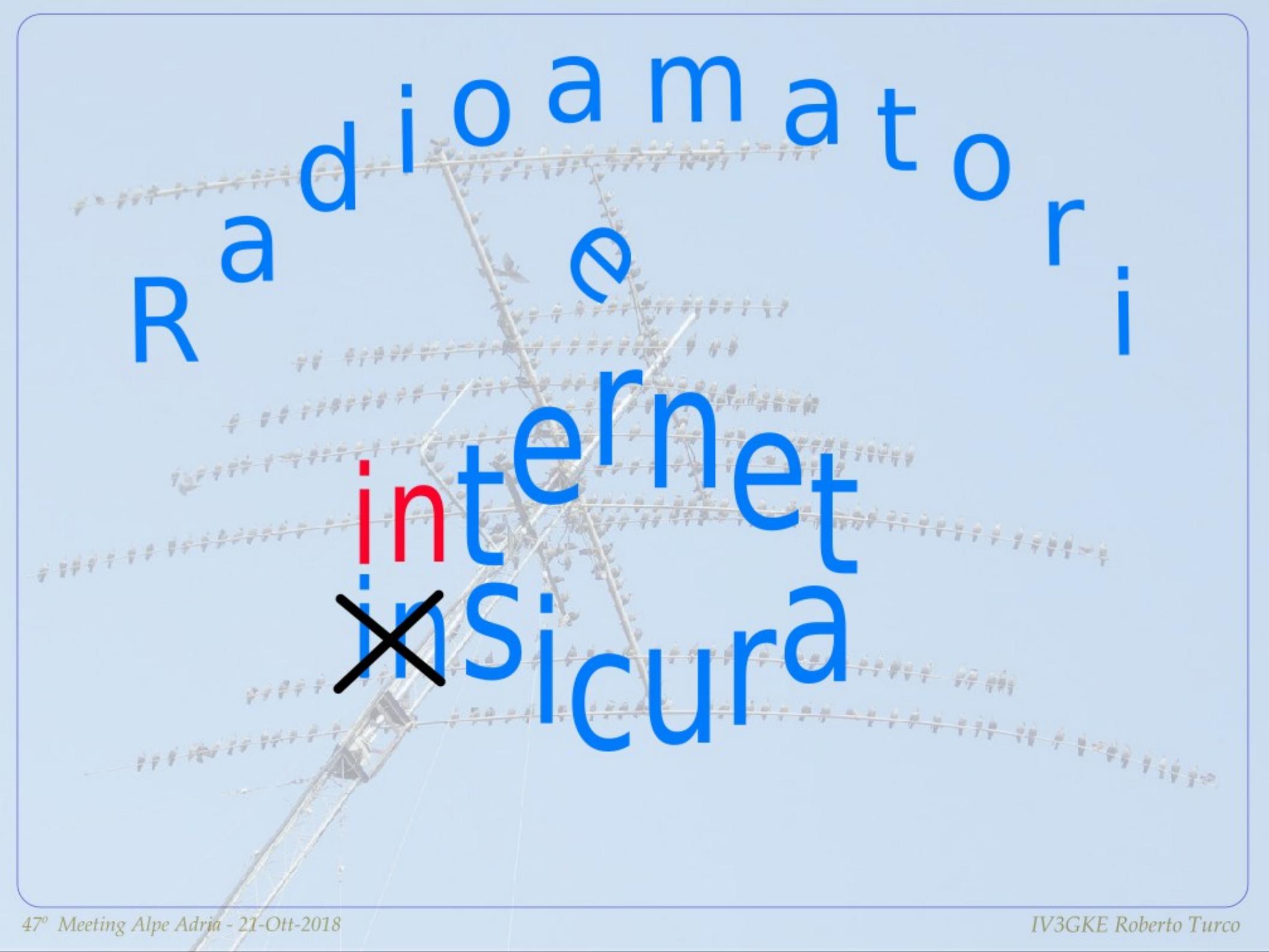

Radioamatori
e
internet
insicura

# DEFINIZIONI

*Sicurezza:*

TRECCANI

**La condizione che rende e fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli, e simili.**

# DEFINIZIONI

## *Sicurezza:*

La condizione che rende → *quindi possiamo agire*

e fa sentire → *implica soggetività*

di essere esente da pericoli, → *riconoscimento dei pericoli*

o che dà la possibilità → *un costo*

di prevenire, eliminare o rendere meno gravi

danni, → *un valore (anche morale)*

rischi, → *probabilità* $x$ *gravità*

diffi coltà, evenienze spiacevoli, e simili.

# Il rischio è un concetto probabilistico

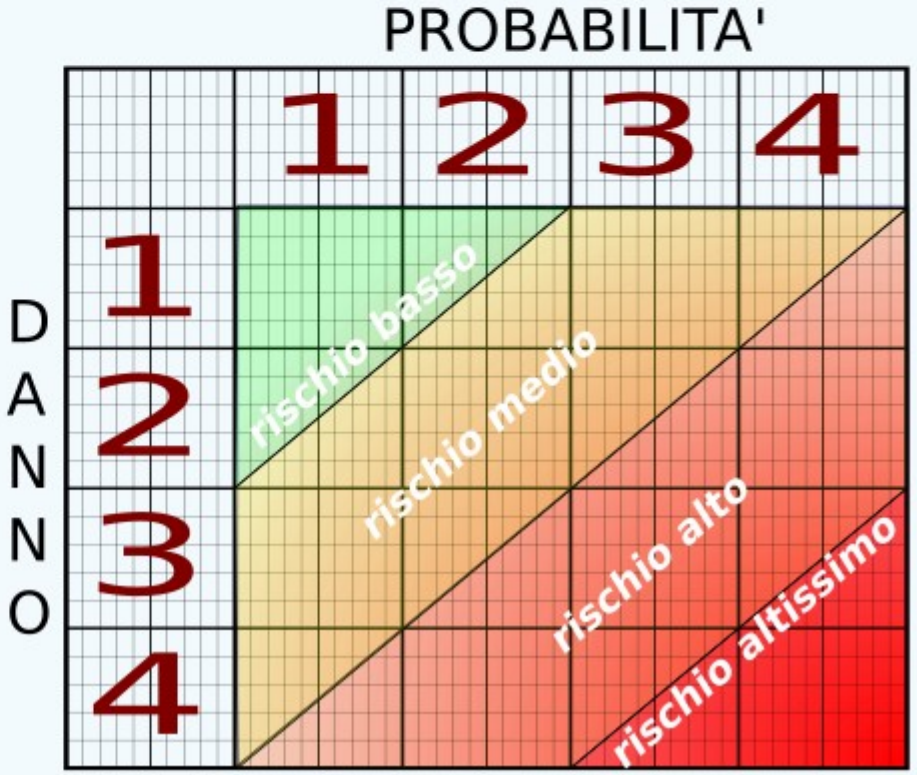
è la probabilità che accada un certo
evento capace di causare un danno.

La nozione di rischio implica l'esistenza di:

una sorgente di pericolo

e

delle possibilità che essa
si trasformi in un danno.



