de porte dérobée » (...). » Hum.
Source : www.lemagit.fr/actualites/4500247703/Microsoft-ouvre-son-centre-de-transparence-europeen
Billets en relation :
03/06/2015. *Microsoft Transparency Center opens in Brussels* : blogs.microsoft.com/eupolicy/2015/06/03/microsoft-transparency-center-opens-in-brussels/

=> **Drone d'histoire et pseudo-terrorisme**. 08/06/2015. «*Autrefois, on appelait ça « lâcher de ballons dans les écoles primaires », « club d'aéromodélisme », « fabrication d'un Cerf-Volant »… aujourd'hui, tout ça est devenu « atteinte à la sûreté de l'Etat » (...).* »
Source : www.cnis-mag.com/drone-dhistoire-et-pseudo-terrorisme.html
Billets en relation :
15/06/2015. *Les défis de la lutte anti-drone* : www.ttu.fr/les-defis-de-la-lutte-anti-drone/

=> **Comment un accord commercial confidentiel pourrait changer l'Internet mondial**. 11/06/2015. «*Auparavant, les accords commerciaux portaient sur des sujets tels que les tarifs douaniers. Aujourd'hui, il n'est plus seulement question de commerce mais aussi de réglementations qui façonnent la vie privée en ligne (...).* »
Source : www.slate.fr/story/102673/accord-commercial-tisa-internet-vie-privee

=> **Wassenaar, un pas de moins pour la démocratie et la sécurité TIC**. 11/06/2015. «*Wassenaar, paisible bourgade des Pays Bas réputée pour son Zoo et le fait qu'il ne s'y passe pratiquement jamais rien fut, en 1996, le lieu où se rédigèrent les fameux « arrangements » portant le nom de la ville, et aux termes desquels les différentes puissances mondiales s'entendaient pour effectuer un contrôle des exportations d'armes (...).* »
Source : www.cnis-mag.com/wassenaar-un-pas-de-moins-pour-la-democratie-et-la-securite-tic.html
Billets en relation :
23/05/2015. *US Govt proposes to classify cybersecurity or hacking tools as weapons of war* : betanews.com/2015/05/23/us-govt-proposes-to-classify-cybersecurity-or-hacking-tools-as-weapons-of-war/
12/06/2015. *Commerce Department FAQ on Proposed Wassenaar Implementation Gives Answers, Raises More Questions* : www.eff.org/deeplinks/2015/06/commerce-department-faq-proposed-wassenaar-implementation-gives-answers-raises

=> **Ni complotisme, ni conformisme**. 12/06/2015. «*Depuis quelques mois, un certain nombre de travaux ont permis de mieux comprendre le phénomène du complotisme. Ou plutôt de comment Internet démultiplie les effets, la visibilité et surtout la viralité de thèses plus ou moins farfelues (...).* »
Source : www.guerres-influences.com/ni-complotisme-ni-conformisme/

=> **Massive route leak causes Internet slowdown**. 12/06/2015. «*Earlier today a massive route leak initiated by Telekom Malaysia (AS4788) caused significant network problems for the global routing system. Primarily affected was Level3 (AS3549 – formerly known as Global Crossing) and their customers. Below are some of the details as we know them now (…).* »
Source : www.bgpmon.net/massive-route-leak-cause-internet-slowdown/
Billets en relation :
12/06/2015. *Global Collateral Damage of TMnet leak* : research.dyn.com/2015/06/global-collateral-damage-of-tmnet-leak/
12/06/2015. *Alerte en Malaisie, une nouvelle fuite BGP* : www.bortzmeyer.org/bgp-malaisie.html

=> **Suggestions à destination du gouvernement**. 15/06/2015. «*Plus sérieusement : s'il demeure de la responsabilité de celui qui l'utilise d'utiliser un marteau pour enfoncer un clou ou la tête d'un passant, aucune technologie n'est neutre et Internet n'échappe pas à la règle (...).* »
Source : page42.org/suggestions-a-destination-du-gouvernement/
Billets en relation :
15/06/2015. *Cazeneuve voit « tous les jours des drames à cause d'internet »* : lehollandaisvolant.net/?d=2015/06/15/19/20/53-cazeneuve-voit-tous-les-jours-des-drames-a-cause-dinternet
15/06/2015. *Cazeneuve voit "tous les jours des drames à cause d'internet"* : www.numerama.com/magazine/33398-cazeneuve-voit-tous-les-jours-des-drames-a-cause-d-internet.html
17/06/2015. *Internet, ennemi de la Sécurité Intérieure* : www.cnis-mag.com/internet-ennemi-de-la-securite-interieure.html

=> **La SNCF a-t-elle raison de vendre ses données ?**. 16/06/2015. «*La SNCF annoncera cet été les tarifs de ses données ouvertes, notamment les horaires des trains, en mode freemium (payant uniquement pour les gros consommateurs) comme annoncé en février dans le plan numérique du Groupe. Un choix qui interroge sur la notion de données d'intérêt général, et fait débat (...).* »
Source : www.usine-digitale.fr/editorial/la-sncf-a-t-elle-raison-de-vendre-ses-donnees.N336238
Billets en relation :
28/05/2015. *OSM Tchoutchou - Du coup ben ... tant pis* : www.raildar.fr
28/05/2015. *La SNCF torpille un site d'info temps réel [de ses propres trains]* : reflets.info/la-sncf-torpille-un-site-dinfo-temps-reel-de-

ses-propres-trains/

=> **Journalistes et lanceurs d'alerte sont-ils menacés par la directive sur le secret des affaires ?**. 17/06/2015. «*Le collectif « Informer n'est pas un délit », emmené par la journaliste de France 2, rédactrice en chef du magazine Cash Investigation, avait réuni plus de 310 000 signatures mardi 16 juin, alors que la commission juridique du Parlement européen donnait son feu vert à la directive sur le secret des affaires (...).*»
Source : www.lemonde.fr/les-decodeurs/article/2015/06/17/journalistes-et-lanceurs-d-alerte-sont-ils-menaces-par-la-directive-sur-le-secret-des-affaires_4655743_4355770.html
Billets en relation :
04/06/2015. *UNESCO publication "Protecting Journalism Sources in the Digital Age"* : www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf
04/06/2015. *UNESCO publication "Protecting Journalism Sources in the Digital Age"* : www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/unesco_research_is_previewed_at_editors_congress/
15/06/2015. *Directive secret des affaires : comment l'Europe est en train de tuer le secret des sources en toute discrétion* : www.atlantico.fr/decryptage/directive-secret-affaires-comment-europe-est-en-train-tuer-secret-sources-en-toute-discretion-nicolas-gros-verheyde-2191575.html

=> **Ces mutuelles santé qui remboursent les objets connectés**. 18/06/2015. «*Pasteur Mutualité crée un forfait de prise en charge d'objets connectés dans ses complémentaires santé. Les mutuelles jouent officiellement la carte de la prévention (...).*»
Source : pro.01net.com/editorial/658194/ces-mutuelles-sante-qui-remboursent-les-objets-connectes/
Billets en relation :
18/05/2015. *Cahier d'exploration "Self Data"* : fing.org/?Cahier-d-exploration-Self-Data
26/05/2015. *Selfdata : quels services pour quels usages ?* : www.internetactu.net/2015/05/26/selfdata-quels-services-pour-quels-usages/
07/06/2015. *E-santé - newsletter n°7 - mai 2015* : billaut.typepad.com/jm/2015/06/-e-sant%C3%A9-newsletter-n7-mai-2015-.html
08/06/2015. *Regards des Français sur les objets connectés dans le domaine de l'assurance* : www.ifop.com/?option=com_publication&type=poll&id=3051

=> **Les machines qui nous écoutent - Ethan Zuckerman**. 19/06/2015. «*Le chercheur Ethan Zuckerman (@EthanZ) s'est rendu récemment à la conférence sur les machines qui écoutent, nous raconte-t-il sur son blog. Les machines dotées d'un micro pour nous écouter sont de plus en plus nombreuses : outre Google ou Siri, outre votre téléphone, il y a aussi votre télé, des jouets et des jeux (des jouets transactionnels, comme le souligne avec justesse le chercheur Olivier Ertzscheid), Echo, des robots, et nombre d'objets connectés. La dernière poupée Barbie, dont le logiciel est développé par ToyTalk, est emblématique (...).*»
Source : alireailleurs.tumblr.com/post/121907188343/les-machines-qui-nous-ecoutent-ethan-zuckerman#_=_
Billets en relation :
14/06/2015. *Teddy Bear 3.0 : des jouets de données* : affordance.typepad.com//mon_weblog/2015/06/teddy-bear-jouets-donnees.html
15/06/2015. *Listening Machines, and the whether, when and how of new technologies* : www.ethanzuckerman.com/blog/2015/06/15/listening-machines-and-the-whether-when-and-how-of-new-technologies/

=> **Les fermetures d'usines de semi-conducteurs vont s'accélérer, prévient IC Insights**. 19/06/2015. «*Depuis 2009, l'industrie des semi-conducteurs a fermé 83 usines dont le monde, dont trois en France, selon IC Insights. Et la vague de consolidation en marche dans le secteur risque d'accélérer les fermetures, prévient le cabinet américain (...).*» L'occasion de redécouvrir la très intéressante trilogie d'articles, déjà évoquée, d'Olivier Ezratty sur STMicroelectronics.
Source : www.usine-digitale.fr/article/les-fermetures-d-usines-de-semi-conducteurs-vont-s-accelerer-previent-ic-insights.N337021
Billets en relation :
23/12/2014. *A la découverte de la "fab" chez STMicroelectronics : 1* : www.oezratty.net/wordpress/2014/decouverte-fab-stmicroelectronics-1/
29/12/2014. *A la découverte de la "fab" chez STMicroelectronics : 2* : www.oezratty.net/wordpress/2014/decouverte-fab-stmicroelectronics-2/
30/12/2014. *A la découverte de la "fab" chez STMicroelectronics : 3* : www.oezratty.net/wordpress/2014/decouverte-fab-stmicroelectronics-3/
08/06/2015. *STMicroelectronics : les syndicats craignent la fermeture d'une usine en France* : www.usine-digitale.fr/article/stmicroelectronics-les-syndicats-craignent-la-fermeture-d-une-usine-en-france.N334362

=> **Notre visage est de plus en plus scanné** . 20/06/2015. «*VIDÉO. La reconnaissance faciale, en plein boom, intéresse désormais les banques, les hôpitaux et les... prisons. Décryptage dans #TECH24 (...).*»
Source : www.lepoint.fr/technologie/notre-visage-est-de-plus-en-plus-scanne-20-06-2015-1938494_58.php
Billets en relation :
02/06/2015. *CRIStAL : 430 chercheurs lillois réunis pour la recherche en STIC* : blogrecherche.wp.mines-telecom.fr/2015/06/02/cristal-430-chercheurs-lillois-reunis-pour-la-recherche-en-stic/
11/06/2015. *Facial recognition technology is everywhere. It may not be legal* : www.washingtonpost.com/blogs/the-

switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/
16/06/2015. *Metalleux «scannés» par la police durant le festival* : www.20min.ch/ro/news/insolite/story/Metalleux--scannes--par-la-police-durant-le-festival-10576215
17/06/2015. *Reconnaissance faciale : avons-nous droit à la confidentialité biométrique ? - Washington Post* : alireailleurs.tumblr.com/post/121737023394/reconnaissance-faciale-avons-nous-droit-a-la#_=_
18/06/2015. *Thales présente des « robots contrôleurs d'identité » pour les aéroports* : www.01net.com/editorial/658174/thales-presente-des-robots-controleurs-d-identite-pour-les-aeroports/

