REPURPOSING BUILDOUKE

A SINGLE CASE STUDY AROUND REUSING NOTION STATE MACHINE
BLOCK HOT USA 2015

Josh Pitts

NOPSEC

Director of Security Research @ NOPSEC

NOPSEC

Author BDF/BDFProxy

https://github.com/secretsquirrel

NOPSEC

Outline

- Repurposing of malware in the media
- OnionDuke discovery
- OnionDuke packer reverse engineering
- OnionDuke repurposing
- Demos

NOPSEC

Repurposing

http://www.designforrepurposing.com/wp-content/uploads/2011/10/repurposed-hooks-by-etsy-980x300.jpg

Kim Jong-Un Named *The Onion*'s Sexiest Man Alive For 2012 [UPDATE]

NEWS
November 14, 2012
VOL 48 ISSUE 46
North Korea · Lifestyle

Sony Attack 2014

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

NOPSEC

Sony Attack 2014

- Named “Destover"

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

NOPSEC

Sony Attack 2014

- Named “Destover"
- Shared Command and control servers as Volgmer used when attacking South Korean targets [2014]

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

NOPSEC

Sony Attack 2014

- Named “Destover"
- Shared Command and control servers as Volgmer used when attacking South Korean targets [2014]
- Similar file names and techniques to malware in the DarkSoul/Jokra attacks (2013)

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

NOPSEC

Sony Attack 2014

- Named “Destover"
- Shared Command and control servers as Volgmer used when attacking South Korean targets [2014]
- Similar file names and techniques to malware in the DarkSoul/Jokra attacks (2013)
- Similar non-malicious drivers to the malware in the Shamoon attacks [2012]

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

Sony Attack 2014

- Named “Destover"
- Shared Command and control servers as Volgmer used when attacking South Korean targets [2014]
- Similar file names and techniques to malware in the DarkSoul/Jokra attacks (2013)
- Similar non-malicious drivers to the malware in the Shamoon attacks [2012]
- NSA used ‘Wiper’ malware similar to the Sony and other attacks (2012)

http://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

http://www.pcworld.idg.com.au/article/564189/report-nsa-only-creates-also-hijacks-malware/

NOPSEC

EQUATION GROUP and The NSA

- 2009 Google asks NSA for help with the Aurora intrusion
- 2015 Kaspersky Report “The EQUATION Group”:
  - Uses the Aurora exploit in Afghanistan [CVE-2013-3918]
  - Two Exploits associated with Stuxnet [MS09-025 and CVE-2010-2568]

http://www.wired.com/2010/02/google-seeks-nsa-help/

https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

NOPSEC

More NSA

- Leveraged South Korean implants on North Korean networks (2012)

- Leveraged existing command and control networks to deploy their implants (2012)

- Repurposed a captured zero day exploit in passive collection (2012)

http://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/

NOPSEC

¯_(ツ)_/¯

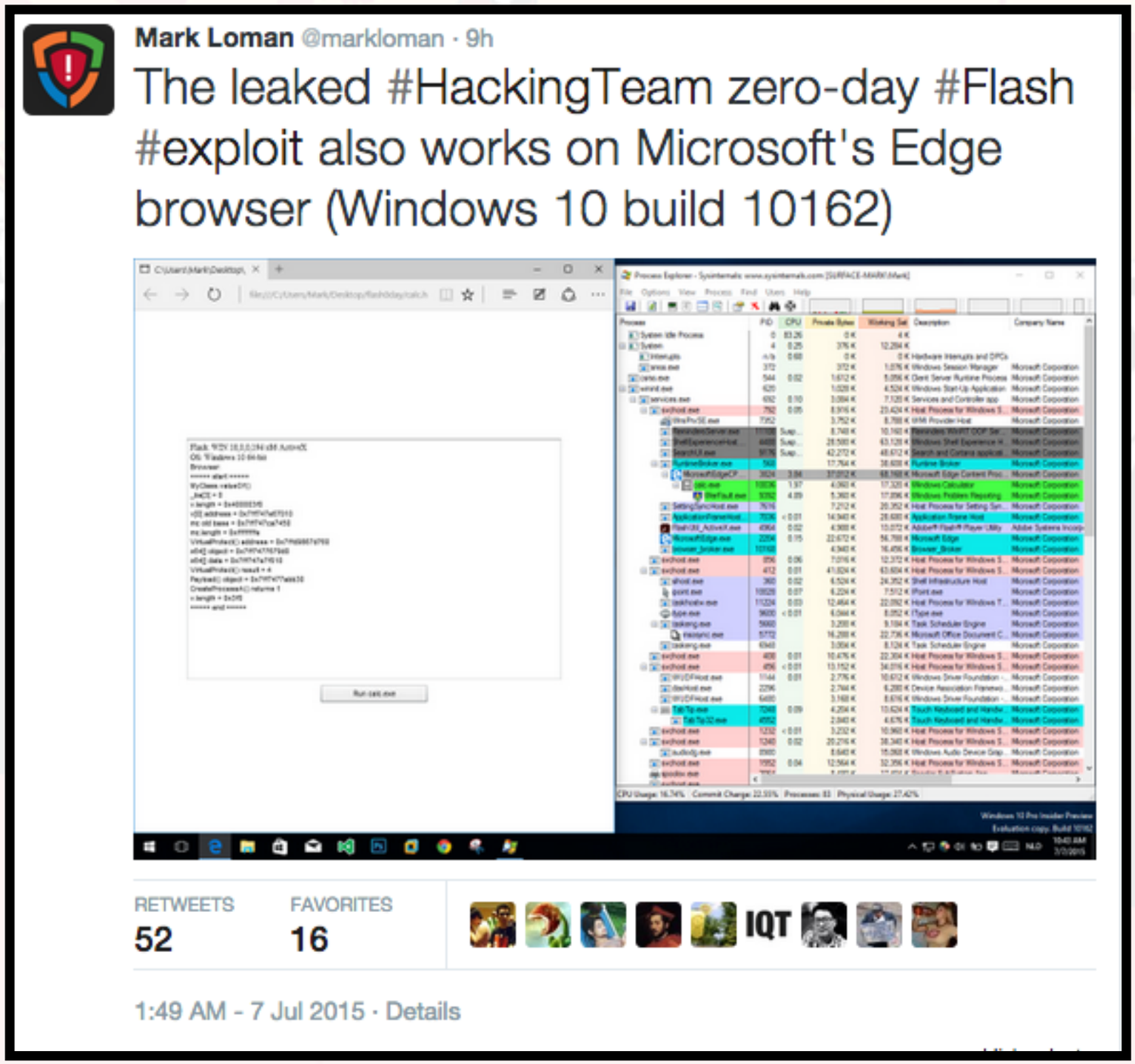
Reuse in Crime

- Snake - 12 reused components
- BlackPOS - eight reused components
- Gyges - eight reused components
- Dragonfly - six reused components
- ZBerp - four reused components

http://www.cyactive.com/wp-content/uploads/2014/12/Infamous-5-Final-SM-15.12-Sony.pdf

NOPSEC

HackingTeam



NOPSEC

HackingTeam

metasploit-framework / modules / exploits / multi / browser / **adobe_flash_hacking_team_uaf.rb**

wchen-r7 6 hours ago Add more requirement info

1 contributor

https://github.com/rapid7/metasploit-framework/blob/d30688b1166e37e9f055bf6c13d80dd0e9fbbc79/modules/exploits/multi/browser/adobe_flash_hacking_team_uaf.rb

NOPSEC

HackingTeam

#	Result	IP	Protocol	Host	URL	Body	Content-...	MD5
1	200	62.109.13.130	HTTP	peoplestyleman.net	/walrus.php?7_3=_kjk6w08fzn1s-i8mdv3_t8&d-05=cs&lv9=yxt7_k04hl&0=8kedgtb34&10h=icfh7a3mf-ba&e4=eoz8qy05vu7&f=nbvpvajd...	107 445	text/html	3e562059f7aaf165d9bb7a9e7e7f7647
2	**200**	**62.109.13.130**	**HTTP**	**peoplestyleman.net**	**/design.xbl?force=eE3EVCC1JE&across=vGjo&structure=gw8s8upaQH&religious=2ZaIbfv8&again=UAP4JrF&six=dc_v...**	**38 692**	**applicati...**	**061c086a4da72ecaf5475c862f178f9d**
3	200	62.109.13.130	HTTP	peoplestyleman.net	/pass.nod?take=yXnjB6NTPQ&she=BnuP3fjWXL&water=PhQGJ4sX&use=&prepare=TnAGBb51d1ool57nBV4v	0	text/html	No body
4	200	62.109.13.130	HTTP	peoplestyleman.net	/research.hdm?may=&become=_s8Wd_&oh=_ccX5SYGMC&possible=5MM_u&remove=mokeJ9&prepare=aPDOtTuO...	186 380	applicati...	54b9802b963b9f14816eedfd3f5c9c5f

Angler EK

CVE-2015-5119
HT 0d

```
GET http://peoplestyleman.net/design.xbl?force=eE3EVCC1JE&across=vGjo&structure=
Accept: */*
Referer: http://peoplestyleman.net/walrus.php?7_3=_kjk6w08fzn1s-i8mdv3_t8&d-05=c
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
DNT: 1
Host: peoplestyleman.net
```

```
HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Tue, 07 Jul 2015 22:07:43 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 38692
Connection: keep-alive
Cache-Control: no-cache, must-revalidate, max-age=1
Pragma: no-cache

CWS
□□□□x□|□□□□H□□F□XŪw□~□□□s□t□lh□□}□}_C□□□□ A□□□□□V□□W□j$□□□Z□J□□□∂́,{▀□%□_□□□□□□□□□U□z/□[□ً2#3"#####□    □[J□bH~□c□□#I□□'□H□γ□□
□□□□□~□□a□□q=□\□$□□9y□1□-□M□s□^HGTH□□□□$□lM□□□-E/h□f□P
□OL□□/□lo□Ar□~□\
4Ūb{□□r□□□Ŗ□@Lr□z□Ẋ@.H□[9g7□□A□
□□□@S^□^\□□□#□<□□ZCqJf□□□□□2□□
□ь□□'□A□Z,%□□□&□&□KW□EY□%y□       □□□□z□□□nD□□□i-□M~Z□□
```

http://malware.dontneedcoffee.com/2015/07/hackingteam-flash-0d-cve-2015-xxxx-and.html

NOPSEC

OnionDuke Backstory

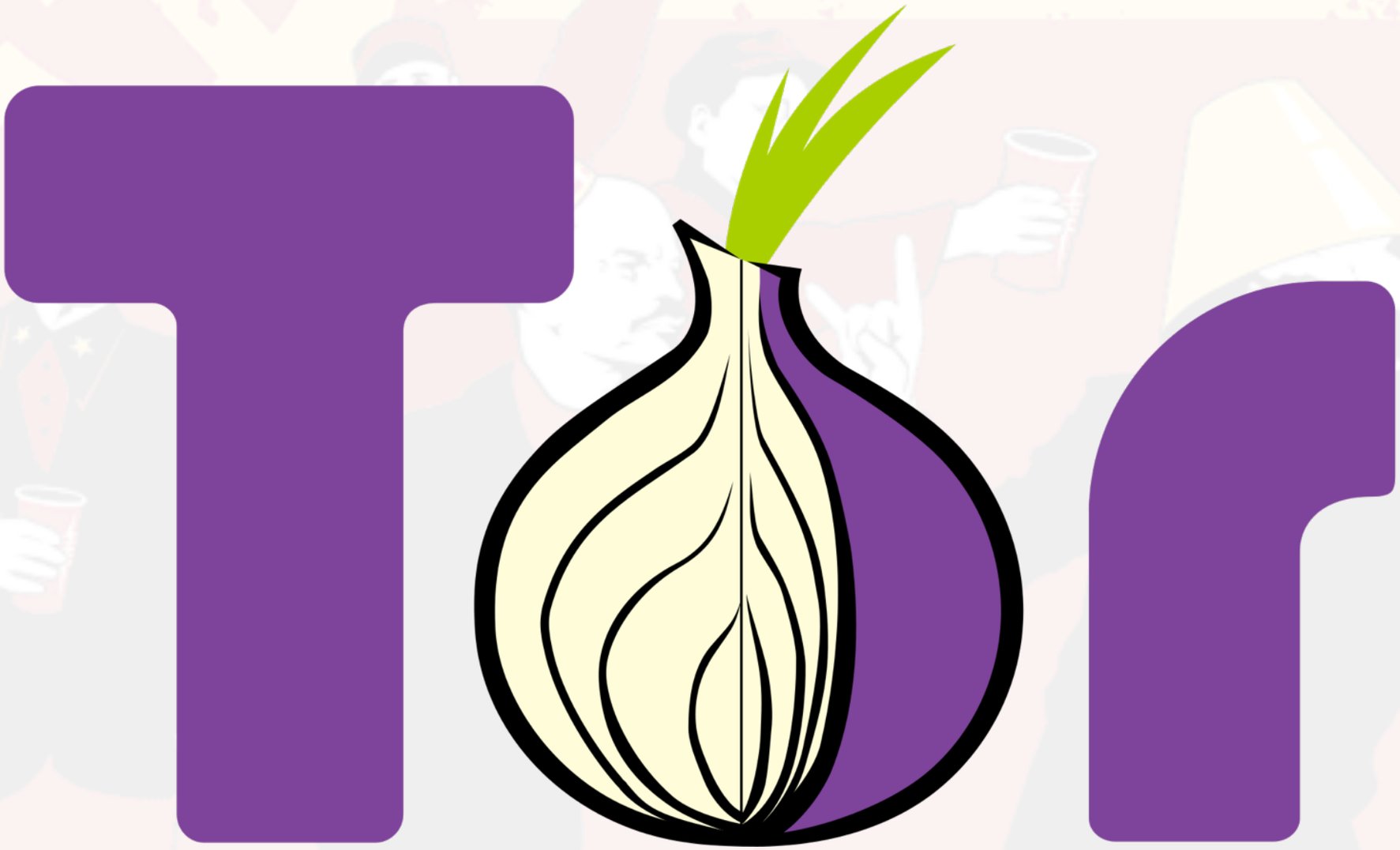
THURSDAY, OCTOBER 23, 2014

THE CASE OF THE MODIFIED BINARIES

https://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries/

NOPSEC

OnionDuke Backstory



NOPSEC

OnionDuke Backstory

- Used Exitmap, by Philipp Winter, to test Tor exit nodes
- Only one malicious node found, in Russia
- Reported to Tor
- Patched ONLY uncompressed x86 PE files
- Multiple samples retrieved
- F-Secure coined the term OnionDuke and attributed the malware to the Russian Gov or affiliated groups

https://github.com/NullHypothesis/exitmap

https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

OnionDuke Backstory

virustotal

SHA256: 9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76dec386b

File name: Everything-1.3.3.658b.x64.exe

Detection ratio: 3 / 48

Analysis date: 2014-01-10 16:51:38 UTC (1 year, 5 months ago)