# Ma... se non conosciamo i pericoli come possiamo valutare i rischi?

Atteggiamenti che aumentano le probabilità

e quindi i rischi

*indifferenza:*

"Nel mio dispositivo non ce niente che possa interessare

agli hackers, e comunque ho copia di tutto"

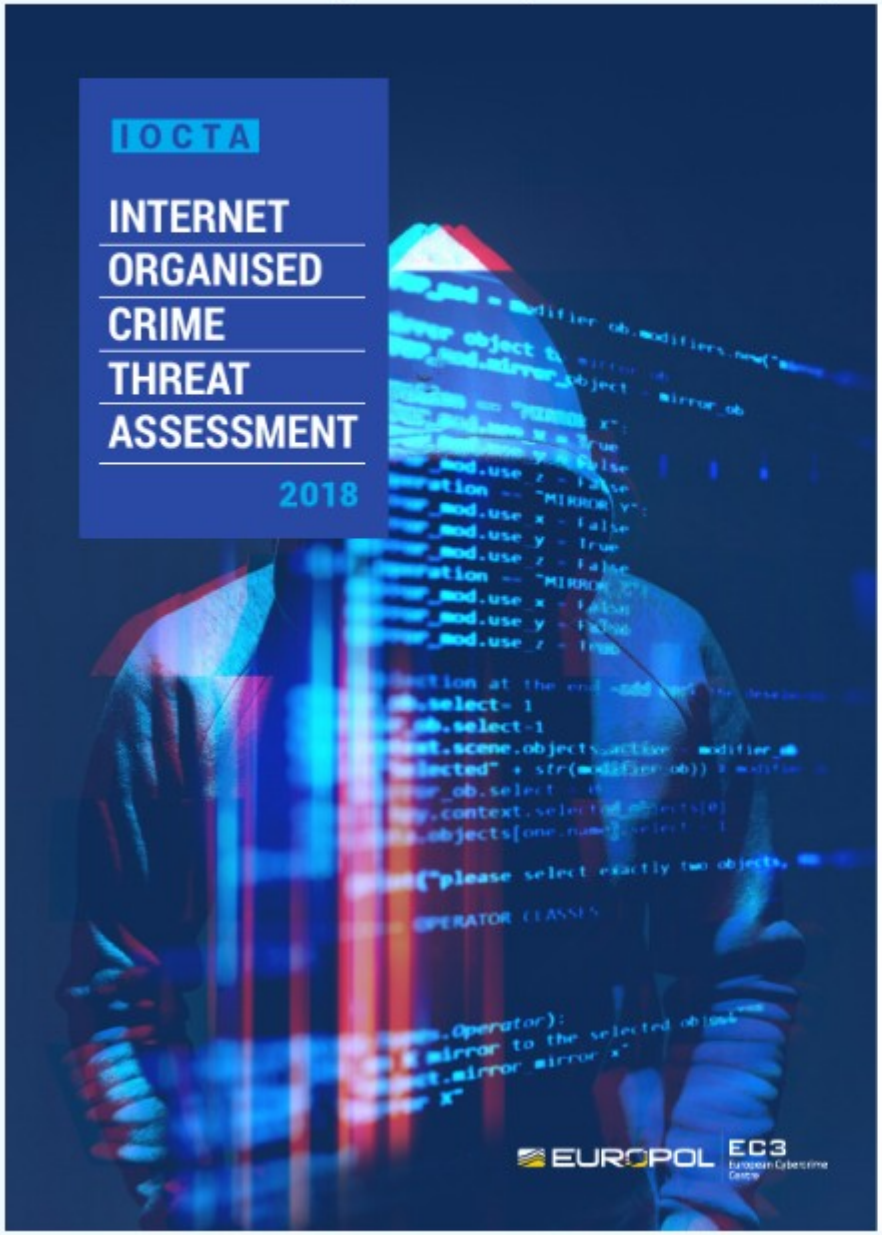
*diniego:*

1) se non lo riconosco non succede

2) non ho nulla da perdere


*www.commissariatodips.it/approfondimenti/mobile-malware-awareness-campaign.html*

# www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf




## contents


https://exploit.kitploit.com/


https://threatpost.com/threatlist-83-of-routers-contain-vulnerable-code/137966/


Now Law Enforcement Agencies Can Possibly Breakthrough into any iPhone Model...

WinstarNssmMiner – A Brutal Computer Crypto-Hijacker Attack Victims over 500,000 Times...

Hackers Launching GandCrab Ransomware via New Fallout Exploit Kit using Malvertising...

86 Vulnerabilities Fixed with Adobe Security Updates for Adobe Acrobat and...

New Bluetooth Vulnerability Affected Millions of Devices that Allow Hackers to...

https://gbhackers.com/

# Vending Machine App Hacked for Unlimited Credit

By Ionut Ilascu

October 16, 2018 05:55 PM 0


A hacker enticed by the payment method used by the vending machines located on a university campus found a way to get free credit after looking at the inner workings of the machine's accompanying mobile app.

The vending machines are from Argenta, a popular provider of coffee services in Italy, now acquired by the Selecta Group B.V.. The machines are used all over the country for automated sales of all sorts of products, from refreshing drinks to cigarettes.

*www.bleepingcomputer.com/news/security/vending-machine-app-hacked-for-unlimited-credit/*
*https://hackernoon.com/how-i-hacked-modern-vending-machines-43f4ae8decec*

**JQuery CVE-2015-9251 Cross Site Scripting Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/105658

**Apache Batik CVE-2018-8013 Information Disclosure Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/104252

**Pivotal Spring Framework CVE-2018-1275 Incomplete Fix Remote Code Execution Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/103771

**Microsoft SQL Server Management Studio CVE-2018-8527 Information Disclosure Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/105474

**Microsoft SQL Server Management Studio CVE-2018-8533 Information Disclosure Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/105476

**Microsoft SQL Server Management Studio CVE-2018-8532 Information Disclosure Vulnerability**
2018-10-18
http://www.securityfocus.com/bid/105475

**Apache Log4j CVE-2017-5645 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/97702

**OpenSSL CVE-2018-0739 Denial of Service Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/103518

**FasterXML Jackson-databind CVE-2017-15095 Incomplete Fix Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/103880

**FasterXML Jackson-databind CVE-2018-7489 Incomplete Fix Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/103203

**Multiple CPU Hardware CVE-2017-5715 Information Disclosure Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/102376

**Novell NetIQ Sentinel CVE-2016-1000031 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/93604

**Apache Tomcat CVE-2018-1305 Security Bypass Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/103144

**Multiple RedHat JBoss Products CVE-2015-7501 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/78215

**Apache Tomcat CVE-2018-8014 Security Bypass Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/104203

**Apache Struts CVE-2018-11776 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/105125

**Apache Struts CVE-2018-11776 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/105125

**Spring Security and Spring Framework CVE-2018-1258 Authorization Bypass Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/104222

**RESTEasy Incomplete Fix XML Entity References Information Disclosure Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/69058

**OpenSSL Padding Oracle Incomplete Fix Information Disclosure Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/89760

**Apache MyFaces Trinidad CVE-2016-5019 Remote Code Execution Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/93236

**Objective Systems ASN1C CVE-2016-5080 Heap Based Buffer Overflow Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/91836

**Multiple Oracle Products CVE-2016-0635 Remote Security Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/91869

**Apache Xerces-C CVE-2016-0729 Buffer Overflow Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/83423

**GNU glibc CVE-2015-0235 Remote Heap Buffer Overflow Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/72325

**Apache HTTP Server CVE-2017-9798 Information Disclosure Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/100872

**Oracle PeopleSoft Enterprise PeopleTools Multiple Remote Security Vulnerabilities**
2018-10-17
http://www.securityfocus.com/bid/105609

**Oracle PeopleSoft Enterprise PeopleTools Multiple Remote Security Vulnerabilities**
2018-10-17
http://www.securityfocus.com/bid/105598

**Oracle Java SE/Java SE Embedded CVE-2018-3211 Local Security Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/105591

**Cisco Wireless LAN Controller Software CVE-2018-0388 Cross Site Scripting Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/105665

**Cisco Wireless LAN Controller Software CVE-2018-0442 Information Disclosure Vulnerability**
2018-10-17
http://www.securityfocus.com/bid/105664

Vulnerabilities (Page 1 of 3289)

*https://www.securityfocus.com/vulnerabilities*

# Internet delle cose

"Gartner, Inc. forecasts that 20.4 billion connected devices will be in use worldwide by 2020.
Total spending of $2 trillion on endpoints and services is estimated by the end of 2017.
The Internet of Things (IoT) has a potential economic impact of up to $11.1 trillion a year by 2025."

