

Turning your managed **Anti-Virus**

... into my Botnet 😊

Jérôme NOKIN

<http://funoverip.net>

About me

id

- Jérôme Nokin
- <http://funoverip.net>
- jerome.nokin@gmail.com

job

- Penetration Tester
- Verizon Enterprise Solutions

sudo certs

- OSCE
- OSCP
- CEH

Research

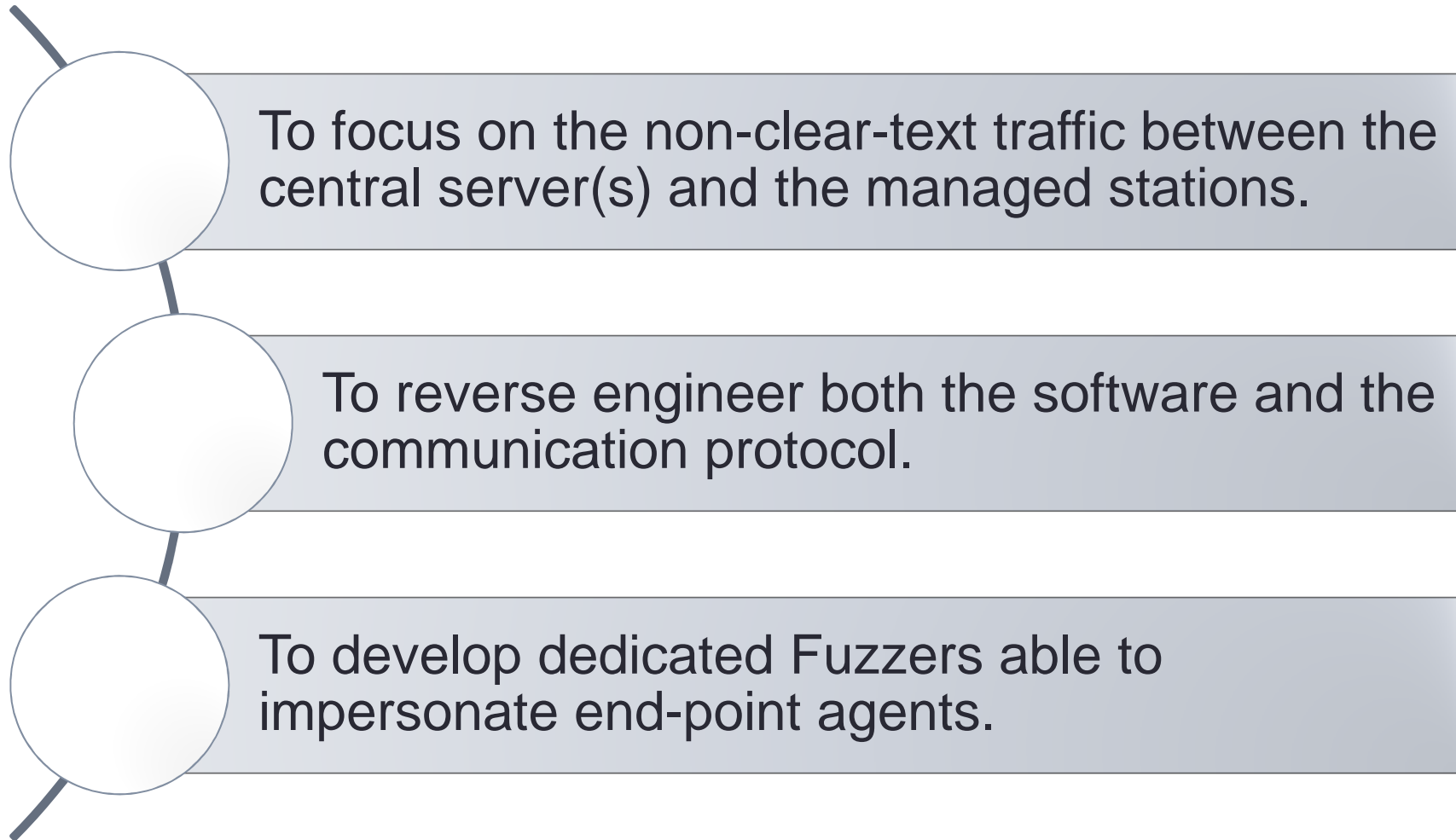
Topic: Managed Antivirus

- Central server(s) of such software regularly communicate with the endpoints and perform privileged actions against them.
- From an attacker's perspective, vulnerabilities in such servers might have a very large impact against the whole set of managed stations.

Yes, we found vulnerabilities. However:

- This talk isn't full of reversing/debugging/fuzzing screenshots. Paper will soon address such details.
- This talk is about **how we used** these vulnerabilities (impact).