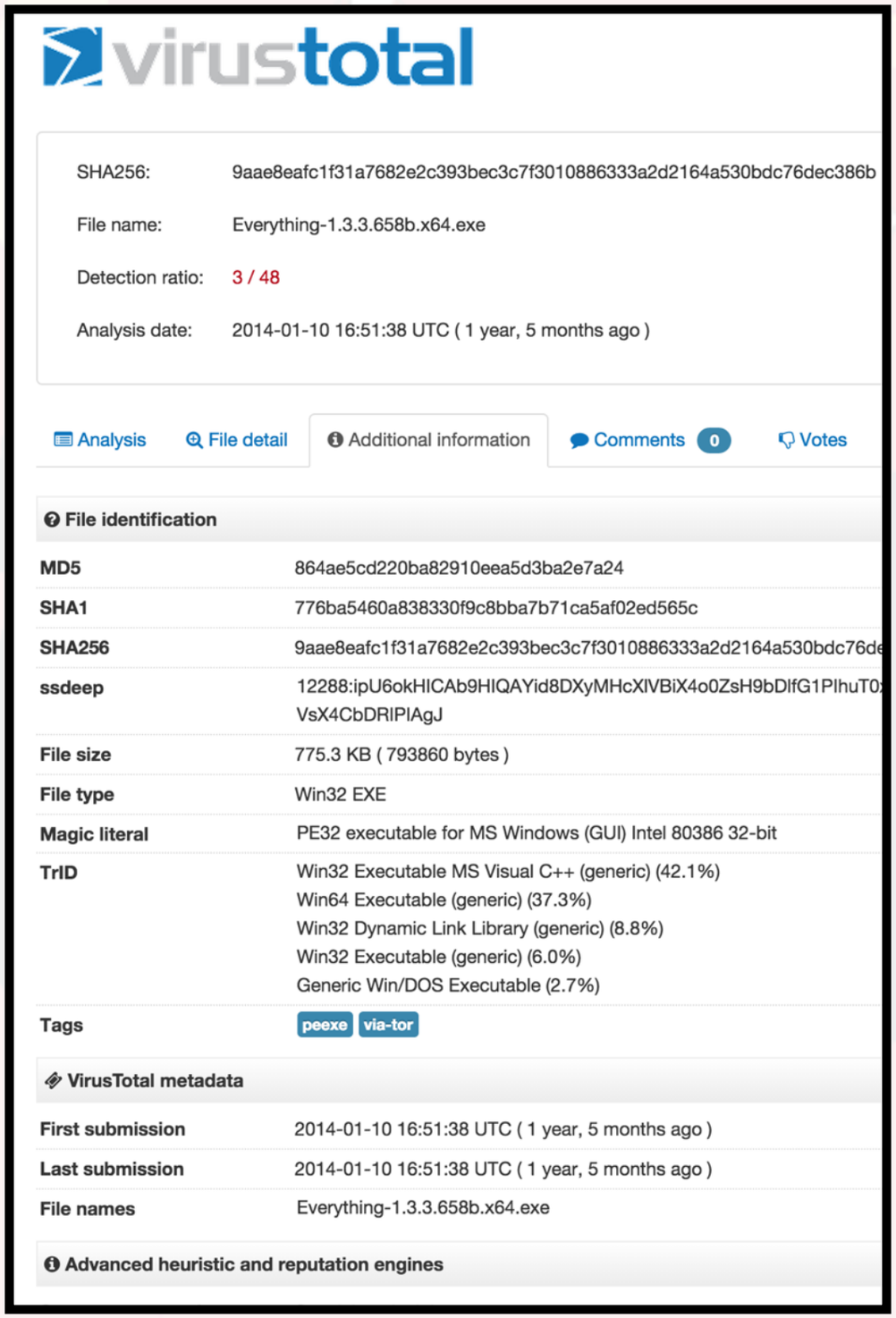
Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Win32/DH{AAE2NVg3Enk}	20140110
AntiVir	TR/Crypt.XPACK.Gen2	20140110
DrWeb	Trojan.DownLoader9.2162	20140110
Ad-Aware	✓	20140110
Agnitum	✓	20140110

https://www.virustotal.com/en/file/9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76dec386b/analysis/

NOPSEC

OnionDuke Backstory



virustotal

SHA256:	9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76dec386b
File name:	Everything-1.3.3.658b.x64.exe
Detection ratio:	3 / 48
Analysis date:	2014-01-10 16:51:38 UTC (1 year, 5 months ago)

Analysis | File detail | Additional information | Comments 0 | Votes

File identification

MD5	864ae5cd220ba82910eea5d3ba2e7a24
SHA1	776ba5460a838330f9c8bba7b71ca5af02ed565c
SHA256	9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76de
ssdeep	12288:ipU6okHICAb9HIQAYid8DXyMHcXlVBiX4o0ZsH9bDlfG1PlhuT0 VsX4CbDRlPlAgJ
File size	775.3 KB (793860 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (42.1%) Win64 Executable (generic) (37.3%) Win32 Dynamic Link Library (generic) (8.8%) Win32 Executable (generic) (6.0%) Generic Win/DOS Executable (2.7%)
Tags	peexe via-tor

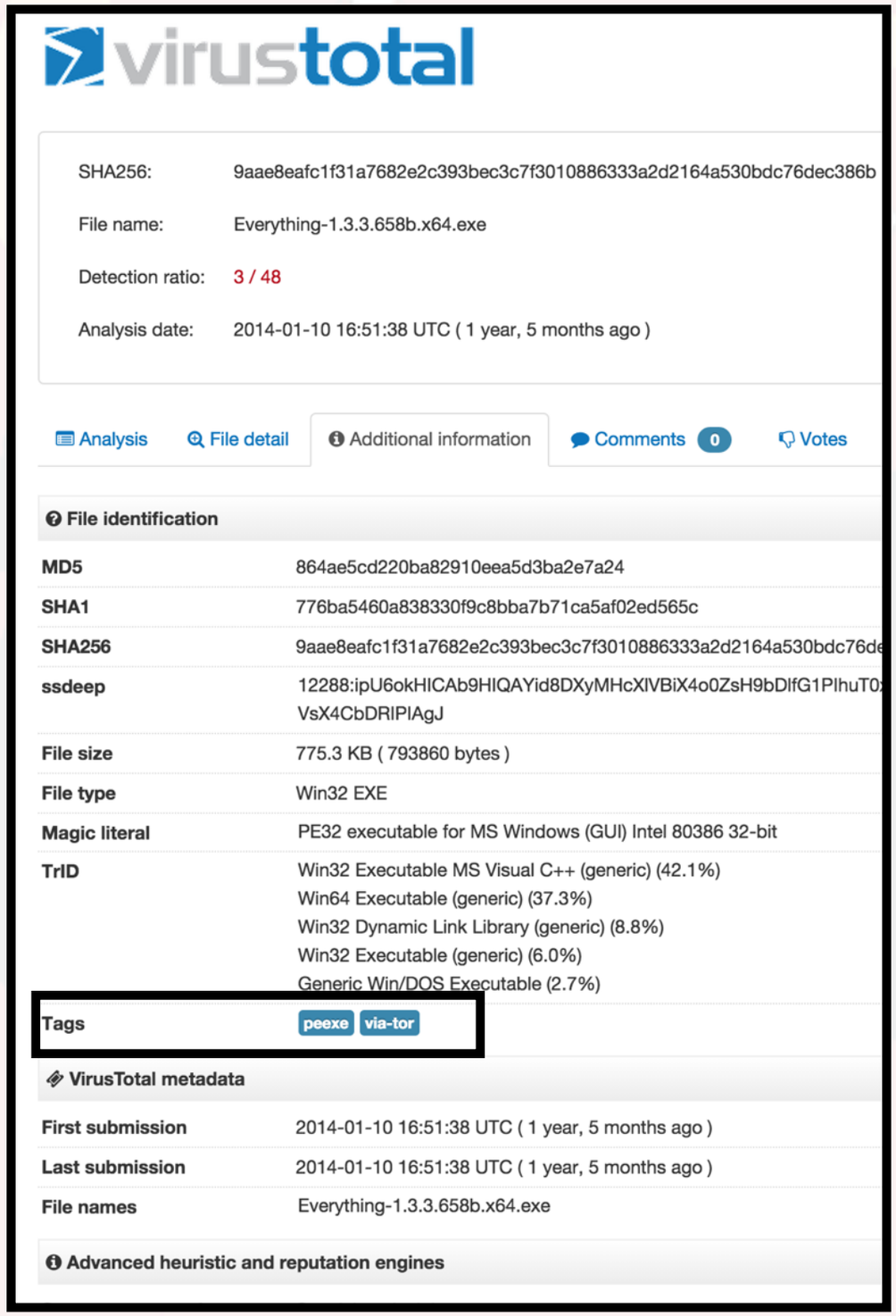
VirusTotal metadata

First submission	2014-01-10 16:51:38 UTC (1 year, 5 months ago)
Last submission	2014-01-10 16:51:38 UTC (1 year, 5 months ago)
File names	Everything-1.3.3.658b.x64.exe

Advanced heuristic and reputation engines

NOPSEC

OnionDuke Backstory



virustotal

SHA256:	9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76dec386b
File name:	Everything-1.3.3.658b.x64.exe
Detection ratio:	3 / 48
Analysis date:	2014-01-10 16:51:38 UTC (1 year, 5 months ago)

Analysis | File detail | Additional information | Comments 0 | Votes

File identification

MD5	864ae5cd220ba82910eea5d3ba2e7a24
SHA1	776ba5460a838330f9c8bba7b71ca5af02ed565c
SHA256	9aae8eafc1f31a7682e2c393bec3c7f3010886333a2d2164a530bdc76de
ssdeep	12288:ipU6okHICAb9HIQAYid8DXyMHcXlVBiX4o0ZsH9bDlfG1PlhuT0 VsX4CbDRlPlAgJ
File size	775.3 KB (793860 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (42.1%) Win64 Executable (generic) (37.3%) Win32 Dynamic Link Library (generic) (8.8%) Win32 Executable (generic) (6.0%) Generic Win/DOS Executable (2.7%)
Tags	peexe via-tor

VirusTotal metadata

First submission	2014-01-10 16:51:38 UTC (1 year, 5 months ago)
Last submission	2014-01-10 16:51:38 UTC (1 year, 5 months ago)
File names	Everything-1.3.3.658b.x64.exe

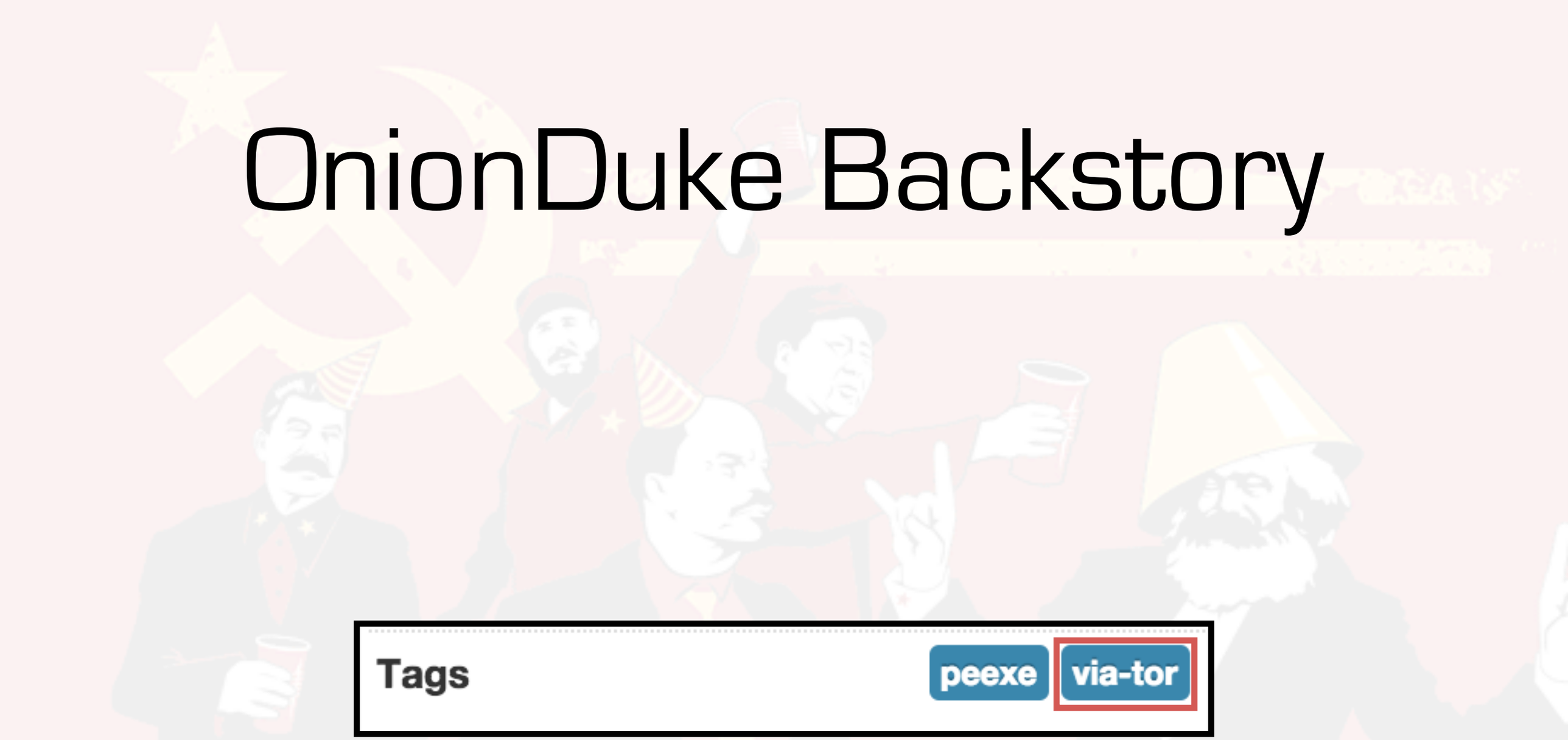
Advanced heuristic and reputation engines

NOPSEC

OnionDuke Backstory

Tags peexe via-tor

OnionDuke Backstory



Tags peexe via-tor

Repurposing Software

NOPSEC

Repurposing MALWARE

NOPSEC

Repurposing MALWARE

- Different than incident response

Repurposing MALWARE

- Different than incident response
- Understand everything about the malware

NOPSEC

Repurposing MALWARE

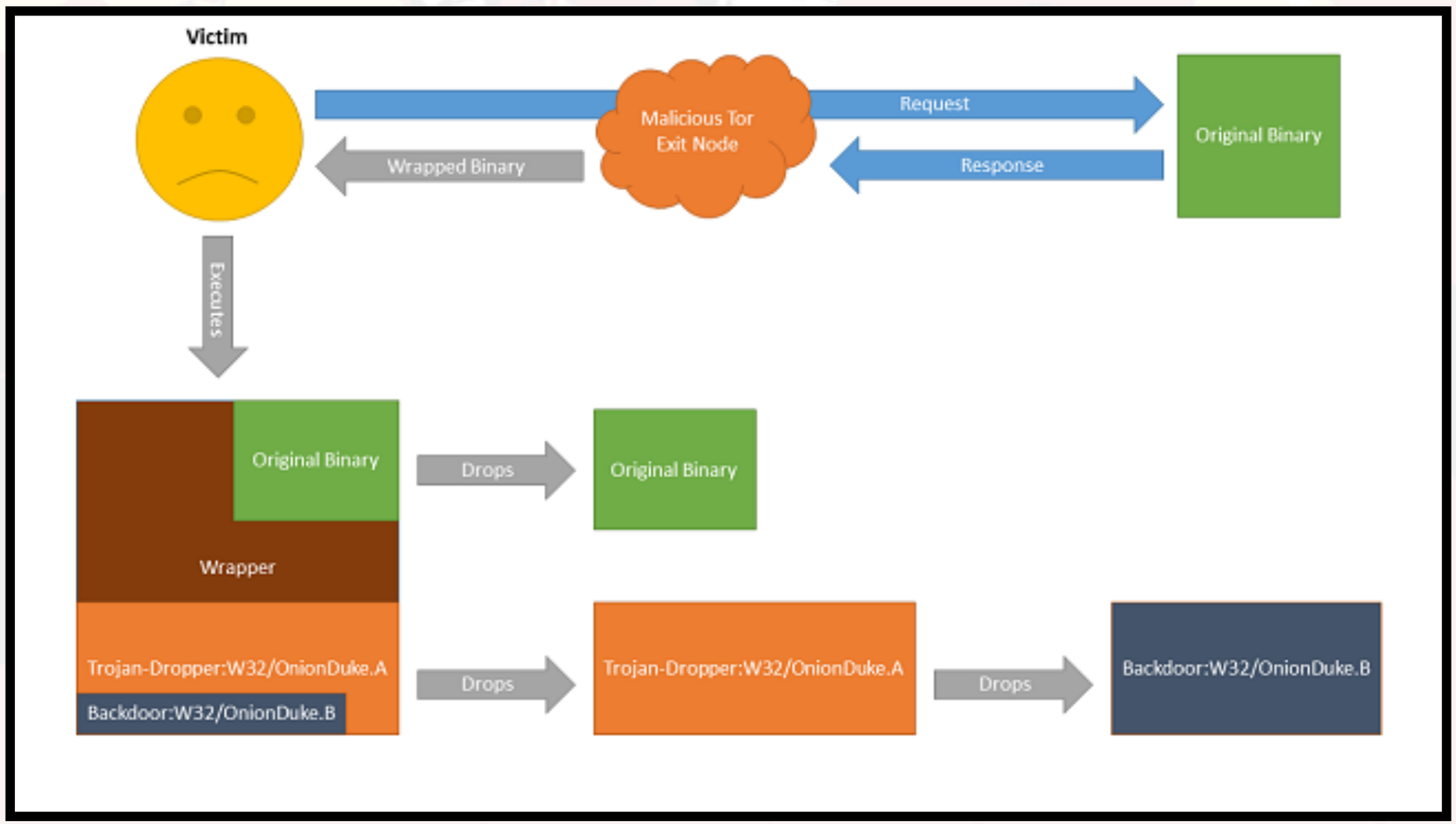
- Different than incident response
- Understand everything about the malware
- Little risk of legal retribution from the original authors