Outils/Services/Sites à découvrir ou à redécouvrir

=> **Linux-internals**. 26/05/2015. «*A series of posts about the linux kernel and its insides. The goal is simple - to share my modest knowledge about the internals of the linux kernel and help people who are interested in the linux kernel internals, and other low-level subject matter (...).*»
Source : 0xax.gitbooks.io/linux-insides/content/index.html
Billets en relation :
23/05/2015. *Linux-insides* : github.com/0xAX/linux-insides

=> **Yara-Rules**. 26/05/2015. «*Repository of yara rules. This project covers the need of a group of IT Security Researches to have a single repository where different Yara signatures are compiled, classified and kept as up to date as possible, and begin as an open source community for collecting Yara rules. Our Yara ruleset is under the GNU-GPLv2 license and open to any user or organization, as long as you use it under this license (...).*»
Source : github.com/Yara-Rules/rules

=> **"Selfie": A Tool to Unpack Self-Modifying Code using DynamoRIO**. 26/05/2015. «*In this blog post we describe "Selfie", a tool we have developed that automates finding the OEP for a majority of malwares packed with self-modifying code. The tool itself is now open-sourced, compiled to 32-bit, and can be found (...).*»
Source : breakingmalware.com/tools/selfie-a-tool-to-unpack-self-modifying-code-using-dynamorio/
Billets en relation :
26/05/2015. *Selfie* : github.com/BreakingMalware/Selfie

=> **Ces logiciels qui prédisent les crimes**. 27/05/2015. «*Le croisement de bases de données permet de dresser des cartes intelligentes qui se rapprochent dangereusement des pires cauchemars de la science-fiction (...).*»
Source : www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/ces-logiciels-qui-predisent-les-crimes-27-05-2015-1931451_506.php
Billets en relation :
25/05/2015. *Gendarmes et industriels imaginent un nouveau logiciel pour prédire le crime* : www.mediapart.fr/journal/france/250515/gendarmes-et-industriels-imaginent-un-nouveau-logiciel-pour-predire-le-crime
27/05/2015. *Police prédictive : la tentation de « dire quel sera le crime de demain »* : rue89.nouvelobs.com/2015/05/27/police-predictive-tentation-dire-quel-sera-crime-demain-259384
28/05/2015. *Que sait-on de moi quand je prends l'avion ? De plus en plus de choses* : rue89.nouvelobs.com/2015/05/28/sait-quand-prends-lavion-plus-plus-choses-259395
02/06/2015. *How a group of researchers tried to use social media data and algorithms to find breaking news* : www.niemanlab.org/2015/06/how-a-group-of-researchers-tried-to-use-social-media-data-and-algorithms-to-find-breaking-news/

=> **Tracking Protection on Firefox | Firefox Help** . 27/05/2015. «*Oh purée j'avais pas fait gaffe à ça: Dans Firefox, vous pouvez maintenant activer le paramètre "privacy.trackingprotection.enabled". Ce gentil paramètre permet à Firefox de bloquer les traqueurs/publicités en utilisant la liste de blocage de disconnect.me (...).*»
Source : sebsauvage.net/links/?PjTlug

=> **Représenter le droit français avec des images et des schémas**. 27/05/2015. «*On y pensait en 2009], en 2014 c'est fait : le droit est maintenant expliqué en dessins et graphiques. Et cela va jusqu'au film (...).*»
Source : www.precisement.org/blog/Representer-le-droit-francais-avec-des-images-et-des-schemas-c-est-parti.html

=> **CapTipper – Malicious HTTP Traffic Explorer** . 27/05/2015. «*CapTipper is a Python tool independently developed by one of our researchers, Omri Herscovici, which is used to analyze, explore and revive HTTP malicious traffic. It provides the security researcher with easy access to the files and understanding of the network flow, and is useful for researching exploits, as well as various pre-conditions, versions, obfuscations, plugins and shellcodes (...).*»
Source : blog.checkpoint.com/2015/05/27/captipper-malicious-http-traffic-explorer/
Billets en relation :
27/05/2015. *CapTipper* : github.com/omriher/CapTipper

=> **The strange tale of robots.txt**. 28/05/2015. «*A few days ago I read an interesting post. In this post the author explains how he was able to build a list of subdirectories to brute force web servers and find hidden resources, relying on publicly available information from robots.txt files. Before we dive into the details, here is a quick reminder of robots.txt (...).*»
Source : blog.imperva.com/2015/05/the-strange-tale-of-robotstxt.html
Billets en relation :
17/05/2015. *What one may find in robots.txt* : thiébaud.fr/robots.txt.html

=> **More than 60 undisclosed vulnerabilities affect 22 SOHO routers**. 28/05/2015. «*As a part of the dissertation, we have discovered multiple vulnerability Issues on the following SOHO routers (...).*»
Source : seclists.org/fulldisclosure/2015/May/129
Billets en relation :
02/06/2015. *New SOHO router security audit uncovers over 60 flaws in 22 models* : www.itworld.com/article/2930295/security/new-soho-router-security-audit-uncovers-over-60-flaws-in-22-models.html
03/06/2015. *Failles à tout va : Routeurs Wifi et amour du fuzzing fantaisie* : www.cnis-mag.com/failles-a-tout-va-routeurs-wifi-et-amour-du-fuzzing-fantaisie.html
03/06/2015. *Sixty serious security flaws found in home routers* : blog.avast.com/2015/06/03/sixty-serious-security-flaws-found-in-home-routers/

=> **TRAFFIC ANALYSIS EXERCISE**. 29/05/2015. «*I'm trying something different this time: I'm not writing a summary about this traffic. Instead, the answers section has a series of 20 images that show how to find some of the important stuff. SCENARIO: You're working as an analyst at your organization's Security Operations Center (SOC). One of the other analysts was investigating alerts on a Windows host, and the computer is infected. That analyst retrieved a pcap of network traffic from the associated IP address (...).*»
Source : www.malware-traffic-analysis.net/2015/05/29/index.html

=> **Base de données des embargos sur les armes**. 29/05/2015. «*Dans le cadre de la "Cellule de veille sur l'évolution de la production et des transferts d'armes en Belgique, en Europe et dans le monde", subventionnée par la Région wallonne, le GRIP propose désormais au public une base de données consacrée aux embargos sur les armes dans le monde (...).*»
Source : www.grip.org/en/node/1755
Billets en relation :
29/05/2015. *Base de données des embargos sur les armes* : www.grip.org/fr/node/1558

=> **When I Analysed Firmware And Found A Complete DDNS Server Fail**. 29/05/2015. «*I am continuing the research I provided in this post. I have some notes before we go into this, as I'd just like to point a few things out. I've censored the hosts because I don't have money for a lawyer, but I think it is vital to release this information (...).*»
Source : itsjack.cc/blog/2015/05/when-i-analysed-firmware-and-found-a-complete-ddns-server-fail/
Billets en relation :
25/04/2015. *Unpacking CCTV Firmware* : itsjack.cc/blog/2015/04/unpacking-cctv-firmware/

=> **Net of insecurity - A flaw in The design**. 30/05/2015. «*This is a multi-part project on the Internet's inherent vulnerabilities and why they may never be fixed.. The Internet's founders saw its promise But didn't foresee users attacking one another. (...).*»
Source : www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/
Billets en relation :
31/05/2015. *Net of insecurity - The long life of a quick 'fix'* : www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/
04/06/2015. *Source* : www.scoop.it/t/arth-ck/p/4045110538/2015/06/04/anatomy-of-a-botnet

=> **Python Tools**. 30/05/2015. «*Following post will help to find vulnerability research, reverse engineering or penetration testing, (...).*»
Source : www.hackersonlineclub.com/python-tools
Billets en relation :
21/05/2015. *Shellconv* : github.com/hasherezade/shellconv

=> **PowerQuinsta**. 31/05/2015. «*I wanted to do a quick writeup on one of PowerView's latest features- the ability to enumerate RDP sessions on remote machines (...).*»
Source : www.harmj0y.net/blog/powershell/powerquinsta/

=> **Sécurité WEB : bloquer l'exécution de binaire sur Apache**. 31/05/2015. «*Afin de sécuriser votre serveur WEB, il est possible de limiter l'accès aux binaires Linux par le serveur WEB. Par défaut les utilisateurs ont les droits en execution sur /bin et /usr/bin Bien entendu, cela ne règle pas tous les problèmes mais renforce la sécurité. Il est tout à fait possible de bloquer l'accès à ces binaires pour l'utilisateur apache2 (httpd, www-data ou apache2 selon la distribution) et laisser les autres utilisateurs y avoir accès, notamment par SSH (...).*»
Source : forum.malekal.com/securite-web-bloquer-execution-binaire-sur-apache-t51888.html

=> **Manually Testing SSL/TLS Weaknesses**. 01/06/2015. «*This post presents a review of the main SSL/TLS (mis)configurations and simple ways to test your system's susceptibility (...).*»
Source : www.contextis.com/resources/blog/manually-testing-ssltls-weaknesses/
Billets en relation :
04/06/2015. *New Critical Security Controls Guidelines for SSL/TLS Management* : www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-guidelines-ssl-tls-management-35995

=> **Microsoft Research Social Media Conversation Corpus**. 01/06/2015. «*A collection of 12,696 Tweet Ids representing 4,232 three-step conversational snippets extracted from Twitter logs (...) It is released to the natural language processing community for academic research purposes only. In order to access the underlying tweets and related metadata, you will need to call the Twitter API (...).*»
Source : research.microsoft.com/en-us/downloads/6096d3da-0c3b-42fa-a480-646929aa06f1/default.aspx

=> **Ministre, Loi renseignement, Stratégie européenne** . 01/06/2015. «*Interview d'Axelle Lemaire (secrétaire d'Etat chargée du numérique) sur la Loi Renseignement, la stratégie européenne, la neutralité du net, la surveillance de masse, etc. au côté de Gilles Babinet, Benjamin Bayart, Eric Scherer et Eric Leandri. En bonus une question de notre guest : Jérémie Zimmermann (...).*»
Source : www.youtube.com/watch?v=01gGuXRKH5I
Billets en relation :
10/06/2015. *Deux ans pour faire aboutir un projet de loi, c'est trop long* : www.usine-digitale.fr/article/pour-axelle-lemaire-deux-ans-pour-faire-aboutir-un-projet-de-loi-c-est-trop-long.N334854
11/06/2015. *2015 : année de l'urgence numérique. Rencontre avec Axelle Lemaire* : www.rslnmag.fr/post/2015/06/11/2015-annee-de-lurgence-numerique-Rencontre-avec-Axelle-Lemaire.aspx
15/06/2015. *Renseignement: comment les politiques ont fermé les yeux* : www.mediapart.fr/journal/france/150615/renseignement-comment-les-politiques-ont-ferme-les-yeux
16/06/2015. *Loi Renseignement : Axelle Lemaire aurait songé "tous les jours" à la démission* : www.numerama.com/magazine/33406-loi-renseignement-axelle-lemaire-aurait-songe-tous-les-jours-a-la-demission.html

=> **Auditing GitHub users' SSH key quality**. 02/06/2015. «*If you have just/as of late gotten an email about your keys being revoked, this is because of me, and if you have, you should really go through and make sure that no one has done anything terrible to you, since you have opened yourself to people doing very mean things to you for what is most likely a very long time. (...).*»
Source : blog.benjojo.co.uk/post/auditing-github-users-keys

=> **Table ronde sur l'intelligence économique**. 02/06/2015. «*Commission des affaires économiques. Mardi 2 juin à 17h, la commission a réuni des personnalités qualifiées qui ont été auditionnées sur le thème de l'intelligence économique (...).*»
Source : videos.assemblee-nationale.fr/video.6835.commission-des-affaires-economiques--table-ronde-sur-l-intelligence-economique-2-juin-2015
Billets en relation :
02/06/2015. *Vidéos : table ronde sur l'intelligence économique* : videos.assemblee-nationale.fr/video.6835.commission-des-affaires-economiques--table-ronde-sur-l-intelligence-economique-2-juin-2015
04/06/2015. *Source* : www.arnaudpelletier.com/2015/06/04/pour-comprendre-lintelligence-economique-et-nos-concurrents-en-video/
12/06/2015. *L'IE en quête de compatibilité* : www.ttu.fr/lie-en-quete-de-compatibilite/