Approach



Selected Targets



McAfee ePolicy Orchestrator



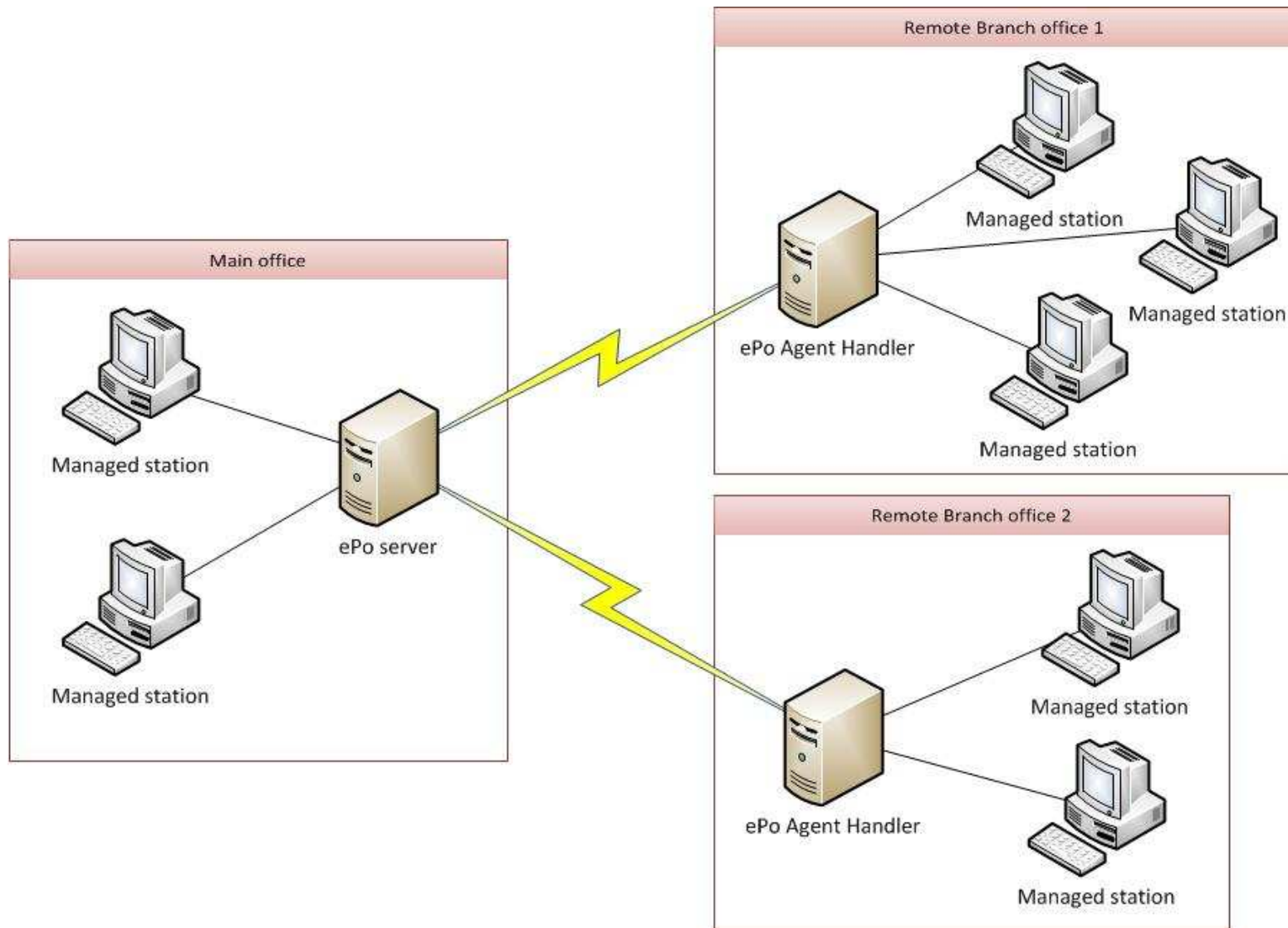
Symantec Endpoint Protection



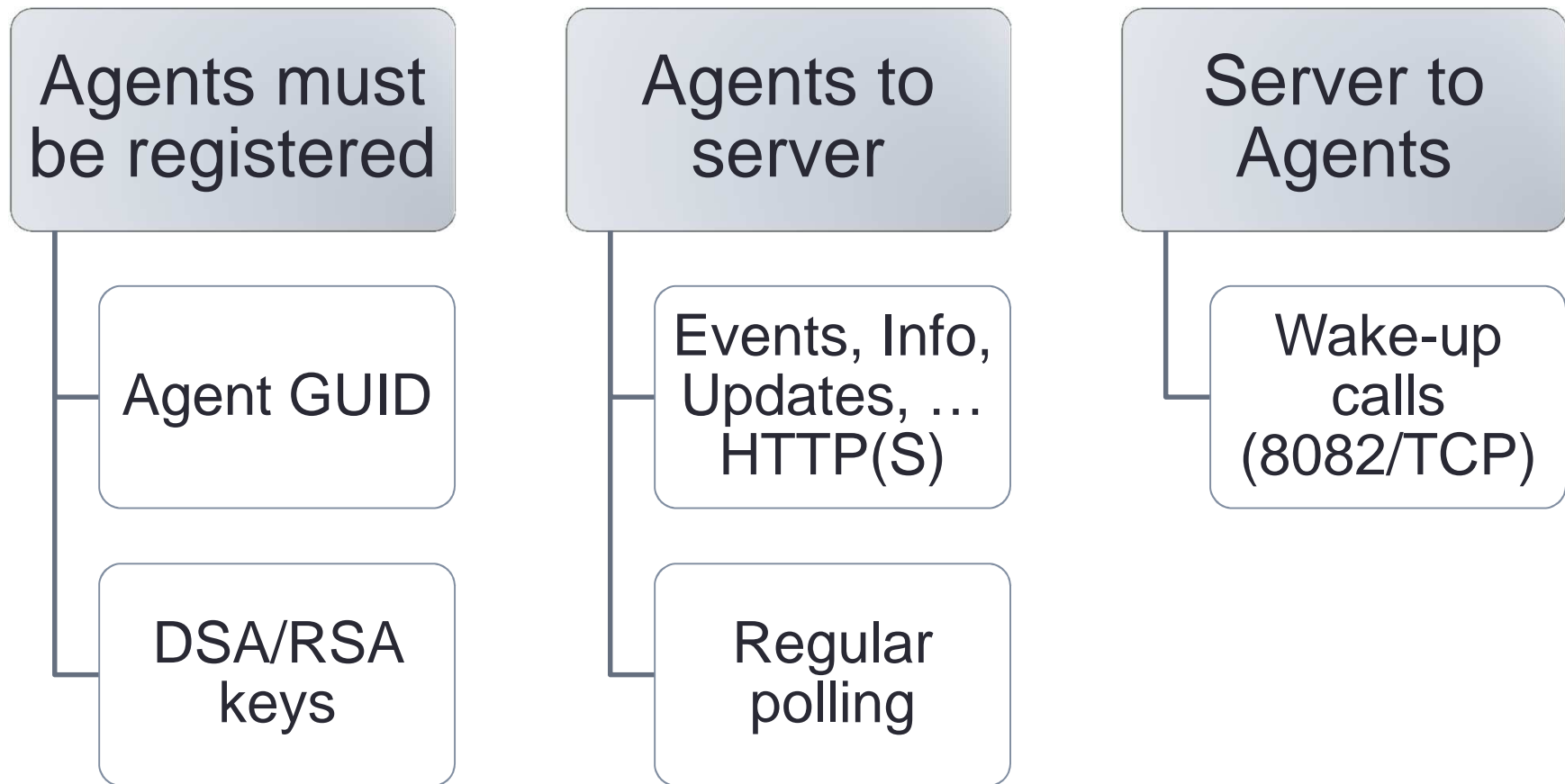
McAfee

ePolicy Orchestrator

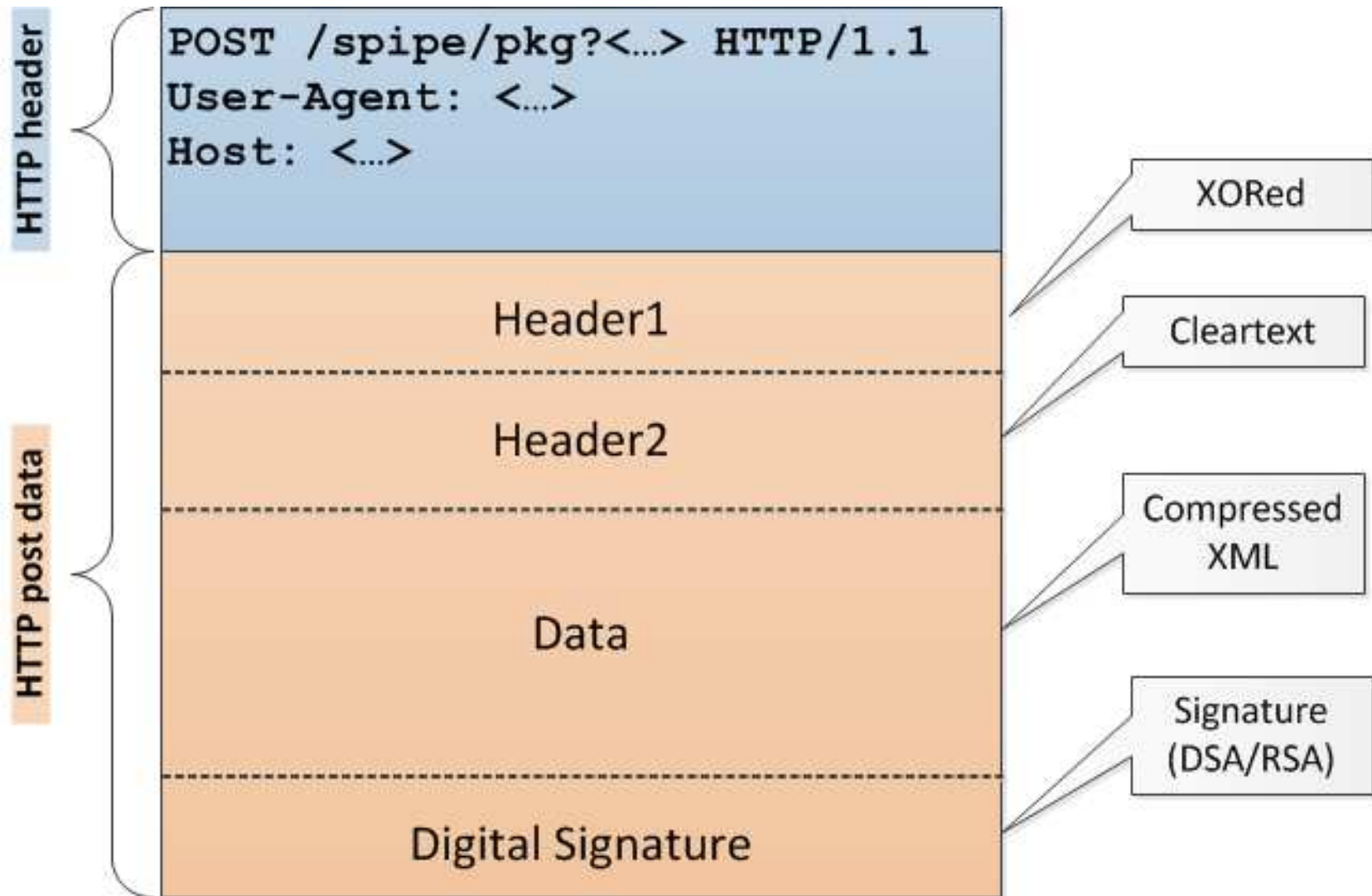
Common deployment



Some notes & protocols



HTTP request sample (client → server)



CVE-2013-0140 – SQL Injection

- SQL Injection issues were discovered inside the XML “Full Properties” message (data section)

```
[...SNIP...]
<ProductProperties SoftwareID="EPOAGENT3000" delete="false">
  <Section name="General">
    <Setting name="AgentBroadcastPingPort">8082</Setting>
    <Setting name="AgentGUID">') ; EXEC sp_configure 'show
advanced options',1 ; RECONFIGURE ; EXEC sp_configure 'xp_cmdshell',1 ;
RECONFIGURE ; EXEC master.dbo.xp_cmdshell 'ping 192.168.60.100'; --
</Setting>
    <Setting name="AgentPingPort">8081</Setting>
  </Section>
[...SNIP...]
</ProductProperties>
```

