

ANTI-VIRUS SOFTWARE UPDATE - GSD THOUGHTS

<http://grandstreamdreams.blogspot.it/2015/02/anti-virus-software-update-gsd-thoughts.html>

FISHY CODE BUNDLED ON LENOVO LAPTOPS FOUND IN OTHER PROGRAMS

<http://arstechnica.com/security/2015/02/ssl-busting-code-that-threatened-lenovo-users-found-in-a-dozen-more-apps/>

LENOVO RELEASES SUPERFISH REMOVAL TOOL

<http://www.computerworld.com/article/2887136/lenovo-releases-tool-to-purge-superfish-crapware.html>

ANTHEM NOW SAYS 78.8M WERE AFFECTED BY BREACH

<http://www.computerworld.com/article/2888267/anthems-now-says-788m-were-affected-by-breach.html>

EUROPOL: RAMNIT BOTNET TAKEN DOWN

<http://arstechnica.com/tech-policy/2015/02/europol-cracks-down-on-botnet-infecting-3-2-million-computers/>

http://www.theregister.co.uk/2015/02/25/europol_shuts_down_ramnit_botnet_hampshire/

US OFFERS \$3 MILLION REWARD FOR CAPTURE OF GAMEOVER/ZEUS BOTNET ADMIN

<http://arstechnica.com/tech-policy/2015/02/us-offers-3-million-reward-for-capture-of-gameover-zeus-botnet-admin/>

<http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev>

HOW AL-QAEDA USES ENCRYPTION POST-SNOWDEN

<https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/>

<https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/>

=====
LEGGI, DOTTRINA, GIURISPRUDENZA
=====

CASSAZIONE: ILLEGITTIMO IL SEQUESTRO PREVENTIVO DEI SITI DEI GIORNALI

<http://www.zeusnews.it/n.php?c=22420>

HOME BANKING: RESPONSABILITÀ PARZIALE IN CASO DI ATTACCO

<http://www.quotidianodiritto.ilsole24ore.com/art/amministrativo/2014-11-26/colpa-parziale-se-cliente-non-nota-l-hacker--194747.php>;

<http://www.creditofinanzanews.it/2014/12/03/home-banking-responsabilita-parziale-del-cliente-che-non-nota-lhacker/>

POSTE ITALIANE DEVONO RIMBORSARE UNA VITTIMA DI PHISHING

<http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=68463>

PROVVEDIMENTO GARANTE BIOMETRIA

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992>

DEI DANNI DELLA VIOLAZIONE DELLA PRIVACY

<http://www.filodiritto.com/news/2014/cassazione-civile-per-il-risarcimento-della-violazione-della-privacy-la-lesione-deve-essere-grave-e-il-danno-non-futile.html>

AGGIORNAMENTO SUL REGOLAMENTO EUROPEO SULLA PRIVACY (C'È TEMPO...)

<http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-12-11/regolamento-europeo-privacy-ancora-discussione-162857.php>

SOCIAL NETWORK ASSIMILATO A LUOGO PUBBLICO

<http://thinkinginforensics.net/2014/11/social-network-assimilato-ad-un-luogo-aperto-al-pubblico/>

NUOVE LINEE GUIDA CONFIDUSTRIA PER 231

http://www.confindustria.it/wps/portal/IT/AreeTematiche/Diritto-d-impresa/Documenti/Dettaglio-doc-diritto-impresa/4eaa0336-f353-4bc8-aa05-35dfda228a50/4eaa0336-f353-4bc8-aa05-35dfda228a50!/ut/p/a0/04_Sj9CPykyssy0xPLMnMz0vMAfGjzOJ9PT1MDD0NjLz83UxNDBxNgpwCfYzdLCzDTPQLsh0VAVhK9gI!/

=====
PAPERS/TUTORIALS
=====

[ITA] RAPPORTO SULLA SICUREZZA NELLE PA

<http://www.cis.uniroma1.it/csr2014>

WINDOWS PHONE 8 FORENSIC ARTIFACTS

<http://www.sans.org/reading-room/whitepapers/forensics/windows-phone-8-forensic-artifacts-35787>

FORENSICS AND BITCOIN

<http://articles.forensicfocus.com/2015/01/16/forensics-bitcoin/>

IN-MEMORY SHELLCODE DETECTION USING A PATTERNS-BASED METHODOLOGY

<http://blog.norsecorp.com/2015/02/24/in-memory-shellcode-detection-using-a-patterns-based-methodology/>

DEFEATING TRUCCRYPT: PRACTICAL ATTACKS AGAINST TRUCCRYPT SECURITY

<http://resources.infosecinstitute.com/defeating-truencrypt-practical-attacks-truencrypt-security>

FORENSIC ANALYSIS OF SQLITE DATABASES: FREE LISTS, WRITE AHEAD LOG, UNALLOCATED SPACE AND CARVING

<http://articles.forensicfocus.com/2015/02/16/forensic-analysis-of-sqlite-databases-free-lists-write-ahead-log-unallocated-space-and-carving>

PROCESS HOLLOWING MEETS CUCKOO SANDBOX

<http://journeyintoir.blogspot.it/2015/02/process-hollowing-meets-cuckoo-sandbox.html>

WHAT'S NEW IN WINDOWS APPLICATION EXECUTION?