NOPSEC

Case Study:The OnionDuke MITM METHOD

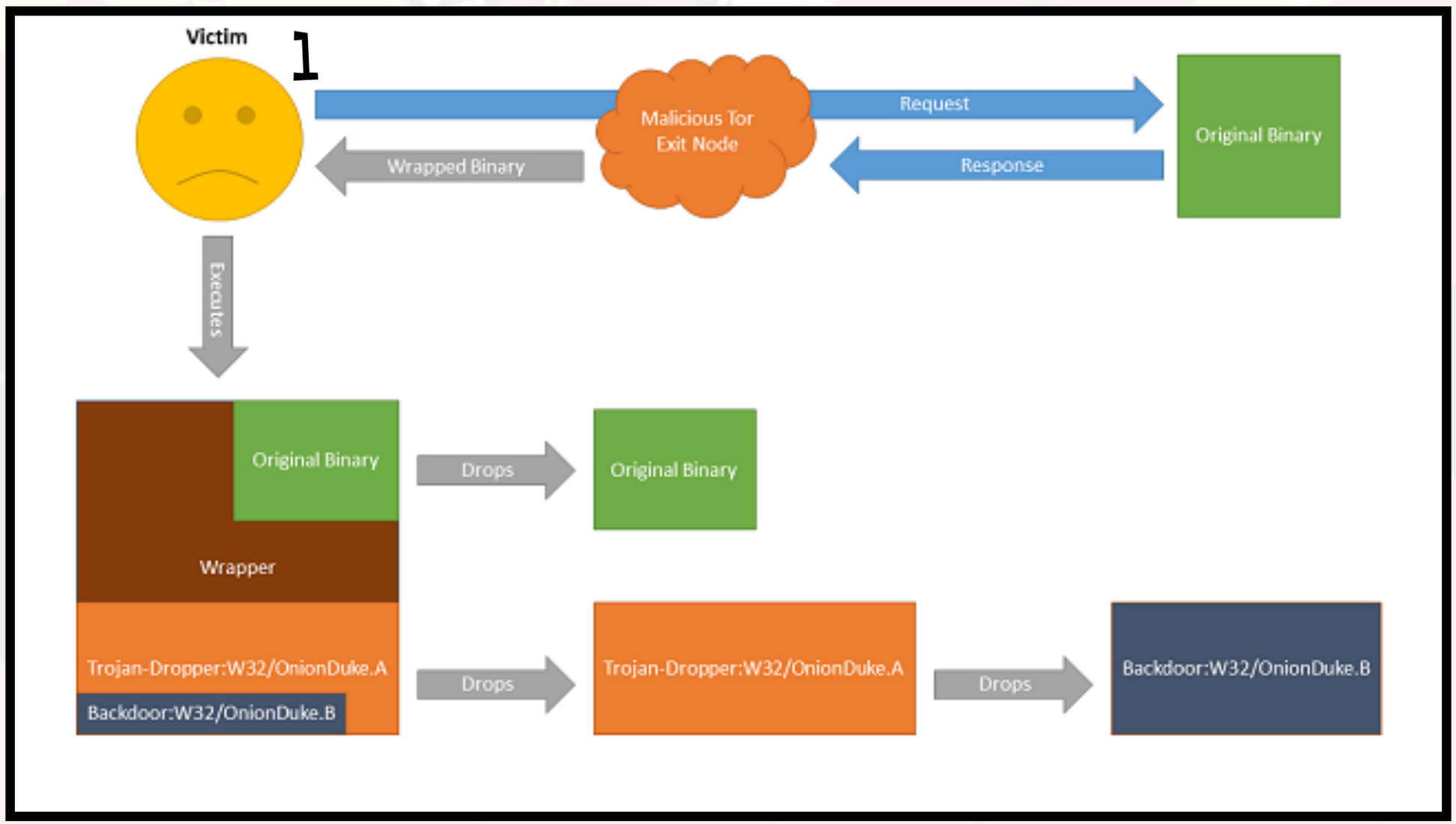
NOPSEC

Distribution & Infection



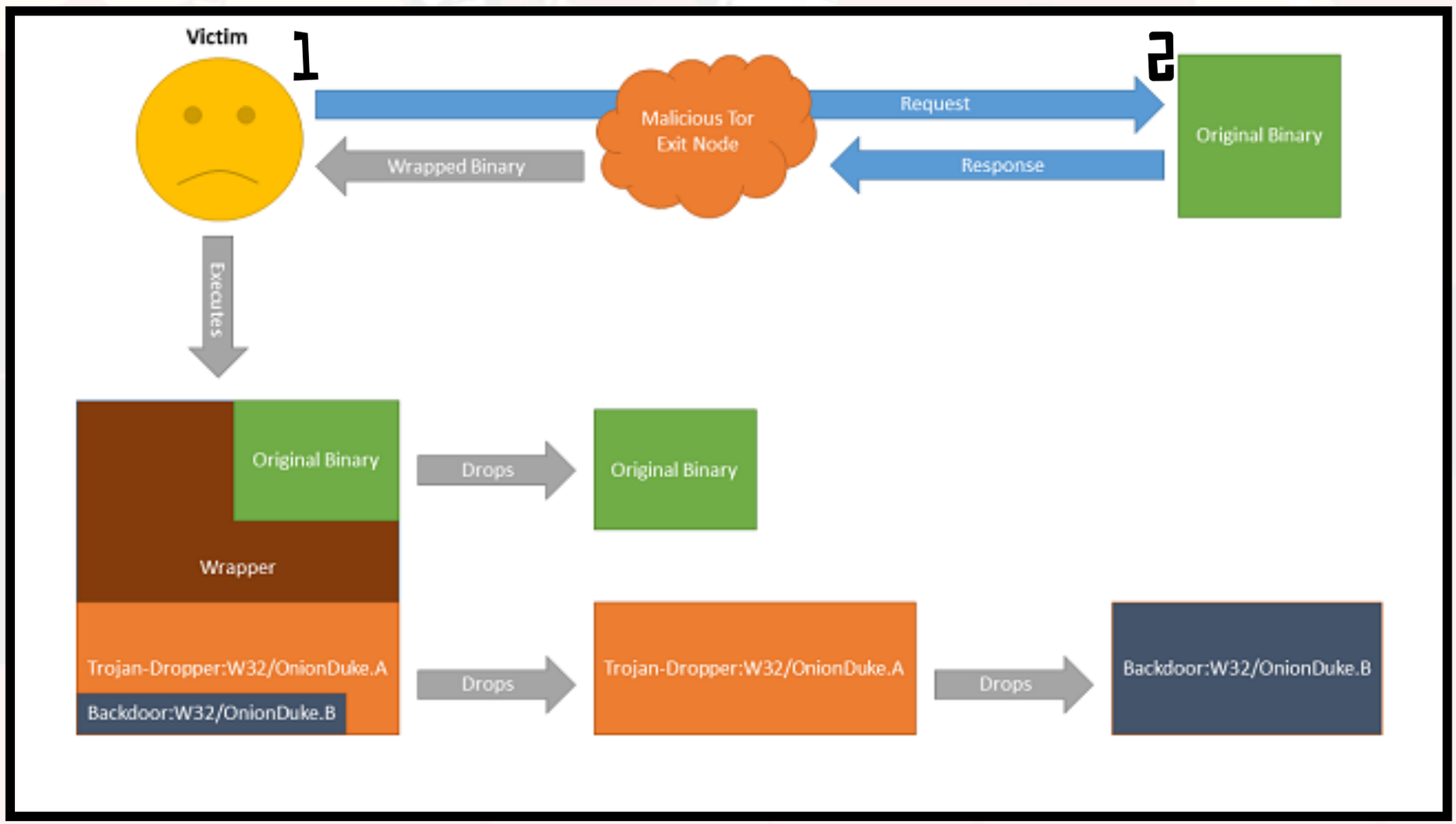
https://www.f-secure.com/weblog/archives/00002764.html

Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

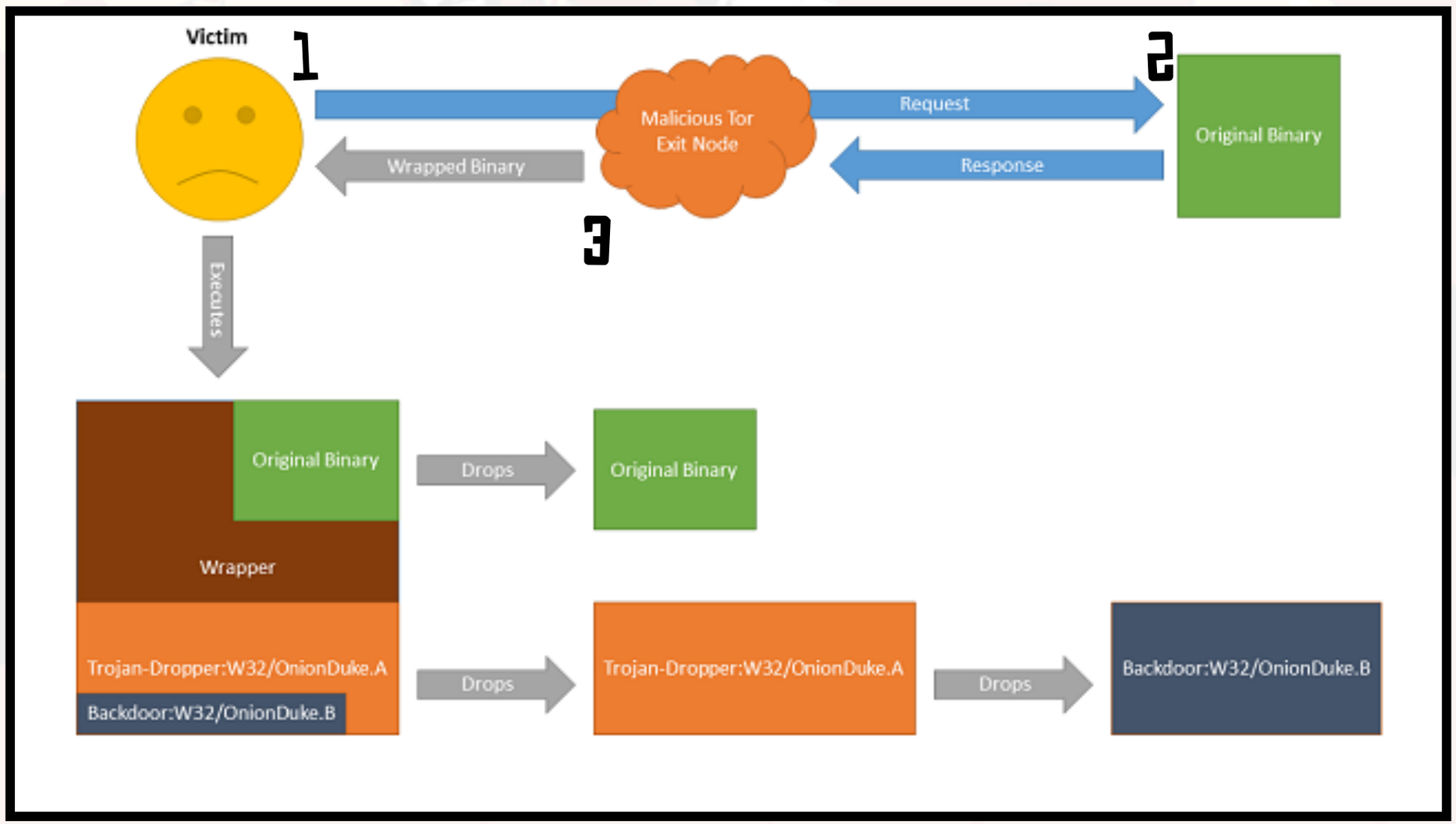
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