CVE-2013-0141 – Directory Path Traversal

- Below is an **Event Request** content (data section)
- This request creates an XML file on the server, which contains data about an event.

```
01 00 21 00 32 30 31 32 31 32 31 30 31 32 31 33 |...!.201212101213|
34 30 38 37 31 39 31 33 38 30 30 30 30 30 44 36 |40871913800000D6|
30 2e 78 6d 6c 45 03 00 00 3c 3f 78 6d 6c 20 76 |0.xmlE...<?xml v|
65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 |ersion="1.0" enc|
6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c |oding="UTF-8"?><|
```

- BLUE → Destination filename
- GREEN → Length of the filename
- RED → Length of the data
- BLACK → The “data”

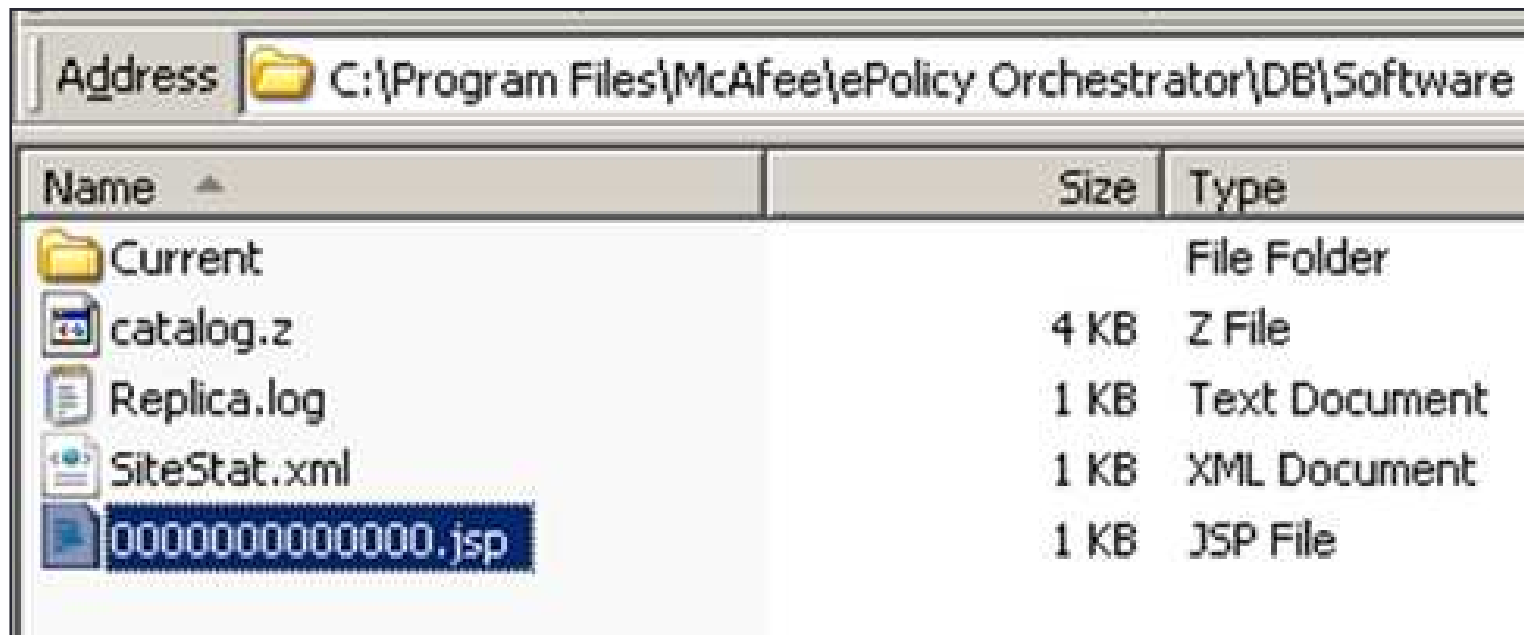
CVE-2013-0141 – Directory Path Traversal

What happens if we replace the filename from:

`20121210121340871913800000D60.xml`

to:

`../../../../Software/0000000000000000.jsp`



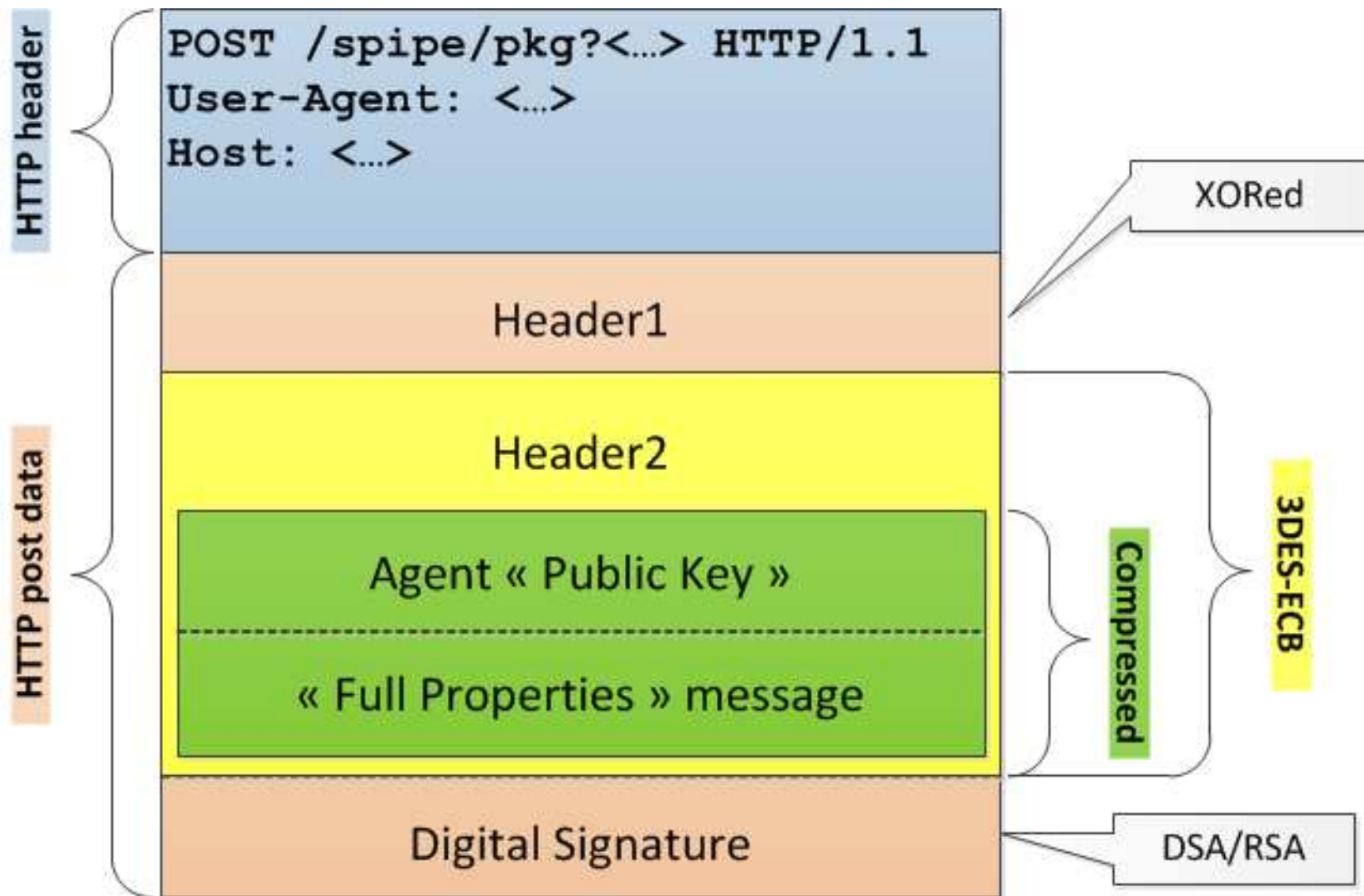
Post-Authenticated vulnerabilities

Prior to any communication between an agent and the ePo server, the agent must be registered.



So far, we can only trigger vulnerabilities by impersonating a registered agent.

Registration request



Reqseckey – the published private key

- How does ePo verify the signature if it doesn't know the **public** key yet ?
- The signature is actually not generated using the “**agent**” private key, but using a dedicated **ePo** key ... which is published to everyone ...
- That private key is called “**reqseckey**” and is embedded in the agent installation package.
- Additionally, that key is available for download from the ePo server:

<https://epo/Software/Current/EPOAGENT3000/Install/0409/reqseckey.bin>

Did you say 3DES ?





- Part of the registration request is encrypted using **3DES**
- The symmetric key is obfuscated inside the binaries and therefore is the same in **all** ePo environments (and versions) 😊
- At your office, the key is:

```
echo -n '< !@# $%^>' | sha1sum  
3ef136b8b33befbc3426a7b54ec41a377cd3199b
```


Sign Up

(It's free and always will be)

3 5:50:10 PM CEST | User: admin | [Log Off](#)

 Dashboards  System Tree  Queries & Reports  Policy Catalog

Systems | Assigned Policies | Assigned Client Tasks | Group Details

Preset: Custom: Quick find: [Clear](#)

<input type="checkbox"/>	System Name ▲	Managed State	Tags	IP Address
<input type="checkbox"/>	Hax0r	Managed	Workstation	52.196.234.215
<input type="checkbox"/>	WIN2K3R2-X64	Managed	Server	192.168.60.167
<input type="checkbox"/>	WIN7X64	Managed	Workstation	192.168.60.175

Post-Authenticated vuln



Rogue Agent Registration:



(Kind of) Pre-Authenticated

Remote Command Execution

Remote command execution – Method 1

Extended stored procedure

Using SQLi and '**xp_cmdshell**'

If available (dba privs ?)

MSSQL isn't always running with
SYSTEM privileges 😞

Enhancement: In recent ePo versions,
admin is warned if ePo starts with DBA
privs

Remote command execution – Method 2

- Reuse ePo features ! **Registered Executable**

Registered Executables	
For security purposes, registered executables cannot be a	
Name ▲	Path
cmd.exe	C:\WINDOWS\system32\cmd.exe

- To be used as an **Automatic Response** with “Rogue Event requests”

Select a registered executable, and specify any arguments for it.	
Registered executable	cmd.exe ▼
Arguments	/c {hostName}

- Always run with SYSTEM privileges 😊

So far, so good ...

Registration

- “Published” private key
- Static encryption key (3DES)

Database access

- SQL Injection (CVE-2013-0140)

Upload

- Directory Path Traversal (CVE-2013-0141)

