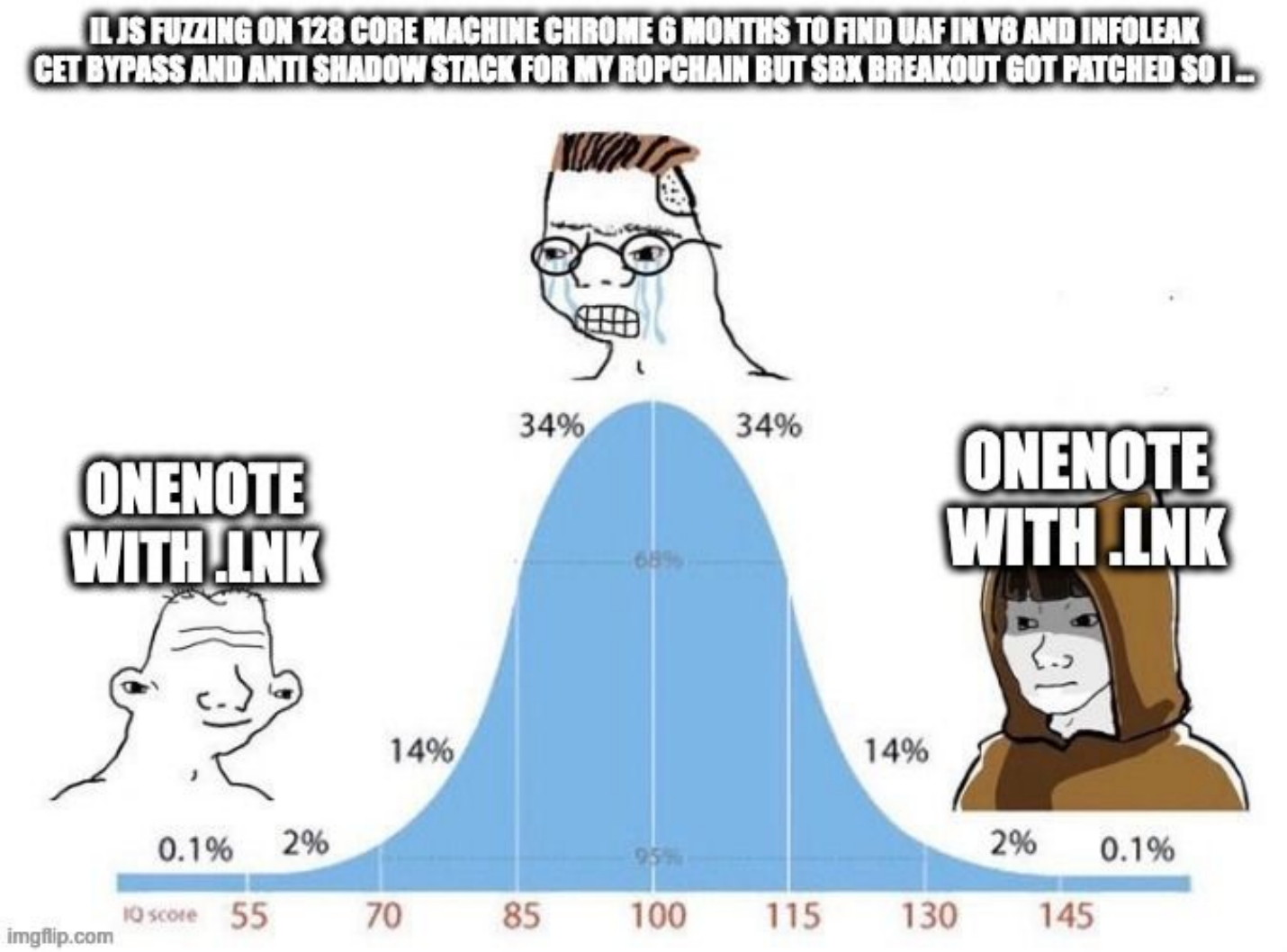

IL JS FUZZING ON 128 CORE MACHINE CHROME 6 MONTHS TO FIND UAF IN V8 AND INFOLEAK
CET BYPASS AND ANTI SHADOW STACK FOR MY ROPCHAIN BUT SBX BREAKOUT GOT PATCHED SO I...
ONENOTE WITH .LNK
ONENOTE WITH .LNK
34%
34%
68%
14%
14%
0.1%
2%
2%
0.1%
95%
IQ score
55
70
85
100
115
130
145
imgflip.com

