Mobiles workstations *in*security... Mitigating crawling trojans

Cédric BLANCHER

http://sid.rstack.org

sid@rstack.org / cedric.blancher@eads.net
EADS Corporate Research Center
DCR/SSI Departement
Suresnes, FRANCE

Cansecwest/core05 - 4-6 may 2005
http://www.cansecwest.com/

Agenda

EADS CCR

Plan

EADS CCR

What is this all about ?

Remote access to central Information System (IS)

- Fashionable marketing concept
- Ability to get a "home-like" connection
- Connect from various terminals (laptop, PDA, phone, etc.)
- Connect from many places (home network, office, WiFi hotspot, etc.)

Terminals, connections and technical means are available to make all this possible

EADS CCR

Access means

One can access valuable IS ressources through

- Webified access to ressources : email, files, etc.
- SSL VPN : clientless port redirection (à la SSH)
- Classical VPN stuff : full IP through secured tunnel

Thoses access can be secured

- Authentication (OTP, RSA sigs, x509)
- Privacy (chiphering)

EADS CCR

SSL VPN focus

SSL VPN is a so called clientless VPN solution
Can provide from simple web portal to full IP tunneled access

Issues

- Port redirection requires local code execution (Java, ActiveX) : many solutions requires IE
- DNS overwrite to localhost requires privileged access (hosts file overwrite)
  $\Longrightarrow$ IE + Admin : win-win situation ?
- Full IP trafic tunneling requires dedicated client to provide PPP over SSL

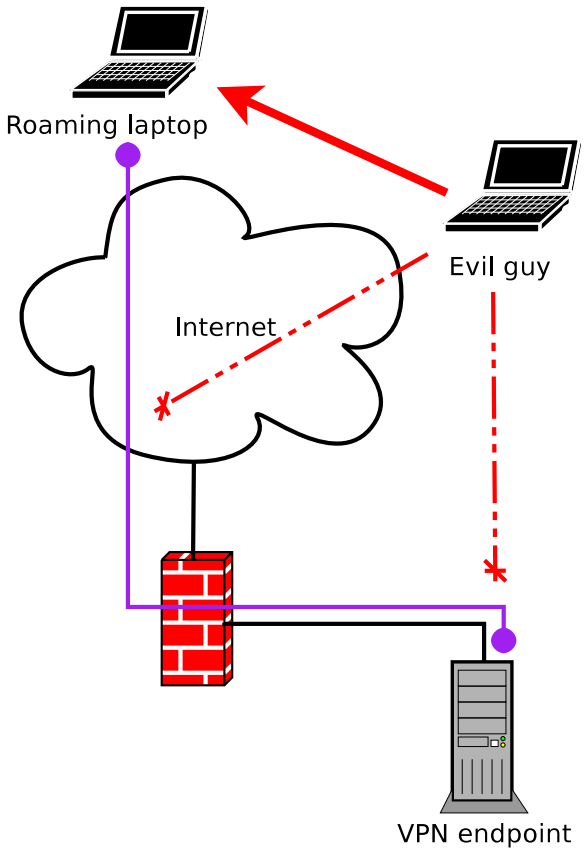
EADS CCR

So what ?

Thoses links are secure, but...

The endpoint problem

Is roaming endpoint fully trustable ?
What if mobile station is compromised ?



EADS CCR

Plan

EADS CCR

Mobile user vs. Information system

Remotly connect a mobile user to central IS

- Mobile workstation specifics
- Environment specifics

Theses specifics raises security issues

EADS CCR

Mobile workstation

A mobile workstation is an interesting target

- Is physically available
- Is connected to the network
- Has access to critical ressources
- Is operated by a *(l)user*

Regular workstation vs. mobile workstation

Mobile workstation only relies on its own protection means

Regular workstation

- Physically protected
- External network protection
- Local antivirus
- Personal firewall
- Automatic updates

Mobile workstation

- No physical protection
- No network protection
- Local antivirus (updates ?)
- Personal firewall
- No updates when offline

Mobile station exposure

Mobile workstations (laptops) are far more exposed than regular workstations (desktops)

Question

Would you let a bunch of desktops directly connected to the Internet a full day and put them back into LAN just like this ?

$\Longrightarrow$ That's however the case with most laptops configuration...

Physical issues

Laptops, PDAs and other mobile devices are easy to steal.