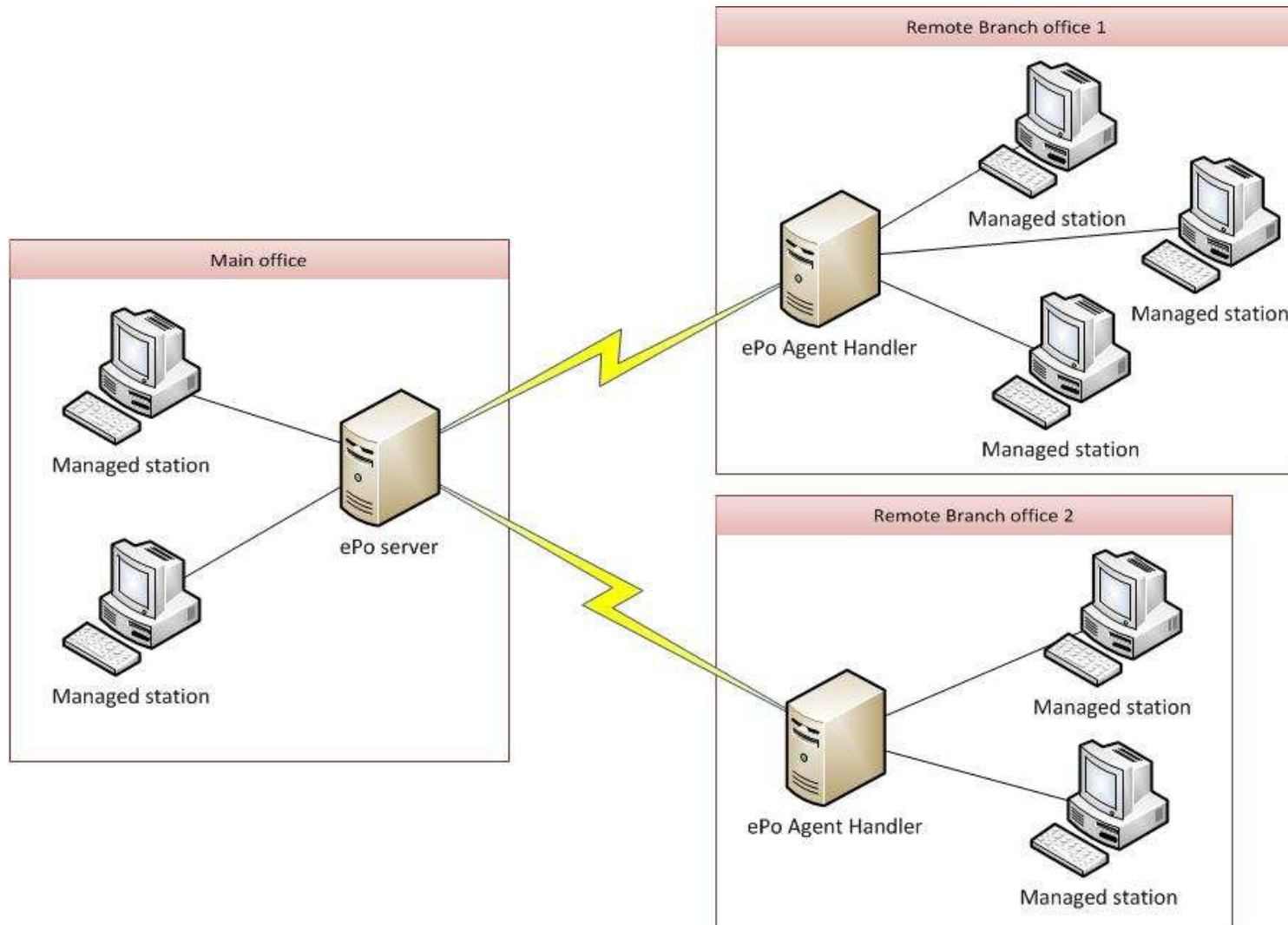
Remote Command Execution

- Registered Executable
- Automatic Responses

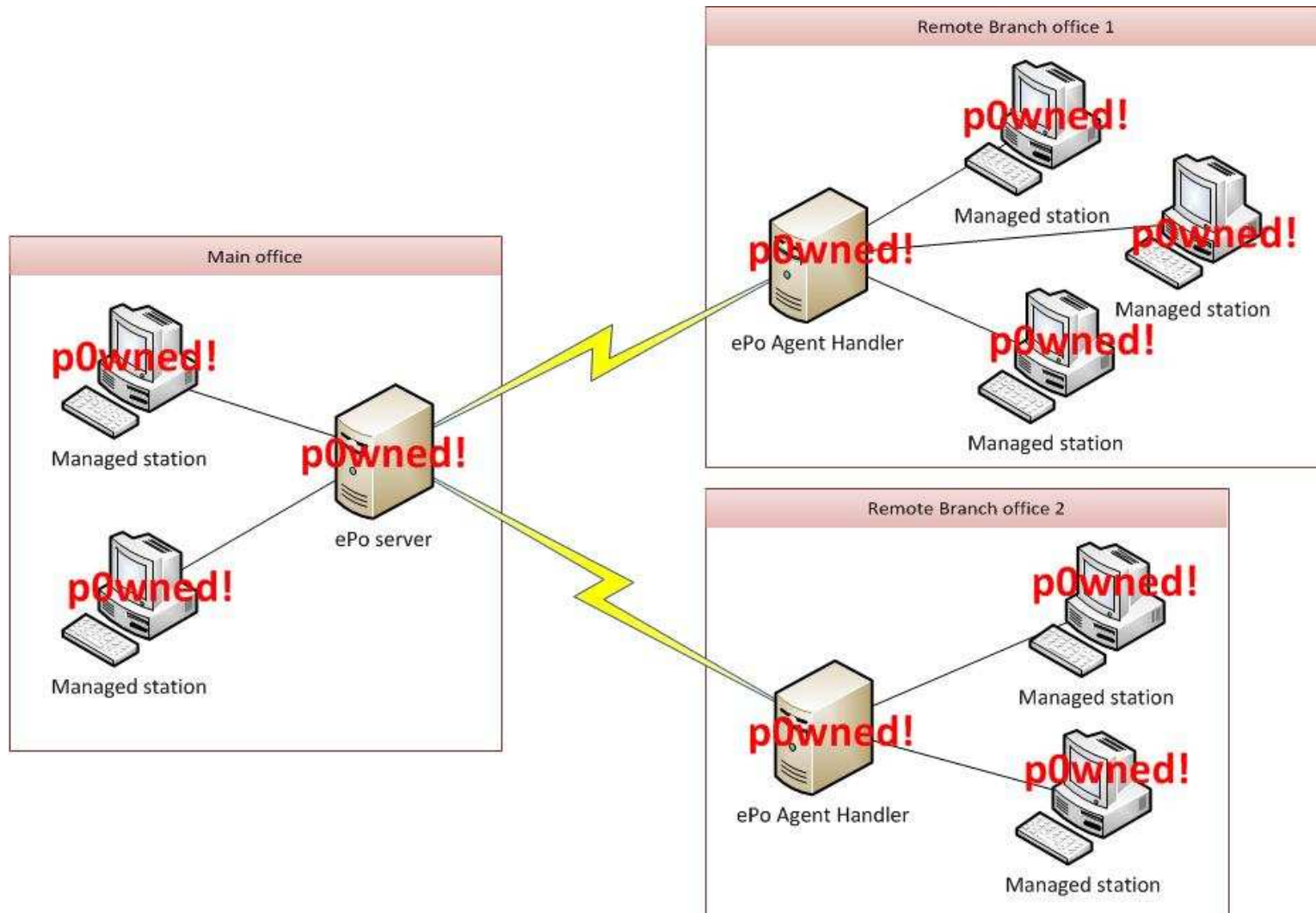
Download

- After all, It's a web server ...
- Just have to move files using RCE

Remember this ?



