FinFisher

New techniques and infection vectors revealed

ENJOY SAFER TECHNOLOGY™

FINFISHER GMBH
BAIERBRUNNER STRASSE 15
81379 MUNICH
GERMANY

TEL +49 89 785 761 75
INFO@FINFISHER.COM

WWW.FINFISHER.COM

GAMMAGROUP

Home • Company Profile • Contact Us

Tactical Comms Monitoring

We provide law enforcement agencies with solutions to overcome the challenges of tactical off-air monitoring by identifying, locating and intercepting targets within 2G/3G/4G Networks

Strategic Comms Monitoring

We provide our clients with strategic Turnkey monitoring solutions that can capture, process and analyze all types of information sent over a wide spectrum of telecommunications networks

Gamma Group

Gamma Group is an international manufacturer of surveillance & monitoring systems with technical and sales offices in Europe, Asia, the Middle East and Africa. We provide advanced technical surveillance, monitoring solutions and advanced government training as well as international consultancy to National and State Intelligence Departments and Law Enforcement Agencies.

Through in-house developments and strategic partnerships with many leading security companies, we provide government agencies with customized solutions based on their national security requirements.

Previous research

YOU ONLY CLICK TWICE

FinFisher's Global Proliferation

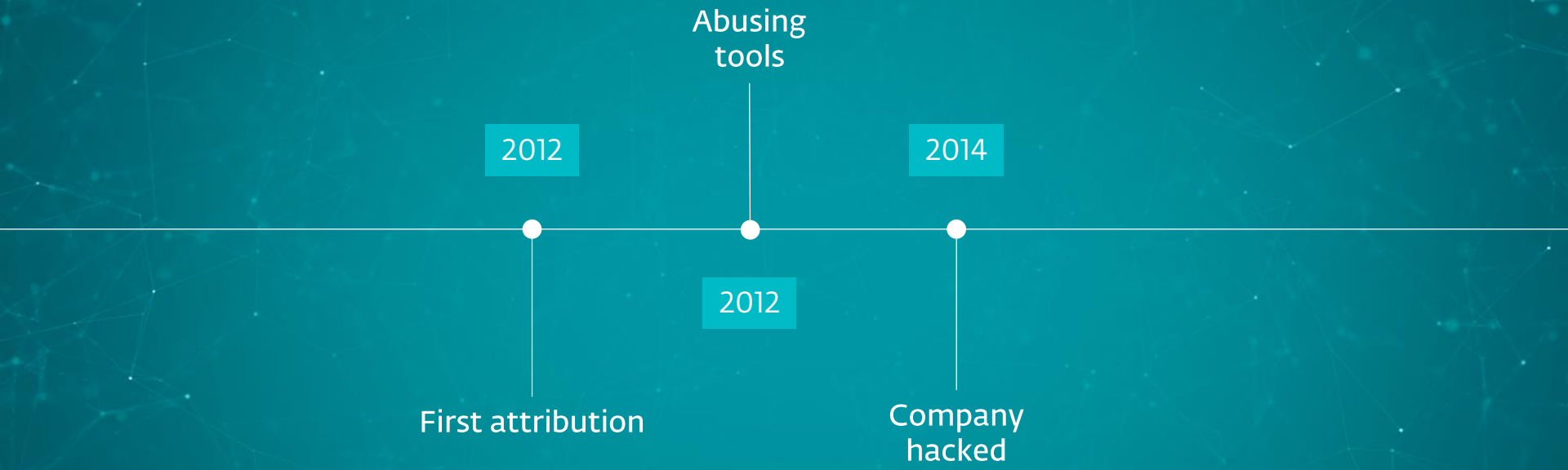
By Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton March 13, 2013

This post describes the results of a comprehensive global Internet scan for the command and control servers of FinFisher's surveillance software. It also details the discovery of a campaign using FinFisher in Ethiopia used to target individuals linked to an opposition group. Additionally, it provides examination of a FinSpy Mobile sample found in the wild, which appears to have been used in Vietnam.

Summary of Key Findings

- We have found command and control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in a total of 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.
- A FinSpy campaign in Ethiopia uses pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. This continues the theme of FinSpy deployments with strong indications of politically-motivated targeting.
- There is strong evidence of a Vietnamese FinSpy Mobile Campaign. We found an Android FinSpy Mobile sample in the wild with a command & control server in Vietnam that also exfiltrates text messages to a local phone number.
- These findings call into question claims by Gamma International that previously reported servers were *not* part of their product line, and that previously discovered copies of their software were either stolen or demo copies.

Previous research



(on 2014-09-15)

SpyFiles 4

Release | Documents | Customers | Database

Today, 15 September 2014, WikiLeaks releases previously unseen copies of weaponised German surveillance malware used by intelligence agencies around the world to spy on journalists, political dissidents and others.

FinFisher (formerly part of the UK based Gamma Group International until late 2013) is a German company that produces and sells computer intrusion systems, software exploits and remote monitoring systems that are capable of intercepting communications and data from OS X, Windows and Linux computers as well as Android, iOS, BlackBerry, Symbian and Windows Mobile devices. FinFisher first came to public attention in December 2011 when WikiLeaks published documents detailing their products and business in the first SpyFiles release.

Since the first SpyFiles release, researchers published reports that identified the presence of FinFisher products in countries around the world and documented its use against journalists, activists and political dissidents.

Julian Assange, WikiLeaks Editor in Chief said: "FinFisher continues to operate brazenly from Germany selling weaponised surveillance malware to some of the most abusive regimes in the world. The Merkel government pretends to be concerned about privacy, but its actions speak otherwise. Why does the Merkel government continue to protect FinFisher? This full data release will help the technical community build tools to protect people from FinFisher including by tracking down its command and control centers."

FinFisher Relay and **FinSpy Proxy** are the components of the FinFisher suite responsible for collecting the data acquired from the infected victims and delivering it to their controllers. It is commonly deployed by FinFisher's customers in strategic points around the world to route the collected data through an anonymizing chain, in order to disguise the identity of its operators and the real location of the final storage, which is instead operated by the **FinSpy Master**.

