Dealing with
Linux Malware

Rootkits, Backdoors, and More...

Michael Boelen
michael.boelen@cisofy.com

Utrecht, 19 March 2016

CISOFY
AUDITING-HARDENING-COMPLIANCE

Agenda

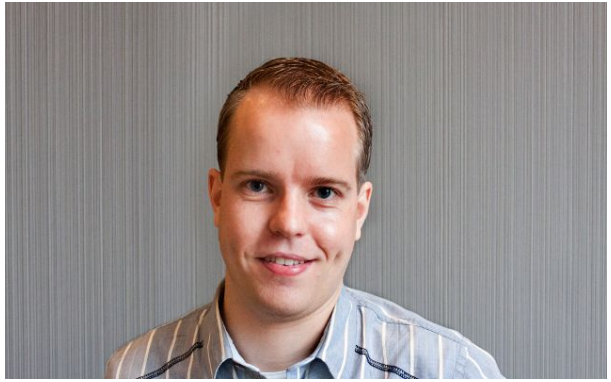
Today

1. How do “they” get in
2. Why?
3. Malware types
4. In-depth: rootkits
5. Defenses

Interactive

- Ask
- Share
- Presentation

Michael Boelen



- Security Tools
  - Rootkit Hunter (malware scan)
  - Lynis (security audit)
- 150+ blog posts
- Founder of CISOfy