Would that be possible ?



YES WE CAN



Creating Rogue McAfee packages

Creating rogue packages (1)

- Updating **catalog.z** on the ePo server (available software list)
 - XML file containing “the software catalog”
 - Compressed as a CAB file
 - Digitally signed using:
 - DSA: `C:\Program~1\McAfee\Epo\DB\Keystore\sm<hostname>.zip`
 - RSA: `C:\Program~1\McAfee\Epo\DB\Keystore\sm2048<hostname>.zip`
 - Encrypted using 3DES
 - **Same key as before**. Seems to be an universal key in McAfee world ?
- Creating a McAfee package
 - Generating a **PkgCatalog.z** file (metadata information).
 - Also XML → CAB → Signature → 3DES
 - Add evil files

Creating rogue packages (2)

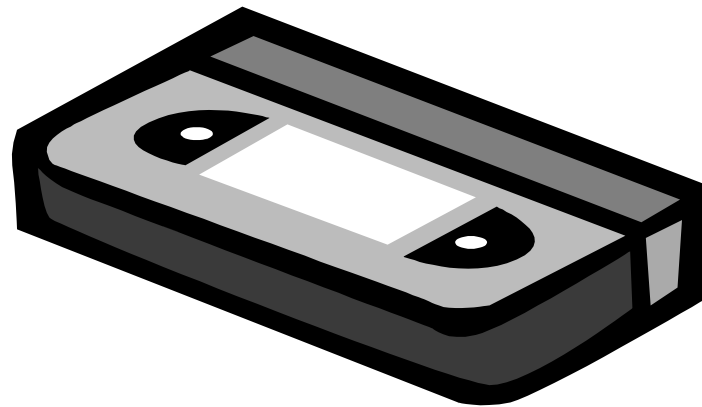
- Updating ePo repository files (using “Dir Path Traversal”)
- Kindly ask other ePo repositories to update their caches (using SQLi)
- Creating a Deployment Task (using SQLi)

“... Dears agents, please download and install the following package.
I have digitally signed the package so you can trust it...”

- Abusing the “**Wake Up**” calls (using SQLi)

“... By the way, do you mind to obey now ? ...”

ePolicy Owner – Tiny Demo



(Get the full version here: <http://funoverip.net/?p=1405>)

Security patch & references

- McAfee released a security patch in **May 2013**.
 - All of these issues are resolved in ePO **5.0**, **4.6.6**, and **4.5.7**
 - <https://kc.mcafee.com/corporate/index?page=content&id=SB10042>
- US-CERT advisory
 - <http://www.kb.cert.org/vuls/id/209131>
- CVE
 - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0140>
 - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0141>

Internet survey – Getting data

Fingerprint

- Using ePo SSL server certificates

Shodan

- SSL DB not ready yet

Zmap

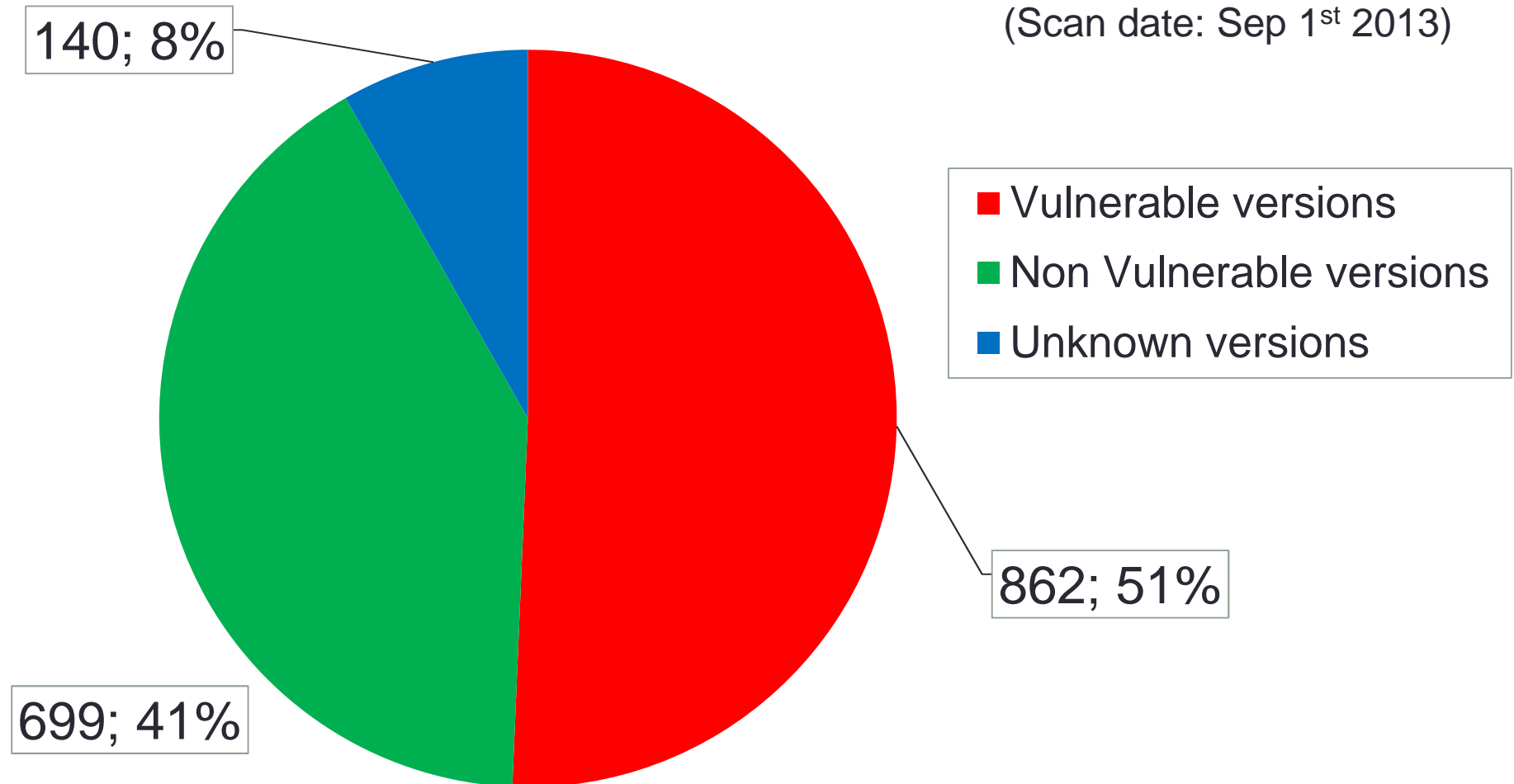
- Internet wide scan using Zmap at 70Mbps (~13h) + SSL extract (~2 weeks)