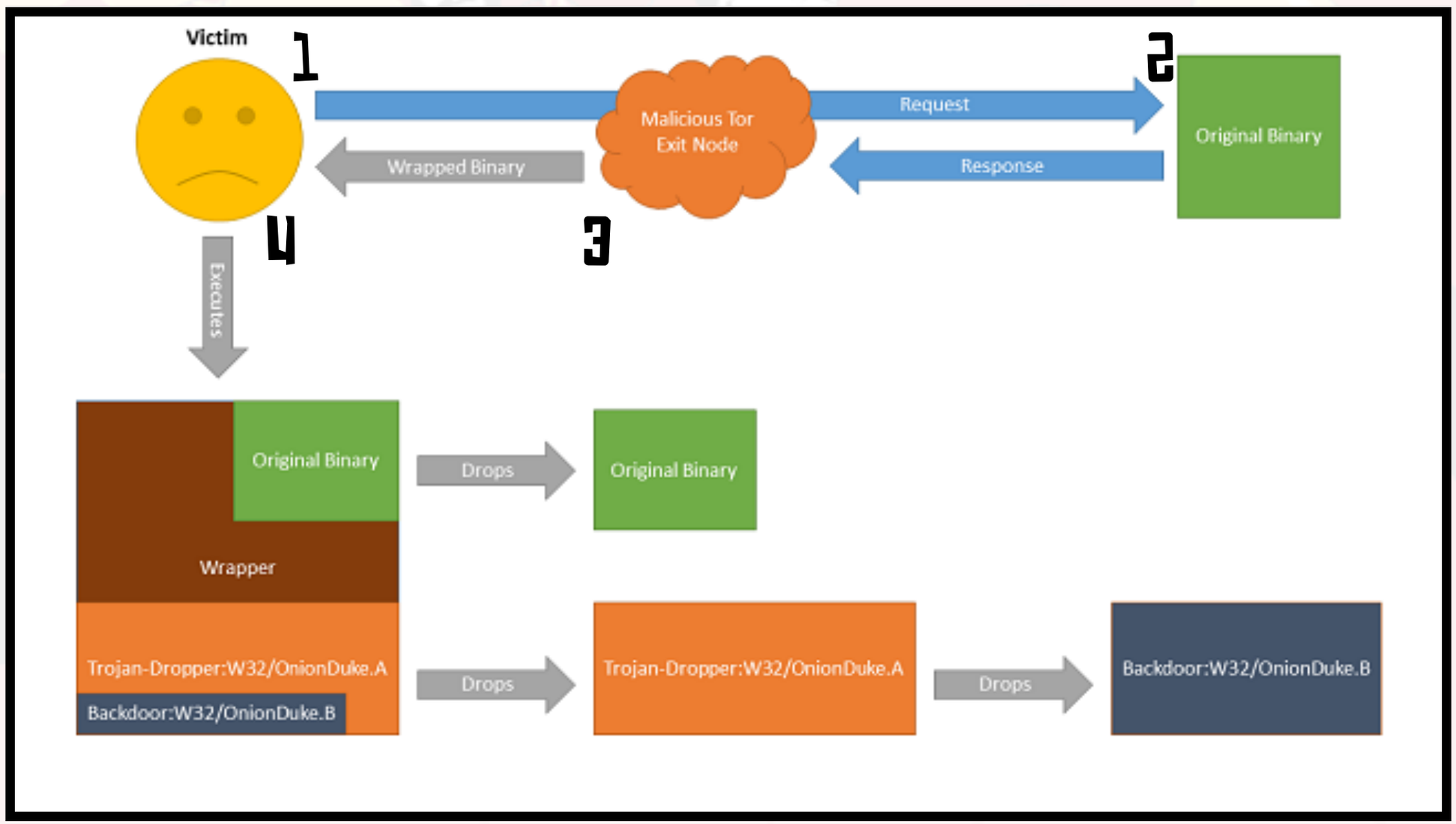
NOPSEC

Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

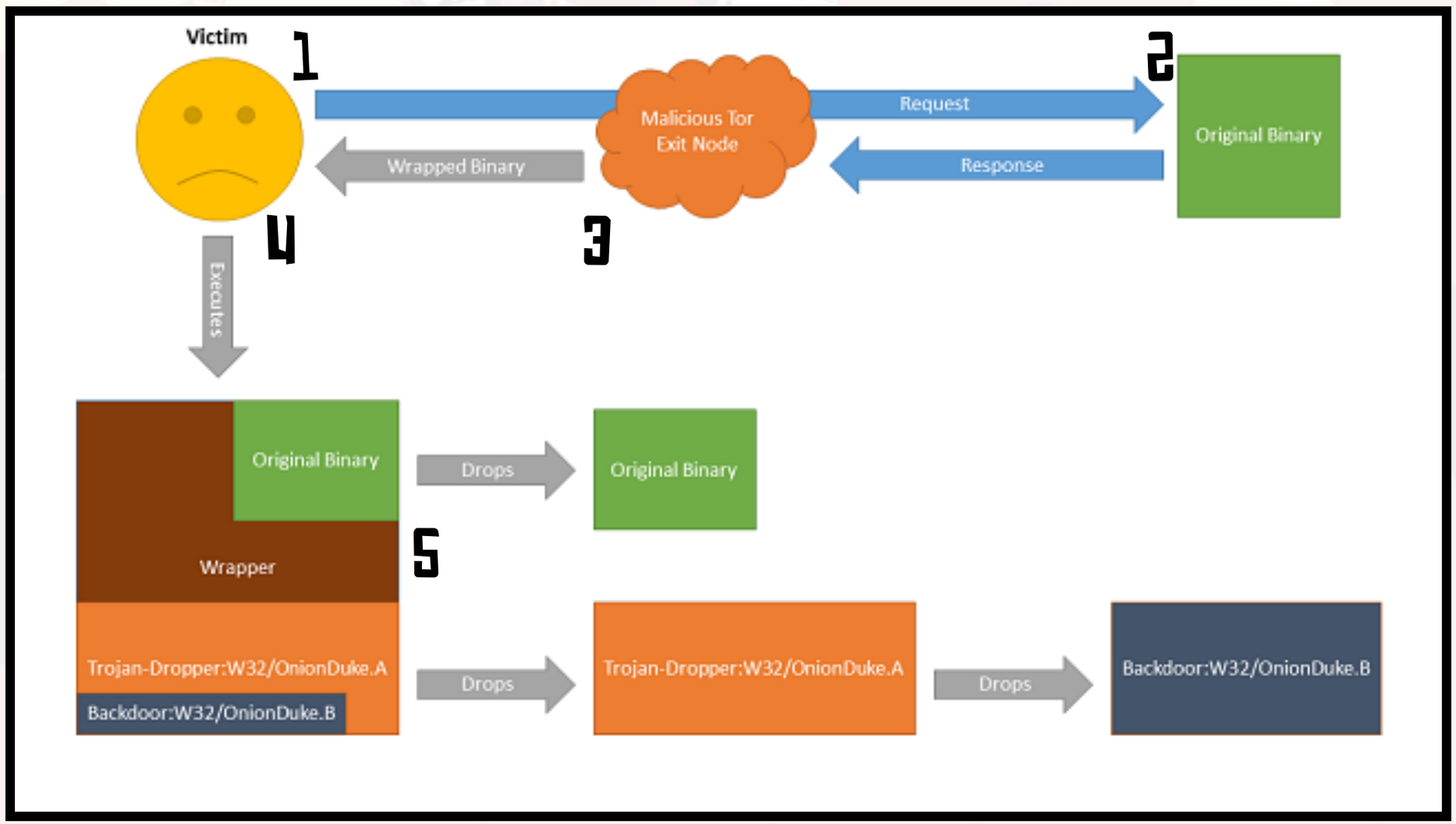
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

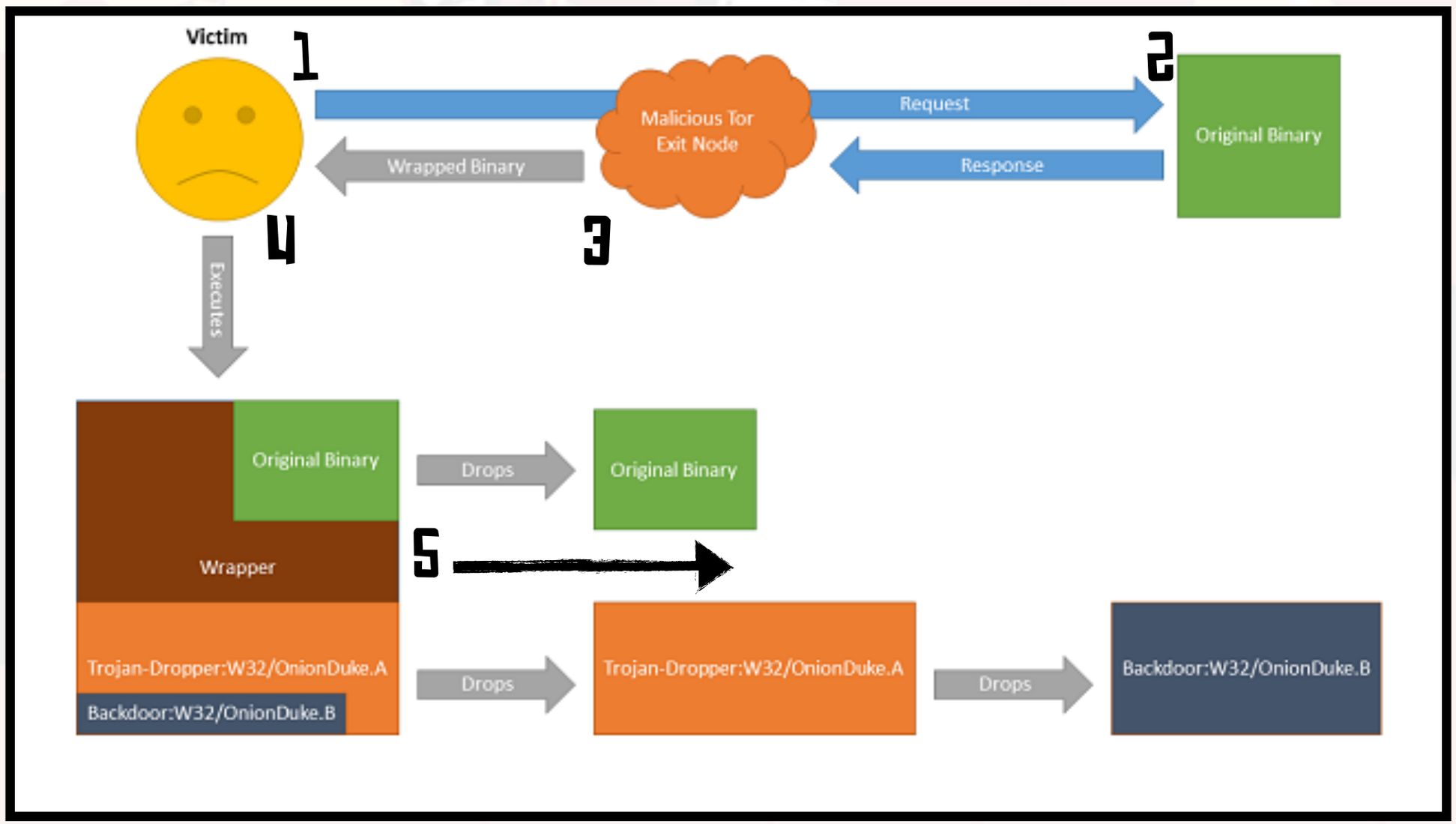
NOPSEC

Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

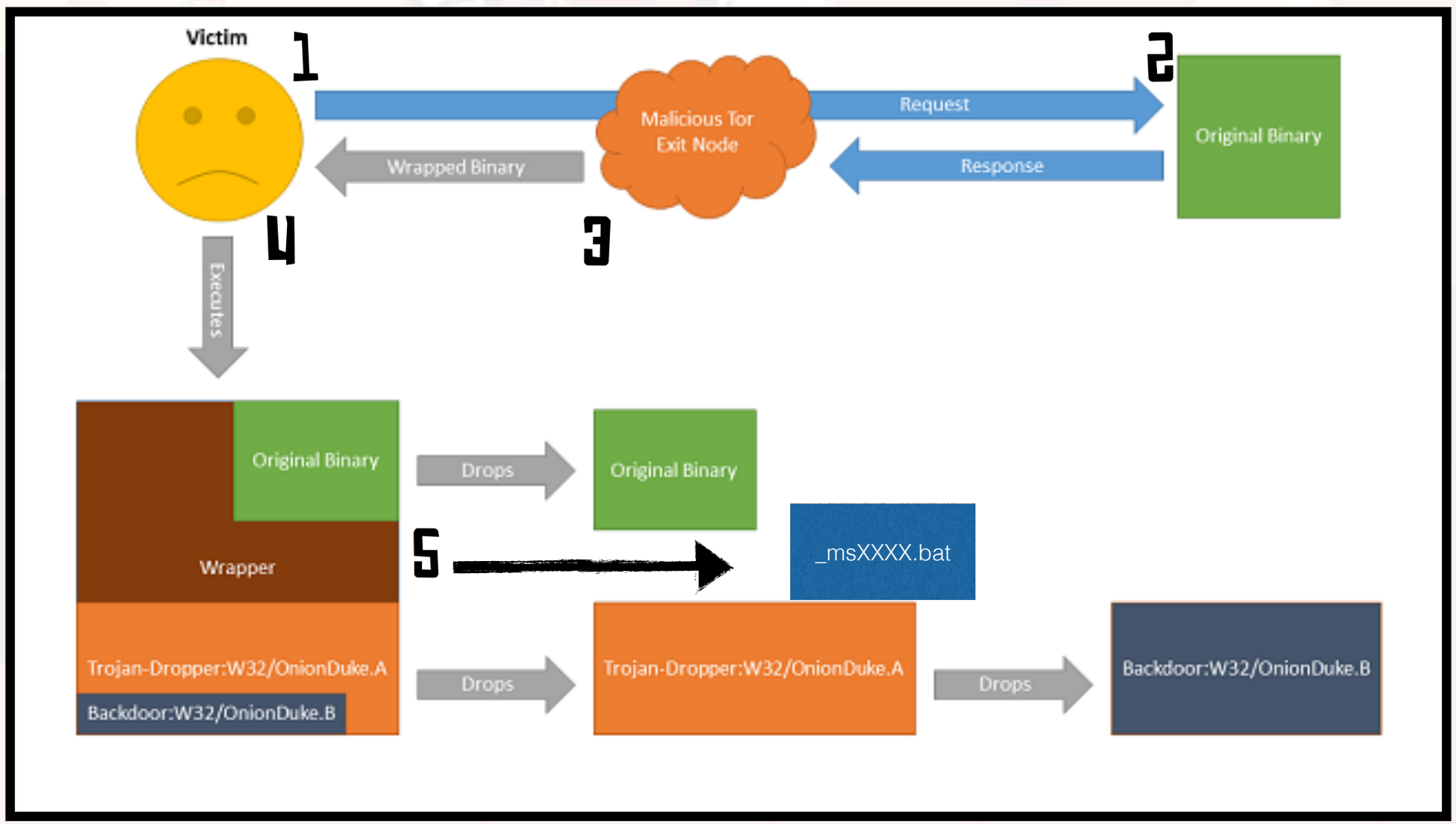
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

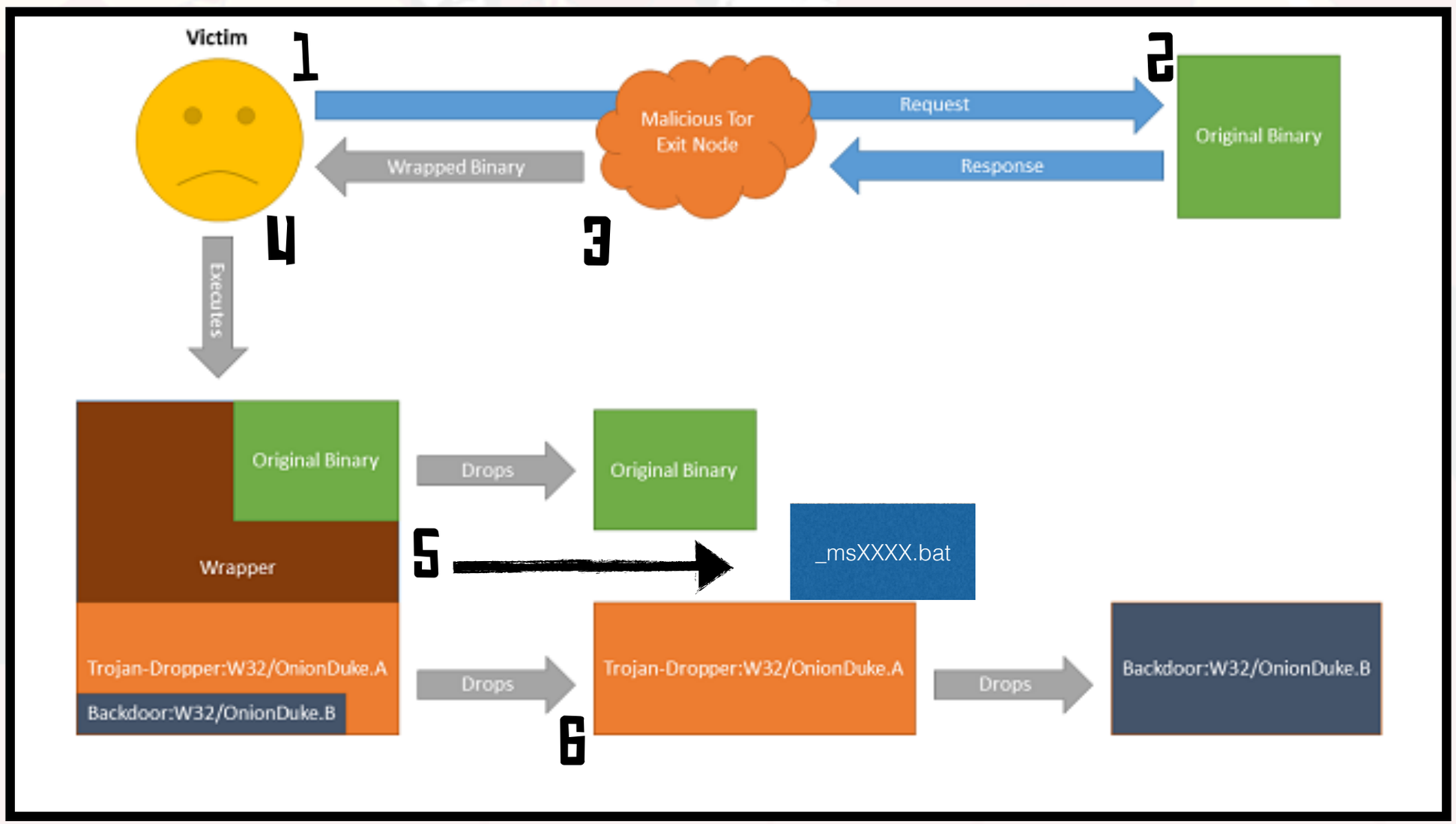
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