How do “they” get in

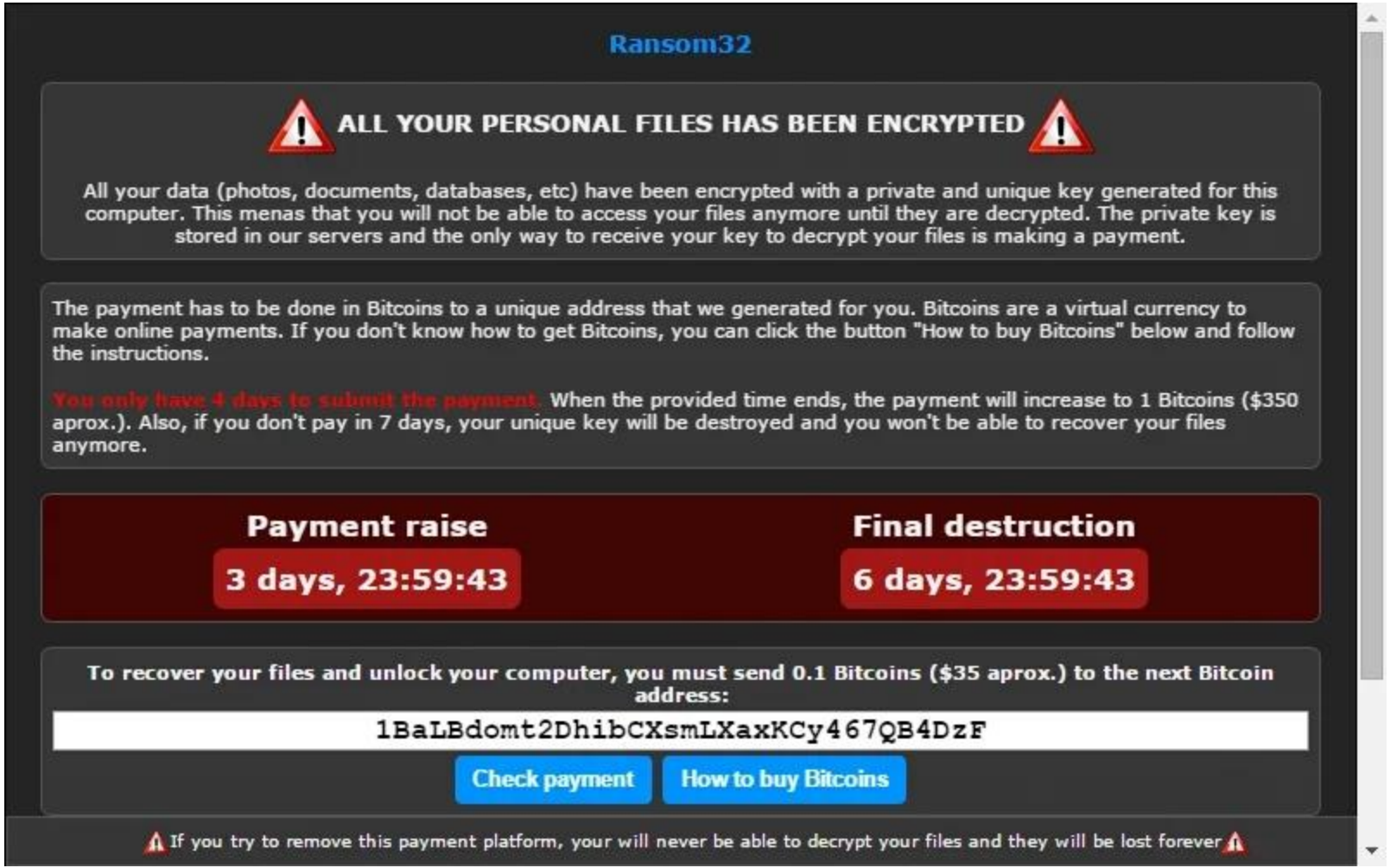
Intrusions

- Simple passwords
- Vulnerabilities
- Weak configurations
- Clicking on attachments
- Open infected programs

Why?

Why?

- Spam
- Botnet


Ransom32
ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED
All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This menas that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.
The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can click the button "How to buy Bitcoins" below and follow the instructions.
You only have 4 days to submit the payment. When the provided time ends, the payment will increase to 1 Bitcoins ($350 aprox.). Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.
Payment raise
3 days, 23:59:43
Final destruction
6 days, 23:59:43
To recover your files and unlock your computer, you must send 0.1 Bitcoins ($35 aprox.) to the next Bitcoin address:
1BaLBdomt2DhibCXsmLXaxKCy467QB4DzF
Check payment
How to buy Bitcoins
If you try to remove this payment platform, your will never be able to decrypt your files and they will be lost forever

Types

Types

- Virus
- Worm
- Backdoor
- Dropper
- Rootkit

Rootkits 101

Rootkits

- (become | stay) **root**
- (software) **kit**

Rootkits

- Stealth
- Persistence
- Backdoor

How to be the best rootkit?

Hiding ★

In plain sight!