*https://www.cioreview.com/news/why-invest-in-the-internet-of-things-nid-25255-cid-133.html*

- IoT Hacks
  - Thingbots
  - RFID
  - Home Automation
  - Connected Doorbell
  - Hub
  - Smart Coffee
  - Wearable
  - Smart Plug
  - Cameras
  - Traffic Lights
  - Automobiles
  - Airplanes
  - Light Bulbs
  - Locks
  - Smart Scale
  - Smart Meters
  - Pacemaker
  - Thermostats
  - Fridge
  - Media Player & TV
  - Rifle (Weapon)
  - Toilet
  - Toys

*https://github.com/nebgnahz/awesome-iot-hacks*

# L'aspirapolvere che ti spia con il microfono e la telecamera.

Vulnerabilities in a range of robot vacuum cleaners allow miscreants to access the gadgets' camera, and remote-control the gizmos.

Security researchers at Positive Technologies (PT) this week disclosed that Dongguan Diqee 360 smart vacuum cleaners contain security flaws that hackers can exploit to snoop on people through the night-vision camera and mic, and take control of the Roomba rip-off.

Think of it as a handy little spy-on-wheels.

The security issues, discovered by PT's Leonid Krolle and Georgy Zaytsev, likely affect products sold under other brands as well.

The first vulnerability (CVE-2018-10987) involves remote code execution. A hacker can discover the vacuum on the same wireless network by obtaining its MAC address, and then send a UDP request, which, if crafted in a specific way, results in execution of a command with superuser rights on the vacuum. A miscreant must first log onto the device, but this process is trivial because many still have the default username and password combination (admin and 888888).

Attackers need physical access to exploit the second vulnerability (CVE-2018-10988). A microSD card could be used to exploit weaknesses in the vacuum's update mechanism.

*https://www.theregister.co.uk/2018/07/20/iot_insecurity_robo_vacuum_cleaners/*

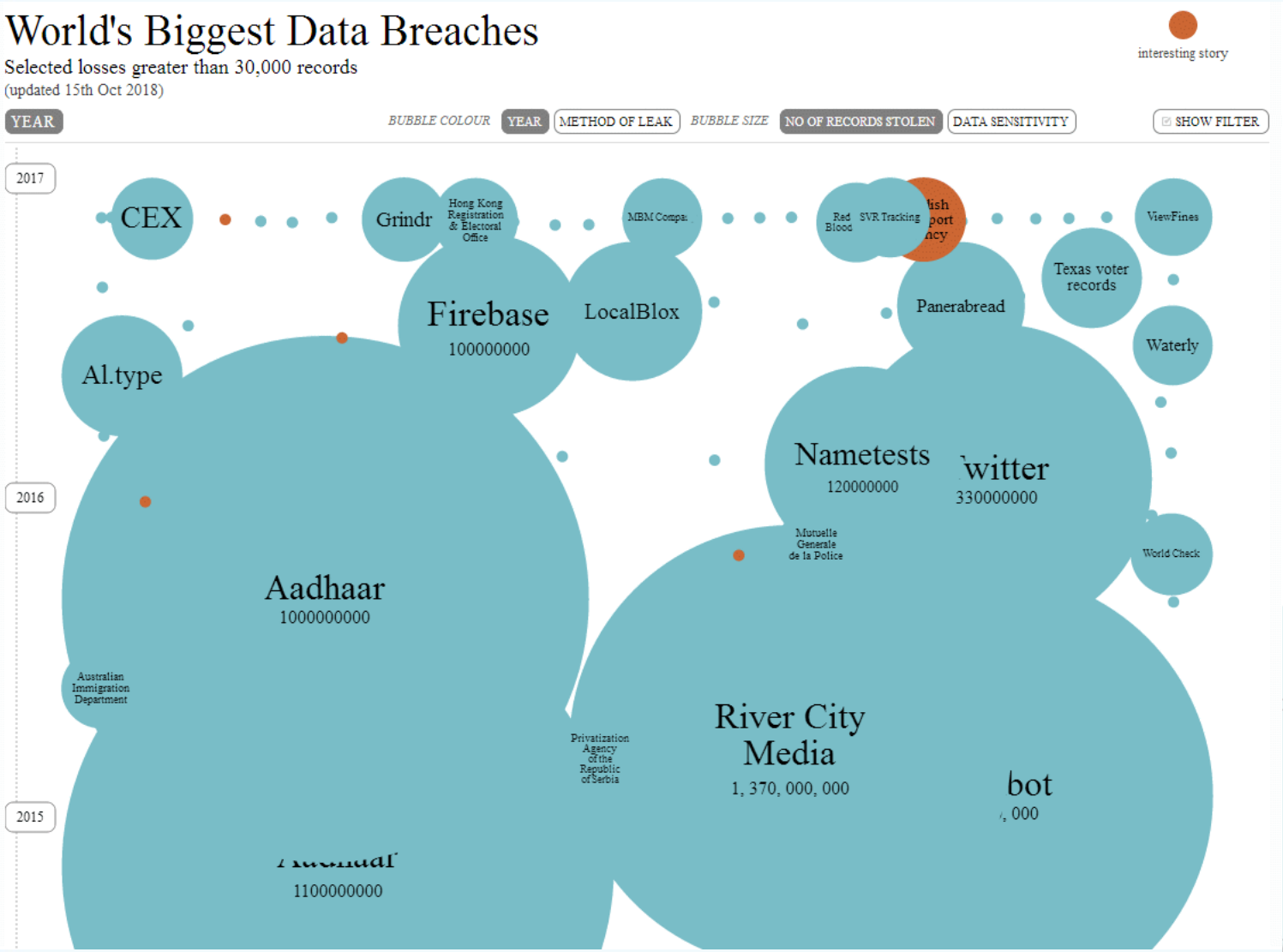
Attualità Redazione Bruxelles
16 ottobre 2018 14:06

# Italia tra i 10 Paesi da cui partono più cyber attacchi

Siamo al nono posto, i primi tre sono Russia, Usa ed Egitto. Otto Stati membri chiedono di mettere il tema sul tavolo del Consiglio europeo di questa settimana: "Serve un regime sanzionatorio"

L'Italia è tra i Paesi del mondo dai cui partono la maggior parte dei cyber attacchi. Il nostro Paese entra nella top ten, piazzandosi al nono posto, della classifica stilata dai laboratori della società di sicurezza Trend Micro, secondo le cui rilevazioni ai primi tre posti si trovano Russia, Stati Uniti ed Egitto. I dati, raccolti dalla Smart Home Network, e le analisi coinvolgono gli indirizzi IP dei router attivi, per determinare la fonte di un evento o possibile attacco. Nel momento in cui un router, che supporta le soluzioni della compagnia e ha abilitato le funzionalità di security, attiva una procedura di sicurezza, i laboratori confermano da quale direzione proviene l'attacco controllando ulteriormente quale origine ha attivato l'evento di sicurezza. In questo modo è possibile capire i Paesi da dove provengono gli attacchi. I dati raccolti ad agosto mostrano che **i cinque Paesi più colpiti da attacchi provenienti dall'Italia sono stati: Stati Uniti, Taiwan, Hong Kong, Regno Unito e Olanda**. Per quanto riguarda invece gli attacchi in generale, che hanno colpito l'Italia sempre ad agosto, Trend Micro ha rilevato 1.229.390 malware e 57.430.080 minacce via mail.