=> **Extrémiste ? Oui. Et même fier de l'être !**. 02/06/2015. «*Certains l'auront peut-être remarqué, mais une « bataille » interne s'est déclenchée parmi les participants aux Cafés Vie Privée. Certains ont été taxés d'extrémistes, ne cherchant qu'à convertir les « n00b » à la Vérité Vraie, des ayatollahs barbus, j'en passe et sûrement des meilleures (...).*»
Source : blog.imirhil.fr/extremiste-oui-et-meme-fier-de-letre.html
Billets en relation :
30/05/2015. *Comment je gère mes mots de passe* : www.libre-parcours.net/post/comment-je-gere-mes-mots-de-passe/
04/06/2015. *Voici à quoi ressemble l'Internet d'un hyper prudent* : www.slate.fr/story/101631/internet-hyper-prudent

=> **Playing with IP Reputation with Dshield & OSSEC**. 02/06/2015. «*When investigating incidents or searching for malicious activity in your logs, IP reputation is a nice way to increase the reliability of generated alerts. It can help to prioritize incidents. Let's take an example with a WordPress blog (...).*»
Source : blog.rootshell.be/2015/06/02/playing-with-ip-reputation-with-dshield-ossec/
Billets en relation :
02/06/2015. *Isc-ipreputation.py* : github.com/xme/toolbox/blob/master/isc-ipreputation.py

=> **2Mb Web Pages: Who's to Blame?**. 03/06/2015. «*I was hoping it was a blip. I was hoping 2015 would be the year of performance. I was wrong. Average web page weight has soared 7.5% in five months to exceed 2Mb (...).*»
Source : www.sitepoint.com/2mb-web-pages-whos-blame/
Billets en relation :

04/06/2015. *Des pages web de plus de 2 Mo, à qui la faute ?* : 4design.xyz/des-pages-web-de-plus-de-2-mo-a-qui-la-faute

=> **La garantie du canari**. 03/06/2015. «*Dans les mines de charbon, on a longtemps utilisé des canaris en cage du fait de leur grande sensibilité aux gaz toxiques. Quand l'oiseau s'évanouissait, il était temps de s'inquiéter pour les hommes (...).*»
Source : www.internetactu.net/2015/06/03/la-garantie-du-canari/

=> **Le "cochon" bien gras de la communauté américaine du renseignement**. 03/06/2015. «*71,8 milliards de dollars: c'est le budget prévisionnel de la communauté US du renseignement pour l'année fiscale 2016 (FY2016). (...).*»
Source : lignesdedefense.blogs.ouest-france.fr/archive/2015/06/02/le-cochon-bien-gras-de-la-communaute-americaine-du-renseignement.html

=> **Faut-il se méfier du paiement sans contact ?**. 03/06/2015. «*Ouvrir son porte-monnaie, tendre un billet et vérifier qu'on récupère bien la monnaie, ou scruter ses petites pièces pour faire l'appoint : ces gestes pourraient bien être relégués au rang de souvenirs, remplacés par le paiement sans contact. Cette technologie se déploie rapidement sur les cartes bancaires, et plus timidement sur les téléphones mais peine à entrer dans les habitudes des Français et suscite des inquiétudes. Explications (...).*»
Source : www.lemonde.fr/les-decodeurs/article/2015/06/03/faut-il-se-mefier-du-paiement-sans-contact_4646106_4355770.html
Billets en relation :
01/06/2015. *Les Assises des moyens de paiement* : www.economie.gouv.fr/assises-des-moyens-paiement-2-juin

=> **Mise en place et utilisation d'un serveur BAN/BANO pour un usage personnalisé sous Ubuntu 14.04**. 04/06/2015. «*Le but est de rappeler ce qu'est le géocodage. A quoi généralement, cela sert. Dans une deuxième temps, nous introduisons la Base Adresse Nationale (BAN) et la Base Adresse Nationale Ouverte (BANO, historique). En effet, dans ce contexte, des outils pour géocoder ont été mis en oeuvre. Nous expliquerons comment les utiliser, comment installer un serveur pour géocoder chez vous si par exemple, vous avez des besoins de géocodage massif ou de personnaliser la recherche d'adresse avec vos critères lors du géocodage (...).*» En plus de la BAN, la Poste a mis en ligne une base tierce.
Source : geotribu.net/node/811
Billets en relation :
30/05/2015. *Geocoding French addresses with BAN* : www.frenchkpi.com/geocoding-french-addresses-with-ban/
12/06/2015. *Liste des boîtes aux lettres de rue France métropolitaine et DOM* :
www.data.gouv.fr/fr/datasets/557ac950c751df3e461d4bfd/

=> **Cobalt Strike Pen Testing Lab DVD material is now available for download**. 04/06/2015. «*I've had several requests to put these labs online. If you're one of those interested parties, then today is your lucky day. The Cobalt Strike Pen Testing Lab DVD material is now available for download (...).*»
Source : blog.cobaltstrike.com/2015/06/04/cobalt-strike-penetration-testing-labs-download/

=> **Having fun with Tyupkin (ATM Malware)** . 04/06/2015. «*Malware targeting Persona series of NCR ATMs. Also know as 'Backdoor:MSIL/Sidkey.A' by Microsoft and 'Backdoor.Padpin' by Symantec. (...).*» Vidéos de Xylit0l.
Source : www.youtube.com/watch?v=tpzyWbPILzA
Billets en relation :
07/06/2015. *Having a look on DarkComet RAT config* : www.youtube.com/watch?v=vItjpQCFvPs
07/06/2015. *Having a look on CryptoFortress config* : www.youtube.com/watch?v=h4V7VXojGCA
09/06/2015. *Chinese adware and steganography* : www.youtube.com/watch?v=cxImN-9Qhwo

=> **Dire, Ne pas dire (juin 2015)** . 04/06/2015. «*Quels mots, quelles tournures choisir, retenir ou rejeter parmi ce qui s'entend et se dit ? La série du mois de juin 2015 de Dire, Ne pas dire, qui donne, depuis plus de trois ans, le sentiment de l'Académie française sur les fautes, les tics de langage et les ridicules le plus fréquemment observés dans le français contemporain, est accessible (...).*»
Source : www.academie-francaise.fr/actualites/dire-ne-pas-dire-juin-2015

=> **ADSB, quand « spot the fed » devient « flashe les aérobarbouzes »**. 05/06/2015. «*Ce sont les "datajournalistes" de l'agence Associated Press qui ont découvert le pot aux roses. Le Gouvernement Fédéral US, masquant ses activités derrière des compagnies aériennes bidon, effectue une surveillance aérienne particulièrement active au-dessus des principales métropoles des Etats-Unis (...).*»
Source : www.cnis-mag.com/adsb-quand-spot-the-fed-devient-flashe-les-aerobarbouzes.html
Billets en relation :
26/05/2015. *Domestic Aerial Surveillance Aircraft Master-List* : cryptome.org/2015/06/fbi-sky-spies.htm
05/06/2015. *FBI behind mysterious surveillance aircraft over US cities* :
bigstory.ap.org/urn:publicid:ap.org:4b3f220e33b64123a3909c60845da045

=> **The ssdeep team, version 2.13, and moving to GitHub**. 05/06/2015. «*Here are a few updates about ssdeep. In the post I'll be talking about the people in the project, the latest release, and our upcoming move to Github. For the impatient, we have published ssdeep version 2.13 (...).*»

Source : jessekornblum.livejournal.com/295999.html

=> **Rencontres IHEDN - La défense comme vous ne l'avez jamais abordée**. 06/06/2015. «*La de´fense est un enjeu trop vital pour e^tre le domaine re´serve´ d'experts et de professionnels. La de´fense engage la survie de la Nation. Ses institutions, son territoire, ses inte´re^ts vitaux, tout autant que ses valeurs et sa capacite´ a` re´sister a` l'adversite´. La de´fense est bien su^r une politique. C'est un engagement pour les hommes et les femmes qui ont choisi le me´tier des armes. Mais c'est aussi l'expression de la volonte´ d'un peuple de rester mai^tre de son destin (...).*» Les vidéos des interventions commencent à être disponible. Certaines thématiques, originales par leur angle d'approche, pourraient intéresser quelques lecteurs des brèves. Je n'ai pas pu prendre le temps de regarder plus en détails.
Source : www.ihedn.fr/?q=content/rencontres-ihedn-6-juin-2015
Billets en relation :
15/05/2015. *Rencontres IHEDN – La défense comme vous ne l'avez jamais abordée* : www.anaj-ihedn.org/rencontres-ihedn/
06/06/2015. *2 - "Même pas peur ! Les leçons des attentats de janvier 2015"* : vimeo.com/130184028
06/06/2015. *6 - " Les 7 mercenaires : Des gardes suisses à Blackwater"* : vimeo.com/130302350
06/06/2015. *7 - Conférence de clôture : Citoyenneté et défense* : vimeo.com/130410889
06/06/2015. *4 - "L'empire contre-attaque : ers une nouvelle guerre majeure en Europe ?"* : vimeo.com/130203357
06/06/2015. *1 - Aux armes, citoyens ! Peut-on rétablir le service national ?* : vimeo.com/130184026
06/06/2015. *3 - "La bourse ou la vie ? A-t-on encore les moyens de défendre nos couleurs ?* : vimeo.com/130184029
06/06/2015. *5 - " Les dieux sont-ils tombés sur la tête ? Guerre et religion "* : vimeo.com/130214411
15/06/2015. *11 - Like, hashtag et poke : les réseaux sociaux transforment-ils la guerre ?* : vimeo.com/130956856
15/06/2015. *8 - Call of duty, Battlefield : jeux vidéo et violence* : vimeo.com/130749034
15/06/2015. *13 - Cyborgs & transformers : quelle place pour l'Homme sur le champ* : vimeo.com/130956857
15/06/2015. *12 - Hiroshima, mon amour : quelle place pour la dissuasion aujourd'hui ?* : vimeo.com/130956858
15/06/2015. *9 - Boules de cristal, NG : Le savant, le politique et l'artiste* : vimeo.com/130749035
15/06/2015. *10 - "Bulles et bullets : la guerre en BD"* : vimeo.com/130749036

=> **Exploring the Top 100 ebooks of The Pirate Bay**. 06/06/2015. «*I wrapped up an analysis of the Top 100 ebooks of the Pirate Bay. Rather than posting to code I decided to use a notebook viewer. All the data and code can be found on my bit-bucket repo (...).*»
Source : hooked-on-mnemonics.blogspot.fr/2015/06/exploring-top-100-ebooks-of-pirate-bay.html

=> **HOLA VPN – Les dessous du VPN**. 06/06/2015. «*Gardez en toujours en tête cette phrase clé : lorsqu'un service est gratuit, c'est vous le produit. Beaucoup font la promotion à tout va des VPN gratuits, soit disant fiables et sécurisés. Mais le récent scandale causé par HOLA VPN est un exemple typique de ce qu'il faut éviter… (...).*»
Source : www.undernews.fr/anonymat-cryptographie/scandale-hola-vpn-les-dessous-du-vpn-gratuit-israelien.html

=> **The Next 10 Years: 42 Macro Predictions in Cryptography, Blockchains and Consensus Protocols**. 06/06/2015. «*It would be interesting if we could look into a crystal ball and predict the future of Bitcoin, blockchains, cryptocurrency, decentralized applications and cryptography-based protocols and platforms (...).*»
Source : startupmanagement.org/2015/06/06/the-next-10-years-42-macro-predictions-in-cryptography-blockchains-and-consensus-protocols/

