\\\\\\\\\\\\ DIGITAL FORENSICS ALUMNI ////////////

Newsletter 21 - Agosto 2012

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

Indice:


**********

==========
NEWS
==========

TRIBUNALI E DROPBOX
http://blog.cesaregallotti.it/2012/08/tribunali-e-dropbox.html

INTERVIEW WITH PASQUALE STIRPARO by FORENSICS INTERVIEWS
http://f-interviews.com/2012/08/15/interview-with-pasquale-stirparo/

ANONYMOUS ATTACCA IL SITO WEB DELL'INTERPOL
http://www.ilsole24ore.com/art/tecnologie/2012-09-03/anonymous-attacca-sito-interpol-101808.s
[ENG] http://rt.com/news/anonymous-interpol-free-assange-607/

ANONYMOUS RUBA UN MILIONE DI ID APPLE DAL SITO DELL' FBI
http://www.corriere.it/scienze_e_tecnologie/12_settembre_04/hackers-mettono-online-un-milione

FBI HACK YIELDED 12 MILLION IPHONE AND IPAD IDS, ANONYMOUS CLAIMS
http://www.zdnet.com/fbi-hack-yielded-12-million-iphone-and-ipad-ids-anonymous-claims-7000003
http://mashable.com/2012/09/04/hackers-apple-device-id/
http://www.theregister.co.uk/2012/09/04/antisec_hackers_fbi_laptop_hack/

PHILIPS HACKED, PLAINTEXT PASSWORDS REVEALED AS R00TBEER GANG STRIKES AGAIN
http://nakedsecurity.sophos.com/2012/08/21/r00tbeer-returns-philips-hacked-poor-passwords/

RESEARCHERS SHOW HOW TO CRACK ANDROID ENCRYPTION
http://www.forensicfocus.com/News/article/sid=1921/

GAUSS MALWARE BELIEVED TO BE RELATED TO FLAME
http://www.informationweek.com/security/attacks/flame-20-gauss-malware-targets-banking-c/2400
http://www.wired.com/threatlevel/2012/08/gauss-espionage-tool/
http://blogs.computerworld.com/security/20816/gauss-malware-nation-state-cyber-espionage-bank
http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution

GAUSS RESEARCHERS COLLIDE
http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240006095/gau

HACKER GOING TO DEMONSTRATE OPEN SOURCE TOOL TO CRACK HASHES WITH SPEED OF 154 BILLION/SEC
http://thehackernews.com/2012/07/hacker-going-to-demonstrate-open-source.html

APPEALS COURT OKS WARRANTLESS PHONE GPS TRACKING
http://www.policeone.com/police-products/police-technology/gps/articles/5916070-Appeals-court

AUSTRALIA'S PRIVACY COMMISSIONER TELLS GOOGLE TO DESTROY STREETVIEW PAYLOAD DATA
http://www.theregister.co.uk/2012/08/08/google_must_destroy_data/

HAS HACKING TEAM'S GOVERNMENT TROJAN BEEN USED AGAINST JOURNALISTS?
https://www.privacyinternational.org/blog/has-hacking-teams-government-trojan-been-used-again

THIS IS NOT SURVEILLANCE AS WE KNOW IT: THE ANATOMY OF FACEBOOK MESSAGES
https://www.privacyinternational.org/blog/facebook-message-anatomy

FTC AND FACEBOOK REACH SETTLEMENT OVER PRIVACY PRACTICES
http://news.cnet.com/8301-1009_3-57490948-83/ftc-settles-facebook-privacy-complaint-sans-goog
http://www.computerworld.com/s/article/9230171/FTC_gives_final_approval_to_Facebook_privacy_s

RIM DENIES INDIA'S CLAIMS THAT IT HAS ENCRYPTION KEYS FOR ENTERPRISE CUSTOMERS
http://www.v3.co.uk/v3-uk/news/2196348/rim-rebuffs-claims-blackberry-encryption-keys-given-to
http://www.theregister.co.uk/2012/08/02/rim_keys_india/
http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399_1_blackberry-enterprise

DROPBOX CUSTOMER EMAIL BREACH EXPLAINED
http://www.h-online.com/security/news/item/Dropbox-confirms-data-leak-1657230.html
http://www.scmagazine.com/employee-password-reuse-behind-dropbox-spam-outbreak/article/253004

MOBILE DEVICE TROJAN ZITMO NOW TARGETS BLACKBERRY
http://www.scmagazine.com/blackberry-android-users-targeted-by-new-zeus-trojan/article/253940
http://www.theregister.co.uk/2012/08/08/zeus_comes_to_blackberry/