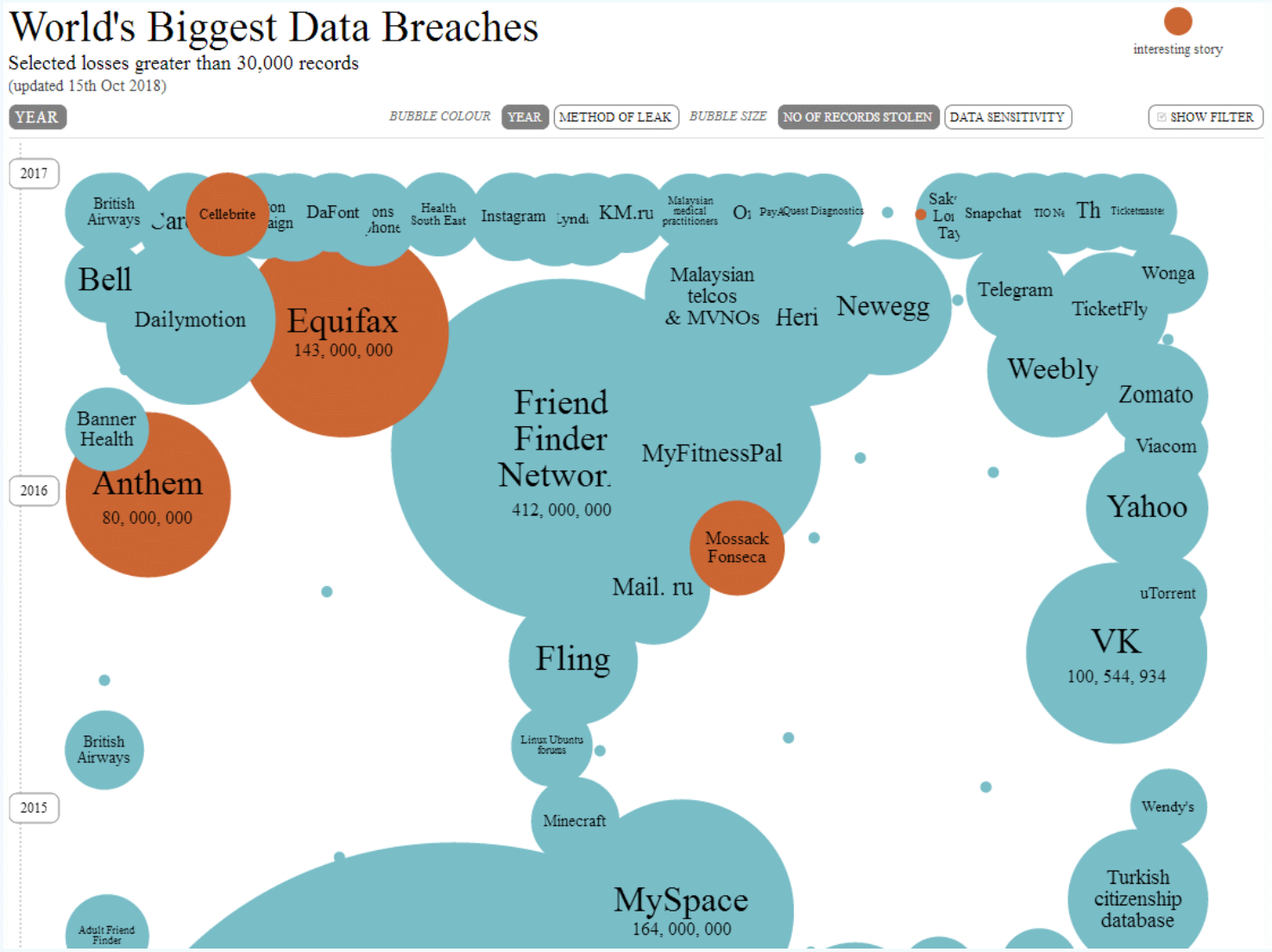
*https://europa.today.it/attualita/cyber-attacchi-italia.html*




**Filter by...**

**ORGANISATIONMETHOD OF LEAK**

| | |
|---|---|
| ☑ all | ○ all |
| ○ academic | ☑ accidentally published |
| ○ app | ○ hacked |
| ○ energy | ☑ inside job |
| ○ financial | ☑ lost / stolen device or media |
| ○ gaming | ☑ poor security |
| ○ government | |
| ○ healthcare | |
| ○ legal | |
| ○ media | |
| ○ military | |
| ○ retail | |
| ○ tech | |
| ○ telecoms | |
| ○ transport | |
| ○ web | |

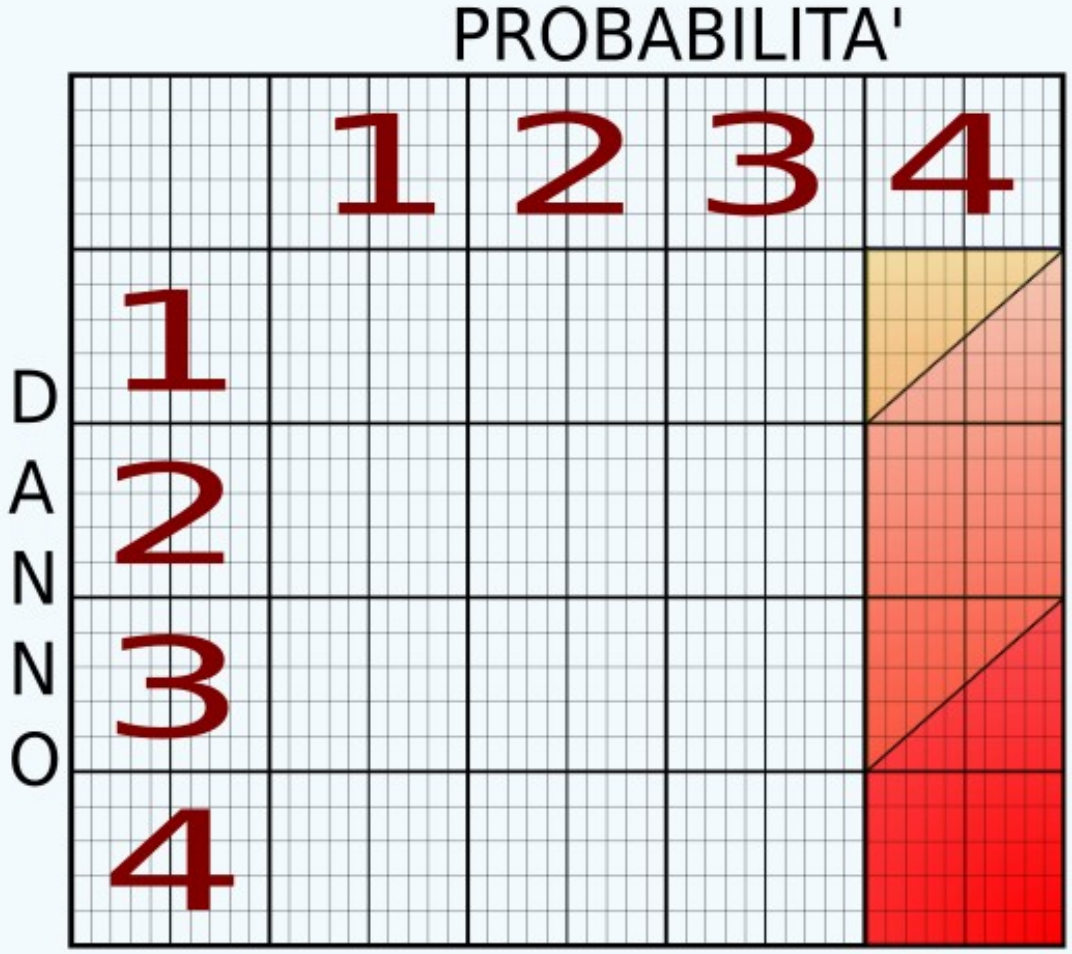



**Filter by...**

**ORGANISATION** **METHOD OF LEAK**

| ORGANISATION | METHOD OF LEAK |
|---|---|
| all | all |
| academic | accidentally published |
| app | hacked |
| energy | inside job |
| financial | lost / stolen device or media |
| gaming | poor security |
| government | |
| healthcare | |
| legal | |
| media | |
| military | |
| retail | |
| tech | |
| telecoms | |
| transport | |
| web | |

Possiamo affermare che siamo a livello 4 di probabilità



# Cosa possono fare gli hackers “black hat”?

## Installare “Malaware” causando:

- **Furto di informazioni dai dispositivi**
- **Perdita dati, perdita configurazioni, blocco sistema operativo,**
- **Blocco uso periferiche, errori casuali, perdita connettività,**
- **Rallentamento dispositivi e rete ed internet, surriscaldamento dispositivi.**
- **Intercettazione dati sensibili**
- **Manomissione risorse a fine richiesta riscatto**
- **Uso dei dispositivi per attacchi verso terzi**
- **Uso dei dispositivi per produzione di cripto valute**
- **Uso dispositivi come server in rete di materiale illecito**
- **Uso dispositivi come proxy e VPN per comunicazioni fraudolente**
- **Furto d'identità**

**ED ALTRO !**

# Come viene inserito il malaware nei nostri dispositivi?

- Via e-mail
- Navigatori Web
- Attraverso “piercing” del firewall
- Attraverso porte e servizi nascosti nel firmaware/software (backdoor)
- Invasione rete WiFi
- Connessione diretta WiFi per falla protocolli
- Connessione bluetooth
- Allacciamento nella nostra rete di dispositivo “lecito” ma compromesso
- Condivisione chiavetta USB infetta
- Installazione di programma lecito ma compromesso

# Come proteggersi?

Come proteggersi?