=> **John Nash, un mathématicien d'exception (1928-2015)**. 07/06/2015. «*Qu'il s'agisse de théorie des équations aux dérivées partielles, de géométrie différentielle ou de théorie des jeux, John Nash a su surmonter les obstacles de la complexité et éclairer le chemin de la connaissance (...).*»
Source : echoradar.eu/2015/06/07/john-nash-un-mathematicien-dexception/

=> **Moteur de 30 000 ressources pédagogiques numériques pour apprendre**. 08/06/2015. «*La plate-forme France Université Numérique (FUN) propose nouvellement une indexation de près de 30 000 ressources pédagogiques numériques proposées par un ensemble d'établissements d'enseignement supérieur et d'organismes de recherche français (Aunege, IUTenLigne, unf3S, Unisciel, Unit, Unjf, UOH, UVED et Canal-U) via le Moteur des ressources pédagogiques numériques (...).*»
Source : www.netpublic.fr/2015/06/moteur-de-30-000-ressources-pedagogiques-numeriques-pour-apprendre/
Billets en relation :
08/06/2015. *FUN Ressources pédagogiques* : www.france-universite-numerique.fr/moteur-ressources/thematic-search.html?submenuKey=all&menuKey=lom

=> **The Power of Execution Graphs 2/3**. 08/06/2015. «*As you may recall, Execution Graphs are highly condensed control flow graphs, showing information about which part of the code has been executed and which not. Execution Graphs highlight additional attributes such API calls, threats starts, and key decisions (...).*»
Source : joe4security.blogspot.fr/2015/06/the-power-of-execution-graphs-23.html
Billets en relation :
22/04/2015. *The Power of Execution Graphs Part 1/3* : joe4security.blogspot.ch/2015/04/the-power-of-execution-graphs-part-13.html

=> **Hospira Plum A+ Infusion Pump Vulnerabilities**. 08/06/2015. «*In May of 2014, I reported to the Department of Homeland Security (and eventually the FDA) a series of vulnerabilities affecting the PCA 3 Lifecare infusion pump made by Hospira. Over 400 days later, we have yet to see a single fix for the issues affecting the PCA 3. On April 28th of this year, a researcher named Jeremy Richards Hextech Security publically disclosed many of the same vulnerabilities I reported in May of 2014. The public disclosure caused a chain of events (...).*»
Source : xs-sniper.com/blog/2015/06/08/hospira-plum-a-infusion-pump-vulnerabilities/
Billets en relation :
28/04/2015. *Hospira PCA3 Drug Infusion Pump* : hextechsecurity.com/?p=123
13/05/2015. *Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication* : www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm
25/05/2015. *Le secteur de la santé est-il suffisamment protégé ?* : www.lesechos.fr/idees-debats/cercle/cercle-133356-experience-de-cyberattaque-reussie-sur-un-robot-de-chirurgie-le-secteur-de-la-sante-est-il-suffisamment-protege-1122213.php
15/06/2015. *La vengeance du retour du hack médical 2.0* : www.cnis-mag.com/la-vengeance-du-retour-du-hack-medical-2-0.html

=> **Pcap-rename**. 09/06/2015. «*Pcap-rename.py is a program to rename pcap files with a timestamp of the first packet in the pcap file. (...).*»
Source : blog.didierstevens.com/2015/06/09/pcap-rename-py/

=> **Routing in QGIS… with OSM**. 09/06/2015. «*Routing with Google is quite cool as the database/network is probably the best currently available. But the terms of services limit the possible usage. So what about OpenStreetMap? By figuring out how to use OSM for routing I found it much easier to get routes into QGIS with OSM compared to the Google way. Check it out…. (...).*»
Source : www.digital-geography.com/routing-in-qgis-with-osm/
Billets en relation :
03/06/2015. *Routing in QGIS … with Google* : www.digital-geography.com/routing-in-qgis-with-google/

=> **The Untold Story Of Microsoft's Surface Hub**. 10/06/2015. «*A man with a dream. A company in flux. A secret factory outside Portland. And a hyper-ambitious gambit to reimagine how meetings happen (...).*»
Source : www.fastcompany.com/3046819/the-untold-story-of-microsofts-surface-hub?partner=rss

=> **Introduction à la sécurité SCADA**. 10/06/2015. «*Scada, Stuxnet... Des mots qui ont largement fait le "buzz" depuis 2010, et continuent à faire froid dans le dos puisqu'ils font écho aux menaces sur les environnements informatiques industriels. Mais au-delà du bruit médiatique, de quoi s'agit-il exactement ? (...).*»
Source : korben.info/securite-scada.html
Billets en relation :
12/06/2015. *Introduction au hardware hacking* : korben.info/hardware-hacking.html

=> **Any Yahoo Pipes true substitute out there ?**. 10/06/2015. «*Focusing on RSS feed merging and filtering (...).*»
Source : www.precisement.org/blog/Any-Yahoo-Pipes-true-substitute-out-there.html

=> **Plan du métro représenté sous Git**. 11/06/2015. «*Certaines interconnexions ou stations créant des cycles ont dû être enlevées. En effet, Git ne permet de représenter que des graphes orientés acycliques (...).*»
Source : www.data.gouv.fr/fr/reuses/5579dfafc751df7ee1e57269/
Billets en relation :
07/06/2015. *MetroGit* : github.com/vbarbaresi/MetroGit

=> **Just-Metadata – Intel Gathering and Analysis of IP Metadata**. 11/06/2015. «*To answer these questions, I wrote Just-Metadata, which I am happy to release today (...).*»
Source : www.christophertruncer.com/just-metadata-intel-gathering-and-analysis-of-ip-metadata/
Billets en relation :
11/06/2015. *Just-Metadata* : github.com/ChrisTruncer/Just-Metadata

=> **Découpage communal : table d'appartenance géographique des communes**. 11/06/2015. «*Ce fichier fournit pour toutes les communes le code géographique des niveaux géographiques supérieurs auxquels elles appartiennent. Relié aux tables d'indicateurs chiffres clés, ce fichier permet d'obtenir des résultats agrégés d'indicateurs sur un territoire communal personnalisé ou des territoires supracommunaux (...).*»
Source : www.insee.fr/fr/methodes/default.asp?page=zonages/table-appartenance-geo-communes.htm

=> **Reversing DexGuard's String Encryption**. 11/06/2015. «*DexGuard is a commercial tool used for protecting android binaries (APK) mainly from reversing and tampering. It provides features like code obfuscation, class encryption, string encryption, asset/resource encryption, tamper protection, anti-debugger checks, VM/Environment checks, SSL pinning etc (...).*»
Source : opensecurity.in/reversing-dexguards-string-encryption/

=> **Explorer les cartes de la Grande Guerre**. 12/06/2015. «*Entre 1914 et 1918, on assiste à une explosion de la production cartographique. Aujourd'hui, environ 14000 cartes concernant la Première Guerre mondiale, dressées par le Service géographique de l'armée, sont conservées au Service historique de la Défense. Les cartes restent une source mal connue alors qu'elles peuvent s'avérer très utiles pour les chercheurs et certains professionnels. Le projet « Explorer les cartes de la Première Guerre mondiale» en constitue un exemple remarquable. Avant de vous de le présenter, prenons le temps de découvrir cette source (...).*»
Source : sourcesdelagrandeguerre.fr/WordPress3/?p=4037

=> **Cours en ligne ouvert à tous (MOOC) consacré aux questions stratégiques**. 12/06/2015. «*Le Conseil supérieur de formation et recherche stratégiques (CSFRS) en partenariat avec le Cnam, doit diffuser sur France Université Numérique en septembre et octobre 2015 un cours en ligne ouvert à tous consacré aux "Questions stratégiques". Les inscriptions sont ouvertes et gratuites. Ce MOOC rassemble plus de quarante chercheurs, enseignants et personnalités autour d'un projet pédagogique : Quels sont les facteurs déterminants d'une analyse de situation et d'une prise de décision stratégiques ? (...).*»
Source : www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/evenements-22750/article/cours-en-ligne-ouvert-a-tous-mooc

=> **E14 : Anatomie d'un accéléromètre numérique**. 12/06/2015. «*Un épisode consacré à l'étude de 2 accéléromètres capacitifs numériques. Nous allons voir en détail leur principe de fonctionnement et observer la surface de leurs circuits intégrés pour tenter d'en apprendre un peu plus sur leur architecture. Vous pouvez télécharger les datasheets et documents techniques en rapport avec cet épisode sur le site internet (...).*»
Source : youtu.be/V_zRvc1tNBM
Billets en relation :
12/06/2015. *DEUS EX SILICIUM est le premier projet 100% francophone de chaine dont la thématique principale est l'électronique numérique* : www.dexsilicium.com/

=> **Science informatique dites vous ? Deux revues et un blog à votre service**. 12/06/2015. «*Il est important que, des actrices et acteurs … aux utilisateurs et utilisatrices du numérique, nous partagions une culture en sciences du numérique, pour comprendre et maîtriser les technologies qui en sont issues. Pour concrétiser ce partage avec le monde de la recherche, la Société Informatique de France, Inria et le CNRS proposent deux revues et un blog : profitons-en ! (...).*»
Source : binaire.blog.lemonde.fr/2015/06/12/science-informatique-dites-vous-deux-revues-et-un-blog-a-votre-service/

=> **Damn the Equities, Sell Your Zero-Days to the Navy!**. 12/06/2015. «*Noted eagle eye and EFF Investigative Researcher Dave Maass happened on an interesting item from earlier this week on FedBizOpps, the site for government agencies to post contracting opportunities. The Navy put up a solicitation explaining that the government wants "access to vulnerability intelligence, exploit reports and operational exploit binaries affecting widely used and relied upon commercial softwar (...).*»
Source : www.eff.org/deeplinks/2015/06/damn-equities-sell-your-zero-days-navy
Billets en relation :
15/06/2015. *US Navy Soliciting Zero Days* : threatpost.com/us-navy-soliciting-zero-days/113308
16/06/2015. *EFF : l'US Navy* : www.developpez.com/actu/86493/EFF-l-US-Navy-cherche-a-payer-les-vulnerabilites-zero-day-pour-les-exploiter-les-logiciels-les-plus-utilises-sont-cibles/
18/06/2015. *In the Navy (chanson populaire)* : www.cnis-mag.com/in-the-navy-chanson-populaire.html

=> **Planet (agrégation des flux RSS/blog) de tous les fablabs de France**. 12/06/2015. «*Un petit mot pour vous informer qu'un planet (agrégation des flux RSS/blog) de tous les fablabs de France est mis en place (...).*» Via la liste de discussion NYBI.CC
Source : planet.fablab.fr/

=> **Phrozen freeware**. 12/06/2015. «*Phrozen freeware (...).*» A une époque, ils avaient quelques outils intéressants, sous Windows. Je pense notamment à un outil générique d'analyse des metadata de divers documents génériques (bureautiques, audio/vidéo, etc.). Je viens de voir qu'ils ont fait le ménage, tout viré, et proposé depuis de nouvelles ressources que je ne connais pas. A 'zieuter' peut-être de temps en temps, voir ce qui s'y propose. Je n'ai pas regardé de près les éléments ci-dessous.
Source : www.phrozensoft.com/freeware
Billets en relation :
29/05/2015. *RunPE Detector* : www.phrozensoft.com/2015/06/runpe-detector-1
12/06/2015. *Phrozen ADS Revealer* : www.phrozensoft.com/2015/06/phrozen-ads-revealer-catch-alternate-data-stream-2

=> **Modular arithmetic + division by multiplication + reversible LCG (PRNG) + cracking LCG with Z3**. 13/06/2015. «*Many practicing reverse engineerings are fully aware that division operation is sometimes replaced by multiplication (...).*»
Source : yurichev.com/blog/modulo/

