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

Newsletter 34 - Marzo/Aprile 2014

\\\

Indice:

****

DFA OPEN DAY 2014 – 5 giugno 2014 – Milano
Argomenti: "OSINT e Investigazioni Digitali" e "Security e Incident Response aziendale"
Ingresso gratuito.
http://dfaopenday2014.eventbrite.it/

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

IO NON CRAKKO LE PASSWORD! LE SO: RILASCIATO MIMIKATZ OFFLINE
http://mattiaep.blogspot.it/2014/03/io-non-crakko-le-password-le-so.html

CORTE UE RIDIMENSIONA IL CONTROLLO DEI DATI TELEMATICI, MA SI RISCHIA UN VUOTO NORMATIVO
http://www.wired.it/internet/regole/2014/04/08/ue-corte-di-giustizia-data-retention-dati-personali-privacy/

iCLOUD: PANORAMICA SULLA SICUREZZA E SULLA PRIVACY IN iCLOUD
http://support.apple.com/kb/HT4865?viewlocale=it_IT&locale=it_IT

DERUBATO DEL COMPUTER ATTIVA LA WEBCAM E METTE ONLINE LE FOTO DEL LADRO.
http://www.ilmessaggero.it/primopiano/esteri/pablo_mac_computer_rubato_turista_usa/notizie/563984.shtml

FOTO A VENEZIA CON IPAD RUBATO, SCOPERTO
http://www.ansa.it/lombardia/notizie/2014/04/22/foto-a-venezia-con-ipad-rubato-scoperto_8f61503f-c61c-42f6-

RAPPORTO CLUSIT 2014 DISPONIBILE
http://clusit.it/rapportoclusit/

MULTA A GOOGLE PER STREET VIEW
http://www.lastampa.it/2014/04/03/tecnologia/multa-a-google-per-street-view-8wvap7SgfQ4IXVVoIiQfEN/pagina.h
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2954309

IL MALWARE CRYPTODEFENSE CIFRA I DATI DIMENTICANDO LA CHIAVE SUL PC
http://attivissimo.blogspot.it/2014/04/cryptodefense-cifra-i-dati-delle-sue.html

CRYPTODEFENSE, THE CRYPTOLOCKER IMITATOR, MAKES OVER $34,000 IN ONE MONTH
http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month

HIDDEN "SIGNATURE" IN ONLINE PHOTOS COULD HELP NAB CHILD ABUSERS
http://www.scientificamerican.com/article/hidden-signature-in-online-photos-could-help-nab-child-abusers/

40 MILLION STOLEN CREDIT CARD NUMBERS: HOW THE TARGET BREACH HAPPENED
http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

EU LEGISLATORS APPROVE NEW CYBERSECURITY LAW
http://www.networkworld.com/news/2014/031314-new-eu-cybersecurity-law-avoids-279681.html

EU DATA RETENTION DIRECTIVE RULED INVALID
http://www.bbc.com/news/world-europe-26935096
http://www.irishtimes.com/business/sectors/technology/european-court-declares-data-retention-directive-inva

NSA'S PLANS REPORTEDLY INVOLVE INFECTING MILLIONS OF COMPUTERS WITH SURVEILLANCE MALWARE

http://www.networkworld.com/news/2014/031214-nsa39s-plans-reportedly-involve-infecting-279666.html?source=N

NSA INFILTRATED HUAWEI NETWORKS, INSTALLED BACKDOORS
http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0
http://www.zdnet.com/nsa-spies-on-china-networking-giant-huawei-7000027599/

WHITE HOUSE CALLS ON LAWMAKERS TO END NSA BULK METADATA COLLECTION
http://www.washingtonpost.com/world/national-security/white-house-pushes-congress-to-quickly-pass-changes-t
http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?hp&_r=0
http://arstechnica.com/tech-policy/2014/03/white-house-to-propose-law-to-end-nsa-bulk-collection-of-phone-c

CRIMINAL GROUP OF ONLINE FRAUDSTER DISMANTLED
https://www.europol.europa.eu/content/criminal-group-online-fraudsters-dismantled