## E-mail

- Settare il programma mail per NON scaricare immagini e annessi automaticamente
- Evitare di aprire e-mail provenienti da sconosciuti
- Non abboccare alle offerte troppo invitanti
- Non aprire allegati
- Non cliccare sui links

# Come proteggersi?

Come proteggersi?

## Navigatori Internet

- Abilitare  il Java Script solo per siti indispensabili
- Non accettare cookies da terze parti
- Settare il navigatore per cancellare i cookies alla chiusura del programma
- Non lasciare il navigatore eternamente aperto
- Settare il navigatore per NON scaricare annessi automaticamente

# Come proteggersi?

## Installazione di programma lecito ma compromesso

*Come proteggersi?*

- assicurarsi che il software sia integro testando la sua firma digitale
- non installare software di dubbia provenienza
- evitare software pirata
- attenzione a software “sbloccati”

# Come proteggersi?

## Porte e servizi nascosti nel firmaware/software (backdoor)

Come proteggersi?

- Disabilitare servizi non utilizzati
- Chiudere tutte le porte non necessarie
- Disabilitare il Plug&Play
- Abilitare il software di protezione di rete (firewall)
- Affinare il settaggio del firewall
- Disabilitare il protocollo IPV6
- In windows disabilitare il tunnel “teredo”
- Disabilitare ogni altro servizio di rete che non sia lo IPV4
- Controllare non siano installate reti virtuali private (VPN) non autorizzate

# Come proteggersi?

## Attraverso “piercing” del firewall

*Un recente studio negli USA ha rilevato che 83% dei modems/routers utilizzati per connettersi a internet è sensibilmente vulnerabile.*

- **Utilizzare un firewall / proxy dedicato a valle del modem/router**
- **Bloccare tutte le porte eccetto quelle utilizzate**
- **Configurare il firewall per un log completo**

# Come proteggersi?

## Invasione rete WiFi

Come proteggersi?

- Usare solamente WiFi con Autenticazione WAP2
- Usare Passwords con la lunghezza massima ammessa(32 caratteri)
- Cambiare la Password Regolarmente
- Disabilitare l'opzione di collegamento facile con bottone WPS
- Usare il WiFi solo per collegamenti Internet a monte del secondo firewall
- Dove possibile, settare il router per escludere la comunicazione tra WiFi e rete interna
- Non condividere la rete interna con dispositivi IoT (Telecamere, Televisori, citofoni IP, ecc)

# Come proteggersi?

## Connessione diretta WiFi per falla protocolli (WiFi Krack)

Come proteggersi?

- Mantenere aggiornato il firmware del WiFi
- Se non fosse disponibile un aggiornamento, cambiare il router con uno resistente alla falla WiFi Krack

## Connessione bluetooth

Come proteggersi?

- Usare il bluetooth SOLO quando non ce altra possibilità
- Mantenere il bluetooth disabilitato quando non si usa

# Come proteggersi?

## Allacciamento nella nostra rete di dispositivo “lecito” ma compromesso

Come proteggersi?

- Non usare WiFi all’interno della zona di sicurezza (a valle del secondo firewall)
- Non permettere dispositivi mobili con accesso Internet alla vostra rete WiFi

## Condivisione chiavetta USB infetta

Come proteggersi?

- Evitare scambio di dispositivi di memoria USB con altre reti/persone
- Non permettere dispositivi mobili con accesso Internet alla vostra rete WiFi

## Installazione di programma lecito ma compromesso

Come proteggersi?

- Testare una installazione su piattaforma virtuale con antivirus attualizzato

# Sigcheck v2.70

05/22/2017 • 2 minutes to read • Contributors

By Mark Russinovich

Published: October 17, 2018

 Download Sigcheck (514 KB)

## Introduction

Sigcheck is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains. It also includes an option to check a file's status on VirusTotal, a site that performs automated file scanning against over 40 antivirus engines, and an option to upload a file for scanning.

*https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck*

# Process Explorer v16.21

05/16/2017 • 2 minutes to read • Contributors

By Mark Russinovich

Published: May 16, 2017

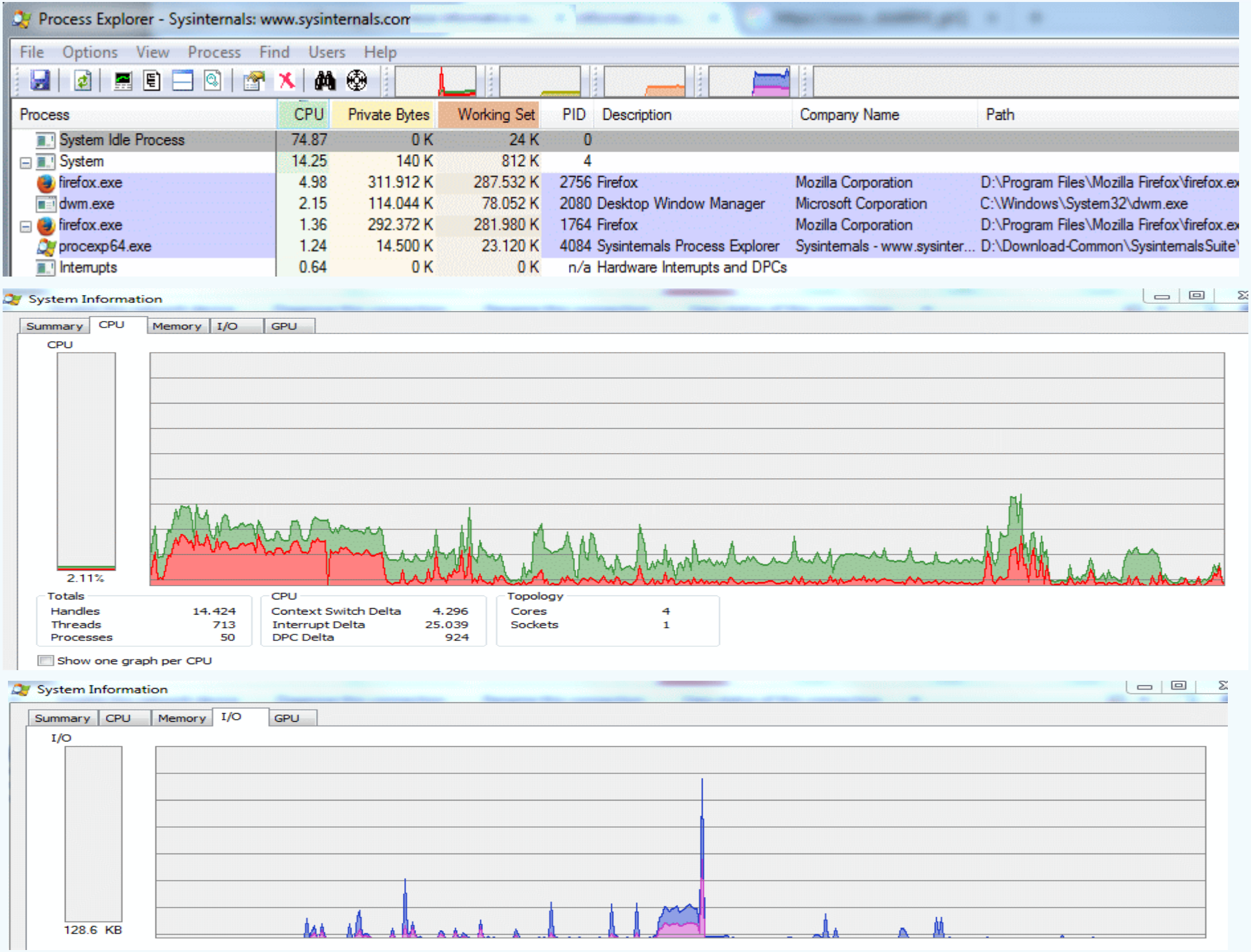
 Download Process Explorer (1.8 MB)