To Proxy or not to Proxy

Gaining RCE with files
And what to do about it

Dobin Rutishauser
mastodon.social/@dobin

Developer // TerreActive

Pentester // Compass Security

Developer // Universitätsspital Zürich

SOC Analyst // Infoguard

RedTeam Lead // Raiffeisen

Memory Corruption Exploits & Mitigations
// BFH - Bern University of Applied Sciences

Gaining Access
// OST - Eastern Switzerland University of Applied Sciences

SSL/TLS Recommendations
// OWASP Switzerland

Burp Sentinel - Semi Automated Web Scanner
// BSides Vienna

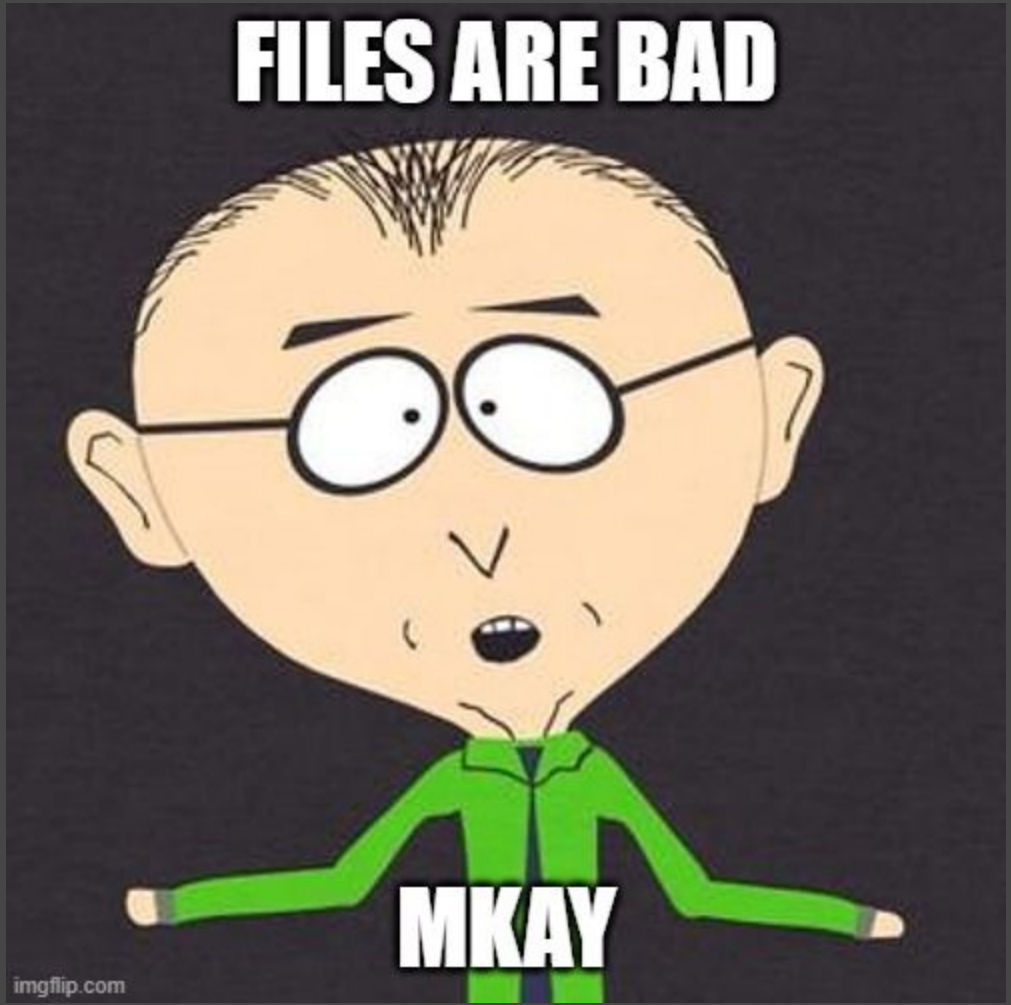
Automated WAF Testing and XSS Detection
// OWASP Switzerland Barcamp