File Name	Product Name	MD5	File Size
ffrelay-debian-4.30.ggi.zip	FinFisher Relay v4.30	180caf23dd71383921e368128fb6db52	224K
finspy_proxy.zip	FinSpy Proxy v2.10	3dfdac1304eeaaaff57cc11317768511	320K
finspy_master.zip	FinSpy Master v2.10	03d93c49a536d149206f5524d87fa319	2.5M

WikiLeaks is also publishing previously unreleased copies of the **FinFisher FinSpy PC** spyware for Windows. This software is designed to be covertly installed on a Windows computer and silently intercept files and communications, such as Skype calls, emails, video and audio through the webcam and microphone (you can find more details on FinSpy in the first SpyFiles release). In order to prevent any accidental execution and infection, the following files have been renamed and compressed in password protected archives (the password is "infected"). They are weaponised malware, so handle carefully.

File Name	Product Name	MD5	File Size
finfisher.1.zip	FinSpy PC	2d5c810035dc0f83036fb12e8775817a	736K
finfisher.2.zip	FinSpy PC	434b83eba7619cb706492ff019ade0d5	576K

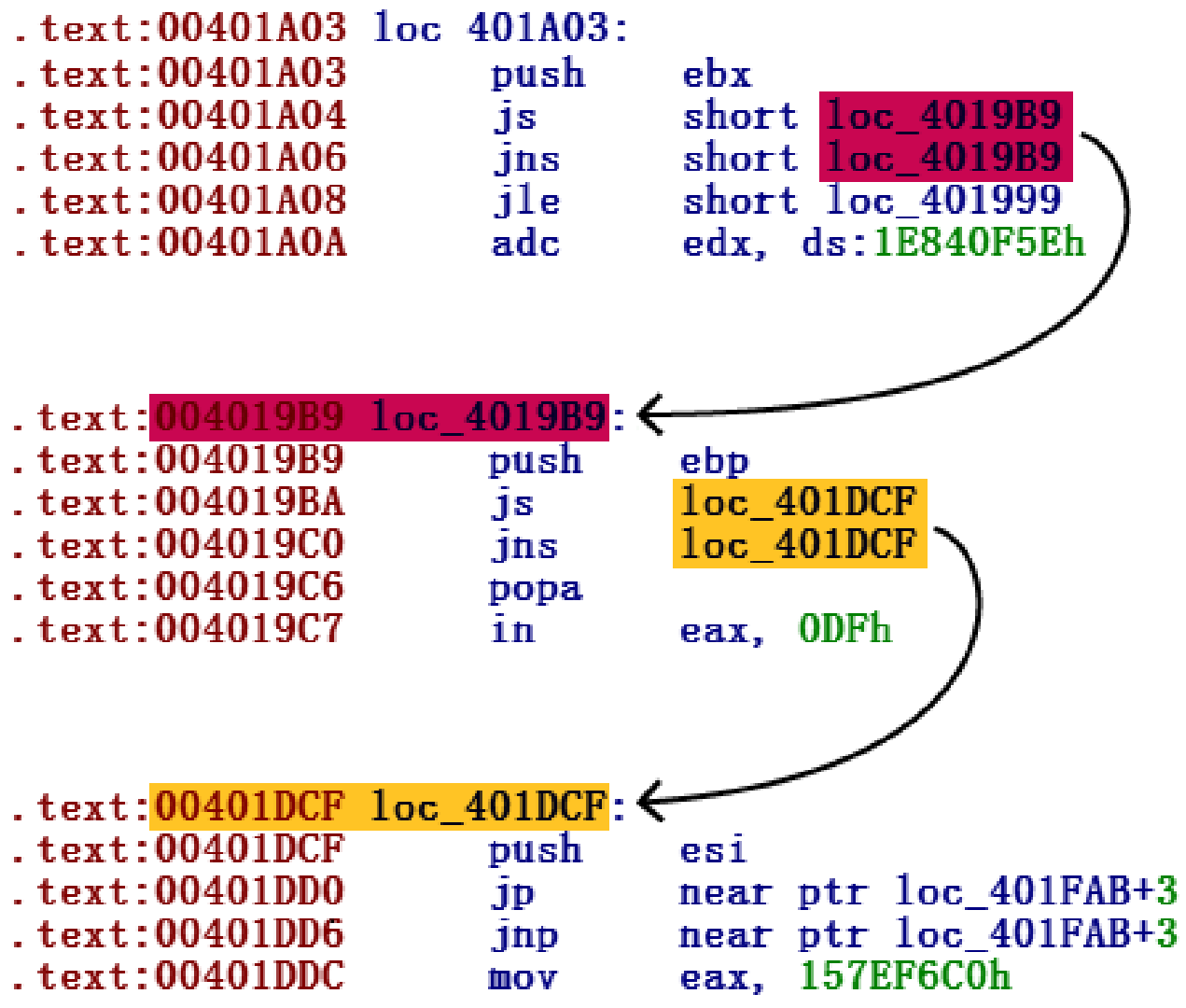
SpyFiles

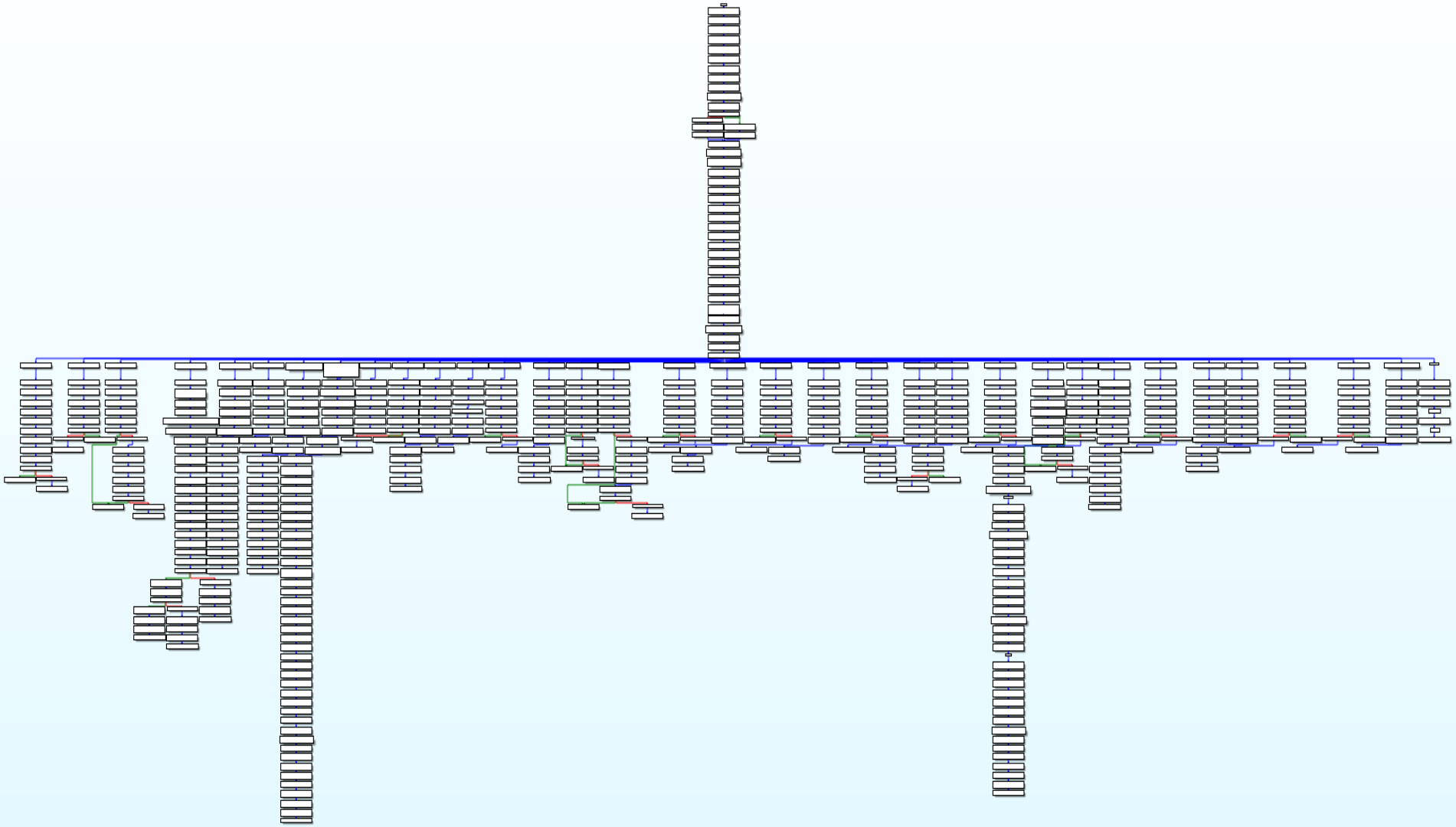
Previous SpyFiles releases:
SpyFiles 1 - 2011-12-01
SpyFiles 2 - 2011-12-08
SpyFiles 3 - 2013-09-04

Previous research

Technical improvements

- Anti-disassembly
- Custom virtual machine
- Anti-emulation
- Anti-sandbox
- Anti-virtual machine
- Anti-debug