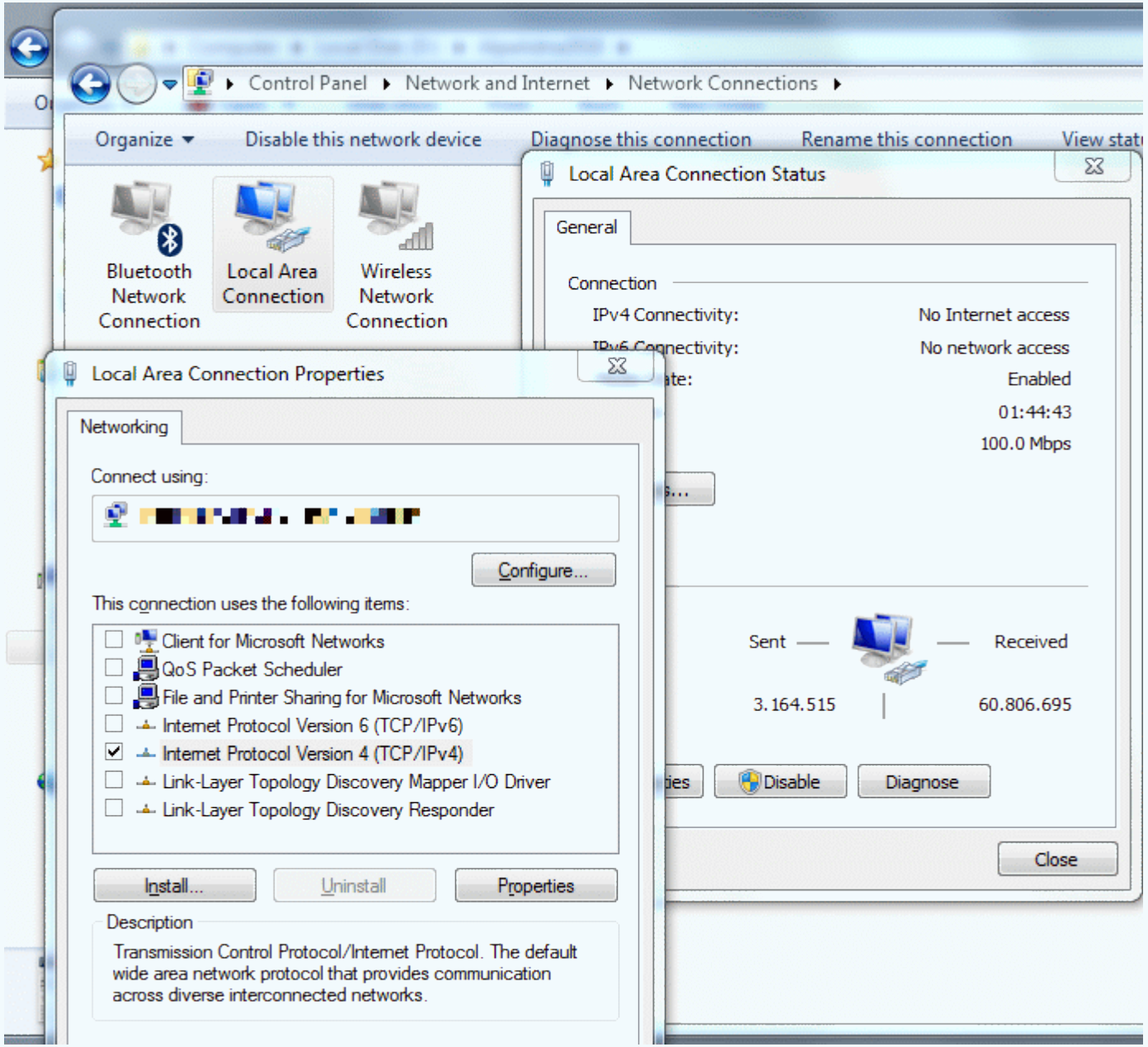
Run now from Sysinternals Live.