- Sensible data
- Credentials (logon cache, passwords storages, configuration files, etc.)
- Preconfigured access to IS through VPN

PDA and portable storage are weak against physical access...

Environmental issues

A mobile station is often connected to an insecure environment

- Unknown LAN, e.g. Cyberbase, home network, etc.
- WLAN, e.g. hotspot, WEP *"protected"* home network, etc.

Thoses environment can be compromised...

Remote access

Do you trust the system connecting to your VPN ?

- Home workstation : can be infected or compromised
- Heavily tweaked laptop : is it still secure ?
- Unknown workstation (for clientless ressources)

EADS CCR

Back home

Can you let a mobile station reconnect to IS after a journey outside ?

- Where has it been connected ?
- Is it infected ?
- Is it compromised ?
- Will it infect the whole network ?

Do not forget unknown laptops connecting to your network (e.g. pre-sales needing to download his slides)

Plan

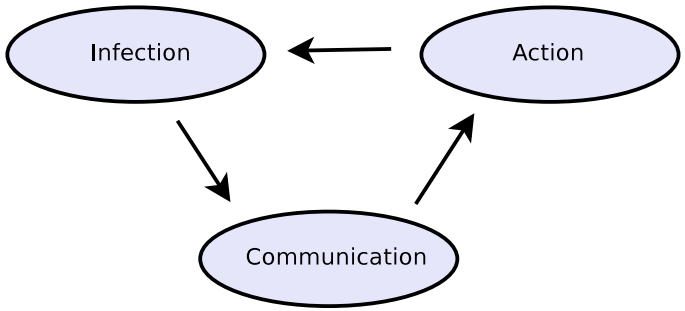
EADS CCR

Infection scenario

Information System attack using mobile workstation[1]

Three steps attack :

1. Infection
2. Communication with outter world
3. Action



[1] Thanks to french LCEN law, some mentionned tools may not be available online anymore...

EADS CCR

Infection

The important, but *easy* part...

Attack means

- Physical access
- Direct attack through network
- Malicious traffic injection

Physical access

Information gathering

- Scan hard drive for sensible data
- Find credentials
- Find remote access configuration stuff

Real life example

Hard drive is plugged to another box and scanned

- Batch file contains VPN group password
- VPN group password is stored ciphered, but can be retrieved in memory by using a vulnerable VPN client application
- Domain credentials are brute forced from logon cache

Consequence

Unrestricted remote VPN access to central IS

Physical access

Boot another system when possible through CDROM, USB or network[2]

- Change superuser credentials
- Bypass FS access control
- Access to some protected areas

Consequence

Access to sensible data

[2]Some laptops BIOSes boot from network PXE without asking for password...

Physical access

Attempt to tamper system

- Autorun infection : CDROM, USB key[MAY05], any removable storage
- Network attack : connect cable, assign DHCP, attack
- Firewire attack[DOR04] : tamper system memory
- Execute something from console if available

Consequence

Laptop compromisation, malicious code execution

Real life example

WinXP laptop booted but locked

- PCMCIA Cardbus network adapter insertion
- Adapter is recognized as new connection
- DHCP requests that can be answered
- NetBIOS requests and communication on affected network or 169.254.0.0/16

```
cbr@anduril:~$ sudo tcpdump -i eth0 -n
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
06:54:21.796332 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
06:54:26.812788 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
06:54:34.814723 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
06:55:56.930198 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
06:55:56.931675 arp who-has 192.168.2.94 tell 192.168.2.1
06:55:57.001834 IP 192.168.2.1.67 > 192.168.2.94.68: BOOTP/DHCP, Reply, length:
300
06:55:57.931571 arp who-has 192.168.2.94 tell 192.168.2.1
06:55:58.931467 arp who-has 192.168.2.94 tell 192.168.2.1
06:56:00.928677 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
06:56:00.929059 IP 192.168.2.1.67 > 192.168.2.94.68: BOOTP/DHCP, Reply, length:
300
06:56:09.931168 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:
01:03:dc:2d:83, length: 300
```

Consequences

Local network link to the station up and running

Network initiation

Laptop may not be connected : wireless links exploitation

- IR stuff : close to physical access
- Bluetooth stuff : efficient against mobile phones
- WiFi stuff : many ways of getting a driver associated
  $\Longrightarrow$ Open rogue AP[MZ04] often successful...