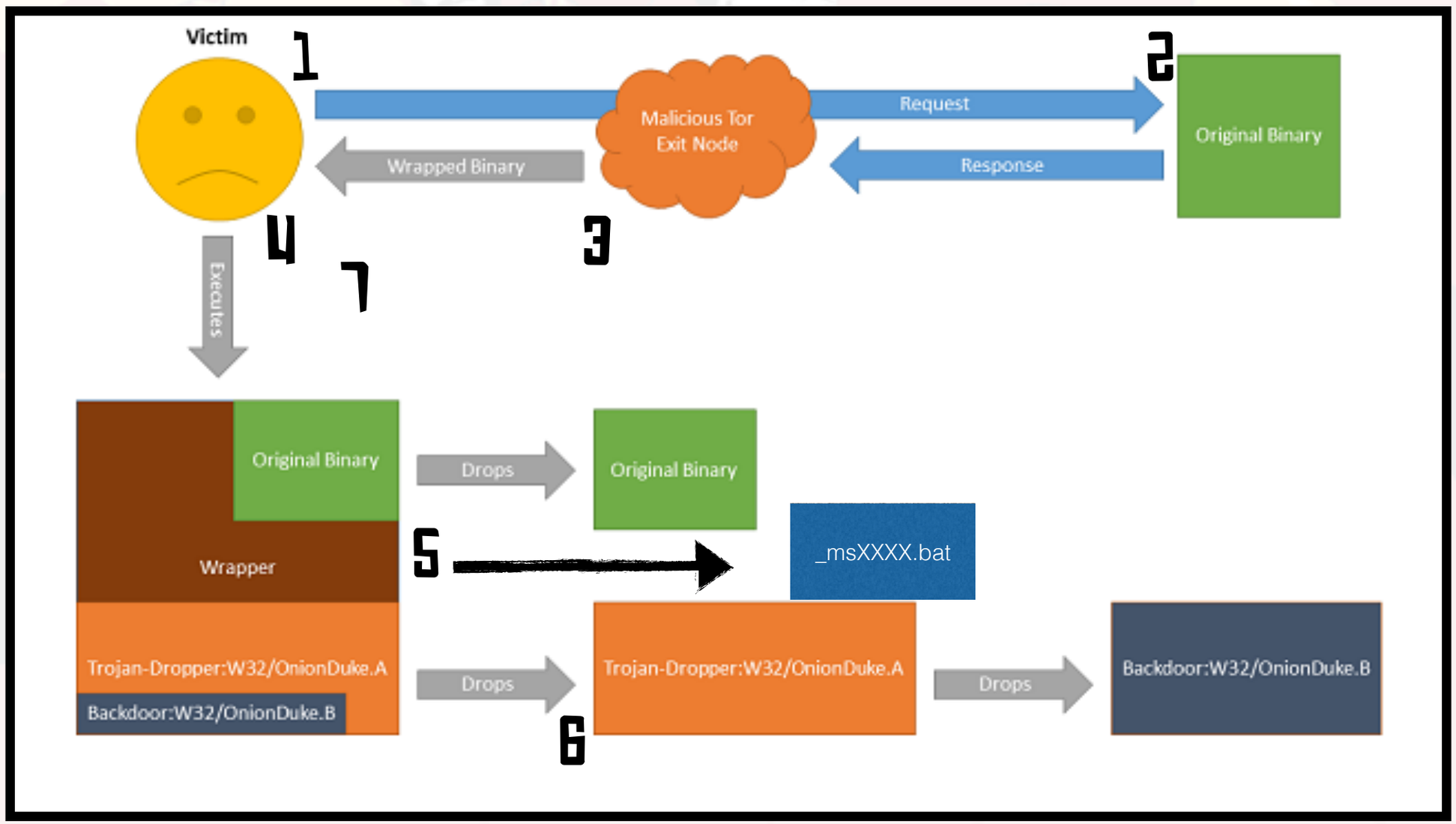
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

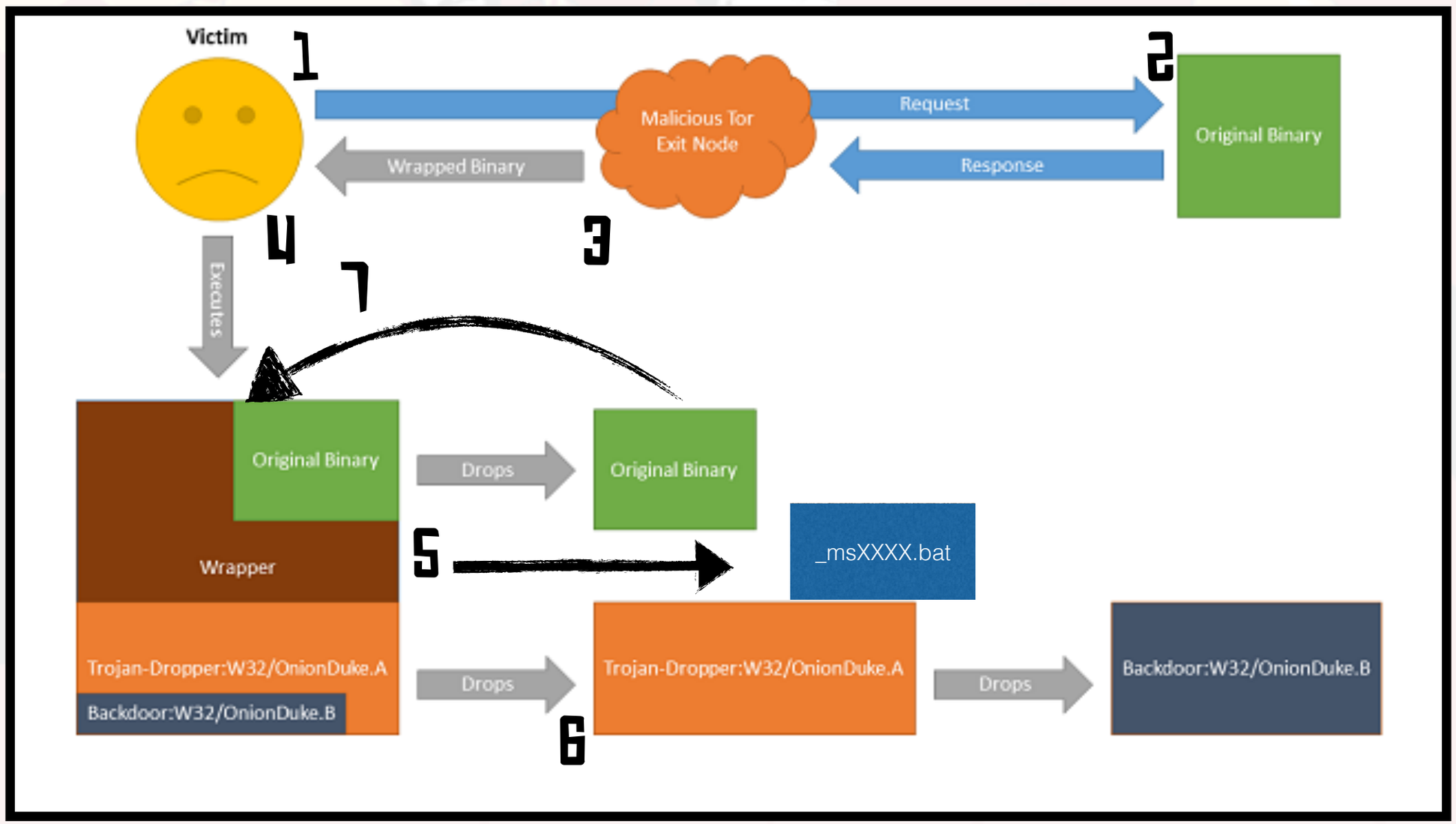
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

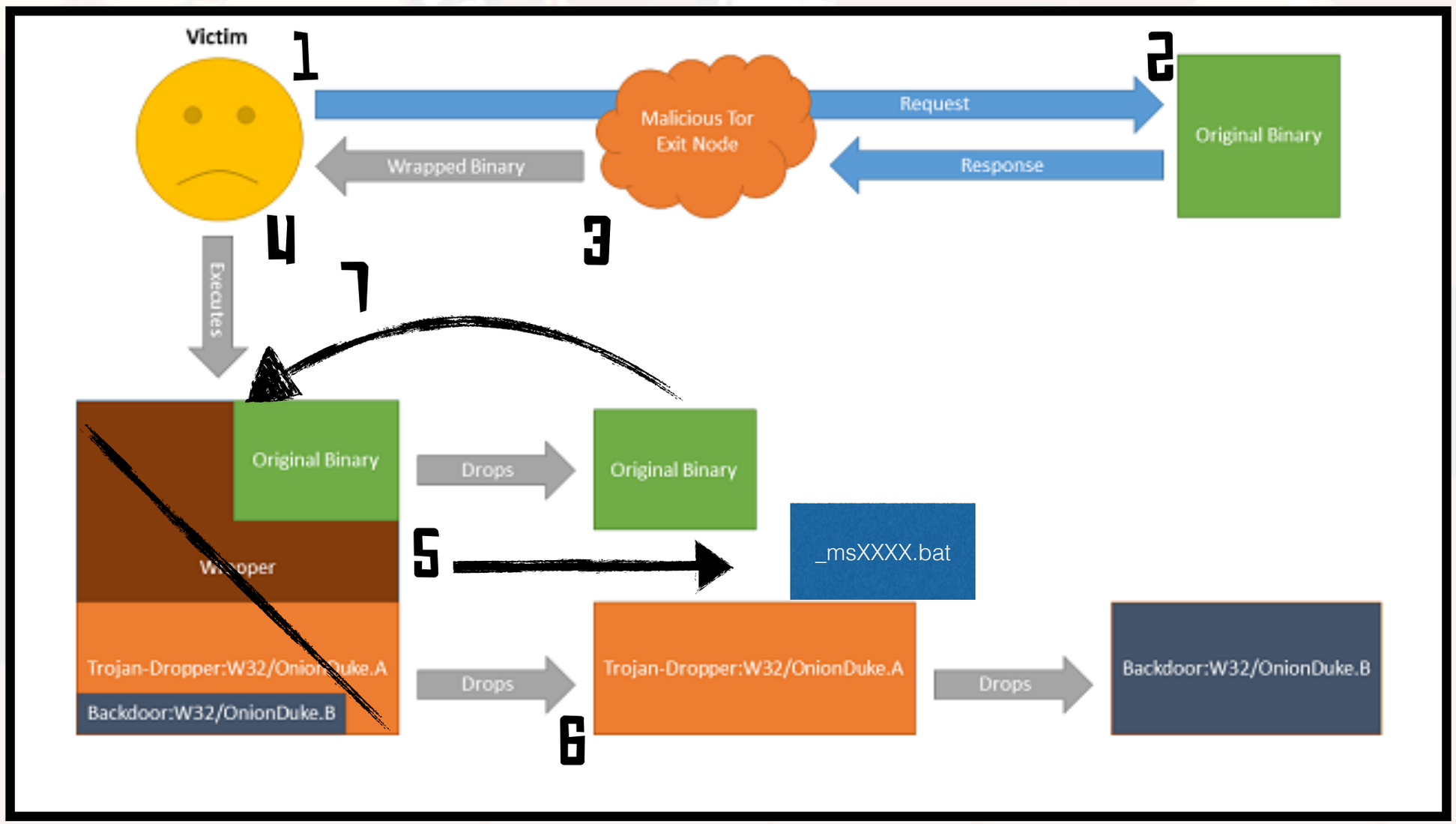
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

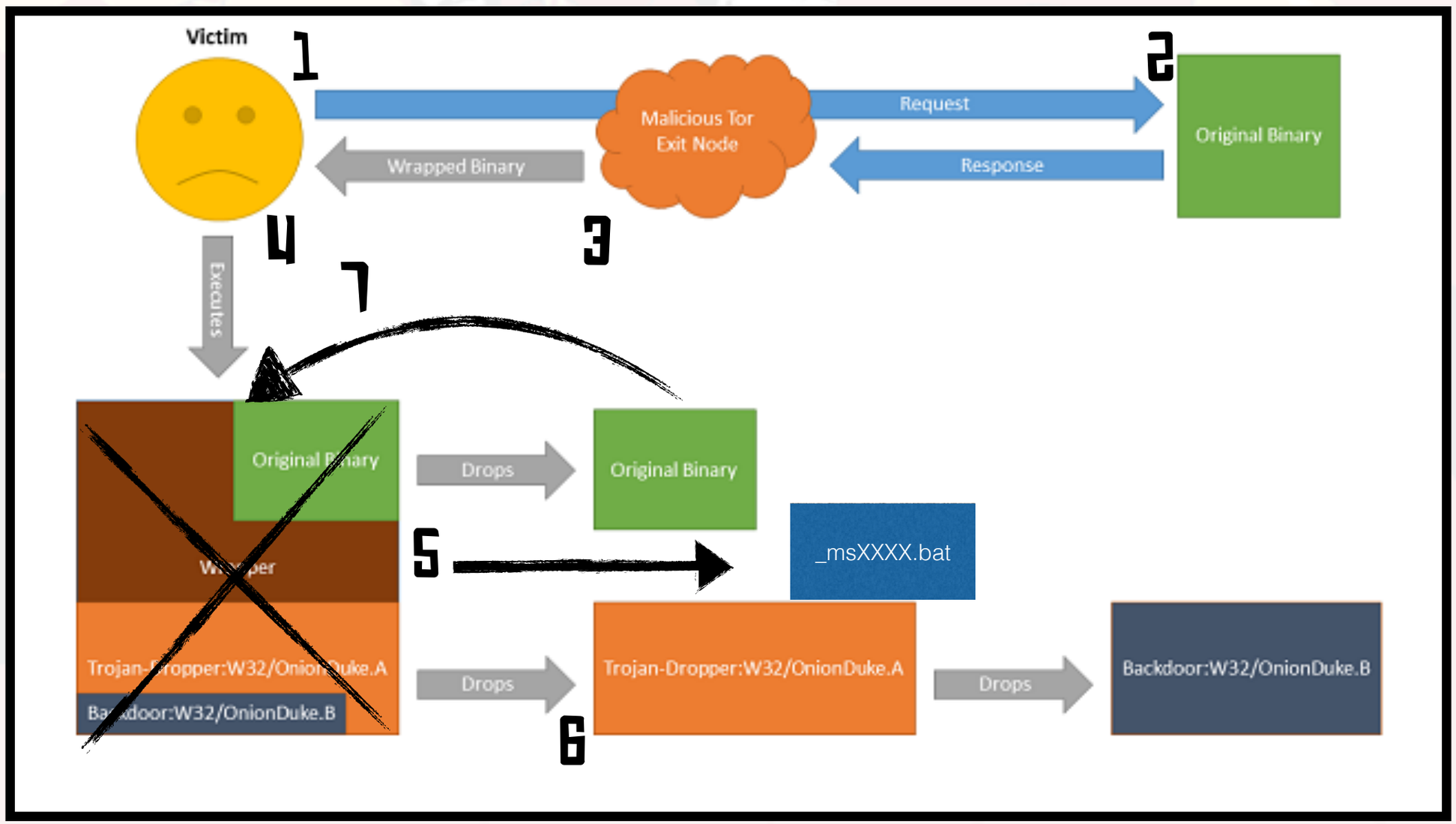
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

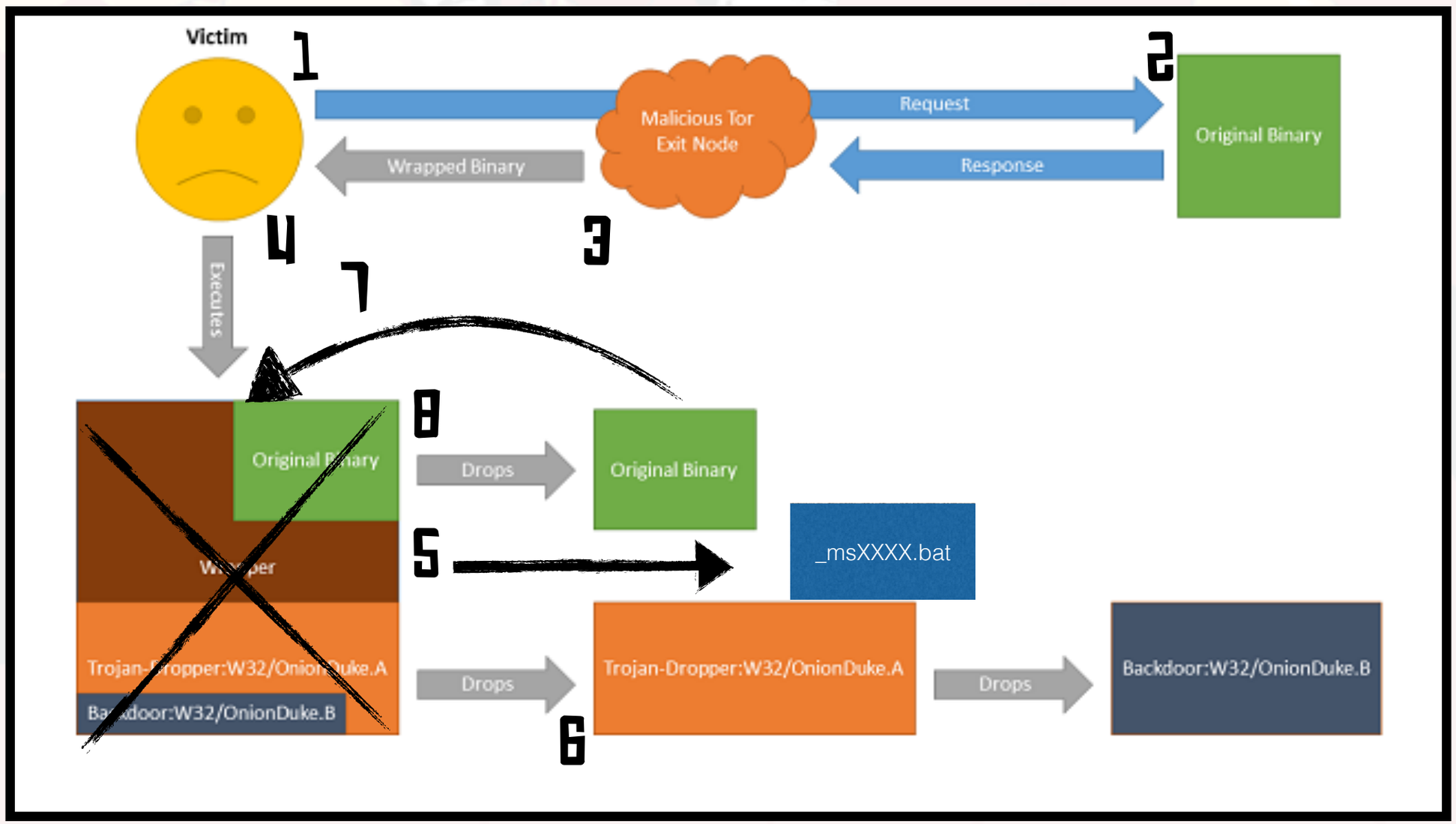
Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