EU COURT OF JUSTICE RULES AGAINST DATA RETENTION DIRECTIVE
http://www.siliconrepublic.com/enterprise/item/36422-eu-court-of-justice-rules/
[ITA] http://www.wired.it/attualita/politica/2014/04/08/data-retention-corte-di-giustizia/

RUSSIA vs ITALY OVER COPYRIGHT VIOLATIONS
http://www.techandlaw.net/news/russia-v-italy-copyright-violations.html

NIST REMOVES CRYPTOGRAPHY ALGORITHM FROM RANDOM NUMBER GENERATOR RECOMMENDATIONS
http://www.nist.gov/itl/csd/sp800-90-042114.cfm

NEW ANDROID BITCOIN MINING MALWARE FOUND ON GOOGLE PLAY
http://www.esecurityplanet.com/mobile-security/new-android-bitcoin-mining-malware-found-on-google-play.html

MASSIVE COLLECTION OF LEAKED PASSWORDS
http://www.cyberwarzone.com/free-leaked-password-files

DEMYSTIFYING POINT OF SALE MALWARE AND ATTACKS
http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks

ANDROID BOTNET TARGETS MIDDLE EAST BANKS
http://krebsonsecurity.com/2014/04/android-botnet-targets-middle-east-banks/

BITCOIN MINING MALWARE FOUND ON SURVEILLANCE CAMERA DVRS
http://threatpost.com/dvr-infected-with-bitcoin-mining-malware/105167

POLICE HID USE OF CELL PHONE TRACKING DEVICE FROM JUDGE BECAUSE OF NDA
http://arstechnica.com/tech-policy/2014/03/police-hid-use-of-cell-phone-tracking-device-from-judge-because-

EDWARD SNOWDEN SPEAKS AT SOUTH BY SOUTHWEST CONFERENCE
http://www.washingtonpost.com/world/national-security/snowden-mass-surveillance-is-backfiring-on-us-in-effo
http://www.wired.com/threatlevel/2014/03/edward-snowdens-tech-call-arms/
http://www.darkreading.com/vulnerability/snowden-encryption-is-defense-against-th/240166547

THE IMPORTANCE OF FORENSIC TOOLS VALIDATION
http://www.zdziarski.com/blog/?p=3112

THE IMPORTANCE OF COMMAND AND CONTROL ANALYSIS FOR INCIDENT RESPONSE
http://digital-forensics.sans.org/blog/2014/03/31/the-importance-of-command-and-control-analysis-for-incide

REX VS THE ROMANS - ANTI HACKING TEAM KERNEL EXTENSION
http://reverse.put.as/2014/04/08/rex-vs-the-romans-anti-hacking-team-kernel-extension/

MALWARE STEALS APPLE ID CREDENTIALS FROM JAILBROKEN IOS DEVICES
http://arstechnica.com/security/2014/04/active-malware-campaign-steals-apple-passwords-from-jailbroken-ipho

-------------------------------- THE HEARTBLEED SAGA --------------------------------
HEARTBLEED VULNERABILITY IN OPENSSL CRYPTOGRAPHIC LIBRARY
http://www.theregister.co.uk/2014/04/08/running_openssl_patch_now_to_fix_critical_bug/
http://www.zdnet.com/heartbleed-serious-openssl-zero-day-vulnerability-revealed-7000028166/
http://arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eaves
http://heartbleed.com

CONFIRMED: NASTY HEARTBLEED BUG EXPOSES OPENVPN PRIVATE KEYS, TOO
http://arstechnica.com/security/2014/04/confirmed-nasty-heartbleed-bug-exposes-openvpn-private-keys-too/

NSA DENIES IT KNEW ABOUT HEARTBLEED VULNERABILITY
http://www.scmagazine.com/heartbleed-bug-not-leveraged-for-surveillance-nsa-says/article/342579/

http://www.cnet.com/news/nsa-denies-it-knew-of-exploited-heartbleed-kept-flaw-secret/

LAVABIT CASE SUPPORTS NSA'S ASSERTION THAT THEY DID NOT HAVE HEARTBLEED
http://www.zdnet.com/lavabit-case-undermines-claims-nsa-had-heartbleed-early-7000028517/