/etc/sysconfig/…

/tmp/mysql.sock

/bin/audiocnf

Hiding ★★

Slightly advanced

- Rename processes
- Delete file from disk
- Backdoor binaries

Hiding ★★★

Advanced

- Kernel modules
- Change system calls
- Hidden passwords

Demo

Demo

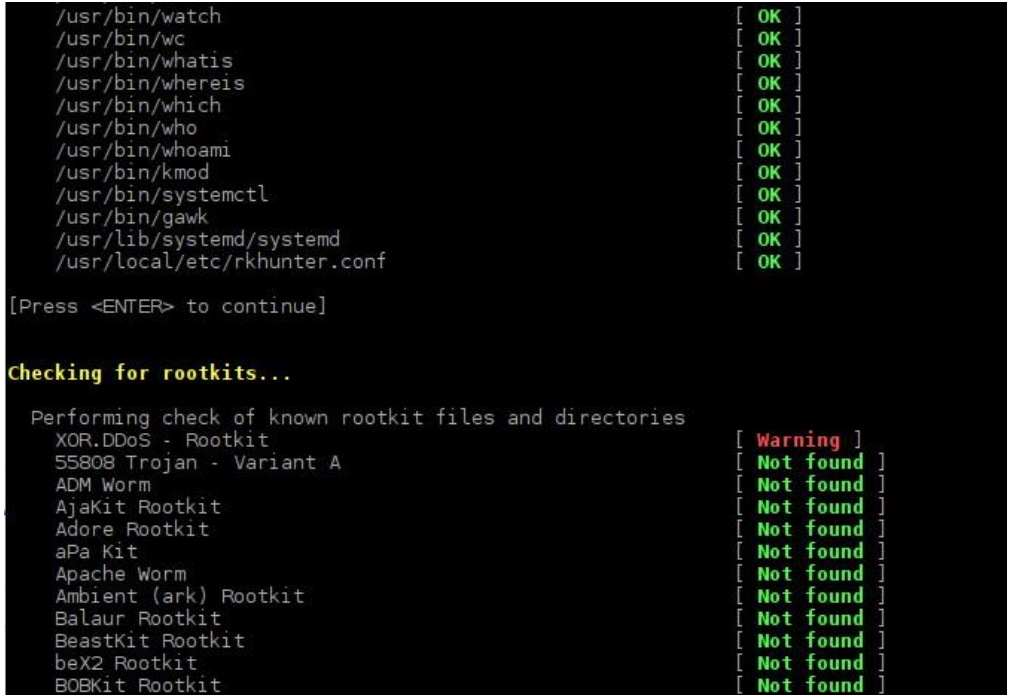
```
[root@centos tmp]# ls -l
total 384
-rw-r--r--. 1 root root 390521 Feb  3 12:31 backdoor.ko
[root@centos tmp]# insmod backdoor.ko
[root@centos tmp]# lsmod | grep backdoor
[root@centos tmp]# ls /proc | grep backdoor
[root@centos tmp]# ls -l
total 0
```

Demo

```
[root@centos tmp]# ls -l
total 0
[root@centos tmp]# touch hideme
[root@centos tmp]# ls -l
total 0
-rw-r--r--. 1 root root 0 Feb  3 12:36 hideme
[root@centos tmp]#
[root@centos tmp]# touch HIDEme
[root@centos tmp]# ls -l
total 0
-rw-r--r--. 1 root root 0 Feb  3 12:36 hideme
```

Rootkit Hunter

Detect the undetectable!