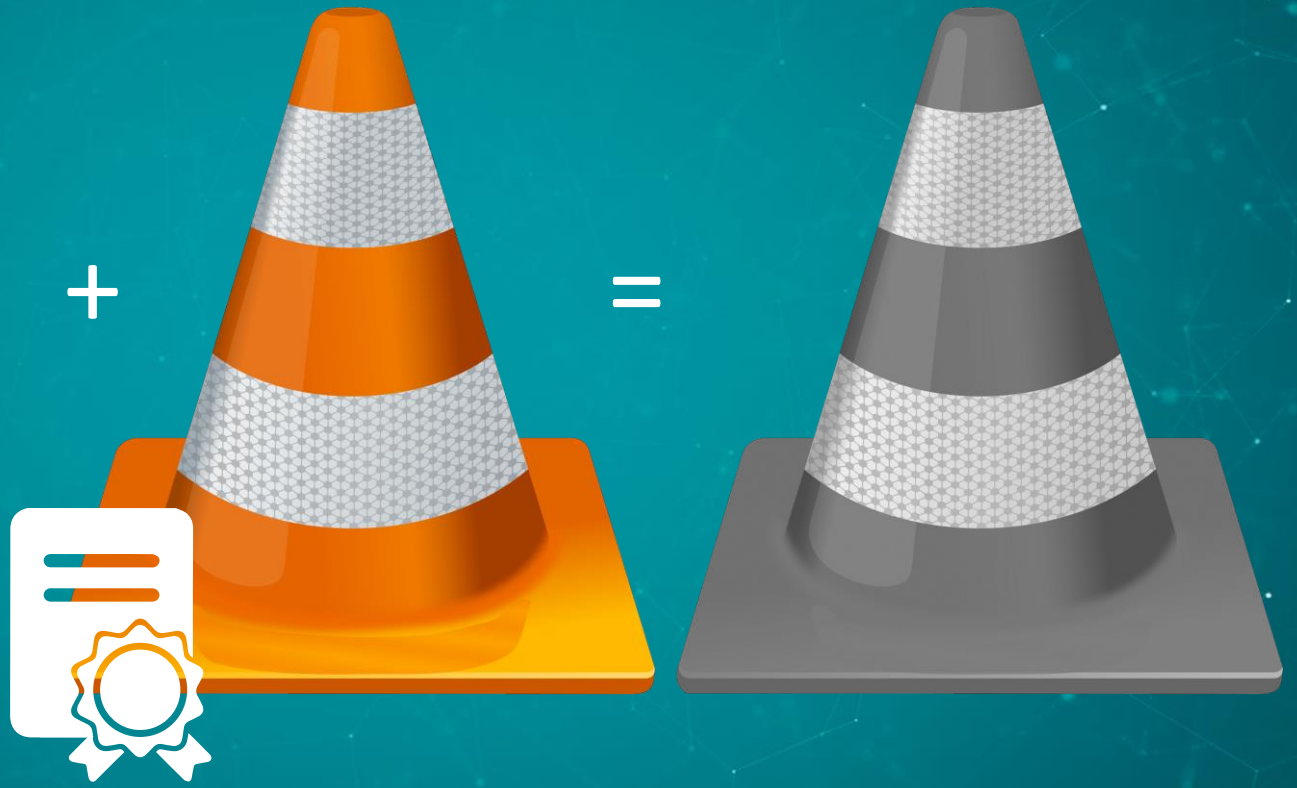

.text:00401A03 loc_401A03:
.text:00401A03 push ebx
.text:00401A04 js short loc_4019B9
.text:00401A06 jns short loc_4019B9
.text:00401A08 jle short loc_401999
.text:00401A0A adc edx, ds:1E840F5Eh
.text:004019B9 loc_4019B9:
.text:004019B9 push ebp
.text:004019BA js loc_401DCF
.text:004019C0 jns loc_401DCF
.text:004019C6 popa
.text:004019C7 in eax, 0DFh
.text:00401DCF loc_401DCF:
.text:00401DCF push esi
.text:00401DD0 jp near ptr loc_401FAB+3
.text:00401DD6 jnp near ptr loc_401FAB+3
.text:00401DDC mov eax, 157EF6C0h



```
1251: MOV EAX, [FS:0x30]
1252: xor REG, REG
1253: add REG, EAX
1254: add REG, 0x8
1255: mov REG, [REG]
1256: mov EAX, REG ; ImageBase
1257: xor REG, REG
1258: add REG, EAX
1259: add REG, 0x3C
125A: mov REG, [REG]
125B: mov ECX, REG ; offset to NT header
125C: TEST BYTE [ECX+EAX+0x8], 0x1 ; Time Stamp
125D: jnz loc_81
125E: call ImageBase+0x670B (0x40670B - 1738) ; AntiVM
125F: TEST EAX, EAX
1260: jz loc_81
1261: mov REG, EDI
1262: push REG
1263: call ImageBase+0x8BCD (0x408BCD - 2C70 - exit)
**loc_81:
1264: MOV EBX, 0x208
```

```
.text:00404B3F                 push    esi
.text:00404B40                 mov     esi, ds:GetTickCount
.text:00404B46                 push    edi
.text:00404B47                 call    esi ; GetTickCount
.text:00404B49                 push    1
.text:00404B4B                 mov     edi, eax
.text:00404B4D                 call    ds:Sleep
.text:00404B53                 call    esi ; GetTickCount
.text:00404B55                 sub     eax, edi
.text:00404B57                 cmp     eax, 4000
.text:00404B5C                 pop     edi
.text:00404B5D                 pop     esi
.text:00404B5E                 ja      short loc_404B68
.text:00404B60                 cmp     eax, 1
.text:00404B63                 jz      short loc_404B68
.text:00404B65                 xor     eax, eax
.text:00404B67                 retn
.text:00404B68 ; ---------------------------------------------------------------
.text:00404B68
.text:00404B68 loc_404B68:                             ; CODE XREF: .text
.text:00404B68                                         ; .text:00404B63↑j
.text:00404B68                 push    0
.text:00404B6A                 call    ds:ExitProcess
```

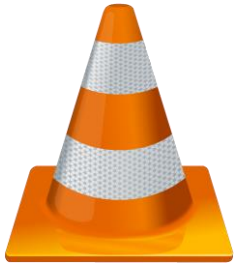
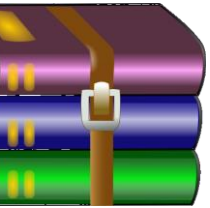
FINFISHER + =











Where is the trojanized application

```
http://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064
```

```
Referer:
http://get.videolan.org/vlc/2.2.4/win32/vlc-2.2.4-win32.exe
```