RESEARCHERS SAY HEARTBLEED NOT EXPLOITED BEFORE DISCLOSURE
http://bits.blogs.nytimes.com/2014/04/16/study-finds-no-evidence-of-heartbleed-attacks-before-the-bug-was-e

OPENSSL HEARTBLEED: BLOODY NOSE FOR OPEN-SOURCE BLEEDING HEARTS
http://www.theregister.co.uk/2014/04/11/openssl_heartbleed_robin_seggelmann/

TECH GIANTS, CHASTENED BY HEARTBLEED, FINALLY AGREE TO FUND OPENSSL
http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-

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

TRASMETTERE I FILE AZIENDALI ALL'AVVOCATO: NON GIUSTIFICA IL LICENZIAMENTO
http://www.laleggepertutti.it/47897_trasmettere-i-file-aziendali-allavvocato-non-giustifica-il-licenziament

Cassazione: per un post non si può oscurare un blog
http://247.libero.it/rfocus/20017946/1/cassazione-per-un-post-non-si-pu-oscurare-un-blog-udine-20/

Cassazione: è diffamazione parlar male su Facebook anche senza fare nomi
http://www.repubblica.it/cronaca/2014/04/16/news/cassazione_diffamazione_su_facebook_anche_senza_fare_nomi-

Crimini informatici: identità personale VS identità digitale
http://www.altalex.com/index.php?idnot=66989

Regole tecniche: protocollo e conservazione digitale
http://www.agid.gov.it/notizie/protocollo-conservazione-digitale-gazzetta-le-nuove-regole-tecniche

Dlgs 21/2014 - Contratti a distanza e Codice del consumo
http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=66790
http://www.filodiritto.com/contratti-tra-consumatori-e-professionisti-litalia-recepisce-la-direttiva-europe

Regolamento Agcom diritto d'autore online
http://www.marchiebrevettiweb.it/29-diritto-di-autore/2397-entra-in-vigore-oggi-il-regolamento-per-la-tutel
https://www.ddaonline.it

Direttiva UE Network and Information Security (NIS)
http://www.networkworld.com/news/2014/031314-new-eu-cybersecurity-law-avoids-279681.html

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

2014 DATA BREACH INVESTIGATIONS REPORT
http://www.verizonenterprise.com/DBIR/2014/insider/

REVERSE ENGINEERING FOR BEGINNER
http://yurichev.com/writings/RE_for_beginners-en.pdf

RUSSIAN UNDERGROUND ECONOMY REVISITED
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-r

PE INJECTION EXPLAINED
http://packetstorm.interhost.co.il/papers/general/PE_Injection_Explained.pdf

DLL SIDE-LOADING: A THORN IN THE SIDE OF THE ANTI-VIRUS INDUSTRY
http://www.fireeye.com/resources/pdfs/fireeye-dll-sideloading.pdf?utm_content=buffere220a&utm_medium=social

JTAG GALAXY SIII
http://forensicfocus.files.wordpress.com/2014/03/jtag-galaxy_siii_4_31.pdf

KINDLE PAPERWHITE EXPLORATORY FORENSICS

https://www.dropbox.com/s/weoar0khn1kz10z/ForensicsPaperFinalDraft.pdf

A FORENSIC EXAMINER'S GUIDE TO GOOGLE GLASS
http://desautelsja.blogspot.it/2014/04/a-forensic-examiners-guide-to-google.html

[ITA] LE FRODI NELLA RETE
http://frodi.clusit.it/_files/le_frodi_nella_rete.pdf

WINDOWS 8 FORENSIC GUIDE
http://propellerheadforensics.files.wordpress.com/2012/05/thomson_windows-8-forensic-guide2.pdf

[ITA] CLOUD FORENSICS
http://mattiaep.blogspot.it/2014/04/pubblicata-la-mia-presentazione-su.html

MIMIKATZ OFFLINE - DUMPING PASSWORD IN WINDOWS HIBERNATION FILE
http://blog.digital-forensics.it/2014/03/et-voila-le-mimikatz-offline.html
http://blog.digital-forensics.it/2014/03/mimikatz-offline-addendum_28.html