ANDROID TROJAN INFECTS 500,000 DEVICES
http://www.theregister.co.uk/2012/08/20/android_smszombie/

APPLE PHONES ARE AES-TOUGH, SAYS FORENSICS EXPERT
http://www.forensicfocus.com/News/article/sid=1922/

------------------- MAT HONAN EPIC HACKING SAGA -------------------
HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING
http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

AMAZON QUIETLY CLOSES SECURITY HOLE AFTER JOURNALIST'S DEVASTATING HACK
http://www.wired.com/gadgetlab/2012/08/amazon-changes-policy-wont-add-new-credit-cards-to-acc

APPLE CONFIRMS SUSPENSION OF OVER-THE-PHONE PASSWORD RESETS
http://www.wired.com/gadgetlab/2012/08/apple-confirms-it-has-suspended-over-the-phone-appleid
http://arstechnica.com/security/2012/08/apple-freezes-over-the-phone-password-resets-in-respo

AFTER EPIC HACK, APPLE SUSPENDS OVER-THE-PHONE APPLEID PASSWORD RESETS
http://www.wired.com/gadgetlab/2012/08/apple-icloud-password-freeze/?utm_source=Contextly&utm

APPLE ACCOUNT HACK RAISES CONCERN ABOUT CLOUD STORAGE
http://edition.cnn.com/2012/08/06/tech/mobile/icloud-security-hack/index.html?utm_source=feed

MAT HONAN: HOW I RESURRECTED MY DIGITAL LIFE AFTER AN EPIC HACKING
http://www.wired.com/gadgetlab/2012/08/mat-honan-data-recovery/

==========
LEGGI, DOTTRINA, GIURISPRUDENZA
==========
MODIFICHE ALLA NORMATIVA SUL SEGRETO DI STATO
http://www.adnkronos.com/IGN/News/Politica/Servizi-segreti-Senato-approva-la-riforma-e-legge_

GARANTE PRIVACY: COMUNICAZIONE DELLE VIOLAZIONI DI DATI PERSONALI
http://www.garanteprivacy.it/garante/doc.jsp?ID=1915485

GARANTE PRIVACY: LA PRIVACY A SCUOLA
https://www.ansa.it/web/notizie/rubriche/speciali/2012/09/05/Apripista-studenti-Bolzano-Salas
http://www.garanteprivacy.it/garante/document?ID=1922869#1

==========
LINKS
==========

BLOGS & PORTALS
http://www.forensicfocus.com/computer-forensics-blog
http://articles.forensicfocus.com/
http://www.forensicblog.org
http://windowsir.blogspot.com
http://computer-forensics.sans.org/blog

http://computer.forensikblog.de/en/
http://www.forensickb.com
http://www.forensicinnovations.com/blog
http://forensicsfromthesausagefactory.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/
[ITA] http://pierluigiperri.com/
http://www.techandlaw.net/
http://xwaysclips.blogspot.it/ <--- NEW
http://justaskweg.com/ <--- NEW
http://memoryforensics.blogspot.it/ <--- NEW
https://www.privacyinternational.org/ <--- NEW

PODCASTS
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 <--- NEW

TOOLS
http://www.opensourceforensics.org/
http://www.cftt.nist.gov/
http://computercrimeinfo.com/info.html
http://www.mikesforensictools.co.uk/software.html
http://regripper.wordpress.com/
http://code.google.com/p/regripperplugins/
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

==========
TOOLS
==========

MFT2CSV - MFT DECODER, NTFS FILE EXTRACTER & CMDLINE FILEINFO DUMPER
http://code.google.com/p/mft2csv/wiki/SetRegTime

PESECTIONEXTRACTOR – EXTRACTING PE SECTIONS AND THEIR STRINGS
http://www.hexacorn.com/blog/2012/09/02/pesectionextractor-extracting-pe-sections-and-their-s

VOLATILITY 2.1
https://code.google.com/p/volatility/

BUSTER SANDBOX ANALYZER
http://bsa.isoftware.nl/

REGISTRY DECODER 1.4
http://dfsforensics.blogspot.it/2012/08/registry-decoder-14-released-and.html

MINIMAL IR LIVE CD
http://fdtk.com.br/www/ferramentas/

TCPFLOW 1.3.0
https://github.com/simsong/tcpflow/downloads

SANTOKU - LINUX DISTRO FOR MOBILE SECURITY, MALWARE ANALYSIS, AND FORENSICS

https://santoku-linux.com/
http://articles.forensicfocus.com/2012/08/28/new-linux-distro/

==========
PAPERS
==========

CHASING APT
http://www.secureworks.com/research/threats/chasing_apt/
http://krebsonsecurity.com/2012/07/tagging-and-tracking-espionage-botnets/