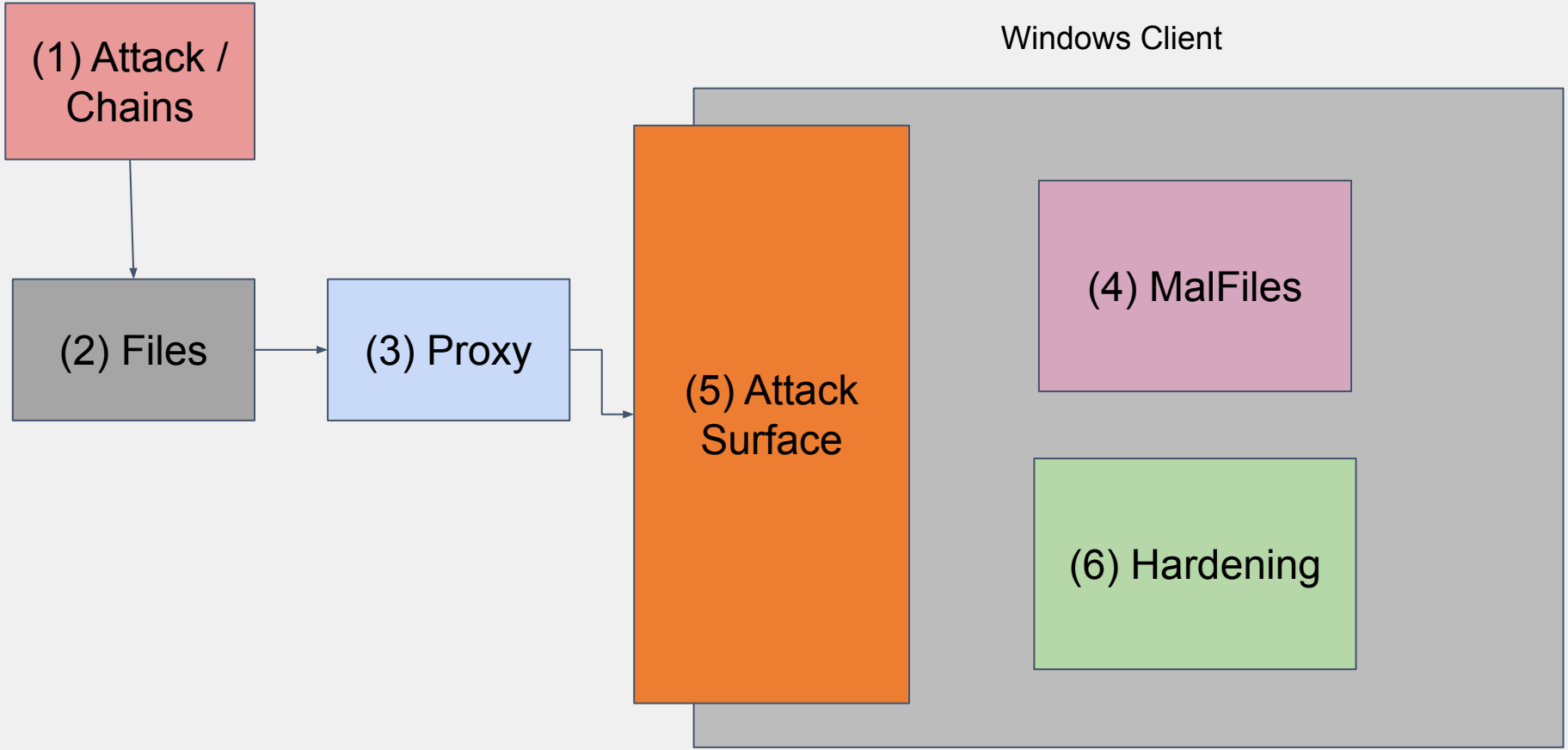
Fuzzing For Worms - AFL For Network Servers
// Area 41