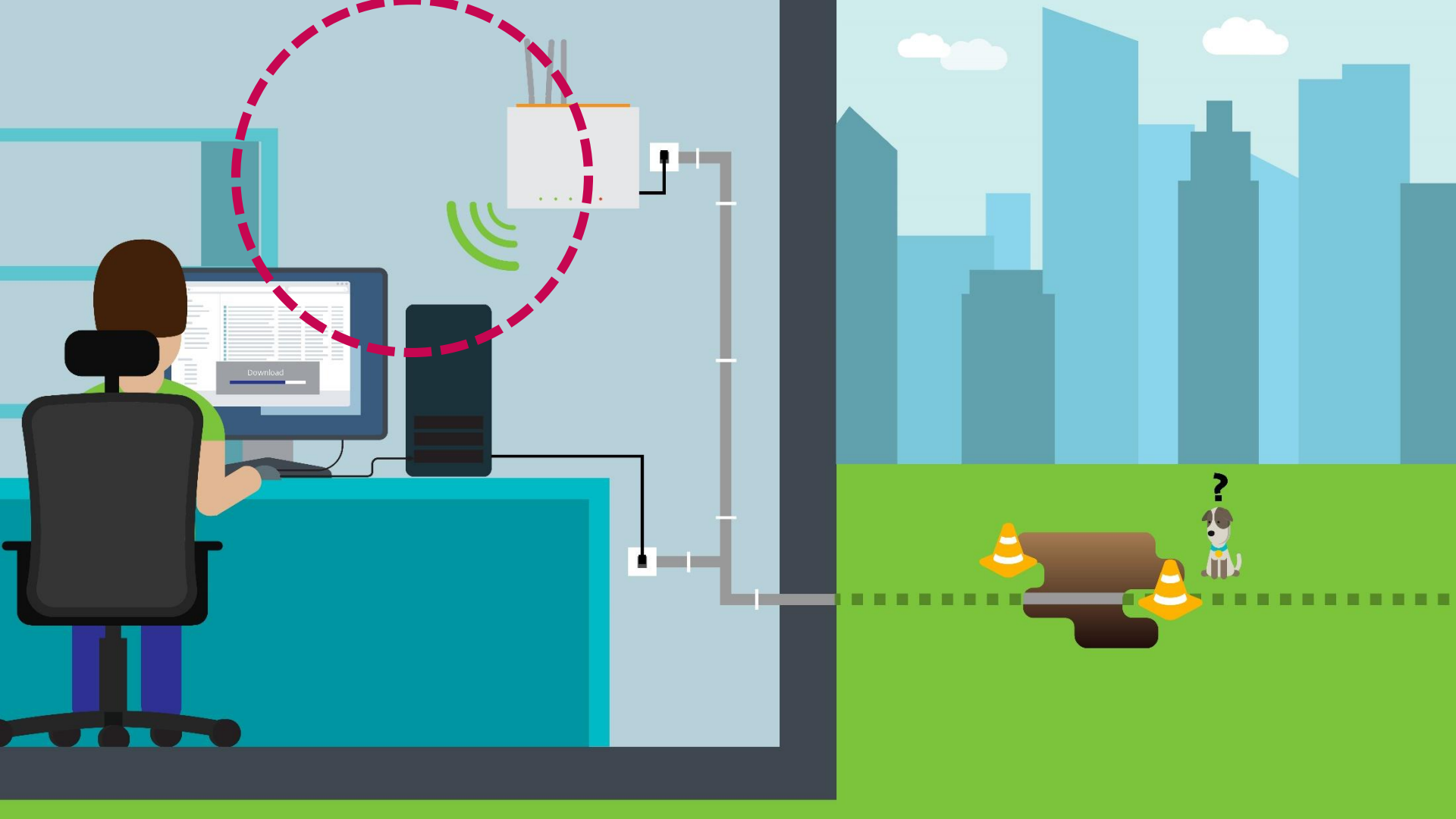
Redirect

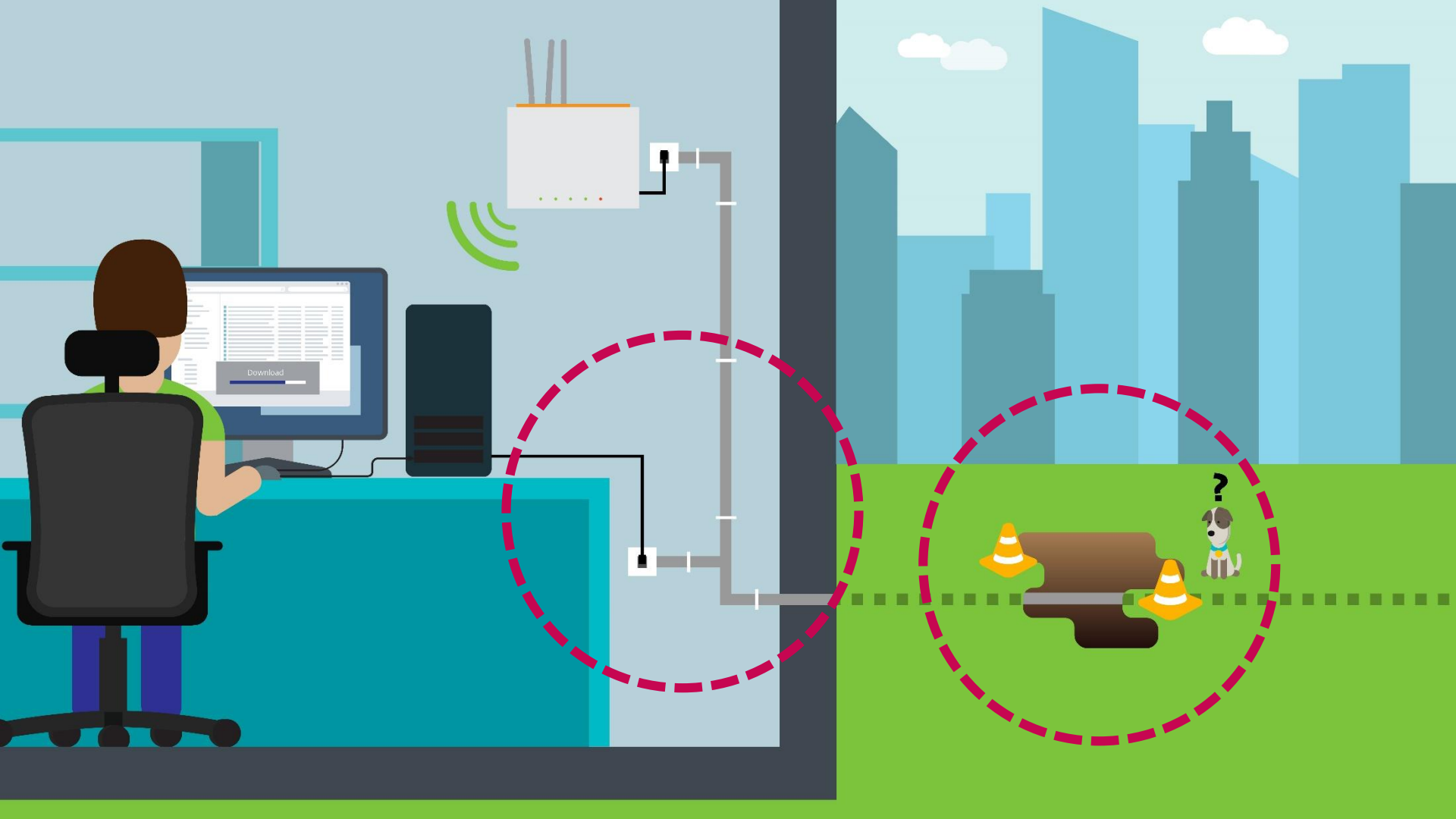
HTTP/1.1 307 Temporary Redirect