DETECTING DATA THEFT USING STOCHASTIC FORENSICS
https://media.blackhat.com/bh-us-12/Briefings/Grier/BH_US_12_Grier_Catching_Insider_Data_Thef

INTO THE DROID – GAINING ACCESS TO ANDROID USER DATA
https://viaforensics.com/mobile-security-category/droid-gaining-access-android-user-data.html

20 CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE
http://www.sans.org/critical-security-controls/winter-2012-poster.pdf

WINDOWS 8 FORENSICS, TIMELINE ANALYSIS, ETC
http://windowsir.blogspot.it/2012/09/links-tools-etc.html

AUTOMATED PLIST PARSER
http://az4n6.blogspot.it/2012/08/automated-plist-parser.html

EXFILTRATION FORENSICS IN THE AGE OF THE CLOUD
http://computer-forensics.sans.org/summit-archives/2012/exfiltration-forensics-in-the-age-of-
http://forensicaliente.blogspot.it/2012/07/sans-dfir-summit-2012-thoughts-links.html

CLOUD BASED FORENSICS ARTIFACTS
http://forensicartifacts.com/tag/cloud-forensics/

DROPBOX FORENSICS FOLLOW-UP
http://forensicaliente.blogspot.it/2011/07/dropbox-forensics-follow-up.html

TRACKING USB FIRST INSERTION IN EVENT LOGS
http://www.swiftforensics.com/2012/08/tracking-usb-first-insertion-in-event.html

WILL DIGITAL FORENSICS CRACK SSD'S?
http://articles.forensicfocus.com/2012/08/24/will-digital-forensics-crack-ssds/

MAKING THE MOST OF GPS EVIDENCE
http://articles.forensicfocus.com/2012/08/27/computer-analysts-and-experts-making-the-most-of

[ITA] NORMAZIONE TECNICA VOLONTARIA: LE REGOLE DEL GIOCO
http://www.uni.com/index.php?option=com_content&view=article&id=1555%3Aun-libro-per-lestate-l

==========
FORMAZIONE
==========

SEMINARIO IISFA
Settembre 21, sala conferenze della società Eur Spa - Roma
Ore 14.30 – 16.30
Eugenio Albamonte – Sostituto Procuratore presso la Procura della Repubblica di Roma – Pool r
"Rapporti tra Pubblico Ministero e consulente tecnico negli accertamenti aventi ad oggetto su
Ore 16.30-18.30
Sergio Civino – Computer Forensics Expert
Accertamenti Tecnici su Dispositivi "Mobile"

TECH AND LAW CENTER - LECTURE WITH SUSAN LANDAU ON "SURVEILLANCE OR SECURITY?"
Settembre, 24, Politecnico di Milano
Ore 14:00 - 17:00
http://www.techandlaw.net/event/interview-with-prof-susan-landau/
http://www.techandlaw.net/2012/08/24/september-24-surveillance-or-security/

Interview http://www.techandlaw.net/resources/interviews/

FIRST POLICY WORKSHOP: SURVEILLING SURVEILLANCE
Settembre 25-26, Firenze
http://www.ittig.cnr.it/smart2012/

SANS PRAGUE FORENSICS
Ottobre 7-13, 2012 - Prague, Czech Republic
http://www.sans.org/prague-forensics-2012/

SANS LONDON 2012
26 November - 3 December - London, UK
https://www.sans.org/event/london-2012

==========
CONFERENCES & CFP
==========

SECURITY SUMMIT
Ottobre 4, Verona
https://www.securitysummit.it

2012 SLEUTH KIT AND OPEN SOURCE DIGITAL FORENSICS CONFERENCE
October 3, 2012 - Chantilly, VA, USA
CfP Deadline: April 16, 2012
http://www.basistech.com/about-us/events/open-source-forensics-conference/

IWCCF 2012 - FIRST INTERNATIONAL WORKSHOP ON CLOUD COMPUTING FOR FORENSICS USE
October 3-5, 2012, St. Petersburg, Russia
http://www.icumt.org/2012/images/stories/PDF/iwccf.pdf

RSA CONFERENCE EUROPE 2012
October 9-11, London
www.rsaconference.com/events/2012/europe

ICDF2C - 4th International Conference on Digital Forensics & Cyber Crime
October 24-26, 2012 - Lafayette, Indiana, USA
http://d-forensics.org/2012/show/home

2012 EUROPEAN SCADA SUMMIT
Pre-Summit Course: 5-9 December, 2012
Summit: 10-11 December, 2012
Barcelona, Spain
http://www.sans.org/info/112039

==========
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 c
==========