=> **PolyBoRi is dead, it needs your help**. 13/06/2015. «*On the Sage development list a discussion is going on what to do about PolyBoRi. For those who do not know PolyBoRi, for computing Gröbner bases for Boolean polynomials it is pretty much the only (open-source)*

game in town (as far as I know) (...) The trouble with PolyBoRi is that both authors of PolyBoRi – Alexander Dreyer and Michael Brickenstein – left academia and have jobs now which have nothing to do with PolyBoRi. Hence, PolyBoRi is currently not maintained. This is a big problem (...).»
Source : martinralbrecht.wordpress.com/2015/06/13/polybori-is-dead-it-needs-your-help/

=> **Mozilla Password Based Encryption**. 14/06/2015. «*Mozilla Password Based Encryption: files formats and crypto algorithms in one poster (...).*»
Source : github.com/lclevy/firepwd/blob/master/mozilla_pbe.pdf
Billets en relation :
14/06/2015. *Source* : twitter.com/lorenzo2472/status/610181033443651585
14/06/2015. *Firepwd.py, an open source tool to decrypt Mozilla protected passwords* : github.com/lclevy/firepwd

=> **Cartographie des contrôles CNIL en 2014**. 15/06/2015. «*Cartographie des contrôles CNIL 2014. (...).*»
Source : www.data.gouv.fr/fr/reuses/557ee754c751df14301d4bfc/
Billets en relation :
15/06/2015. *Open data : la CNIL publie 8 nouveaux jeux de données sur data.gouv.fr* :
www.cnil.fr/nc/linstitution/actualite/article/article/open-data-la-cnil-publie-9-nouveaux-jeux-de-donnees-sur-datagouvfr/
19/06/2015. *Cartographie des organismes ayant déclarés un CIL* : www.data.gouv.fr/fr/reuses/558447b8c751df0414a453b9/

=> **[podcasts] No Limit Sécu - DNSSEC**. 15/06/2015. «*Episode consacré à DNSSEC avec Stéphane Bortzmeyer (...).*»
Source : www.nolimitsecu.fr/dnssec/
Billets en relation :
06/05/2015. *Conférence 2015 - La threat intelligence à la rescousse de la réponse à incident - Thomas Chopitea* :
www.youtube.com/watch?v=jV2ZJlGVHHA
31/05/2015. *No Limit Sécu - Threat Intelligence avec Thomas Chopitea* : www.nolimitsecu.fr/threat-intelligence-thomas-chopitea/
05/06/2015. *Le Comptoir Sécu - Episode 27 Actualité mai* : www.comptoirsecu.fr/2015/06/episode-27-actualite-mai/
07/06/2015. *No Limit Sécu - SSTIC 2015* : www.nolimitsecu.fr/sstic-2015/
21/06/2015. *No Limit Sécu - Pourquoi es-tu venu à NDH15 ?* : www.nolimitsecu.fr/nuit-du-hack-2015/
21/06/2015. *No Limit Sécu - Les WAF (Web Application Firewall) sont-ils indispensables ou superflus ?* : www.nolimitsecu.fr/les-waf-indispensables-superflus/

=> **Darknet Jihad: These Aren't The Sites You Are Looking For**. 15/06/2015. «*I am writing this post to set the record straight and to make a point… A cryptic point that someone reading this will get and you know who you are. The darknet is on the whole NOT being used by jihadi's to hide their comm's in the sense of going to darknet sites. Please for the love of everything sane, all you gubment types and wanna be spies get that the fuck into your heads right the fuck now (...).*»
Source : krypt3ia.wordpress.com/2015/06/15/darknet-jihad-these-arent-the-sites-you-are-looking-for/
Billets en relation :
31/05/2015. *Fight Against Cybercrime and Terrorism Moves to the Darknet* : www.theepochtimes.com/n3/1371899-fight-against-cybercrime-and-terrorism-moves-to-the-darknet/
17/06/2015. *The Chinese Darknet* : krypt3ia.wordpress.com/2015/06/17/the-chinese-darknet/
18/06/2015. *The Dark Web as You Know It Is a Myth* : www.wired.com/2015/06/dark-web-know-myth
18/06/2015. *Uncovering Tor users: where anonymity ends in the Darknet* : securelist.com/analysis/publications/70673/uncovering-tor-users-where-anonymity-ends-in-the-darknet/

=> **Fonctions de hachage et mots de passe complexes sur Duckduckgo** . 15/06/2015. «*Même s'il est possible que nombre d'entre vous ne le sachiez déjà, j'avoue n'avoir découvert que récemment les fonctions cryptographiques intégrées à Duckduckgo (...).*»
Source : si-vis.blogspot.fr/2015/06/fonctions-de-hachage-et-mots-de-passe.html

=> **Dude, where's my heap?** . 15/06/2015. «*The two mitigations are not meant to be related. However, somewhat unexpectedly, one can be (ab)used to bypass the other. In one sentence, it is possible to use a timing attack on MemoryProtector to reveal the offset used by High-Entropy Bottom-Up Randomization, thus completely bypassing it (...).*»
Source : googleprojectzero.blogspot.fr/2015/06/dude-wheres-my-heap.html

=> **Ghiro**. 16/06/2015. «*Ghiro is a digital image forensics tool. Fully automated and open source. (...).*»
Source : www.getghiro.org/#about-us

=> **Windows 10 vs vie privée : Des points problématiques**. 17/06/2015. «*La récente mise à jour et unification des déclarations de confidentialité de Microsoft comporte des points problématiques pour la vie privée des utilisateurs de Windows 10. Analyse (...).*»
Source : www.undernews.fr/libertes-neutralite/windows-10-vs-vie-privee-des-points-problematiques.html
Billets en relation :
11/06/2015. *Windows 10, Microsoft et vos données privées : ce que vous devez savoir* : www.numerama.com/magazine/33357-

windows-10-microsoft-et-vos-donnees-privees-ce-que-vous-devez-savoir.html
12/06/2015. *Windows 10 : l'exploitation de vos données privées par Microsoft est effrayante* : www.phonandroid.com/windows-10-exploitation-donnees-privees-microsoft-effrayante.html

=> **Pourquoi je ne propose pas de hackathon à mes clients**. 17/06/2015. «*Le hackathon est à la mode. Mais est-il vraiment LA recette miracle pour innover dans les entreprises, s'interroge dans cette tribune Julien Pouget, consultant et auteur du livre Intégrer et Manager la génération Y (Vuibert) (...).*»
Source : www.usine-digitale.fr/article/pourquoi-je-ne-propose-pas-de-hackathon-a-mes-clients.N336469

=> **Cambridge Cloud Cybercrime Centre**. 17/06/2015. «*We have recently won a major grant (around £2 million over 5 years) under the EPSRC Contrails call which we will be using to set up the "Cambridge Cloud Cybercrime Centre" (...).*»
Source : www.lightbluetouchpaper.org/2015/06/17/cambridge-cloud-cybercrime-centre/

=> **La stratégie européenne de sécurité intérieure est officiellement renouvelée pour 2015-2020**. 17/06/2015. «*Voici ce qu'ont déclaré formellement les ministres de l'Intérieur le 16 juin dans des conclusions approuvées par le Conseil. Le texte valide donc la stratégie de sécurité intérieure pour l'Union européenne pour la période 2015-2020. (...).*»
Source : securiteinterieurefr.blogspot.fr/2015/06/la-strategie-europeenne-de-securite.html
Billets en relation :
10/06/2015. *Projet de conclusions du Conseil sur la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015 - 2020* : data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/fr/pdf
16/06/2015. *L'Union Européenne et l'enjeu sécuritaire (2/2)* : les-yeux-du-monde.fr/actualite/europe/22661-lunion-europeenne-lenjeu-securitaire

=> **Tor : Mails-toi de tes oignons**. 18/06/2015. «*Favorisant l'anonymat, Tor, réseau à la réputation sulfureuse, serait utilisé par 2 millions de personnes chaque jour. Les révélations d'Edward Snowden sur la surveillance généralisée remettant en valeur ce rempart contre la censure (...).*»
Source : www.liberation.fr/economie/2015/06/18/tor-mails-toi-de-tes-oignons_1332660

=> **Actualités web de la semaine : blogueur responsable, pseudo-influence et Big Data**. 19/06/2015. «*C'est l'heure des actualités web de la semaine ! Un programme varié ce vendredi, de la décision de la Cour Européenne des droits de l'Homme sur les commentaires de blog aux jolis bureaux LinkedIn (...).*» Diverses veilles thématiques à fouiller et parcourir.
Source : www.blogdumoderateur.com/actualites-web-semaine-49/
Billets en relation :
29/05/2015. *Compilation veille Twitter & RSS #2015-21* : blog.jbfavre.org//2015/05/29/compilation-veille-twitter-rss/
29/05/2015. *Actualités web de la semaine : Pac-Man, YouTube et Periscope* : www.blogdumoderateur.com/actualites-web-semaine-46/
30/05/2015. *Liens vagabonds (la réalité virtuelle accélère, le pouls de l'Internet...)* : meta-media.fr/2015/05/30/liens-vagabonds-la-realite-virtuelle-accelere-le-pouls-de-linternet.html
31/05/2015. *Liens de la semaine* : www.duperrin.com/2015/05/31/liens-de-la-semaine-weekly-268/
01/06/2015. *Augmented Times – les nouvelles hebdomadaires de la réalité augmentée – S22* : www.augmented-reality.fr/2015/06/augmented-times-les-nouvelles-hebdomadaires-de-la-realite-augmentee-s22/
05/06/2015. *Compilation veille Twitter & RSS #2015-22* : blog.jbfavre.org//2015/06/05/compilation-veille-twitter-rss/
05/06/2015. *Actualités web de la semaine : Viuz, Google, Papertweet et Kung Fury* : www.blogdumoderateur.com/actualites-web-semaine-47/
05/06/2015. *56Kast #55 : un Apple-1 à la poubelle et des guilis sur le crâne* : ecrans.liberation.fr/ecrans/2015/06/05/56kast-55-un-apple-1-a-la-poubelle-et-des-guilis-sur-le-crane_1323550
06/06/2015. *Liens vagabonds* : meta-media.fr/2015/06/06/liens-vagabonds-2.html
07/06/2015. *Liens de la semaine* : www.duperrin.com/2015/06/07/liens-de-la-semaine-weekly-269/
08/06/2015. *Augmented Times – les nouvelles hebdomadaires de la réalité augmentée – S23* : www.augmented-reality.fr/2015/06/augmented-times-les-nouvelles-hebdomadaires-de-la-realite-augmentee-s23/
12/06/2015. *GeoTribu - Revue de presse du 12 Juin* : geotribu.net/GeoRDP/20150612
12/06/2015. *Actualités web de la semaine : CV de community manager, #BestOfTweets, bouton Reddit…* : www.blogdumoderateur.com/actualites-web-semaine-48/
14/06/2015. *Compilation veille Twitter & RSS #2015-24* : blog.jbfavre.org//2015/06/14/compilation-veille-twitter-rss/
14/06/2015. *Liens vagabonds (Apple change de musique, Twitter sans boss...)* : meta-media.fr/2015/06/14/liens-vagabonds-apple-change-de-musique-twitter-sans-boss.html
14/06/2015. *Liens de la semaine* : www.duperrin.com/2015/06/14/liens-de-la-semaine-weekly-270/
16/06/2015. *La folle histoire de l'Univers 49* : www.florenceporcel.com/podcast-la-folle-histoire-de-lunivers-49/
16/06/2015. *La sélection cérébrale de la semaine (numéro 46)* : cervenargo.hypotheses.org/665
18/06/2015. *LQDN Newsletter #65* : www.laquadrature.net/fr/newsletter/newsletter-65
19/06/2015. *La sélection scientifique de la semaine (numéro 176)* : passeurdesciences.blog.lemonde.fr/2015/06/19/la-selection-scientifique-de-la-semaine-numero-176/