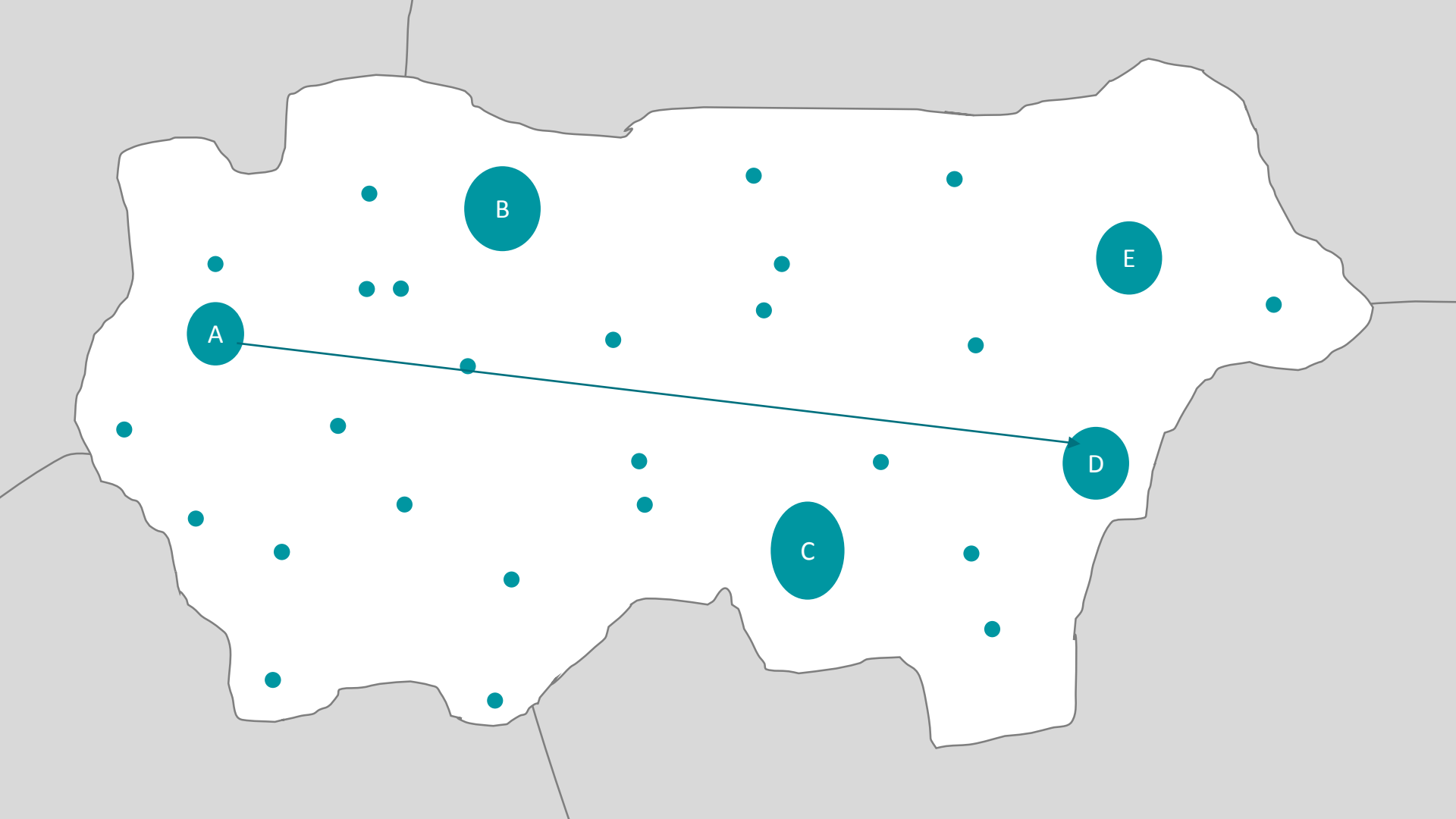
Location: `http://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064`