Real life example

WinXP Laptop in testlab with active WiFi adapter

- Open WiFi network creation with rogue AP
- Configure laptop network with DHCP
- Exploit RPC/DCOM flaw[a]
- Admin account creation for RDP connection
- Recub[EOS04] backdoor Win32 port installation

[a] Personal firewall has "local network" exception

Consequence

Laptop compromisation, backdoor installed and active

Laptop connected to hostile environment

Mobile worstation has network access in some untrusted place prone to attacks

- Rogue AP attack
- Rogue DHCP server
- ARP cache poisoning
- DNS spoofing/cache poisoning (Windows)
- Traffic redirection and tampering
- Access to network shares
- Remote vulnerabilities exploitation

Tools : arp-sk[RAY02], rogue AP stuff[MZ04], dnsa[BET03]

EADS CCR

Real life example

Laptop is connected to regular (= insecure) WiFi hotspot (or WEP home network[3])

- Redirect HTTP traffic using ARP stuff
- Hotspot : Web authentication is needed against captive portal $\Longrightarrow$ Tamper HTTP traffic on the fly using local redirection
- Exploit browser vulnerability through malicious content

Tools : rogue AP stuff[MZ04], arp-sk[RAY02], scapy[BIO02]

Consequence

Malicious code is executed with user privileges
Hint : SSL VPN / IE / Admin / Win-win situation...

[3] PSPF like and MAC filtering are easy to bypass

Personal firewall

What about personal firewall if present and active

- Exploit PF vulnerabilities : frag, remote exec, etc.
- *Infamous* "local network" for file sharing exception
- VPN client protection only active when VPN is up
- Can be bypassed

Consequence

In many cases, protection is not so effective[BLA03]...

Personal firewall

What about personal firewall if present and active

- Exploit PF vulnerabilities : frag, remote exec, etc.
- *Infamous* "local network" for file sharing exception
- VPN client protection only active when VPN is up
- Can be bypassed

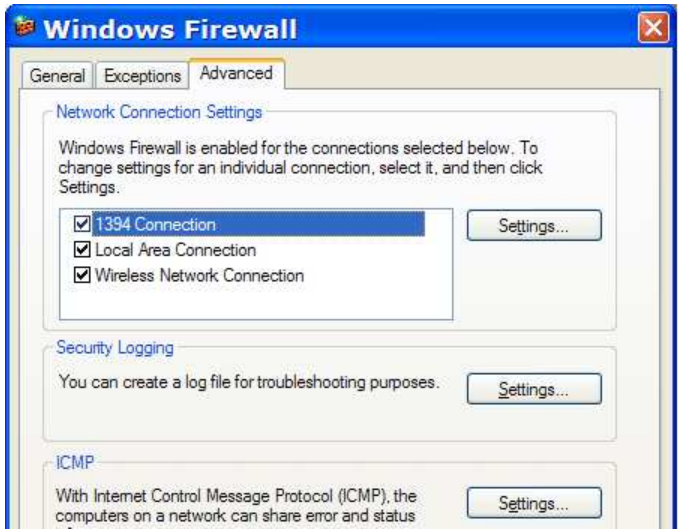
Consequence

In many cases, protection is not so effective[BLA03]...

Personal firewall

What about personal firewall if present and active

- Exploit PF vulnerabilities : frag, remote exec, etc.
- *Infamous* "local network" for file sharing exception
- VPN client protection only active when VPN is up
- Can be bypassed



Consequence

In many cases, protection is not so effective[BLA03]...

Malicious code

Backdoor execution

- Backdoor can writen somewhere to filesystem
- Backdoor modifies startup so it will be launched (registry, start menu)
- Backdoor hooks threads running processes (API hooking) and dies

Tools : Casper[DD04], Recub[EOS04]
A bunch of spywares ar no using this kind of technic and are hell to wipe out

Consequence

Laptop compromised : backdoor/trojan active

EADS CCR

Establish communication channel

Backdoor must communicate with outter world, bypassing personal firewall and perimeter protection if present

- Rely on authorized applications
- Trigger communication on specific trafic patterns
- Use native HTTP/HTTPS API so proxy settings and authorization are automagicly used
- Covered channel over HTTP/HTTPS

Tools : Casper[DD04], Recub[EOS04]

Consequence

Backdoor is able to communicate through authorized protocol

EADS CCR

Backdoor actions

Backdoor can execute actions upon request

- Data theft on workstation and shares available on network
- Extension through uploaded modules
- Local privilege escalation
- Scan environment
- Attack other workstations around

Tool : JAB[GRE03]

Backdoor actions

While hooking processes, backdoor can tamper them

- Credentials theft
- Certificates theft
- Network traffic interception
- Etc.