19/06/2015. *GeoTribu - Revue de presse du 19 juin* : geotribu.net/GeoRDP/20150619
20/06/2015. *En vrac du samedi* : standblog.org/blog/post/2015/06/20/En-vrac-du-samedi
20/06/2015. *Liens vagabonds (journalistes, le retour !)* : meta-media.fr/2015/06/20/liens-vagabonds-journalistes-le-retour.html
21/06/2015. *Liens de la semaine* : www.duperrin.com/2015/06/21/liens-de-la-semaine-weekly-271/
21/06/2015. *Compilation veille Twitter & RSS #2015-25* : blog.jbfavre.org//2015/06/21/compilation-veille-twitter-rss/

=> **WikiLeaks publie 276 000 nouveaux documents de Sony**. 19/06/2015. «*Le site WikiLeaks a publié jeudi 18 juin plus de 276 000 nouveaux documents des studios Sony Pictures Entertainment (SPE), victimes d'un piratage massif révélé en novembre dernier. Ce sont exactement 276 394 documents qui ont été rendus publics par le site, qui justifie son action par le fait que l'information « appartient au domaine public » et que sa diffusion permet de montrer « les engrenages d'une influente multinationale ». Le site avait déjà publié mi-avril une première salve de 30 287 documents d'archives du groupe, ainsi que 173 132 e-mails (...).*»
Source : www.lemonde.fr/pixels/article/2015/06/19/wikileaks-publie-276-000-nouveaux-documents-de-sony_4657840_4408996.html
Billets en relation :
19/06/2015. *WikiLeaks publie les câbles saoudiens* : wikileaksactu.wordpress.com/2015/06/19/wikileaks-publie-les-cables-saoudiens/

=> **Une nouvelle plateforme pour permettre aux PME de mieux appréhender le marketing**. 19/06/2015. «*La Direction générale des entreprises (DGE) vient de mettre en ligne un nouvel outil à destination des petites et moyennes entreprises. Objectif : mieux cerner l'impact du marketing sur les performances des PME (...).*»
Source : www.economie.gouv.fr/plateforme-marketing-pme-dge
Billets en relation :
18/05/2015. *Facebook lance « Local awareness » en France* : www.mikii.fr/blog/2015/05/18/facebook-lance-local-awareness-france/
11/06/2015. *Données personnelles : l'impuissance n'est pas le consentement* : www.internetactu.net/2015/06/11/donnees-personnelles-limpuissance-nest-pas-le-consentement/
15/06/2015. *Assises du Géomarketing : les défis de la géolocalisation de masse* : www.lemagit.fr/actualites/4500248162/Le-geomarketing-face-aux-defis-de-la-geolocalisation-de-masse
19/06/2015. *L'apprentissage douloureux du freelance débutant* : zythom.blogspot.fr/2015/06/lapprentissage-douloureux-du-freelance.html
19/06/2015. *La valeur ajoutée du marketing pour les PME* : marketing-pme.entreprises.gouv.fr/
19/06/2015. *Les performances de l'email marketing en France, secteur par secteur* : www.journaldunet.com/ebusiness/crm-marketing/email-marketing-2014/

=> **Rire avec les robots pour mieux vivre avec**. 19/06/2015. «*Parce que la plupart d'entre nous préféreraient partir en vacances avec l'espiègle R2-D2 plutôt qu'avec l'obséquieux C-3PO, les roboticiens tentent désormais de donner le sens de l'humour et de l'empathie à leurs machines (...).*»
Source : lejournal.cnrs.fr/billets/rire-avec-les-robots-pour-mieux-vivre-avec
Billets en relation :
15/11/2014. *Rapport Éthique de la recherche en robotique* : cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf
15/06/2015. *Electronique, robotique : l'incontournable question de l'intégration et de l'autonomie* : www.enderi.fr/Electronique-robotique-l-incontournable-question-de-l-integration-et-de-l-autonomie_a255.html

=> **In bed with TLS - Part I : TLS, PFS et Logjam**. 20/06/2015. «*In mai, des chercheurs, dont des chercheurs de l'INRIA (cocorico), ont dévoilé, sous le nom de Logjam, des défauts de sécurité impactant TLS. J'avais pensé écrire une série de billets là dessus, ce que je n'avais malheureusement pas eu loisir de faire jusqu'ici. Ce billet vise à illustrer le fonctionnement de TLS et l'échange de clés éphémères Diffie-Hellman (DHE). J'y parle ensuite de la "récente" faille Logjam. Même si je les aborde, j'ai essayé de réduire au minimum les aspects mathématiques des méthodes cryptographiques entrant en jeu et de ne pas rentrer dans le détail des protocoles ou de la configuration. L'Interweb regorge en effet de howtos et autres articles à ces effets. Écrire est aussi un moyen pour moi de mettre mes idées au clair. Bref, c'est parti (...).*»
Source : nonblocking.info/in-bed-with-tls-part1/

=> **La fin du Tigre**. 21/06/2015. «*Contrairement à ce que nous avions annoncé dans l'éditorial du dernier Tigre vendu en kiosques (numéro 48-49, décembre 2014-janvier 2015), il n'y aura pas de numéro spécial pour terminer l'aventure du journal. L'histoire du Tigre est terminée (...).*»
Source : www.le-tigre.net/La-fin-du-Tigre.html
Billets en relation :
21/12/2014. *Éditorial du numéro 48/49, décembre 2014/janvier 2015* : www.le-tigre.net/Chers-lecteurs,27143.html

=> **4 services pour créer des dessins animés gratuitement en ligne**. 21/06/2015. «*Si vous avez besoin de créer des dessins animés et vous n'avez aucune connaissance en Flash je vous propose ci-dessous quelques sources qui peuvent aider à créer vos propres dessins animés facilement et surtout gratuitement (...).*»
Source : www.applicanet.com/2015/06/creer-dessins-animes-gratuitement.html

=> **Pourquoi les nouveaux programmeurs ne lisent plus le code source des autres**. 21/06/2015. «*Dans un ancien post sur son blog, Raymond Hettinger s'attristait de voir les devs lire de moins en moins le code source. Bien qu'il datait de plus de 4 ans, je n'ai pas pu m'empêcher de répondre. Puis je me suis dis que la traduction aurait tout à fait sa place ici. La cause de ce phénomène est très culturel. (...).*»
Source : sametmax.com/pourquoi-les-nouveaux-programmeurs-ne-lisent-plus-le-code-source-des-autres/

=> **538ème édition des LIDD : Liens Idiots Du Dimanche**. 21/06/2015. «*Comme tous les dimanches (ou presque) depuis près de 11 ans maintenant, voici notre sélection des liens les plus insolites de ces derniers jours, tous publiés sur LIDD.fr auparavant (...).*» Inutiles donc indispensables LIDD :)
Source : www.nextinpact.com/news/95498-538eme-edition-lidd-liens-idiots-du-dimanche.htm
Billets en relation :
31/05/2015. *535ème édition des LIDD : Liens Idiots Du Dimanche* : www.nextinpact.com/news/95253-535eme-edition-lidd-liens-idiots-du-dimanche.htm
07/06/2015. *536ème édition des LIDD : Liens Idiots Du Dimanche* : www.nextinpact.com/news/95338-536eme-edition-lidd-liens-idiots-du-dimanche.htm
14/06/2015. *537ème édition des LIDD : Liens Idiots Du Dimanche* : www.nextinpact.com/news/95408-537eme-edition-lidd-liens-idiots-du-dimanche.htm

Mises À Jour importantes

=> **Microsoft Patch Tuesday – June 2015**. 09/06/2015. «*Today, Microsoft has released their monthly set of security bulletins designed to address security vulnerabilities within their products. This month's release sees a total of 8 bulletins being released which address 45 CVE. Two of the bulletins are listed as Critical and address vulnerabilities in Internet Explorer and Windows Media Player. The remaining six bulletins are marked as Important and address vulnerabilities in Microsoft Office, Windows Kernel, Active Directory, Microsoft Exchange Server, and Microsoft Common Controls (...).*»
Source : blogs.cisco.com/security/talos/ms-tuesday-june-2015
Billets en relation :
09/06/2015. *Microsoft Security Updates June 2015* : securelist.com/blog/software/70531/microsoft-security-updates-june-2015/
10/06/2015. *Un Patch Tuesday abyssal* : www.cnis-mag.com/un-patch-tuesday-abyssal.html
10/06/2015. *June 2015 – Microsoft Releases 8 Security Advisories* : www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/6859/june-2015-microsoft-releases-8-security-advisories

=> **Adobe, Microsoft Issue Critical Security Fixes**. 10/06/2015. «*Adobe today released software updates to plug at least 13 security holes in its Flash Player software. Separately, Microsoft pushed out fixes for at least three dozen flaws in Windows and associated software (...).*»
Source : krebsonsecurity.com/2015/06/adobe-microsoft-issue-critical-security-fixes-4/

Actus Législatives et juridiques

=> **148 000€ réclamés à l'ancien admin de mamie tracker**. 26/05/2015. «*En octobre 2012, la cour d'Appel de Pau confirmait la condamnation de l'administrateur de l'ancien site dédié aux torrents, Mamie Tracker. Son concepteur doit payer plus de 148 000€ avant la fin juin 2015. (...).*»
Source : www.zataz.com/148-000e-reclame-a-lancien-admin-de-mamy-tracker-avant-juin/

=> **Vol d'information : une jurisprudence Bluetouff pour la gloire ?**. 26/05/2015. «*Pour l'avocat François Coupez, si l'arrêt de la Cour de cassation dans l'affaire Bluetouff permet d'affirmer que la copie non autorisée d'un fichier s'apparente à un vol, le législateur avait déjà statué en ce sens. D'autre part, l'arrêt ne constitue pas, selon lui, une incitation à ne pas sécuriser les systèmes d'information. Beaucoup de bruit pour rien ? (...).*»
Source : www.silicon.fr/vol-information-jurisprudence-bluetouff-pour-gloire-117057.html?PageSpeed=noscript
Billets en relation :
27/05/2015. *3000€ d'amende et un casier judiciaire pour une requête Google* : reflets.info/3000e-damende-et-un-casier-judiciaire-pour-une-requete-google/
27/05/2015. *Quand l'ignorance et la stupidité font la loi* : www.securiteoff.com/loi/

=> **Copie privée : les ayants droit condamnés à rembourser 1 million d'euros à Auchan et Carrefour**. 26/05/2015. «*Le 22 mai dernier, Copie France a été condamné par le tribunal de grande instance de Paris à rembourser un trop versé de 1,08 million d'euros à Auchan et Carrefour. Les sociétés espéraient plus de dix fois plus. En vain (...).*»
Source : www.nextinpact.com/news/95188-copie-privee-ayants-droit-condamnes-a-rembourser-1-million-deuros-a-auchan-et-carrefour.htm

=> **Adblock Plus remporte une victoire judiciaire en Allemagne**. 28/05/2015. «*C'est un petit programme qui perce un trou de plus en plus gros dans la bourse des revenus publicitaires des médias en ligne : Adblock Plus, édité par la start-up allemande Eyeo, permet gratuitement à tout internaute de faire disparaître les publicités des pages qu'il visite (...).*»
Source : www.lemonde.fr/pixels/article/2015/05/28/adblock-plus-remporte-une-victoire-judiciaire-en-allemagne_4642162_4408996.html
Billets en relation :
03/06/2015. *Un adblock communautaire ? - First Monday* : alireailleurs.tumblr.com/post/120592994365/un-adblock-communautaire-first-monday#_=_

=> **Le fondateur du site de vente de drogue Silk Road condamné à la réclusion à perpétuité**. 29/05/2015. «*Ross Ulbricht, le fondateur du site de vente de drogues en ligne Silk Road a été condamné vendredi 29 mai à la réclusion à perpétuité par un tribunal de New York (...).*»
Source : www.lemonde.fr/pixels/article/2015/05/29/le-fondateur-du-site-de-vente-de-drogue-silk-road-condamne-a-la-reclusion-a-perpetuite_4643825_4408996.html
Billets en relation :
31/05/2015. *Silk Road : Ross Ulbricht condamné à la prison à vie* : www.undernews.fr/lois-justice/silk-road-ross-ulbricht-condamne-a-la-prison-a-vie.html

