

Linux Malware

Looks don't matter

Michael Boelen

michael.boelen@cisofy.com

2016-07-06

's-Hertogenbosch, The Netherlands

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)
- 180+ 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 means 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, you will never be able to decrypt your files and they will be lost forever 

Can't find the files that you need?
Is the content of your files that you need, unreadable?
This is normal because the data within your files has been encrypted.

Congratulations!!
You have become a part of an exclusive community, [BashCrypt](#)

If you are reading this text, that means that the software, BashCrypt, has been installed on your system.

What is encryption?
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons, but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible, e.g. - to be able to decrypt your files, you need to have a special private key.
Additionally, you require the corresponding decryption software with which your files will return to its original form.

I almost understand, but what do I have to do?
The first thing you should do is to read the instructions to end.
Your files have been encrypted with the BashCrypt software. The instructions that you find within your folders, along with your encrypted files, are not infected with malware, but rather they are to assist you.
After reading this text, 100% of people turn to their favorite search engine with the word BashCrypt where you'll find a lot of thoughts, ideas, and instructions.
Think logically - we are the ones who have locked your files and the only ones who can decrypt your files.
Any attempts to restore your files with third-party software or tools can be fatal for your encrypted files.
The fact of the matter is that changing the data within the encrypted files, as 100% of file restoration software and tools do, will irrevocably break your files and make them irrecoverable. Only our special software can restore your files.
Do not reboot your system as your core operating systems have been encrypted. Rebooting will make restoration of your system and files impossible.
Please be weary that attempting to load recovery media via USB or CD-ROM has been disabled. Attempting to do so will result in the corruption of your data.

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

Little 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!

```
/usr/bin/watch [ OK ]
/usr/bin/wc [ OK ]
/usr/bin/whatis [ OK ]
/usr/bin/whereis [ OK ]
/usr/bin/which [ OK ]
/usr/bin/who [ OK ]
/usr/bin/whoami [ OK ]
/usr/bin/kmod [ OK ]
/usr/bin/systemctl [ OK ]
/usr/bin/gawk [ OK ]
/usr/lib/systemd/systemd [ OK ]
/usr/local/etc/rkhunter.conf [ OK ]

[Press <ENTER> to continue]

Checking for rootkits...

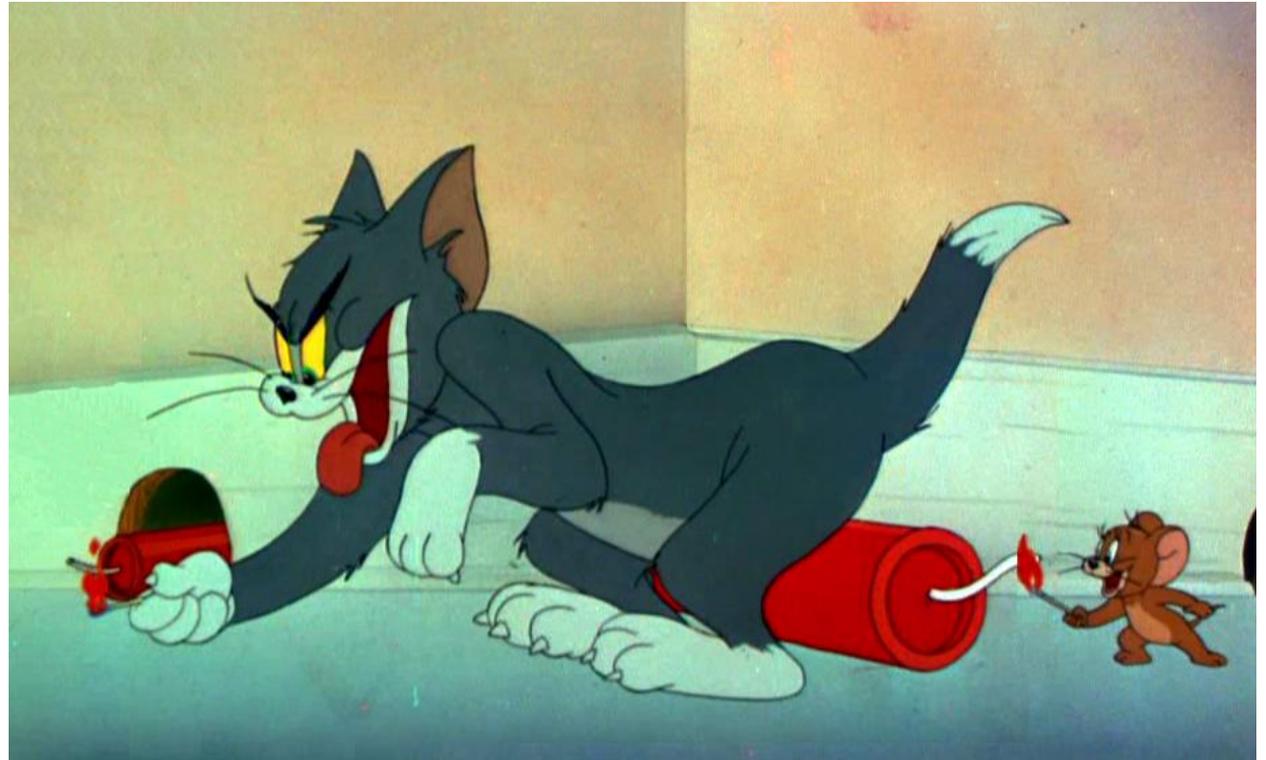
Performing check of known rootkit files and directories
XOR.DDoS - Rootkit [ Warning ]
55808 Trojan - Variant A [ Not found ]
ADM Worm [ Not found ]
AjaKit Rootkit [ Not found ]
Adore Rootkit [ Not found ]
aPa Kit [ Not found ]
Apache Worm [ Not found ]
Ambient (ark) Rootkit [ Not found ]
Balaur Rootkit [ Not found ]
BeastKit Rootkit [ Not found ]
beX2 Rootkit [ Not found ]
BOBKit Rootkit [ Not found ]
```



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

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts...           [ OK ]
- Checking UIDs...                           [ OK ]
- Checking chkgrp tool...                    [ FOUND ]
- Consistency check /etc/group file...       [ OK ]
- Test group files (grpck)...                [ OK ]
- Checking login shells...                   [ WARNING ]
- Checking non unique group ID's...         [ OK ]
- Checking non unique group names...        [ OK ]
- Checking LDAP authentication support      [ NOT ENABLED ]
- Check /etc/sudoers file                   [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Shells
-----
- Checking console TTYS...                   [ WARNING ]
- Checking shells from /etc/shells...
  Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] File systems
-----
- [FreeBSD] Querying UFS mount points (fstab)... [ OK ]
- Query swap partitions (fstab)...           [ OK ]
- Testing swap partitions...                 [ OK ]
- Checking for old files in /tmp...          [ WARNING ]
- Checking /tmp sticky bit...               [ OK ]
```

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](https://linux-audit.com) (linux-audit.com)
- Twitter [@mboelen](https://twitter.com/mboelen)