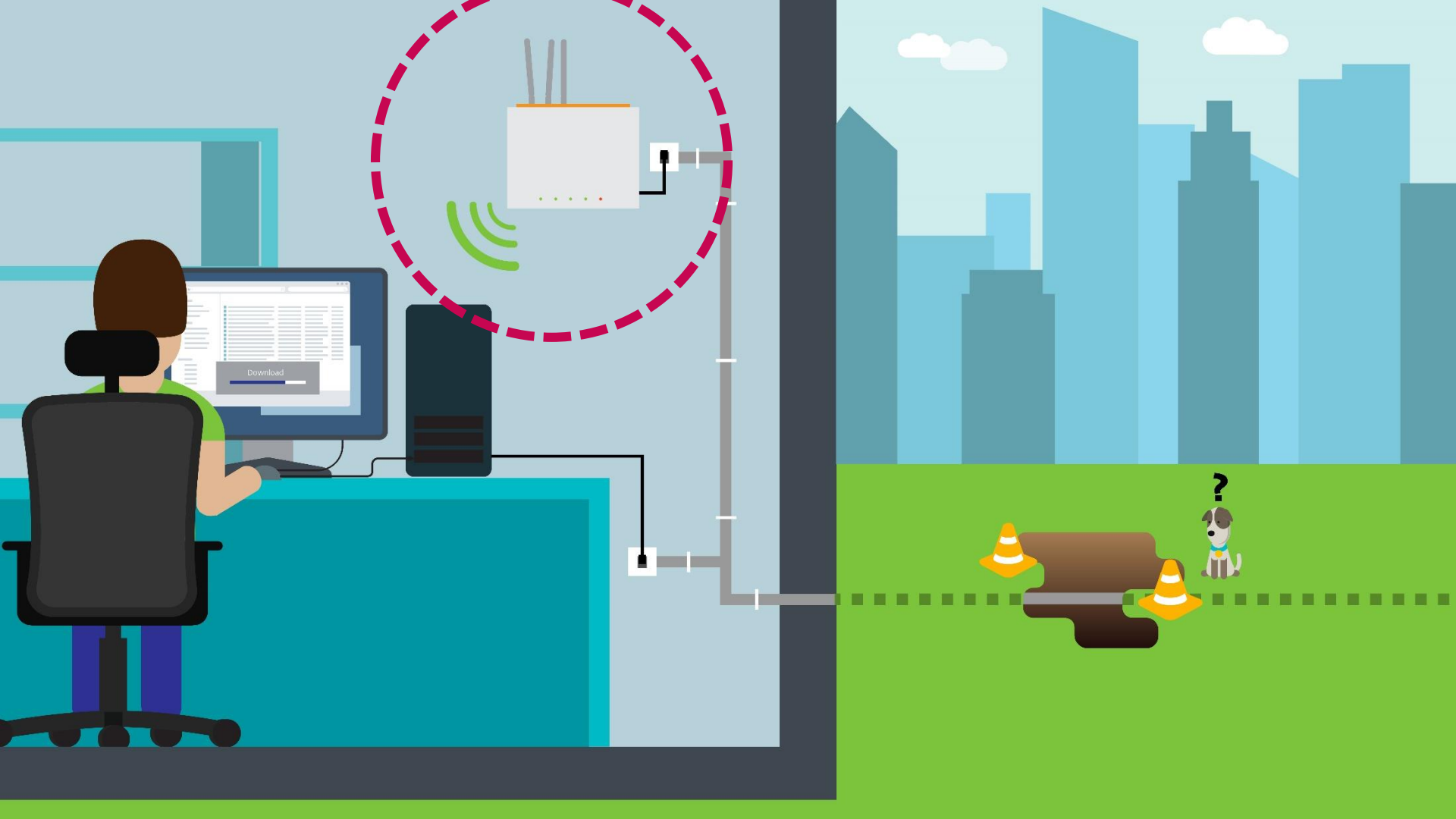
Connection: close

Where is the Man in the MitM attack?