=> **The twins: two brothers on probation were arrested for online-banking theft in Russia**. 02/06/2015. «*This group was using malicious software to gain access to customers' accounts and under the guise of bank employees was extorting SMS authorization codes required to steal the money (...).*»
Source : www.group-ib.com/index.php/7-novosti/929-the-twins-two-brothers-on-probation-were-arrested-for-online-banking-theft-in-russia
Billets en relation :
17/06/2015. *Europol signs agreement with GROUP-IB to cooperate in fighting cybercrime* : www.group-ib.com/index.php/7-novosti/932-europol-signs-agreement-with-group-ib-to-cooperate-in-fighting-cybercrime

=> **QPC sur les données de connexion : interview de Benjamin Bayart**. 05/06/2015. «*Aujourd'hui, le Conseil d'État a donc transmis au Conseil constitutionnel la Question Prioritaire de Constitutionnalité (QPC) déposée par la Quadrature du Net, French Data Network et FFDN. La cible ? Tout simplement l'or noir de la loi de programmation militaire mais aussi du projet de loi Renseignement : les données de connexion, visiblement mal définies par les textes. C'est ce que nous explique Benjamin Bayart, porte-parole de French Data Network (...).*» A PSES, Benjamin Bayart et Fabien Sirjean reviennent sur les finalités et la méthodologie des recours qu'ils ont initié, et leurs conséquences potentielles. Très instructif.
Source : www.nextinpact.com/news/95335-qpc-sur-donnees-connexion-interview-benjamin-bayart.htm
Billets en relation :
02/06/2015. *Données de connexion : interview de Me Spinosi, avocat de la Quadrature, FDN et FFDN* : www.nextinpact.com/news/95277-donnees-connexion-interview-me-spinosi-avocat-quadrature-fdn-et-ffdn.htm
05/06/2015. *Première victoire pour les citoyens contre la surveillance : la Loi de Programmation Militaire devant le Conseil Constitutionnel* : www.laquadrature.net/fr/premiere-victoire-pour-les-citoyens-contre-la-surveillance-la-loi-de-programmation-militaire-devant
05/06/2015. *La collecte de données par l'Etat devant le Conseil constitutionnel* : www.numerama.com/magazine/33308-la-collecte-de-donnees-par-l-etat-devant-le-conseil-constitutionnel.html
06/06/2015. *Notre QPC sur la LPM est transmise au Conseil Constitutionnel* : blog.fdn.fr/?post/2015/06/06/Notre-QPC-LPM-transmise-Conseil-Constitutionnel
19/06/2015. *PSES - FDN contre gouvernement* : lacantine.ubicast.eu/videos/fdn-contre-gouvernement/
19/06/2015. *Comme un hiatus entre Valls et ses «chers geeks» de Pas Sage en Seine* : www.makery.info/2015/06/19/comme-un-hiatus-entre-valls-et-ces-chers-geeks/

=> **Ces 36 sites islamistes interdits… dont vous n'entendrez jamais parler** . 09/06/2015. «*Bernard Cazeneuve l'a annoncé il y a peu : 36 sites web ont été bloqués en France pour apologie du terrorisme. Mais vous ne saurez jamais lesquels ni pourquoi (...).*»
Source : www.lepoint.fr/high-tech-internet/ces-36-sites-islamistes-interdits-dont-vous-n-entendrez-jamais-parler-09-06-2015-1934945_47.php
Billets en relation :
13/06/2015. *Censure administrative des sites pour lutter contre la prostitution, l'Assemblée vote contre* : www.libre-parcours.net/post/censure-administrative-sites-prostitution-suite/

=> **Eurojust and Europol in massive joint action against cybercriminals**. 10/06/2015. «*Yesterday, a total of 49 suspects were arrested and 58 searches carried out in the framework of a massive joint action against cybercrime led by Italian, Spanish and Polish judicial and police authorities with the support of Belgium, the UK and Georgia. The action day represents the successful conclusion of three linked Eurojust cases coordinated by the Italian, Spanish and Polish National Desks, with Europol providing real-time support to the law*

enforcement authorities operating on the ground (...).»
Source : eurojust.europa.eu/press/PressReleases/Pages/2015/2015-06-10.aspx
Billets en relation :
10/06/2015. *CP FR* : eurojust.europa.eu/press/Documents/2015-PR-Translations/2015-06-10_Operation-Triangle_FR.pdf
10/06/2015. *European Authorities Dismantle Cybercrime Ring, Dozens Arrested* : www.tripwire.com/state-of-security/latest-security-news/european-authorities-dismantle-cybercrime-ring-dozens-arrested/
10/06/2015. *International operation dismantles criminal group of cyber-fraudsters* : www.europol.europa.eu/content/international-operation-dismantles-criminal-group-cyber-fraudsters-0
11/06/2015. *49 Corporate Email Phishers arrested in Operation Triangle* : garwarner.blogspot.fr/2015/06/49-corporate-email-phishers-arrested-in.html

=> **Rapport d'information sur le bilan annuel de l'application des lois au 31 mars 2015**. 10/06/2015. «*La question de l'application des lois est un enjeu très important, car à quoi bon faire des lois, si elles doivent rester lettre morte en tout ou partie ? C'est pourquoi, dès les années 1970, le Sénat a mis en place des procédures et des outils permettant à ses commissions permanentes de suivre en temps réel la publication des décrets et des arrêtés attendus. Cette année, le Bureau du Sénat a confié à un des Vice-Présidents la mission de synthétiser les observations des commissions sur la mise en application des lois de leur ressort au titre de l'année parlementaire 2013-2014. (...).*»
Source : www.senat.fr/notice-rapport/2014/r14-495-notice.html

=> **La réalité augmentée a-t-elle besoin d'un droit spécifique aujourd'hui ?** . 11/06/2015. «*Nous revenons régulièrement ici sur certaines conséquences juridiques de l'utilisation et du développement de la Réalité Augmentée. Suite à la publication en février dernier d'un très bon article de Caroline Levardet dans « Expertise », je vous propose de refaire un point sur le domaine. Attention, mon inculture juridique ne me permet pas d'aller au fond des choses, je me contenterai donc d'une vision globale (...).*»
Source : www.augmented-reality.fr/2015/06/la-realite-augmentee-a-t-elle-besoin-dun-droit-specifique-aujourdhui/
Billets en relation :
15/02/2015. *Réalita augmentée - vers un encadrement juridique 3.0 ?* : www.laverdet-avocat.com/publications/Expertises-f%C3%A9vrier-2015-R%C3%A9alit%C3%A9-augment%C3%A9e-vers-un-encadrement-juridique-3-0-Caroline-Laverdet.pdf

=> **L'arme procédurale, la plus efficace**. 12/06/2015. «*Ca fait un petit moment que nous ne vous avons pas parlé du redoutable article 40 de la Constitution, qui interdit à tous les députés (sans exception) de faire des propositions qui augmentent les dépenses de l'Etat. Pour la séance, le juge de cette recevabilité est le Président de la Commission des finances, qui est impitoyable (...).*»
Source : blogs.lexpress.fr/cuisines-assemblee/2015/06/12/larticle-40-partout-tout-le-temps/

=> **La Cour constitutionnelle belge annule une loi controversée sur la surveillance des télécommunications**. 12/06/2015. «*La Cour constitutionnelle belge a adopté, jeudi 11 juin, un arrêt qualifié d'« historique », qui annule une loi de juillet 2013 sur la conservation des données liées à des communications électroniques et téléphoniques. Pour les juges belges, ces dispositions, discriminatoires et contraires aux principes d'égalité, violent la vie privée des citoyens et le secret de certaines professions (...).*» A voir en écho l'actualité QPC initiée par 3 associations.
Source : www.lemonde.fr/pixels/article/2015/06/12/la-cour-constitutionnelle-belge-annule-une-loi-controversee-sur-la-surveillance-des-telecommunications_4653047_4408996.html
Billets en relation :
05/06/2015. *Cinq idées fausses sur la surveillance de masse* : www.liberation.fr/societe/2015/06/05/cinq-idees-fausses-sur-la-surveillance-de-masse_1323369
05/06/2015. *Deux ans après Snowden, ce qui a changé pour la surveillance de masse* : www.lemonde.fr/pixels/article/2015/06/05/deux-ans-apres-snowden-ce-qui-a-change-pour-la-surveillance-de-masse_4648014_4408996.html
09/06/2015. *La résistible montée du Flicage Généralisé* : www.cnis-mag.com/la-resistible-montee-du-flicage-generalise.html
11/06/2015. *Au Royaume-Uni, le contrôleur antiterroriste veut maintenir mais encadrer la surveillance de masse* : www.lemonde.fr/pixels/article/2015/06/11/au-royaume-uni-le-controleur-antiterroriste-veut-maintenir-mais-encadrer-la-surveillance-de-masse_4652375_4408996.html
12/06/2015. *La Cour constitutionnelle belge annule la loi sur la conservation des données personnelles* : www.nextinpact.com/news/95394-la-cour-constitutionnelle-belge-annule-loi-sur-conservation-donnees-personnelles.htm
18/06/2015. *La loi Renseignement « pourrait soulever d'importantes questions de droit » selon Bruxelles* : www.nextinpact.com/news/95474-la-loi-renseignement-pourrait-soulever-dimportantes-questions-droit-selon-bruxelles.htm

=> **Envoi sans consentement de lettres d'information électroniques contenant de la prospection : sanction de 15.000 euros** .
12/06/2015. «*La formation restreinte a prononcé une sanction de 15.000 euros à l'encontre de la société PRISMA MEDIA, spécialisée dans l'édition et la commercialisation de magazines périodiques et des sites internet de ces magazines (...).*»
Source : www.cnil.fr/nc/linstitution/actualite/article/article/envoi-sans-consentement-de-lettres-dinformation-electroniques-contenant-de-la-prospection-sanc/

=> **L'Europe fait des propositions pour protéger les données personnelles**. 15/06/2015. «*Les ministres de la justice de l'Union*

européenne ont clôturé, lundi à Luxembourg, trois ans et demi de discussions sur la protection des données personnelles. Ils ont approuvé une proposition censée être mieux adaptée au développement de l'économie numérique alors que les dispositions actuelles datent de 1995. Le projet doit encore être soumis au Parlement, à Strasbourg, avant son adoption éventuelle (...).»
Source : www.lemonde.fr/economie/article/2015/06/15/l-europe-fait-des-propositions-pour-proteger-les-donnees-personnelles_4654482_3234.html
Billets en relation :
12/06/2015. *Droit à l'oubli : la CNIL exige un déréférencement mondial chez Google* : www.nextinpact.com/news/95397-droit-a-oubli-cnil-exige-dereferencement-mondial-chez-google.htm
12/06/2015. *La CNIL met Google en demeure d'élargir son « droit au déréférencement »* : www.lemonde.fr/pixels/article/2015/06/12/la-cnil-met-google-en-demeure-d-elargir-son-droit-au-dereferencement_4652699_4408996.html
15/06/2015. *La Commission belge de protection de la vie privée poursuit Facebook en justice* : www.lemonde.fr/pixels/article/2015/06/15/la-commission-belge-de-protection-de-la-vie-privee-poursuit-facebook-en-justice_4654604_4408996.html
17/06/2015. *Vie privée en Europe : bientôt le nouveau règlement* : www.droit-technologie.org/actuality-1724/vie-privee-en-europe-bientot-le-nouveau-reglement.html