Distribution & Infection



https://www.f-secure.com/weblog/archives/00002764.html

NOPSEC

Packer Output

- Dropped in %Temp%
- file.exe - the OnionDuke malware
- originalfile.exe.org - the original file
- _msXXXX.bat (EX:_ms0494.bat] - Batch file for moving .org file over the wrapper executable

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

Sample Comparisons

procexp.exe https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.14	092c7e65e61dcef2862c1310aa07ac9f
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	1536512	1536156	5.99	8833c11b02fab5eb0f3864f714ce7d00

psexec.exe https://www.virustotal.com/en/file/de1a78b4a65d76d26f04db0c1fd5eefdb9361f434925df88e45d6cd511f3c013/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	ae0e82daf559ff42d187ae654f23e4b0
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	191488	191218	6.62	fc027c129375455dd8d1727439bbbee6

tcpview.exe https://www.virustotal.com/en/file/a3e5b92ce574397000825dc646e1a7763b7f817bb8ac8d446a31c3252c1076eb/analysis/

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
• .text	4096	46278	46592	6.53	622bf787166636ec6c8ac7c27bcee230
• .rdata	53248	12710	12800	5.32	626386acd8fd64973d6213867f99a094
• .data	69632	12196	4608	2.13	0e6418e9cb5c519d002e1e5979487976
• .reloc	81920	4958	5120	4.03	95c6fa59d1c3ff4e63d4d2f48cfd04da
• .rsrc	90112	9728	9238	4.12	c45ed2f23f3caa391423fad09a1922c3

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00  00 00 00 00  00 00 00 00  00 00 00 00  psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00  EE DE 02 00  00 00 00 00  66 69 6C 65  ........................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00  00 00 00 00  00 00 00 00  00 00 00 00  ............<...............
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.....
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ........................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ............................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ........................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<..................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

Org File LOC|SIZE

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

Org File LOC|SIZE

NOPSEC

.data Differences

```
0000FB20   70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00   00 00 00 00  00 00 00 00  00 00 00 00   psexec.exe.org.............
0000FB3C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB74   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FB90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBAC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FBE4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC00   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC1C   00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00   EE DE 02 00  00 00 00 00  66 69 6C 65   ....................file
0000FC38   2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   .exe............................
0000FC54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC70   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FC8C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCC4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FCFC   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD34   00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00   00 00 00 00  00 00 00 00  00 00 00 00   .............<.................
0000FD50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
0000FD6C   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00  00 00 00 00   ................................
```

Org File LOC|SIZE

NOPSEC

.data Differences

```
0000FB20  70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00  00 00 00 00  00 00 00 00  00 00 00 00  psexec.exe.org.............
0000FB3C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB58  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB74  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB90  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBAC  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBC8  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBE4  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC1C  00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00  EE DE 02 00  00 00 00 00  66 69 6C 65  ....................file
0000FC38  2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  .exe............................
0000FC54  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC70  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC8C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCA8  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCC4  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCE0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCFC  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD18  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD34  00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00  00 00 00 00  00 00 00 00  00 00 00 00  .............<..............
0000FD50  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD6C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
```

Org File LOC|SIZE

Malware File LOC|SIZE

NOPSEC

.rsrc Differences

> A drawback of the current implementation is that the application icon, which is showed by the file browser, is changed to the application icon of the binder. This might raise suspicion by the user.
>
> - Felix Grobert, et al

https://dl.packetstormsecurity.net/papers/general/Software.Distribution.Malware.Infection.Vector.pdf

.rsrc Differences

> A drawback of the current implementation is that the application icon, which is showed by the file browser, is changed to the application icon of the binder. This might raise suspicion by the user.
>
> - Felix Grobert, et al

OnionDuke solves this issue!*

https://dl.packetstormsecurity.net/papers/general/Software.Distribution.Malware.Infection.Vector.pdf

.rsrc Differences

> A drawback of the current implementation is that the application icon, which is showed by the file browser, is changed to the application icon of the binder. This might raise suspicion by the user.
>
> - Felix Grobert, et al

OnionDuke solves this issue!*

*BDFProxy never had this issue

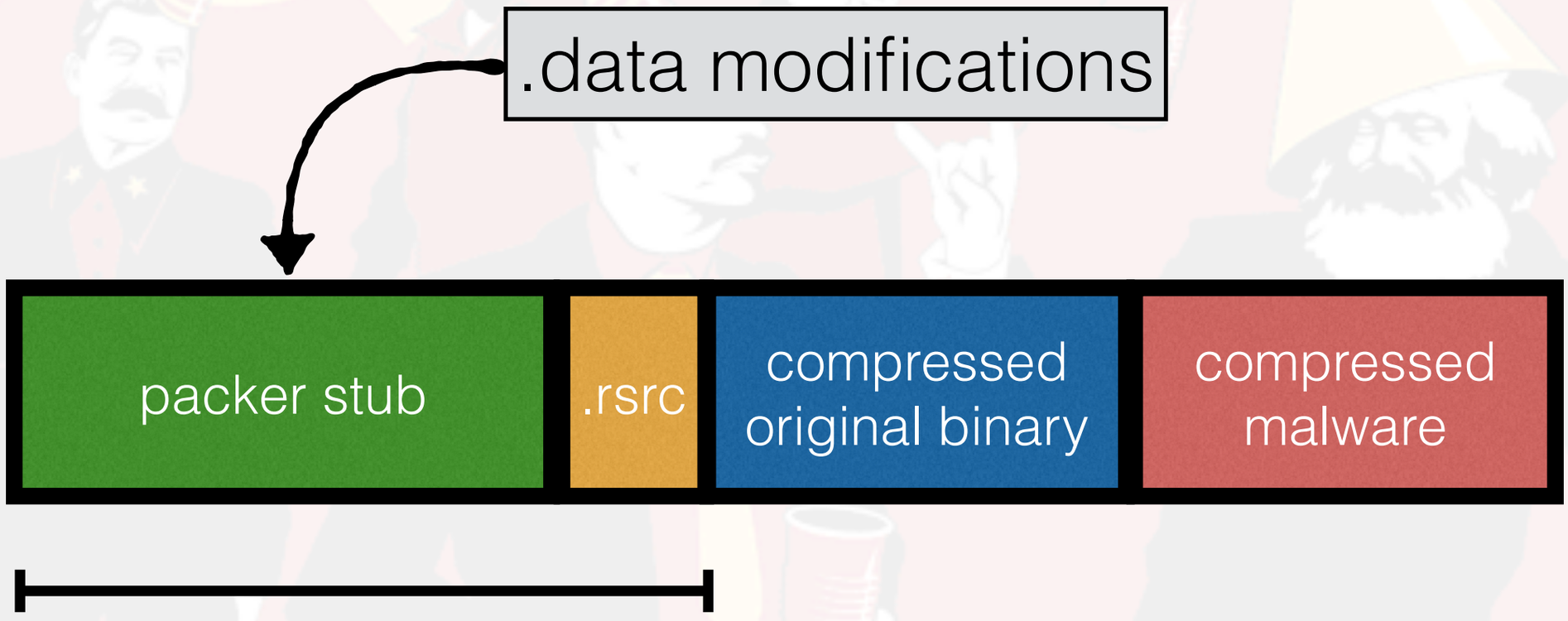
https://dl.packetstormsecurity.net/papers/general/Software.Distribution.Malware.Infection.Vector.pdf

NOPSEC

Aside : Counter Measures?

Anonymizers. Anonymizers[8] like Tor [4] can be deployed to support the mentioned means to hide identities in case Governments deploy infection mechanisms to trace suspects. Note that the state can be considered as a very powerful entity with access rights to many resources. Typically, law enforcement targets a limited number of suspects, thus we can assume that law enforcement has to identify the victim before the attack. However, this would be a hard task if the suspects use anonymizers.

Packer Layout



NOPSEC

Stub Details

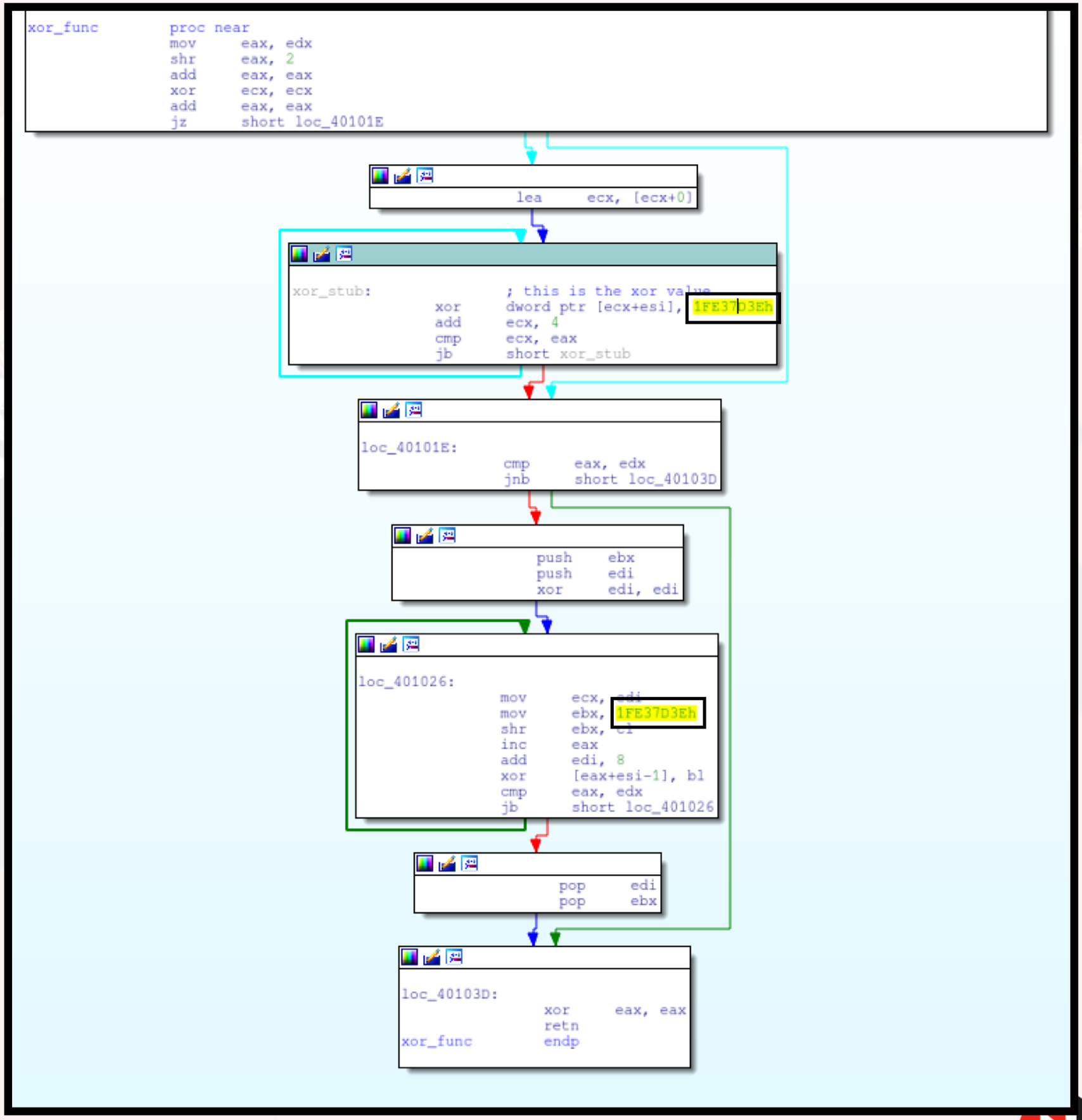
- Compiled with /GS (buffer security check)
- Written in C++
- Captures command line arguments (if any)
- Supports both ANSI/Unicode base filenames and paths
- Additionally supports x64 PE binaries

NOPSEC

XOR

- Each binary file is XOR'ed after compression
- Static XOR key of 0x1FE37D3E

NOPSEC


xor_func proc near
mov eax, edx
shr eax, 2
add eax, eax
xor ecx, ecx
add eax, eax
jz short loc_40101E
lea ecx, [ecx+0]
xor_stub: ; this is the xor value
xor dword ptr [ecx+esi], 1FE37D3Eh
add ecx, 4
cmp ecx, eax
jb short xor_stub
loc_40101E:
cmp eax, edx
jnb short loc_40103D
push ebx
push edi
xor edi, edi
loc_401026:
mov ecx, edi
mov ebx, 1FE37D3Eh
shr ebx, cl
inc eax
add edi, 8
xor [eax+esi-1], bl
cmp eax, edx
jb short loc_401026
pop edi
pop ebx
loc_40103D:
xor eax, eax
retn
xor_func endp

Compression

- The Magic number of the compressed file is AP32
- Compression library called aPLib by Ibsen Software
- Lempel–Ziv (LZ) based
- Written in C

http://ibsensoftware.com/

Malware Deployment

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

NOPSEC

Malware Deployment

- Normal PE executable

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

- Normal PE executable
- Additional binary deployment method

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

- Normal PE executable
- Additional binary deployment method
- Two ways to deploy a DLL:

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

- Normal PE executable
- Additional binary deployment method
- Two ways to deploy a DLL:
  - rundll32 DLLName.dll,printMessage

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

- Normal PE executable
- Additional binary deployment method
- Two ways to deploy a DLL:
  - rundll32 DLLName.dll,printMessage
  - rundll32 DLLName.dll,#[ordinal number]