Develop your own RAT - EDR & AV Defense
// Area 41

Avred - Analyzing & Reverse Engineering AV Signatures
// HITB HKT

My First And Last Shellcode Loader
// HITB BKK


FILES ARE BAD
MKAY
imgflip.com


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

- Intro
- 2025 Initial Access - Attack Chains
- What are files
- Content Filter & Bypasses
- Malicious File Types
- (Windows) Attack Surface
- (Windows) Hardening
- Recommendations
- Practical Examples
- Outro

The research is from 2023

Talk at:
- RedTeam Kabal
- SIGS SOC Forum (June 25)
- Xorlab (October 30)

Security Products not relevant for this talk

- *AntiVirus, EDR, Sandboxes etc.*
- *see my other talks to bypass*
  - *AV: Avred*
  - *EDR: SuperMega*

Red Teaming

Immitate Threat Actors

Compromise Ourselves

Bank

High security posture

Lots of users

Initial Access Vectors

Exploits

- Unpatched Software
- Misconfigured Software

Supply Chain

- Backdoored Software
- Connected Networks

Credential Misuse

- Phishing
- Password Storage
- Authentication
- Cloud
- Brute Force
- MFA
- Cookie Stealing

Gaining RCE with files

And what to do about it

Intro

Attack Surface - 2000's

Attacker

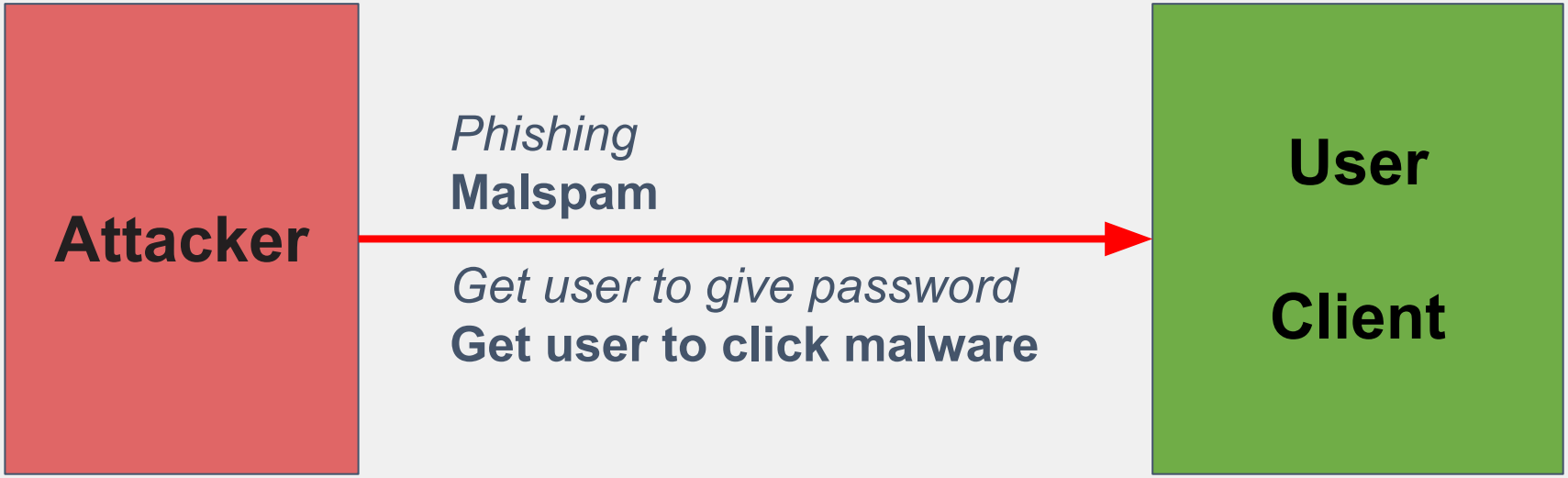
Hostscan
Portscan
Webscan
Vulnscan

Find vulnerabilities