=> **HSC Bulletin d'actualités juridiques n°41**. 15/06/2015. «*Le bulletin d'actualités juridiques HSC est accessible à tous gratuitement. Il est rédigé en français par les consultants du pôle juridique d'HSC (...).*»
Source : baj.hsc-news.com/archives/bulletin/HSC-BAJ-20150615.pdf
Billets en relation :
01/06/2015. *HSC Bulletin d'actualités juridiques n°40* : baj.hsc-news.com/archives/bulletin/HSC-BAJ-20150529.pdf

=> **Salades d'espions en Allemagne**. 16/06/2015. «*Le Président du Parquet Fédéral - chargé des affaires d'espionnage, de terrorisme et de haute trahison- a décidé d'abandonner les charges dans l'affaire des écoutes téléphoniques dont aurait été victime la Chancelière Angela Merkel en 2013. Les preuves, avancées par les documents Snowden, ne constitueraient pas de preuves suffisantes (...).*»
Source : www.cnis-mag.com/salades-despions-en-allemagne.html

=> **Téléchargement illégal : onze nouvelles condamnations**. 17/06/2015. «*Le tribunal correctionnel de Paris a condamné mercredi 17 juin un prévenu à six mois de prison ferme, et dix autres, à des peines de prison avec sursis, dans une affaire de téléchargement de films vieille de dix ans (...).*»
Source : www.lemonde.fr/pixels/article/2015/06/17/telechargement-illegal-onze-nouvelles-condamnations_4656230_4408996.html
Billets en relation :
17/06/2015. *Piratage : douze ans après, fin du procès des "anars du 7e art"* : www.franceinter.fr/depeche-piratage-douze-ans-apres-fin-du-proces-des-anars-du-7e-art
18/06/2015. *Piratage : 11 membres liés au groupe GGTeam condamnés* : www.numerama.com/magazine/33430-piratage-11-membres-lies-au-groupe-ggteam-condamnes.html

=> **La presse en ligne peut être tenue de retirer immédiatement des commentaires illicites**. 17/06/2015. «*Historique, regrettable, censure… Les qualificatifs ne manquent pas après l'arrêt rendu hier par la Grande chambre de la Cour européenne des droits de l'homme. Celle-ci estime qu'un site de presse peut avoir à supprimer les commentaires injurieux sans attendre d'être alertée, ni que ce coup de ciseau soit qualifié d'atteinte à la liberté d'expression (...).*»
Source : www.nextinpact.com/news/95449-la-presse-en-ligne-peut-etre-tenue-retirer-immediatement-commentaires-illicites.htm
Billets en relation :
16/06/2015. *La CEDH encourage la censure des commentaires haineux sur les sites de presse* : www.numerama.com/magazine/33418-la-cedh-encourage-la-censure-des-commentaires-haineux-sur-les-sites-de-presse.html
16/06/2015. *Delfi's Struggle For Freedom Of Expression Did Not Win Support of ECHR* : www.delfi.ee/news/en/news/delfis-struggle-for-freedom-of-expression-did-not-win-support-of-echr?id=71720703
16/06/2015. *AFFAIRE DELFI AS c. ESTONIE* : hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-155627
17/06/2015. *Les sites web seraient responsables des commentaires des utilisateurs* : www.developpez.com/actu/86534/Les-sites-web-seraient-responsables-des-commentaires-des-utilisateurs-d-apres-la-Cour-europeenne-des-droits-de-l-Homme/

=> **#FixCopyright : le bilan du vote par Julia Reda**. 17/06/2015. «*Hier, la commission JURI du Parlement européen s'est réunie pour voter la version finale du rapport Reda, le rapport visant à dépoussiérer et harmoniser le droit d'auteur au niveau européen) avant que de le présenter au parlement. Julia Reda a présenté sur son blog une analyse détaillée de ce qu'est devenu le rapport après des mois de tractations afin qu'il soit accepté par l'ensemble de la commission. L'équipe framalang, armée de cafetières et de courage, a œuvré toute la nuit pour vous fournir une traduction de cette analyse (...).*»
Source : framablog.org/2015/06/17/fixcopyright-le-bilan-du-vote-par-julia-reda/
Billets en relation :
29/05/2015. *Le droit d'auteur (ou copyreich) pour les nuls* : lehollandaisvolant.net/?d=2015/05/29/12/45/15-le-droit-dauteur-ou-copyreich-pour-les-nuls

03/06/2015. *À Bruxelles, la France se fait ambassadrice du lobbying des ayants droit* : www.nextinpact.com/news/95294-a-bruxelles-france-se-fait-ambassadrice-lobbying-ayants-droit.htm
14/06/2015. *Réviser le droit d'auteur au niveau européen* : www.paralipomenes.net/archives/11233

=> **Loi Renseignement**. 18/06/2015. «*Voilà. Le projet de loi sur le renseignement a été arbitré en Commission mixte Paritaire. Le texte final sera discuté au Sénat le 23 juin, puis le lendemain à l'Assemblée nationale (...).*»
Source : www.nextinpact.com/news/95442-loi-renseignement-etrangers-en-france-seront-moins-bien-proteges.htm
Billets en relation :
02/06/2015. *Loi sur le renseignement : ce qu'en pensent vraiment les espions* : www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/loi-sur-le-renseignement-ce-qu-en-pense-vraiment-les-espions-480474.html
11/06/2015. *Loi Renseignement, après le vote du Sénat* : standblog.org/blog/post/2015/06/11/Loi-Renseignement-apres-le-vote-du-Senat
16/06/2015. *Loi Renseignement : le texte final sera voté le 24 juin* : www.numerama.com/magazine/33415-loi-renseignement-le-texte-final-sera-vote-le-24-juin.html
17/06/2015. *La Fabrique de la Loi - Projet de loi relatif au renseignement* : www.lafabriquedelaloi.fr/articles.html?loi=pjl14-424
17/06/2015. *Replay & Transcript s Debates PJL Information* : pad.lqdn.fr/p/Replay_AN_PJL_Rens
18/06/2015. *Loi Renseignement : Waterloo des libertés à la Commission Mixte Paritaire* : www.laquadrature.net/fr/loi-renseignement-waterloo-des-libertes-a-la-commission-mixte-paritaire

=> **Copyright Madness (#109) : une semaine de propriété intellectuelle en délire**. 20/06/2015. «*Tous les samedis, Numerama vous propose de découvrir une sélection d'articles concoctée par Lionel Maurel et Thomas Fourmeux sur les dérives de la propriété intellectuelle. Cette semaine, Apple est à l'honneur dans deux actualités. Mais l'on parle aussi de Lego et de CorbisImage, qui s'est pris les pieds dans le tapis avec une photo du domaine public. Bonne lecture ! (...).*»
Source : www.numerama.com/magazine/33459-copyright-madness-109-une-semaine-de-propriete-intellectuelle-en-delire.html
Billets en relation :
30/05/2015. *Copyright Madness (#106)* : www.numerama.com/magazine/33255-copyright-madness-106-une-semaine-de-propriete-intellectuelle-en-delire.html
03/06/2015. *Pourquoi Saint-Exupéry est-il entré dans le domaine public partout, sauf en France ?* : www.liberation.fr/culture/2015/06/03/pourquoi-saint-exupery-est-il-tombe-dans-le-domaine-public-partout-sauf-en-france_1322085
06/06/2015. *Copyright Madness (#107)* : www.numerama.com/magazine/33311-copyright-madness-107-une-semaine-de-propriete-intellectuelle-en-delire.html
13/06/2015. *Copyright Madness (#108)* : www.numerama.com/magazine/33383-copyright-madness-108-une-semaine-de-propriete-intellectuelle-en-delire.html
19/06/2015. *European Copyright Madness: Court Strikes Down Law Allowing Users to Rip Their Own CDs* : www.eff.org/deeplinks/2015/06/european-copyright-madness-court-strikes-down-law-allowing-users-rip-their-own-cds

Réseaux sociaux et communautaires

=> **The Geography of Tweets: Reading Tweets with QGIS**. 26/05/2015. «*Anita showed some nice examples of tweets in QGIS in 2012. Since then it seemed to be quiet about the twitter-content in QGIS. Yet tweets can be an interesting source of information. Sometimes they can tell you something about the spatiotemporal dimensions regarding a keyword, the digital heartbeat of a defined region and many more. Yet we need to be careful with the data as it is completely biased. But how to get this data stream into QGIS? (...).*» En date du 17/05 initialement.
Source : www.digital-geography.com/the-geography-of-tweets-reading-tweets-with-qgis/#.VWdt0rwxXeS

=> **Twitter bloque Politwoops, un site qui conservait les tweets supprimés des politiques**. 05/06/2015. «*Twitter a bloqué l'accès de son API, son interface de programmation, à Politwoops, un site qui répertorie les tweets supprimés d'hommes et femmes politiques américains. Le site n'a donc plus la possibilité de tracer les tweets effacés depuis le 15 mai (...).*»
Source : www.lemonde.fr/pixels/article/2015/06/05/twitter-bloque-politwoops-un-site-qui-conservait-les-tweets-supprimes-des-politiques_4648121_4408996.html

=> **Radié de sa banque pour avoir dénoncé une appli intrusive ?**. 15/06/2015. «*C'est l'histoire d'une application bancaire intrusive qui vaut à l'un de ses utilisateurs quelques ennuis avec sa banque. Fin mai, ce spécialiste en sécurité informatique autodidacte, Gwen, alias @Sorcier_FXK sur Twitter, jette un œil à la mise à jour que lui demande son application portable du CIC (...).*»
Source : rue89.nouvelobs.com/2015/06/15/radie-banque-avoir-denonce-appli-intrusive-259779
Billets en relation :
15/06/2015. *Un tweet : Cic bloque ses fonds, désactive sa carte et résilie son compte. L'analyse* : www.reputatiolab.com/2015/06/un-tweet-cic-bloque-ses-fonds-desactive-sa-carte-et-resilie-son-compte-lanalyse/
15/06/2015. *Quand le CIC surréagit à une simple question* : korben.info/cic-violence.html
16/06/2015. *Mieux vaut être riche, bien portant et ne pas poser de questions, pour être client au CIC* : reflets.info/mieux-vaut-etre-riche-

bien-portant-et-ne-pas-poser-de-questions-pour-etre-client-au-cic/
17/06/2015. *Opération « Internet propre » pour le CIC* : reflets.info/operation-internet-propre-pour-le-cic/

=> **Les médias sociaux : quel usage pour le marché de l'emploi ?**. 17/06/2015. «*En 2013, 8 % des sociétés de dix personnes ou plus implantées en France utilisent les médias sociaux dans leur processus de recrutement de personnel. Ce recours atteint 32 % dans le secteur de l'information et de la communication et 24 % parmi les sociétés de 250 personnes ou plus. Parallèlement, 30 % des personnes à la recherche d'un emploi mobilisent les réseaux sociaux dans leurs démarches, notamment les plus jeunes et les plus diplômés (...).*»
Source : www.insee.fr/fr/themes/document.asp?ref_id=if30
Billets en relation :
01/06/2015. *Les réseaux sociaux professionnels, peu efficaces pour le recrutement des cadres* : www.blogdumoderateur.com/apec-sourcing-cadres-2015-reseaux-sociaux/
18/06/2015. *Étude Insee : 30% des candidats utilisent les médias sociaux, seulement 8% des recruteurs* : www.blogdumoderateur.com/insee-medias-sociaux-candidats-recruteurs/

=> **Plongée dans les égouts de l'influence Volume 2**. 17/06/2015. «*Il y a un an, je pataugeais dans les crasses des égouts de l'influence où j'avais notamment croisé Cloudwatt pour vous prouver que des vraies personnes pouvaient avoir une fausse influence. Or, j'ai oublié de vous dire que des fausses personnes peuvent avoir une vraie influence (...).*»
Source : www.reputatiolab.com/2015/06/plongee-dans-les-egouts-de-linfluence-volume-2/