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

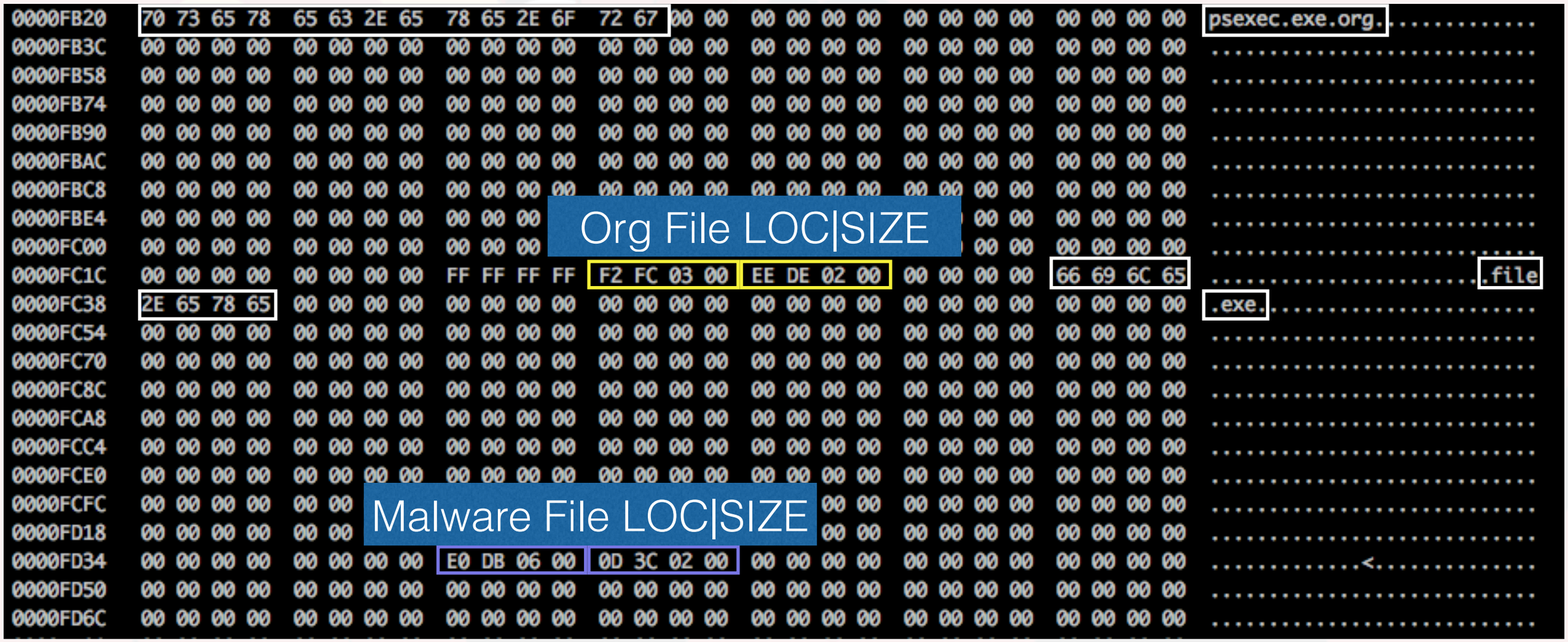
- Normal PE executable
- Additional binary deployment method
- Two ways to deploy a DLL:
  - rundll32 DLLName.dll,printMessage
  - rundll32 DLLName.dll,#[ordinal number]
- F-Secure discovered an OnionDuke DLL but not the associated packer

https://www.virustotal.com/en/file/0102777ec0357655c4313419be3a15c4ca17c4f9cb4a440bfb16195239905ade/analysis/

Malware Deployment

NOPSEC

DLL Flags



NOPSEC

DLL Flags

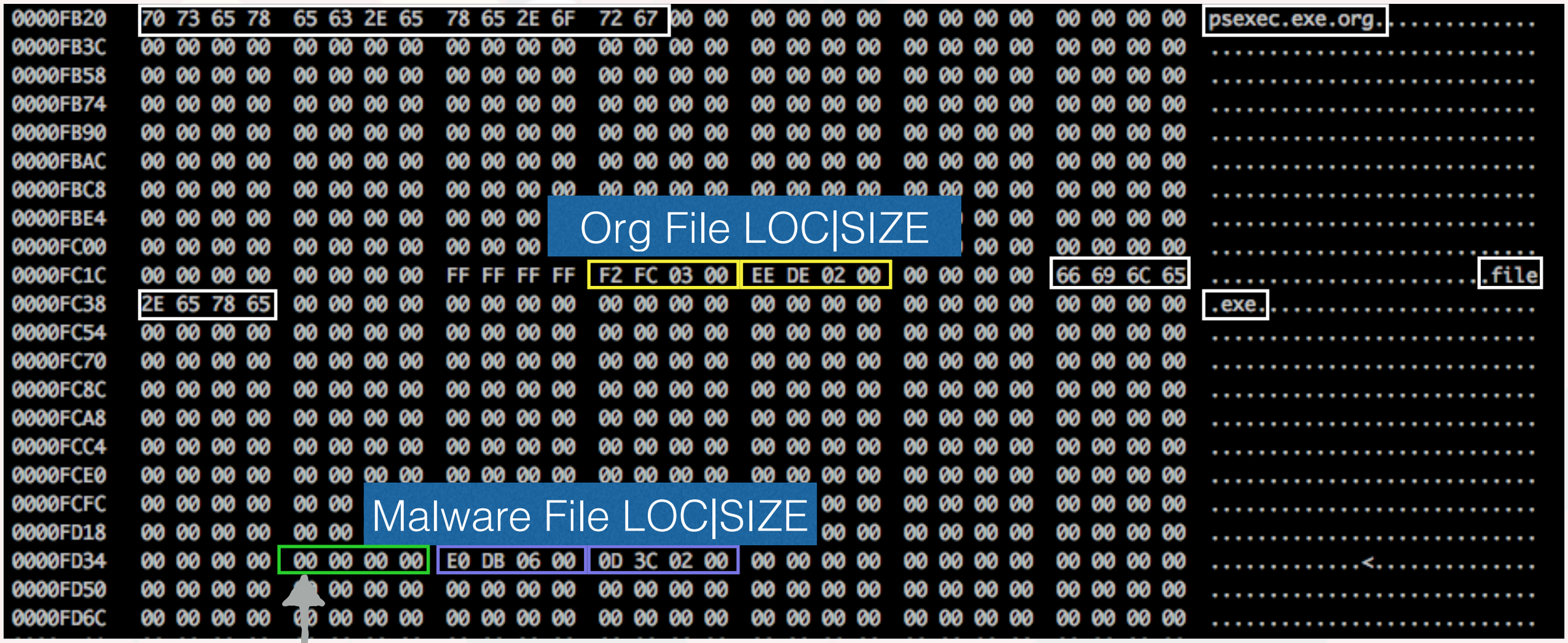
```
0000FB20  70 73 65 78  65 63 2E 65  78 65 2E 6F  72 67 00 00  00 00 00 00  00 00 00 00  00 00 00 00  psexec.exe.org.............
0000FB3C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB58  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB74  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FB90  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBAC  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBC8  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FBE4  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC1C  00 00 00 00  00 00 00 00  FF FF FF FF  F2 FC 03 00  EE DE 02 00  00 00 00 00  66 69 6C 65  ....................file
0000FC38  2E 65 78 65  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  .exe............................
0000FC54  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC70  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FC8C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCA8  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCC4  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCE0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FCFC  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD18  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD34  00 00 00 00  00 00 00 00  E0 DB 06 00  0D 3C 02 00  00 00 00 00  00 00 00 00  00 00 00 00  .............<..............
0000FD50  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
0000FD6C  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................................
```