As an example, you can set a fully transparent SSL MiM[DR05]...

Action perimeter

Backdoor can strike from :

- Remote access through VPN
- Information System itself

Asynchronous adaptative backdoor

- Can take actions without communication with its master
- Rely on configured applications so can act from any network
- Can deliver results and upload orders/extensions upon connection

Real life example

Have a look at Blaster worm (summer 2003)[4]...

- Laptops compromised during holidays while connected to Internet
- Worm spreading through VPN when activated
- Worm spreading when connecting back to office LAN (monday sucks syndrom)

Consequence

Supposely immune networks compromised by mobile users

[4] Same situations with Slammer (may 2004)

Plan

EADS CCR

Risks mitigation

There's no *off the shelf*, ready to go solution
However, risk can be strongly mitigated

- Workstation physical protection
- Workstation system protection
- Integration within existing architecture
- Information System protection

EADS CCR

Physical protection

Prevent laptop theft if possible, or prevent info gathering from it

- Anti-theft measures : marking, security cables[5]
- Choose appropriate hardware (e.g. security chip for BIOS settings storage)
- BIOS password and boot locked on HDD
- ATA HDD password[6]
- Ciphered storage area

[5] Beware of Bic pen lock picking...
[6] Available since ATA3

System protection

Apply strict security measures

- Choose appropriate OS
- Choose appropriate applications
- Harden configuration : unprivileged accounts, user rights management, updates policy, etc.
- Install security tools : antivirus and personal firewall at least
- Look at new tools : system calls interception, security policy enforcement, etc.

Protect your Information System

Think twice before integrating solution in existing architecture

- Do not treat mobile stations as local stations : they're not equal in term exposure
- Restrict mobile stations access to the system
- See beyond *"DisneyLand style"* commercials ;)

Protect your information system

Enforce network access control

- Avoid uncontroled stations connection
- Control physical acces to your network
- Logical access control to network (e.g. 802.1x)
- Think segmentation and quarantine
  - Dedicated VLANs for guests
  - Manual or automatic[7] workstation checking and quarantine

[7] When available

Plan

EADS CCR

Conclusion

Remote access is great, but can ruin the whole IS security.

There's no "off the shelf" solution, but

Mitigation is possible through a strict security policy enforcement

EADS CCR

Greetings

Thanks to...

- **Rstack.org** team
  `http://www.rstack.org/`
- **MISC Magazine**
  `http://www.miscmag.com/`
- **French Honeynet Project**
  `http://www.frenchhoneynet.org/`

Download theses slides from `http://sid.rstack.org/`

EADS CCR

Plan

EADS CCR

Bibliography I

- [BET03] Pierre Bétouin, dnsa, `http://securitech.homeunix.org/dnsa/`
- [BIO02] Philippe Biondi, scapy, `http://www.secdev.org/projects/scapy.html`
- [BLA03] Cédric Blancher, Benefits and limits of personal firewalls concept, SSTIC 2003
- [DD04] Éric Detoisien & Eyal Dotan, Old win32 code for a modern and super-stealth Trojan, Black Hat Europe 2004
- [DET05] Éric Detoisien & Nicolas Ruff, Malwares the threat from within, JSSI 2005

EADS CCR

Bibliography II


[DOR04] Maximillian Dornseif, "0wn3d by an iPod - Firewire/1394 Issues", Cansecwest/core05


[EOS04] EOS India, Recub Win32 port, `http://www.eos-india.net/misc/main.html`


[GRE03] Nicolas Grégoire, JAB - A backdoor for unknown Win32 network, SSTIC 2003


[MAY05] David Maynor, "0wn3d by everything else - USB/PCMCIA Issues", Cansecwest/core05


[MZ04] Shane "K2" Macaulay & Dino Dai Zovi, "Rogue Access Points", Cansecwest/core05

EADS CCR

Bibliography III

 [RAY02] Frédéric Raynal, arp-sk, http://www.arp-sk.org/