Crossing Results

- Thanks to Zmap team for your data!

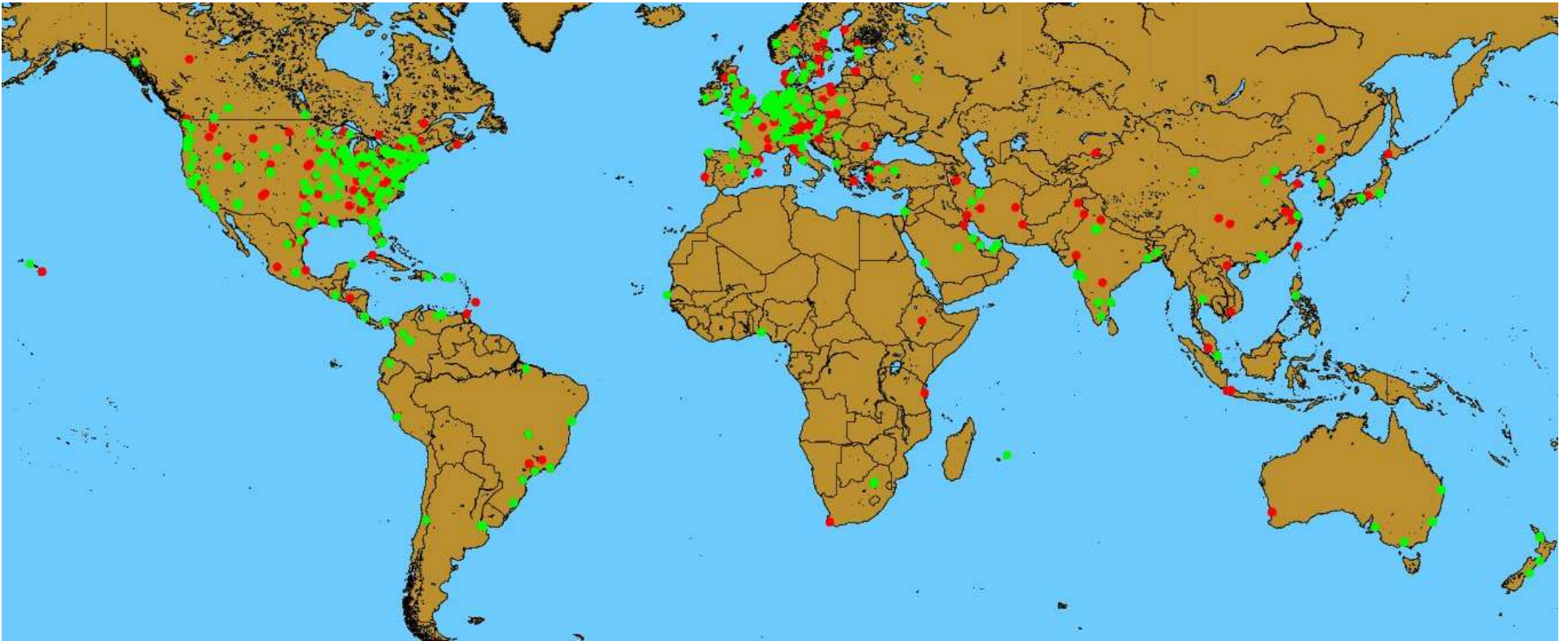
Internet survey – 1701 servers found

(Scan date: Sep 1st 2013)



How many managed devices behind ?

Internet survey – World map view



- Still a draft picture.. Sorry..
- Note: 11 servers vulnerable in this city (Amsterdam)



Conclusion

What did we learn ?

Security issues can be everywhere

- In mature products, since years!
- Hidden by complex protocols or structures
- It's only a matter of time and energy to find them

Chained issues

- Do not under-estimate a single vulnerability
- Impact is much more important if coupled with additional weaknesses

Do not rely on CVSS score only

- ePo **SQL Injection** – base score: **7.9**
- ePo **Dir Path Traversal** – base score : **4.3**
- However, impact for chained vulnerabilities: **We Own the Matrix...**

Give enough time to your testers...

Customer

- I would like you to audit my web application. Security is important for us !

Pentester

- I'm your man!
- I would need 6 days + 1 day for reporting.

Customer

- Awesome!
- You have 4 days, including reporting.

Pentester

- ...

Q&A



Btw, about SEP (Symantec)

- CVE-2013-1612 Remote buffer Overflow