Org File LOC|SIZE

Malware File LOC|SIZE

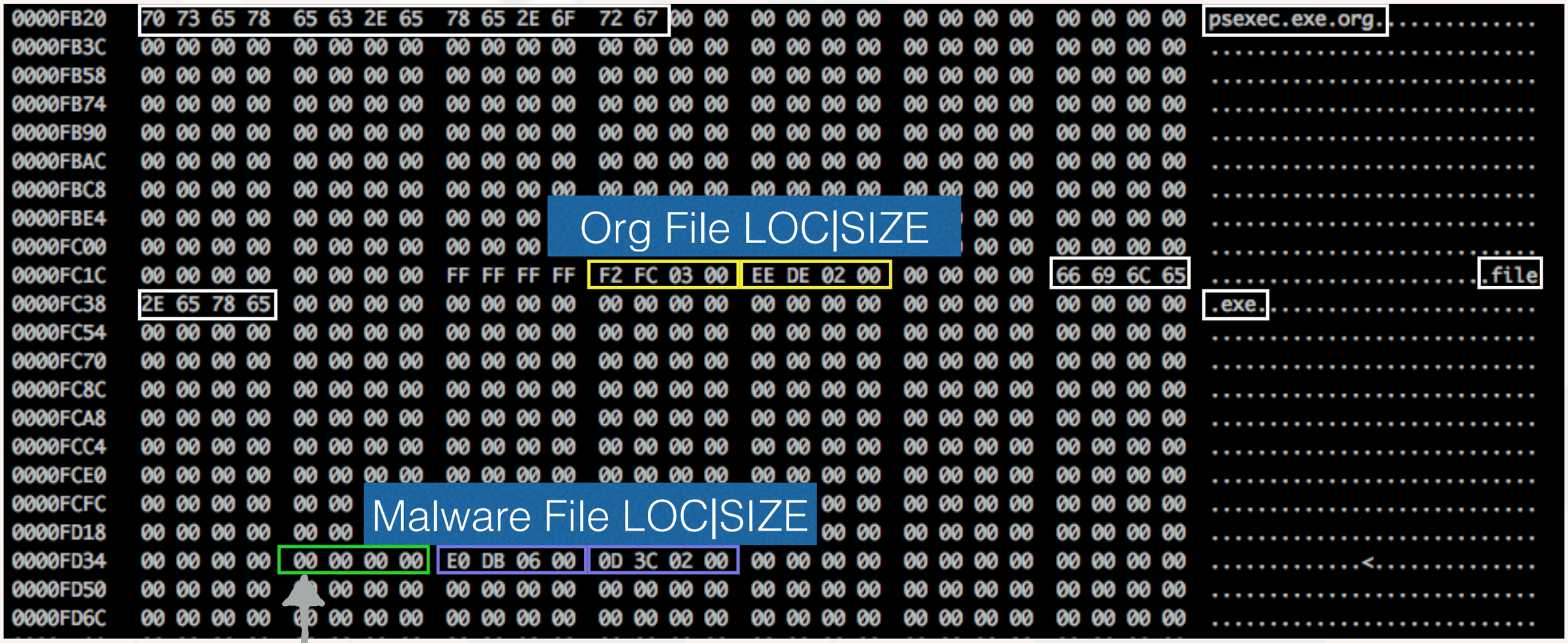
NOPSEC

DLL Flags



NOPSEC

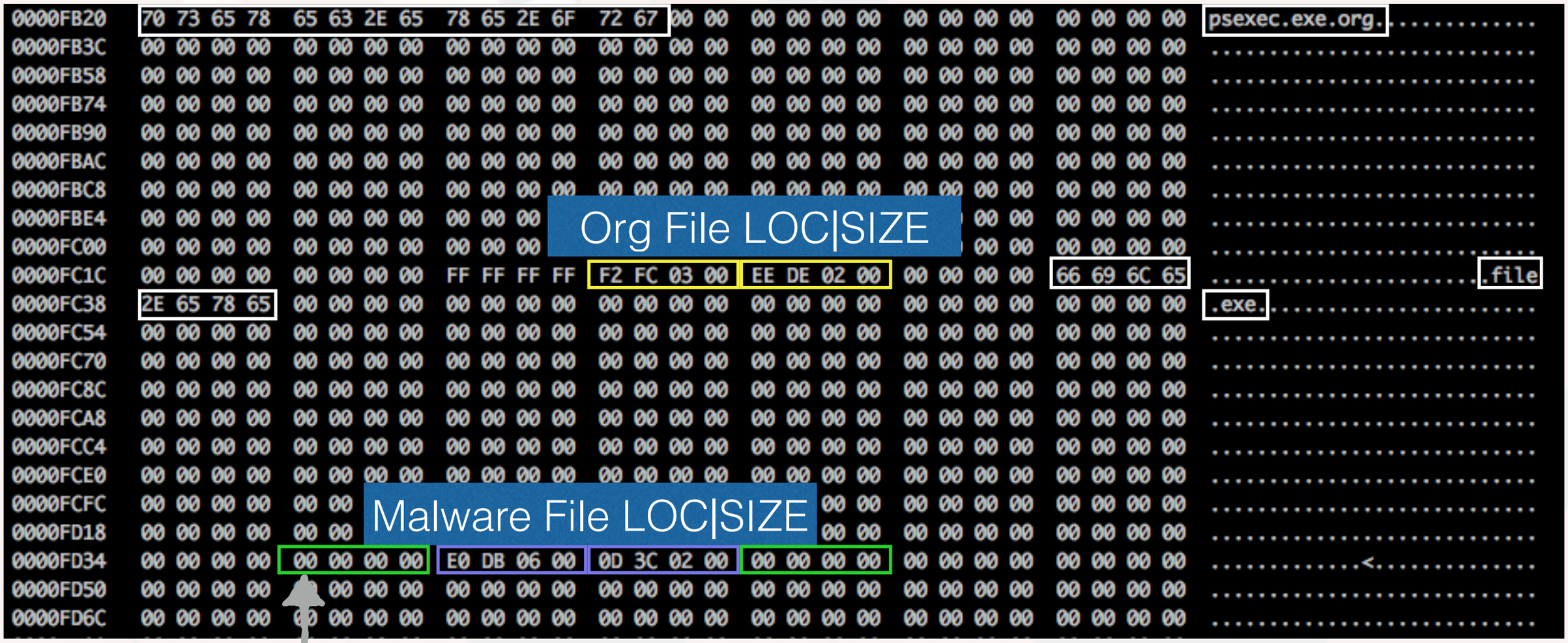
DLL Flags



0x01 Denotes malware as DLL

NOPSEC

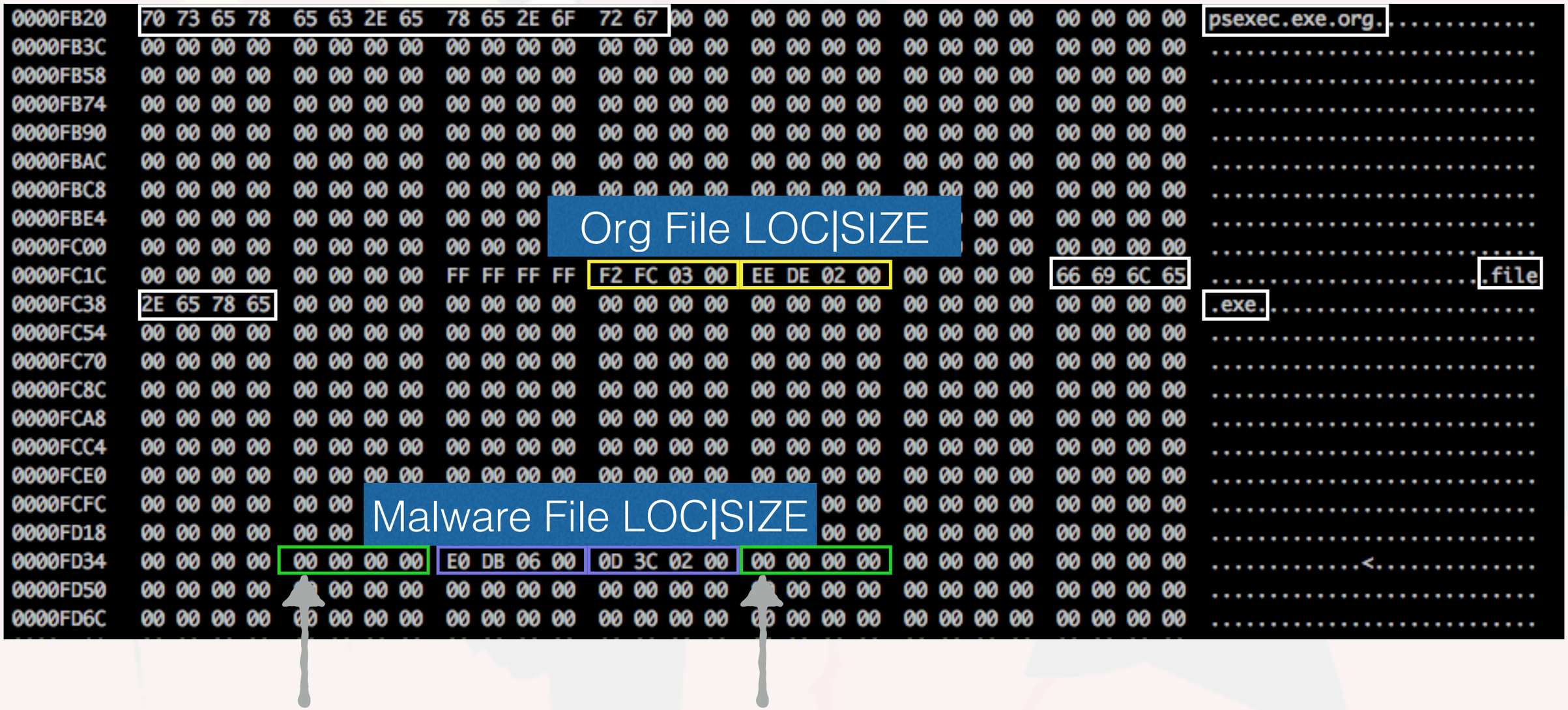
DLL Flags



0x01 Denotes malware as DLL

NOPSEC

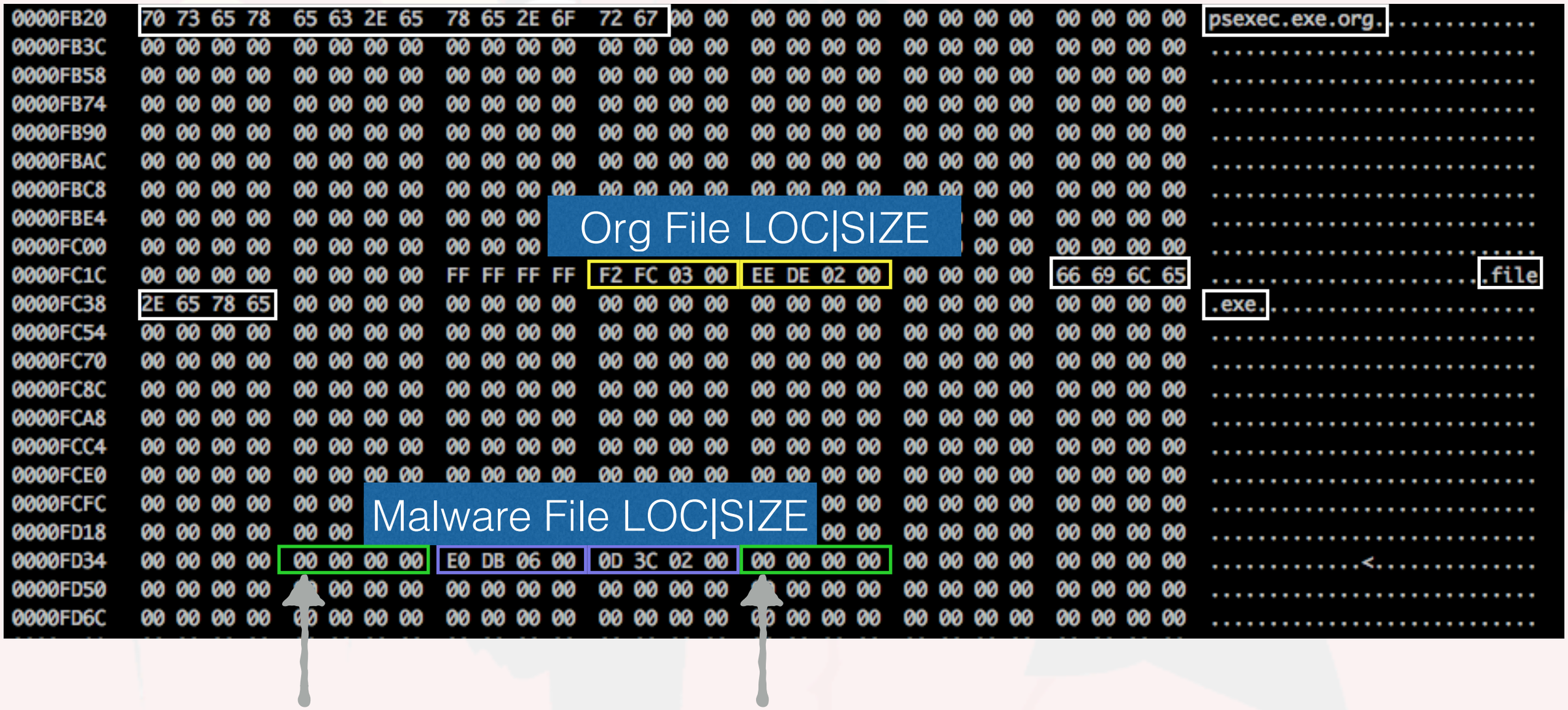
DLL Flags



0x01 Denotes malware as DLL

NOPSEC

DLL Flags



0x01 Denotes malware as DLL

Ordinal - Example: 0x01

NOPSEC

MITM Patching Framework Thoughts

- Written in C/C++
- Modular
- Campaign based
- Will be seen again

NOPSEC

Reusing the Packer

NOPSEC

Reusing the Packer

Reusing the Packer

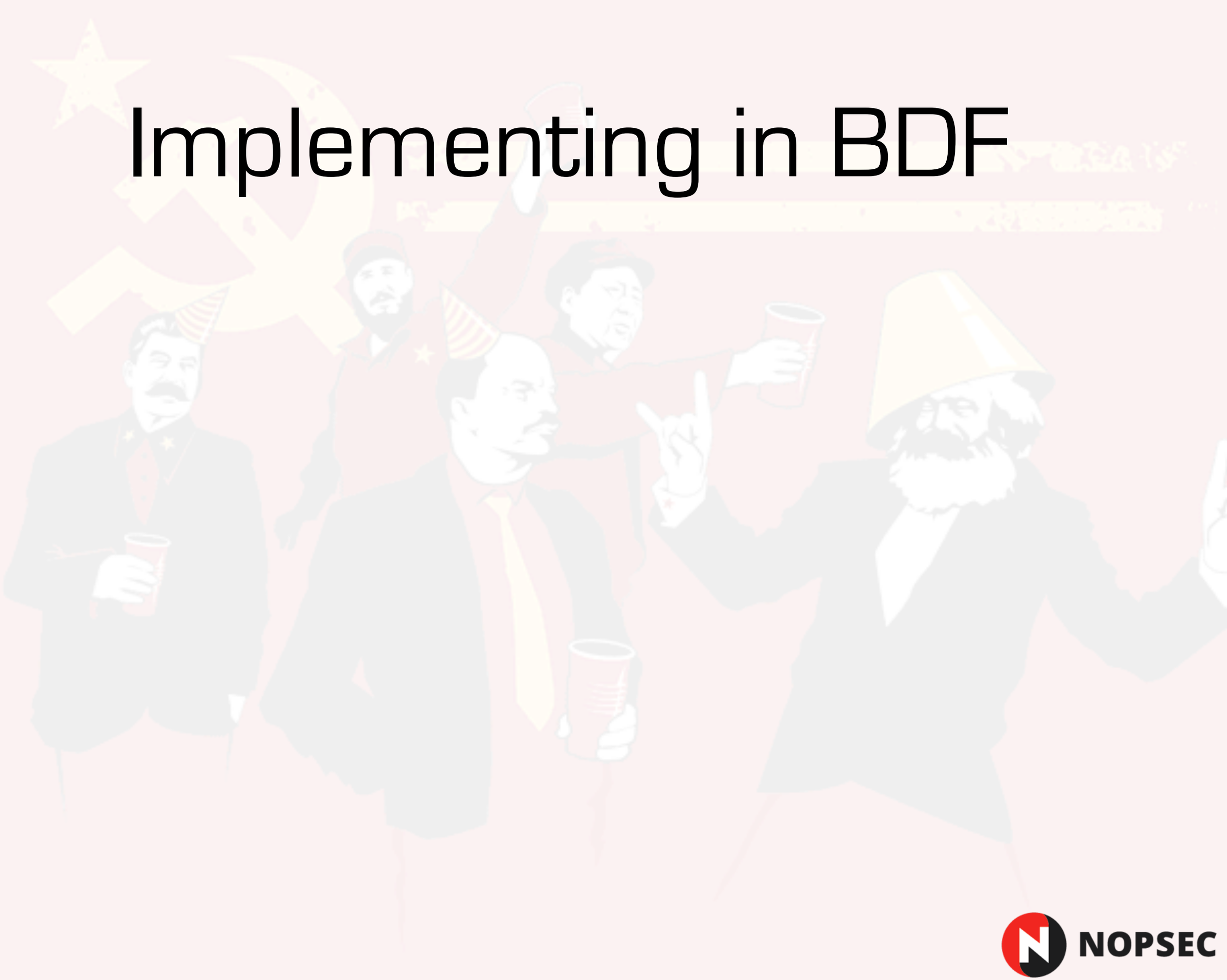
SHA256:	4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1
File name:	8361A794DFA231D863E109FC9EEEF21F4CF09DDD_http:live.sysinternals.c...
Detection ratio:	41 / 55
Analysis date:	2015-06-30 19:54:33 UTC (2 minutes ago)

https://www.virustotal.com/en/file/4910e4a5e2eed444810c62a0e9a32affb8a41693b2fcff49aabd9c125fa796d1/analysis/

Reusing the Packer

Reusing the Packer

Implementing in BDF



NOPSEC

Implementing in BDF

- Randomize XOR key, dropped filenames, and section hashes

Implementing in BDF

- Randomize XOR key, dropped filenames, and section hashes
- Cut out rsrc from incoming PE, update RVA pointers to icons

Implementing in BDF

- Randomize XOR key, dropped filenames, and section hashes

- Cut out rsrc from incoming PE, update RVA pointers to icons

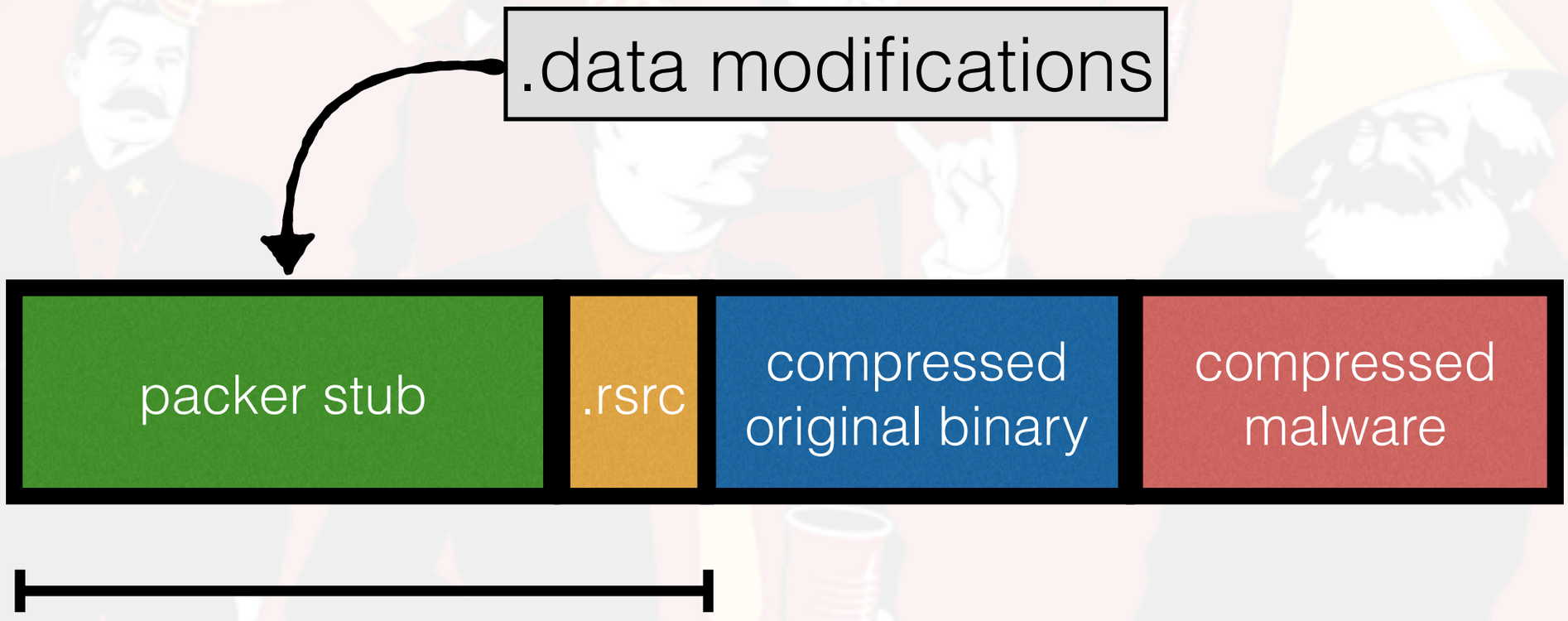
- Compress and XOR incoming file and user provided malware

Implementing in BDF

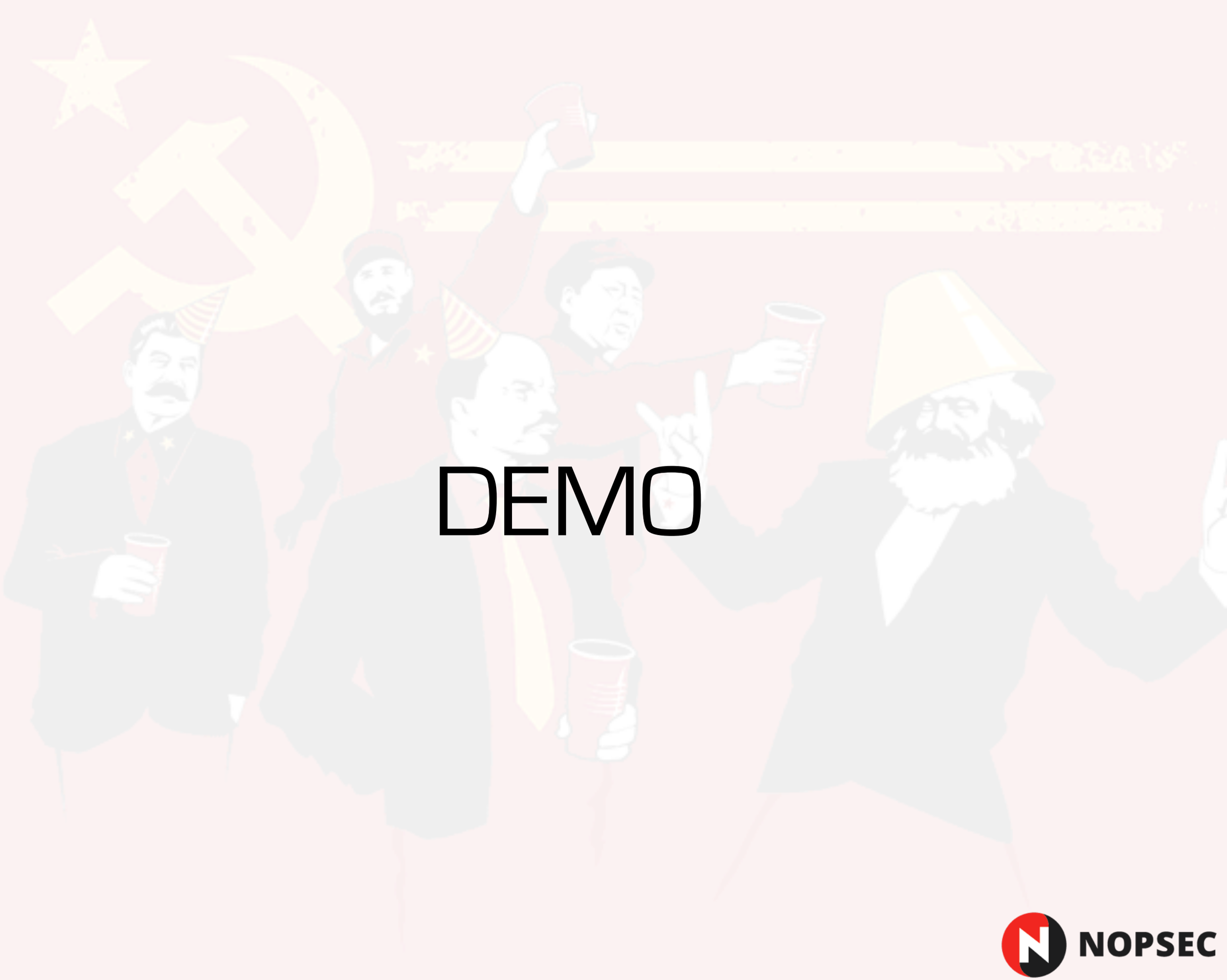
- Randomize XOR key, dropped filenames, and section hashes
- Cut out rsrc from incoming PE, update RVA pointers to icons
- Compress and XOR incoming file and user provided malware
- Update PE Headers, data section, and XOR keys

NOPSEC

Packer Layout



NOPSEC



DEMO

NOPSEC

AV Results

SHA256:	e2776feb7a4381ba7c0e08d2faf08108c9bf42a09dfeac690b466fdc00e5fedf
File name:	ZoomIt64.exe
Detection ratio:	20 / 55
Analysis date:	2015-07-01 22:14:19 UTC (1 minute ago)

https://www.virustotal.com/en/file/e2776feb7a4381ba7c0e08d2faf08108c9bf42a09dfeac690b466fdc00e5fedf/analysis/

Questions

twitter://@midnite_runr
github.com/secretsquirrel

Thanks to:

Travis Morrow
Matt Graeber
Jason Butterfield
Chris Truncer
Will Schroeder

Black Hat Sound Bites

- Nation State malware is effective but not magical
- Reusing ideas, techniques, and software (malware) will continue
- The Wassenaar Arrangement will do little to slow this activity