<http://forensicmethods.com/application-execution>

ENISA THREAT LANDSCAPE 2014

<http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014>

ENISA THREAT LANDSCAPE OF INTERNET INFRASTRUCTURE

<https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iit1>

NIST SP 800-88 GUIDELINES FOR MEDIA SANITIZATION

<http://csrc.nist.gov/publications/PubsSPs.html#800-88>

NIST SP 800-53 - ASSESSING SECURITY

<http://csrc.nist.gov/publications/PubsSPs.html#800-53ar4>

WINDOWS XP RESTORE POINTS

<http://hatsoffsecurity.com/2015/01/20/windows-xp-restore-points/>

=====
TOOLS
=====

USB DEVICE FORENSICS v0.0.2

<https://github.com/woanware/usbdeviceforensics>

<https://github.com/woanware/usbdeviceforensics/releases>

SUPERFETCH DUMPER

<https://code.google.com/p/rewolf-superfetch-dumper/>

CORWD RESPONSE

<http://www.crowdstrike.com/community-tools/>

MAGNET RAM CAPTURE

<http://www.magnetforensics.com/ram-capture/>

COMPARISON OF CLOUD AUTOMATED MALWARE ANALYSIS TOOLS

<http://resources.infosecinstitute.com/comparison-cloud-automated-malware-analysis-tools/>

CIPHERSHED

<https://ciphershed.org/>

GETTING ATTACHED: APPLE MESSAGING ATTACHMENTS

<http://linuxsleuthing.blogspot.ch/2015/01/getting-attached-apple-messaging.html>

HEXINATOR

<https://hexinator.com/>

=====

FORMAZIONE

=====

MALWARE ANALYSIS e LE INTERCETTAZIONI 2.0

2° Seminario IISFA

Aula 304, Università statale di Milano

Via Festa del perdono, Milano, Italy

http://www.iisfa.net/events/event_details.asp?id=606252&group=

Ciclo di seminari presso UNIBO

<http://www.cirsfid.unibo.it/risorse/files/locandine-avvisi-ed-eventi/locandina-ciclo-di-seminari-di-informatica-forense-del-2015>

=====

CONFERENCES & CFP

=====

DFRWS - DIGITAL FORENSICS RESEARCH WORKSHOP 2015

March, 23-26, 2015

Dublin, Ireland

<http://www.dfrws.org/2015eu/cfp.shtml>

DEFTCON

April, 17, 2015

Roma, Italy

<http://www.deftlinux.net/it/2015/02/13/deftcon-2015-a-roma-17-aprile/>

=====

LINKS

=====

BLOGS & PORTALS

<http://www.forensicblog.org>

<http://www.forensicfocus.com/computer-forensics-blog>

<http://articles.forensicfocus.com/>

<http://computer-forensics.sans.org/blog>

<http://computer.forensikblog.de/en/>

<http://windowsir.blogspot.com>

<http://www.forensickb.com>

<http://www.forensicinnovations.com/blog>

<http://forensicsfromthepretsausagefactory.blogspot.com/>

<http://ericjhuber.blogspot.com/>

<http://consoleforensics.com/>

<http://www.forensicphotoshop.blogspot.com/>

<http://forensicmethods.com/>

<http://blog.digital-forensics.it/>

<http://f-interviews.com/>

<http://www.techandlaw.net/>

<http://xwaysclips.blogspot.it/>

<http://justaskweg.com/>

<http://memoryforensics.blogspot.it/>

<https://www.privacyinternational.org/>

<http://volatility-labs.blogspot.it/>

[ITA] <http://www.sig.it/>

[ITA] <http://pierluigiperri.com/>

[ITA] <http://blog.cesaregallotti.it>

[ITA] <http://mattiaep.blogspot.it>

PODCASTS

<http://www.cybercrime101.com>

<http://cyberspeak.libsyn.com>

<http://forensic4cast.com/>

WIKIS

<http://www.forensicswiki.org>
<http://www.forensicwiki.com>
http://www.forensicswiki.org/wiki/Scheduled_Training_Courses
http://www.forensicswiki.org/index.php?title=Upcoming_events
http://cyber.law.harvard.edu/cybersecurity/Cybersecurity_Annotated_Bibliography

TOOLS

<http://www.opensourceforensics.org/>
<http://www.cftt.nist.gov/>
<http://computercrimeinfo.com/info.html>
<http://www.mikesforensictools.co.uk/software.html>
<https://code.google.com/p/regripper/>
<http://www.mobileforensicscentral.com/mfc/>
<http://forensiccontrol.com/resources/free-software/>
<http://winfe.wordpress.com/>

GOOGLE DIGITAL FORENSICS SEARCH

<http://www.google.com/cse/home?cx=011905220571137173365:7eskxxzhjj8>

=====

Newsletter a cura del Consiglio dell'Associazione DFA - Digital Forensics Alumni.

INFORMATIVA AI SENSI DELL'ART. 13 DEL D.LGS. 196/2003

Digital Forensics Alumni in qualità di titolare del trattamento dei dati personali, informa che i dati conferiti, verranno utilizzati esclusivamente per lo scopo di gestione del servizio newsletter. Il trattamento avverrà sia su supporto cartaceo che avvalendosi di strumenti elettronici. I dati non verranno in nessun modo diffusi né comunicati ad alcuni terzi. I diritti di cui all'art. 7 del D.Lgs. 196/2003 (aggiornamento, cancellazione, ecc.), potranno essere esercitati rivolgendosi all'Associazione scrivendo all'indirizzo di posta elettronica info@perfezionisti.it. Al sito www.perfezionisti.it è accessibile la versione più estesa della presente Informativa.

=====