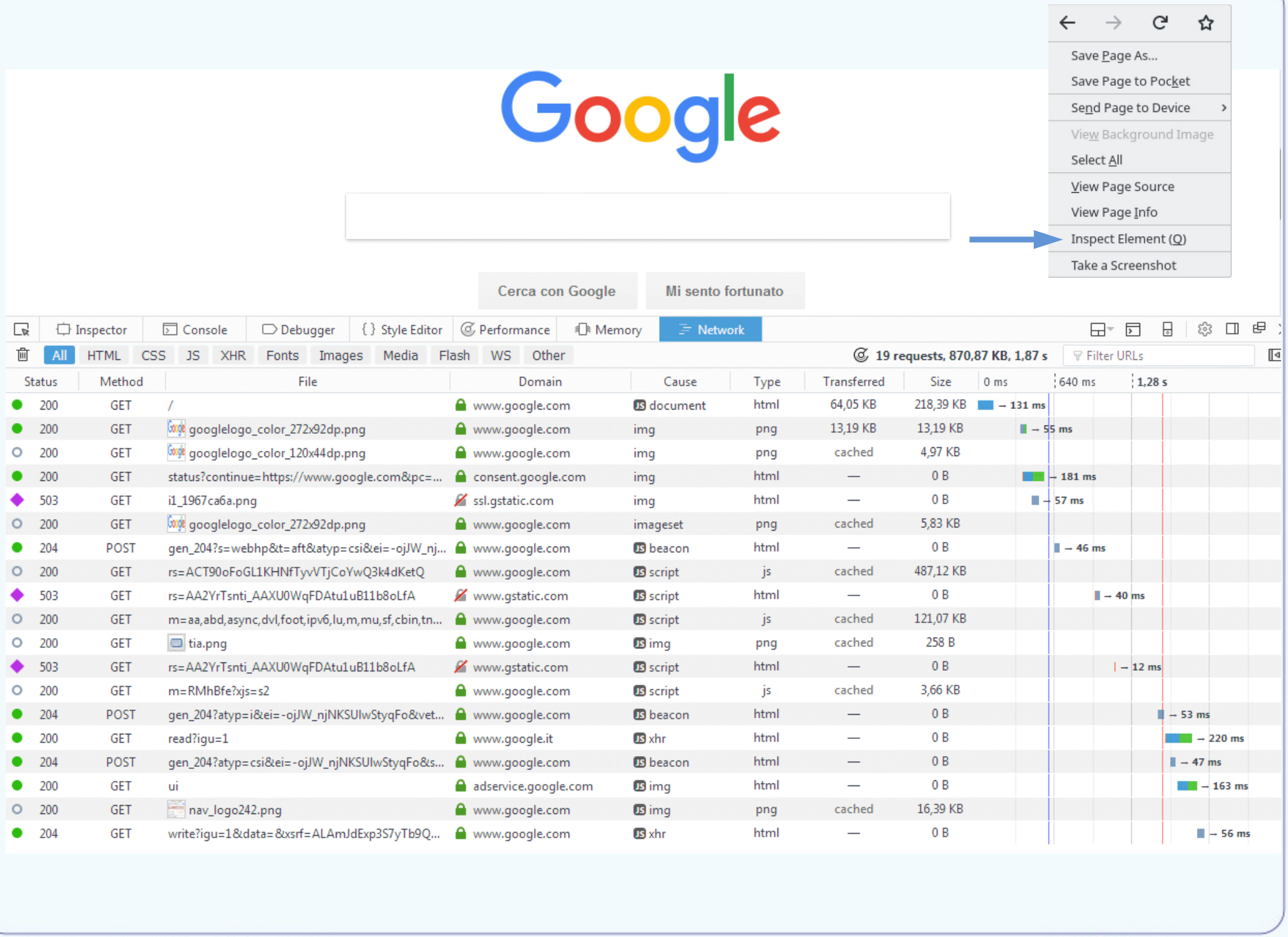
## Introduction

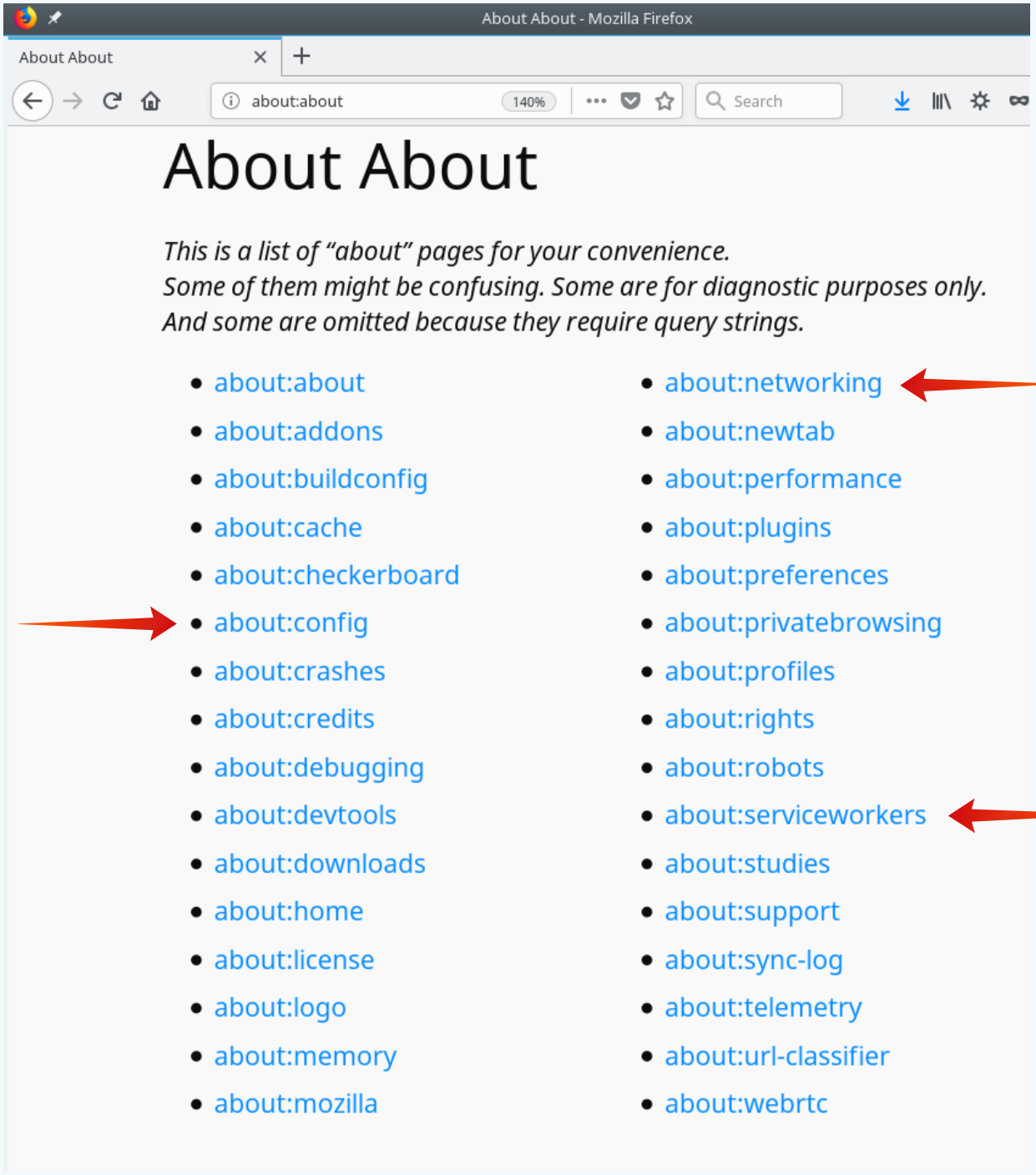
Ever wondered which program has a particular file or directory open? Now you can find out. *Process Explorer* shows you information about which handles and DLLs processes have opened or loaded.

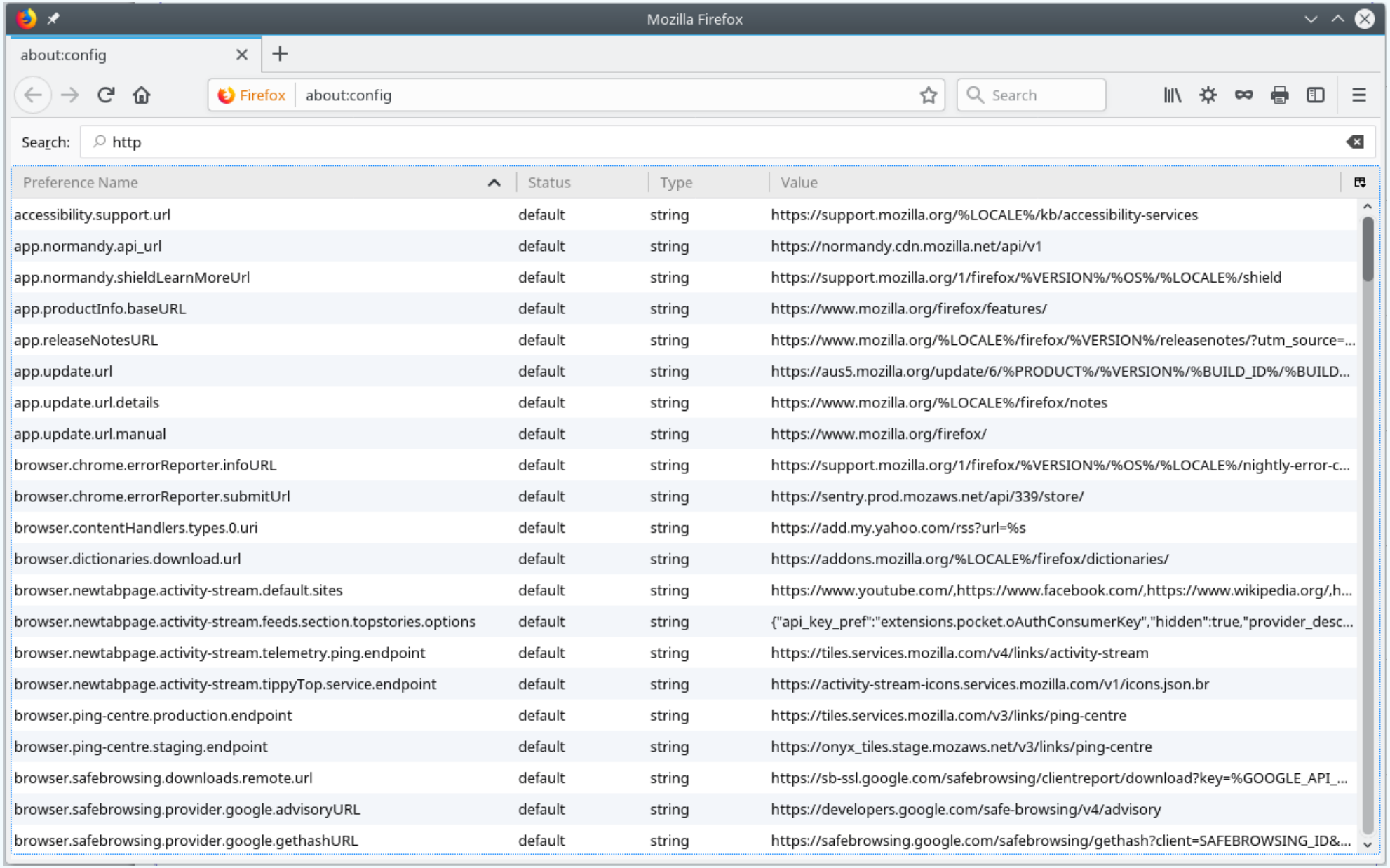
*https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer*