Download
?


Download
?


A
B
C
D
E

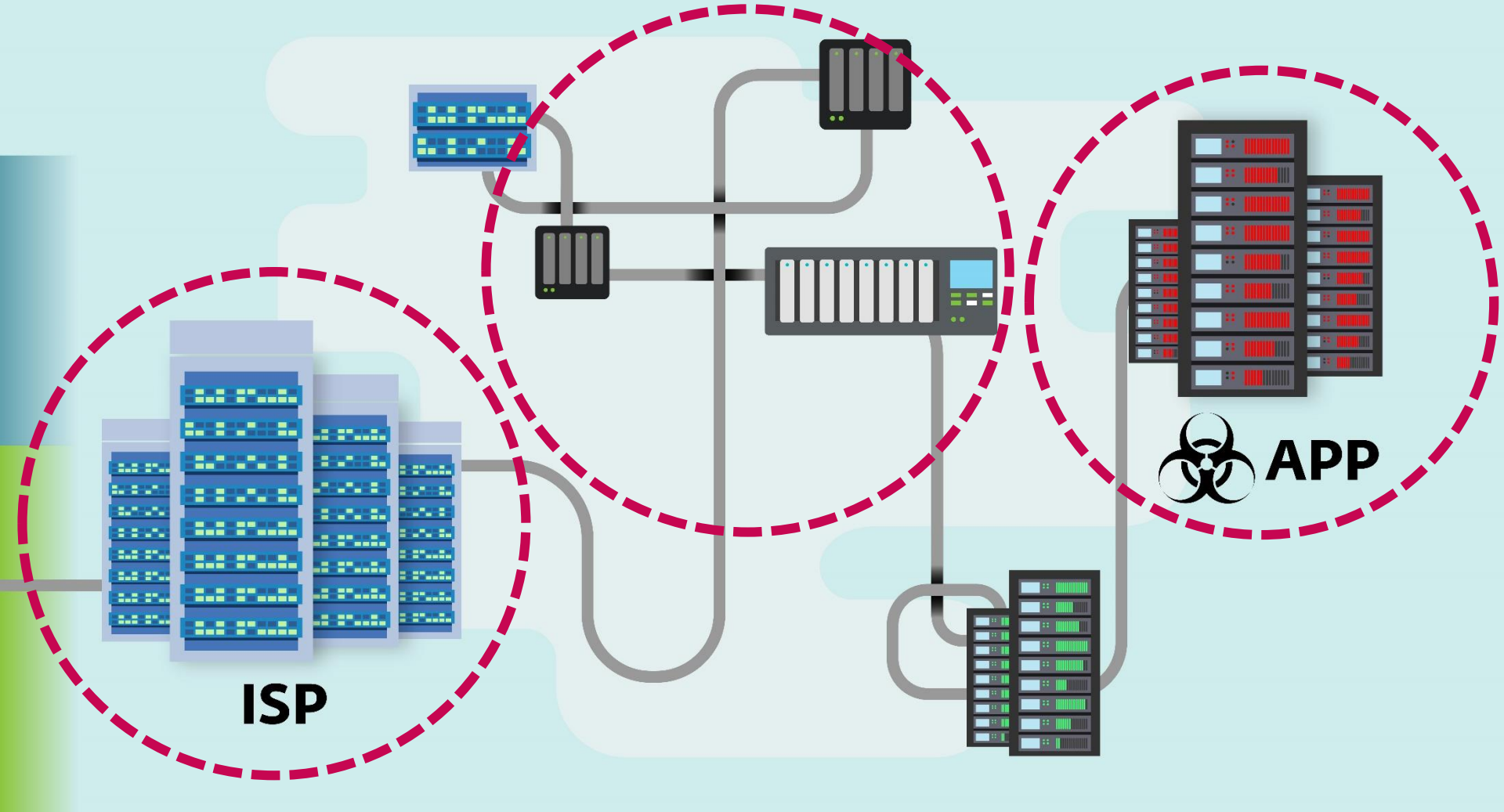

Download
?