OSX 10.9 MEMORY ACQUISITION
http://rekall-forensic.blogspot.de/2014/03/osx-109-memory-acquisition.html

TOOLS FOR ANALYZING STATIC PROPERTIES OF SUSPICIOUS FILES ON WINDOWS
http://digital-forensics.sans.org/blog/2014/03/04/tools-for-analyzing-static-properties-of-suspicious-files

APT ATTRIBUTIONS AND DNS PROFILING
http://espionageware.blogspot.hk/2014/04/apt-attributions-and-dns-profiling.html

SIGNATURE DETECTION WITH CROWDRESPONSE
http://digital-forensics.sans.org/blog/2014/04/09/signature-detection-with-crowdresponse#

NEOPOCKET: A NEW ATM MALWARE
http://securityblog.s21sec.com/2014/04/neopocket-new-atm-malware.html?utm_source=twitterfeed&utm_medium=twi

MO' SHELLS MO' PROBLEMS: WEB SERVER LOG ANALYSIS
http://forensicmethods.com/webshell-log-analysis

THUNDERBIRD PARSER
http://az4n6.blogspot.it/2014/04/whats-word-thunderbird-parser-that-is.html

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

MIMIKATZ OFFLINE
https://googledrive.com/host/0B73hZlpVAfuzN3hYVUNXVi1OV1k/

ELCOMSOFT FORENSIC DISK DECRYPTOR
http://www.elcomsoft.com/efdd.html

W3AF - WEB APPLICATION ATTACK AND AUDIT FRAMEWORK
http://w3af.org/

DEFT 8.1
http://www.deftlinux.net/download/

DEFT 8.1 Virtual appliance
http://www.deftlinux.net/2014/04/24/deft-8-1-virtual-appliance-ready-for-download/

PEFRAME - STATIC MALWARE ANALYSIS
https://github.com/guelfoweb/peframe

RAGPICKER MALWARE CRAWLER
https://code.google.com/p/malware-crawler/

MANTARAY 1.3
http://mantarayforensics.com/
https://github.com/mantarayforensics/mantaray
https://launchpad.net/~mantaray/+archive/stable

FACEBOOK CHAT EXTRACTOR V1.2
http://www.gaetanoconsalvo.it/facebook%20chat%20extractor.html

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

SANS ICS/SCADA SECURITY ESSENTIALS
12-16 May, 2014
London, United Kindom
http://www.sans.org/event/ics-london-2014?utm_source=e-mail&utm_medium=invite&utm_content=20140218_EMEA_ICS

SANS HACKER TECHNIQUES, EXPLOITS & INCIDENT HANDLING
16-21 June, 2014
Milan, Italy
http://www.sans.org/event/sans-milan-2014

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

DFA OPEN DAY 2014
5 June, 2014
Milano, Italy
Argomenti: “OSINT e Investigazioni Digitali” e “Security e Incident Response aziendale”
Ingresso gratuito.
http://www.perfezionisti.it/proposte-formative/dfa-open-day-2014/
http://dfaopenday2014.eventbrite.it/

SANS "HACKER TECHNIQUES, EXPLOITS & INCIDENT HANDLING"
16-21 June, 2014
Milano, Italy
http://www.sans.org/event/sans-milan-2014
NOTA: per codice sconto 10% scrivere a pasquale.stirparo@sefirtech.com o mattia.epifani@realitynet.it

ICDF2C - 6TH INTERNATIONAL CONFERENCE ON DIGITAL FORENSICS & CYBER CRIME
September 18-20, 2014
New Haven, Connecticut, USA
http://d-forensics.org/2014/show/home

CLOUD SECURITY ALLIANCE EMEA CONGRESS 2014
19 - 20 November, 2014
Parco dei Principi Grand Hotel & Spa, Rome

==========
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://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/

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.siig.it/
[ITA] http://pierluigiperri.com/
[ITA] http://blog.cesaregallotti.it
[ITA] http://mattiaep.blogspot.it <--- NEW

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.

==========