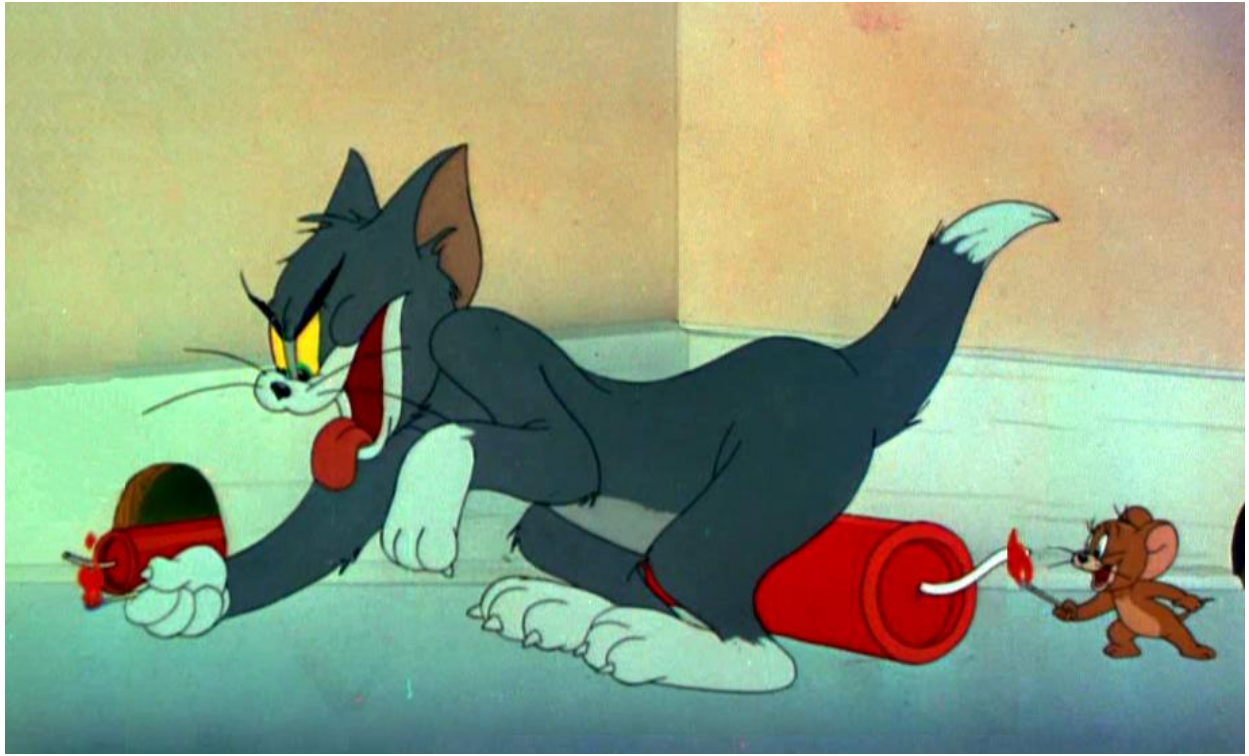



disneyscreencaps.com

Challenges

- We can’t trust **anything**
- Even ourselves
- No guarantees

Continuous Game



Defense

Defenses

At least

- Perform security scans
- Protect your data
- System hardening

Scanning » Scanners

- Viruses → **ClamAV**
- Backdoors → **LMD**
- Rootkits → **Chkrootkit / rkhunter**

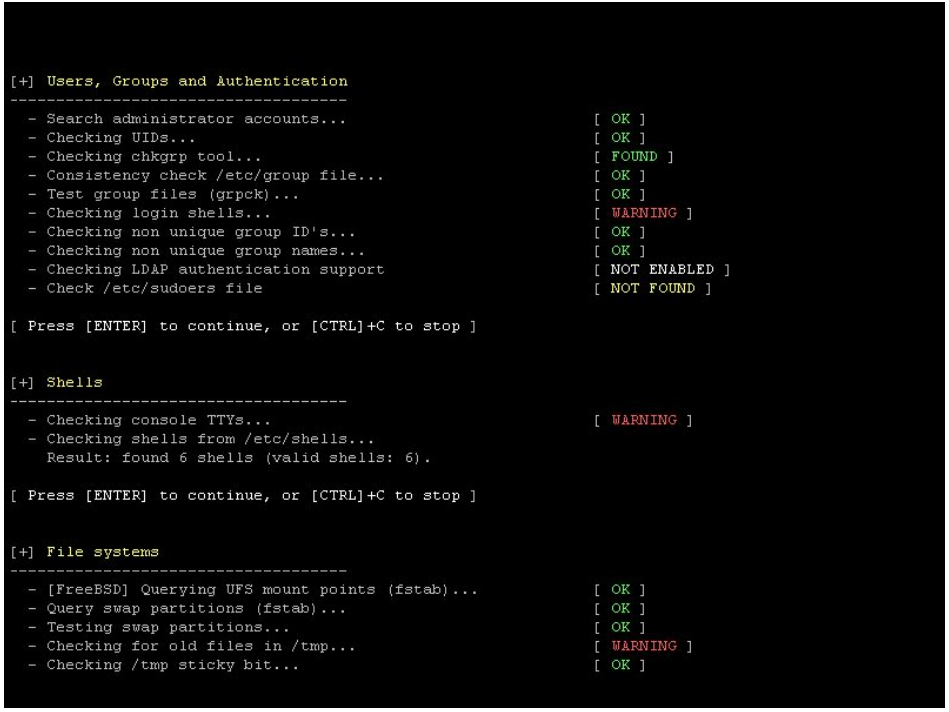
Scanning » File Integrity

- Changes
- Powerful detection
- Noise

AIDE / Samhain

System Hardening » Lynis

- Linux / UNIX
- Open source
- Shell
- Health scan



Conclusions

Conclusions

- Challenge: rootkits are hard to detect
- Prevent: system hardening
- Detect: recognize quickly, and act

Success!

You finished this presentation

More Linux security?

Presentations

michaelboelen.com/presentations/

Follow

- Blog — Linux Audit (linux-audit.com)
- Twitter — @mboelen