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name Path
System Idle Process 74.87 0 K 24 K 0
System 14.25 140 K 812 K 4
firefox.exe 4.98 311.912 K 287.532 K 2756 Firefox Mozilla Corporation D:\Program Files\Mozilla Firefox\firefox.ex
dwm.exe 2.15 114.044 K 78.052 K 2080 Desktop Window Manager Microsoft Corporation C:\Windows\System32\dwm.exe
firefox.exe 1.36 292.372 K 281.980 K 1764 Firefox Mozilla Corporation D:\Program Files\Mozilla Firefox\firefox.ex
procexp64.exe 1.24 14.500 K 23.120 K 4084 Sysinternals Process Explorer Sysinternals - www.sysinter... D:\Download-Common\SysinternalsSuite\
Interrupts 0.64 0 K 0 K n/a Hardware Interrupts and DPCs
System Information
Summary CPU Memory I/O GPU
CPU
2.11%
Totals
Handles 14.424
Threads 713
Processes 50
CPU
Context Switch Delta 4.296
Interrupt Delta 25.039
DPC Delta 924
Topology
Cores 4
Sockets 1
Show one graph per CPU
System Information
Summary CPU Memory I/O GPU
I/O
128.6 KB


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize
Disable this network device
Diagnose this connection
Rename this connection
Bluetooth Network Connection
Local Area Connection
Wireless Network Connection
Local Area Connection Status
General
Connection
IPv4 Connectivity:
No Internet access
No network access
Enabled
01:44:43
100.0 Mbps
Sent
Received
3.164.515
60.806.695
Disable
Diagnose
Close
Local Area Connection Properties
Networking
Connect using:
Configure...
This connection uses the following items:
Client for Microsoft Networks
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.


Save Page As...
Save Page to Pocket
Send Page to Device
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)
Take a Screenshot
Google
Cerca con Google
Mi sento fortunato
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
All
HTML
CSS
JS
XHR
Fonts
Images
Media
Flash
WS
Other
19 requests, 870,87 KB, 1,87 s
Filter URLs
Status Method File Domain Cause Type Transferred Size 0 ms 640 ms 1,28 s
200 GET / www.google.com document html 64,05 KB 218,39 KB 131 ms
200 GET googlelogo_color_272x92dp.png www.google.com img png 13,19 KB 13,19 KB 55 ms
200 GET googlelogo_color_120x44dp.png www.google.com img png cached 4,97 KB
200 GET status?continue=https://www.google.com&pc=... consent.google.com img html — 0 B 181 ms
503 GET i1_1967ca6a.png ssl.gstatic.com img html — 0 B 57 ms
200 GET googlelogo_color_272x92dp.png www.google.com imageset png cached 5,83 KB
204 POST gen_204?s=webhp&t=aft&atyp=csi&ei=-ojJW_nj... www.google.com beacon html — 0 B 46 ms
200 GET rs=ACT90oFoGL1KHNfTyvVTjCoYwQ3k4dKetQ www.google.com script js cached 487,12 KB
503 GET rs=AA2YrTsnti_AAXU0WqFDAtu1uB11b8oLfA www.gstatic.com script html — 0 B 40 ms
200 GET m=aa,abd,async,dvl,foot,ipv6,lu,m,mu,sf,cbin,tn... www.google.com script js cached 121,07 KB
200 GET tia.png www.google.com img png cached 258 B
503 GET rs=AA2YrTsnti_AAXU0WqFDAtu1uB11b8oLfA www.gstatic.com script html — 0 B 12 ms
200 GET m=RMhBfe?xjs=s2 www.google.com script js cached 3,66 KB
204 POST gen_204?atyp=i&ei=-ojJW_njNKSUIwStyqFo&vet... www.google.com beacon html — 0 B 53 ms
200 GET read?igu=1 www.google.it xhr html — 0 B 220 ms
204 POST gen_204?atyp=csi&ei=-ojJW_njNKSUIwStyqFo&s... www.google.com beacon html — 0 B 47 ms
200 GET ui adservice.google.com img html — 0 B 163 ms
200 GET nav_logo242.png www.google.com img png cached 16,39 KB
204 GET write?igu=1&data=&xsrf=ALAmJdExp3S7yTb9Q... www.google.com xhr html — 0 B 56 ms


About About - Mozilla Firefox
About About
about:about
140%
Search
About About
This is a list of "about" pages for your convenience.
Some of them might be confusing. Some are for diagnostic purposes only.
And some are omitted because they require query strings.
about:about
about:addons
about:buildconfig
about:cache
about:checkerboard
about:config
about:crashes
about:credits
about:debugging
about:devtools
about:downloads
about:home
about:license
about:logo
about:memory
about:mozilla
about:networking
about:newtab
about:performance
about:plugins
about:preferences
about:privatebrowsing
about:profiles
about:rights
about:robots
about:serviceworkers
about:studies
about:support
about:sync-log
about:telemetry
about:url-classifier
about:webrtc


Mozilla Firefox
about:config
Firefox
about:config
Search
Search:
http
Preference Name
Status
Type
Value
accessibility.support.url default string https://support.mozilla.org/%LOCALE%/kb/accessibility-services
app.normandy.api_url default string https://normandy.cdn.mozilla.net/api/v1
app.normandy.shieldLearnMoreUrl default string https://support.mozilla.org/1/firefox/%VERSION%/%OS%/%LOCALE%/shield
app.productInfo.baseURL default string https://www.mozilla.org/firefox/features/
app.releaseNotesURL default string https://www.mozilla.org/%LOCALE%/firefox/%VERSION%/releasenotes/?utm_source=...
app.update.url default string https://aus5.mozilla.org/update/6/%PRODUCT%/%VERSION%/%BUILD_ID%/%BUILD...
app.update.url.details default string https://www.mozilla.org/%LOCALE%/firefox/notes
app.update.url.manual default string https://www.mozilla.org/firefox/
browser.chrome.errorReporter.infoURL default string https://support.mozilla.org/1/firefox/%VERSION%/%OS%/%LOCALE%/nightly-error-c...
browser.chrome.errorReporter.submitUrl default string https://sentry.prod.mozaws.net/api/339/store/
browser.contentHandlers.types.0.uri default string https://add.my.yahoo.com/rss?url=%s
browser.dictionaries.download.url default string https://addons.mozilla.org/%LOCALE%/firefox/dictionaries/
browser.newtabpage.activity-stream.default.sites default string https://www.youtube.com/,https://www.facebook.com/,https://www.wikipedia.org/,h...
browser.newtabpage.activity-stream.feeds.section.topstories.options default string {"api_key_pref":"extensions.pocket.oAuthConsumerKey","hidden":true,"provider_desc...
browser.newtabpage.activity-stream.telemetry.ping.endpoint default string https://tiles.services.mozilla.com/v4/links/activity-stream
browser.newtabpage.activity-stream.tippyTop.service.endpoint default string https://activity-stream-icons.services.mozilla.com/v1/icons.json.br
browser.ping-centre.production.endpoint default string https://tiles.services.mozilla.com/v3/links/ping-centre
browser.ping-centre.staging.endpoint default string https://onyx_tiles.stage.mozaws.net/v3/links/ping-centre
browser.safebrowsing.downloads.remote.url default string https://sb-ssl.google.com/safebrowsing/clientreport/download?key=%GOOGLE_API_...
browser.safebrowsing.provider.google.advisoryURL default string https://developers.google.com/safe-browsing/v4/advisory
browser.safebrowsing.provider.google.gethashURL default string https://safebrowsing.google.com/safebrowsing/gethash?client=SAFEBROWSING_ID&...

Se disponete di un vecchio PC dual core o meglio un vecchio notebook (consuma meno), con un paio di adattatori USB a ETHERNET potete farvi un firewall installando una delle distribuzioni Linux in formato ISO (CD/DVD) dedicate a questo scopo