Redirect

HTTP/1.1 307 Temporary Redirect

Location: `http://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064`

Connection: close


ISP
APP

Evidence

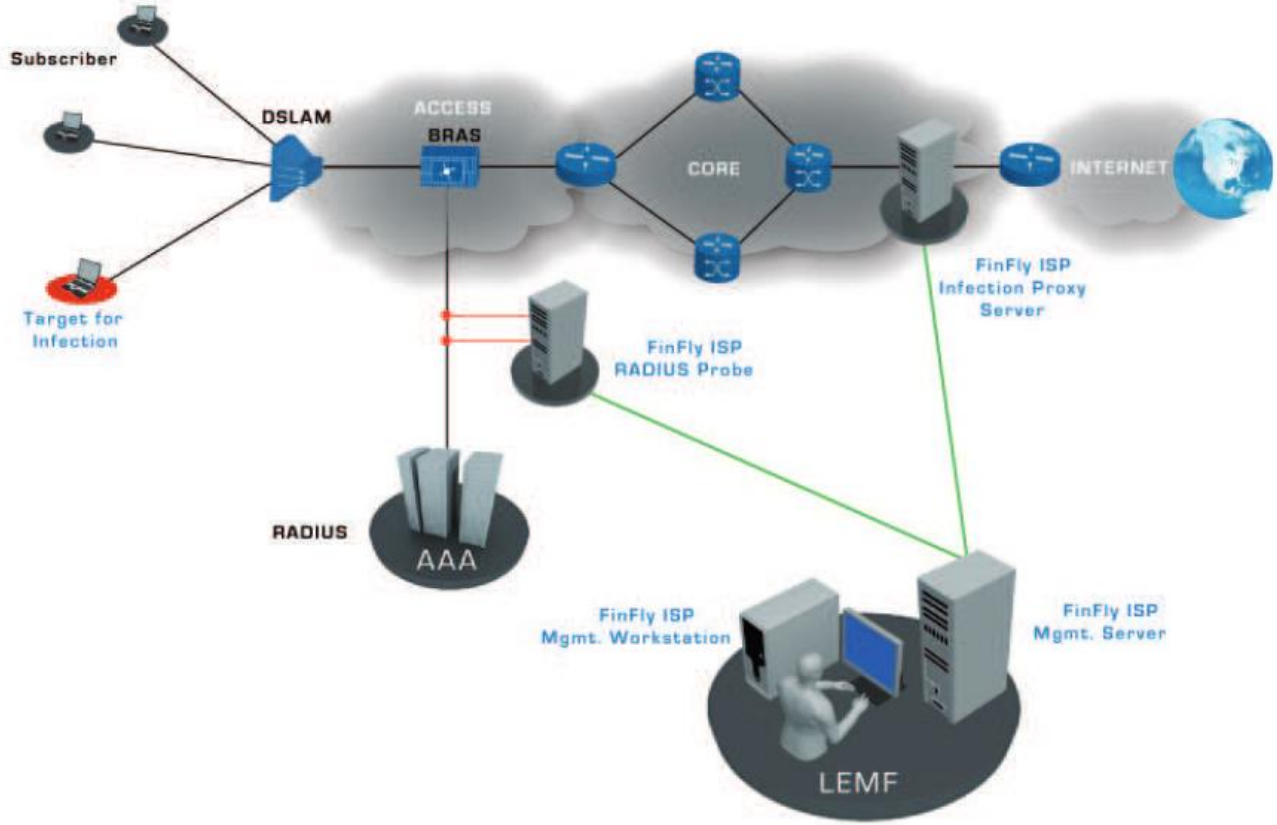
- Geographical dispersion
- All targets are under same ISP

Evidence

- Geographical dispersion
- All targets are under same ISP
- FinFly ISP

Network Setup

Strategic Deployment



Evidence

- Geographical dispersion
- All targets are under same ISP
- FinFly ISP
- Internet content filtering method

What redirects do we know

HTTP redirects, script redirects, replacing content, dns redirect

Script redirects

javascript:

<script>

window.location = "http://URL";

</script>

html:

<meta http-equiv="refresh" content="0; url="http://URL">

Http redirects

30X:

- 301
- 302
- 303
- 307
- 308

Http redirects

30X:

- 301
- 302
- 303
- 307
- 308

HTTP/1.1 307 Temporary Redirect

X-RPHost: zcA2hO9bdp_NBxqOA_OA4A

Location: http://ad.afy11.net/ad?mode=7&publisher_dsp_id=44&external_user_id=IEGO5X2G-17-64G8

Connection: keep-alive

P3P: CP="NOI CURa ADMa DEVa TAIa OUR BUS IND UNI COM NAV INT“

Pragma: no-cache

Cache-Control: no-cache, no-store, must-revalidate

Expires: 0

Content-Length: 0

HTTP/1.1 307 Temporary Redirect

Set-Cookie: c=1; Path=/

Location: /tap.php?cookie_redirect=1&v=4212&nid=1185&put=2360634020977570499&expires=60

P3P: CP="NOI CURa ADMa DEVa TAIa OUR BUS IND UNI COM NAV INT“

Pragma: no-cache

Cache-Control: no-cache, no-store, must-revalidate

Expires: 0

Content-Length: 0

Date: Sat, 05 Sep 2015 04:09:19 GMT

Server: Rubicon Project

HTTP/1.1 307 Temporary Redirect

location: http://api.ge.tt/1/files/6VVQ1ZK2/0/blob?download

Connection: keep-alive

Content-Length: 0

ISP content filtering:

HTTP/1.1 307 Temporary Redirect

Location: http://some.url/that_we/needed_to_redact

Connection: close

Redirect to trojanized application:

HTTP/1.1 307 Temporary Redirect

Location: http://malicious.url/the_browser_is_redirected.to

Connection: close

ISP data limit overrun:

HTTP/1.1 307 Temporary Redirect

Location: http://some.url/that_describes/that_you_are/over_limt

Connection: close

HTTP/1.1 307 Temporary Redirect

Location: http://malicious.url/the_browser_is_redirected.to

Connection: close

FinFly ISP

- http://adf.ly/17QWpp
- http://www.cracksurl.com/2015/08/winrar-with-keygen.html
- http://7petabytes.com/19-8-2016/winrar-x64-540.exe

Skill of operators

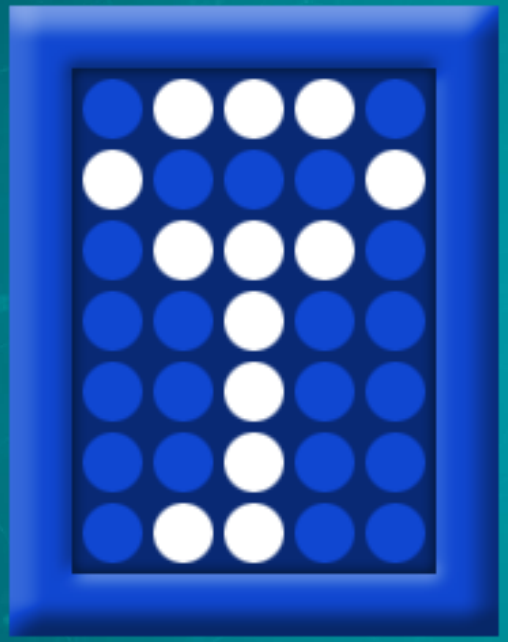
- All redirects to: `http://download.downloading.shop/pcdownload.php?a=MD5_hash`
- Example: `http://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064`

First redirect spotted

2016-04-17

Benefits of “ISP assisted” distribution malware

Privacy concerned people



TrueCrypt.exe

Threema.exe

Takeaway

ENJOY SAFER TECHNOLOGY™

THANK YOU!

Filip Kafka
filip.kafka@eset.sk

www.eset.com | www.welivesecurity.com