Find misconfigurations
Exploit

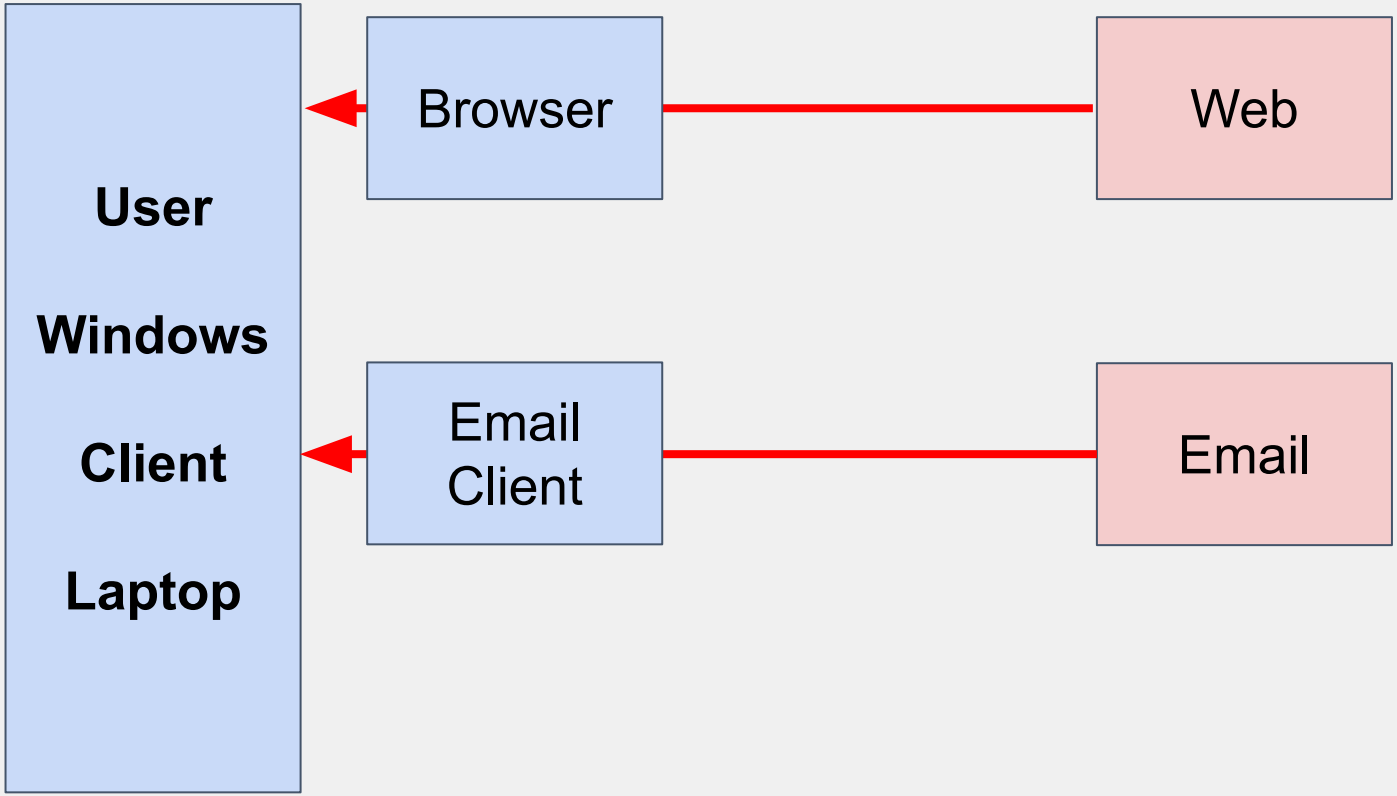
Network

Servers

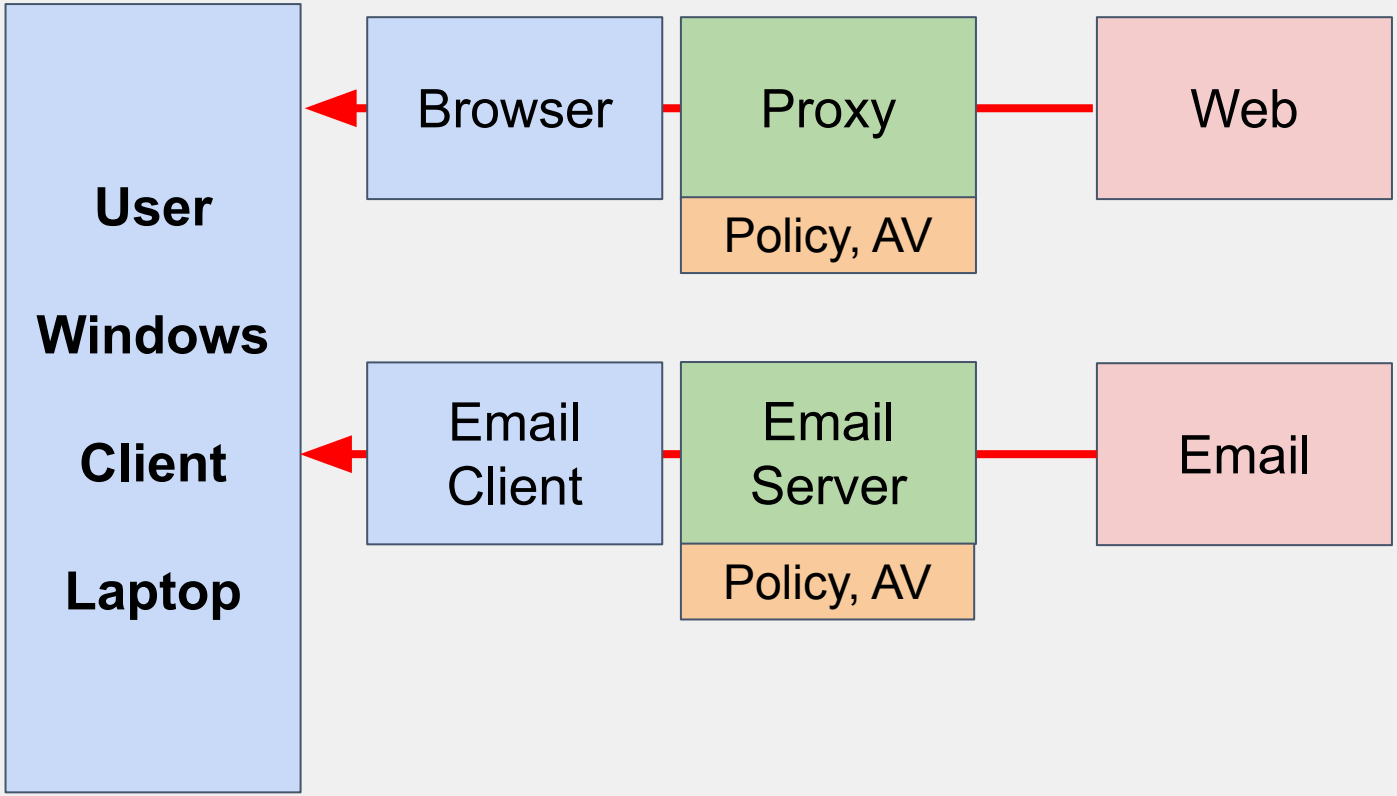
Attack Surface - 2020's



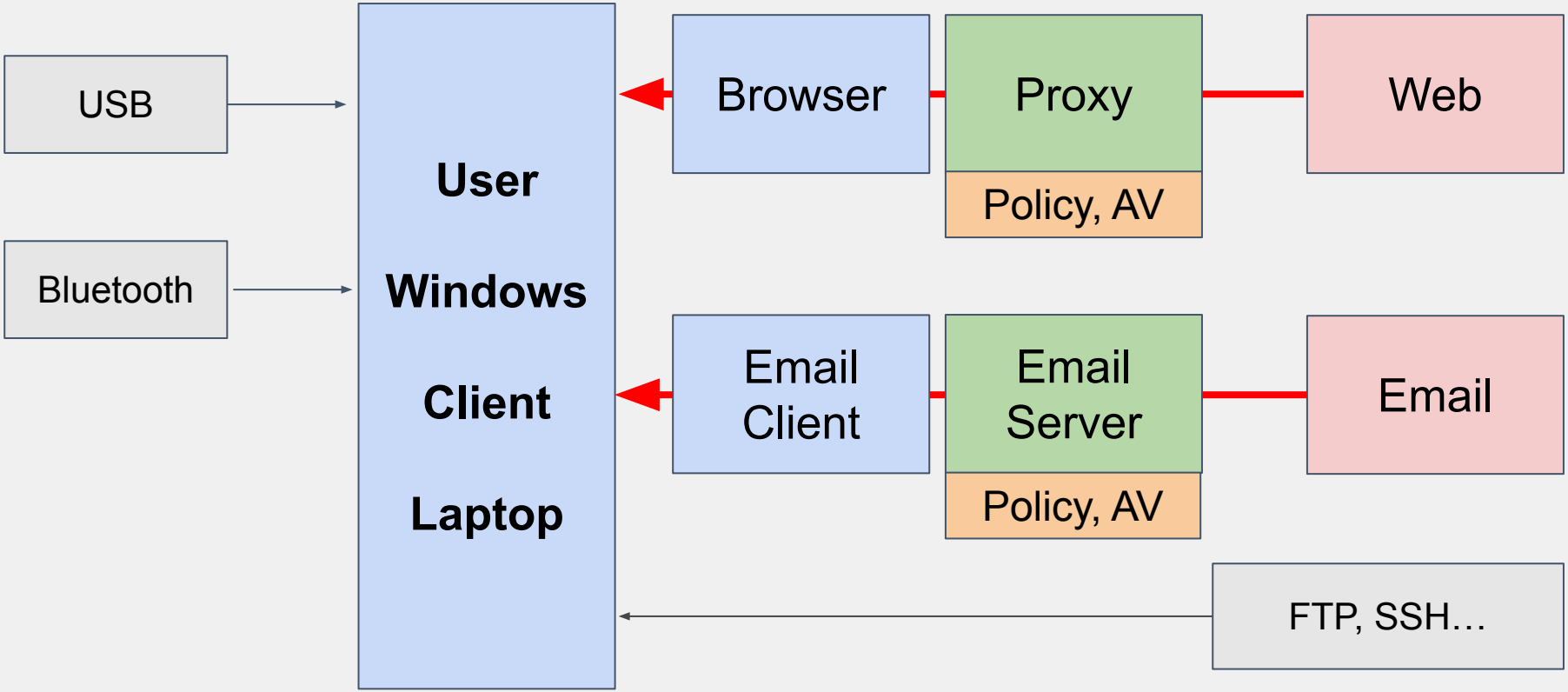
How files reach a client



How files reach a client



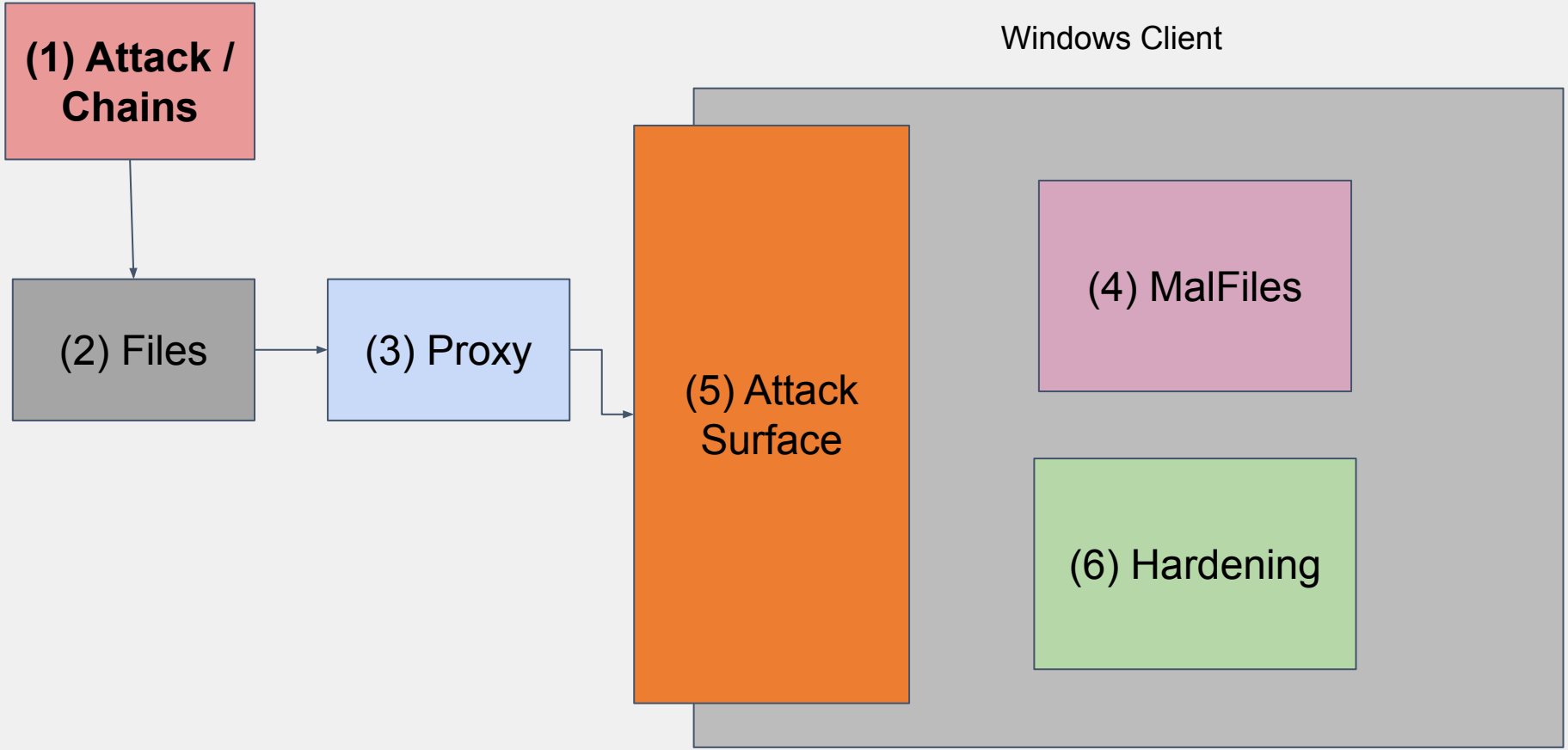
How files reach a client



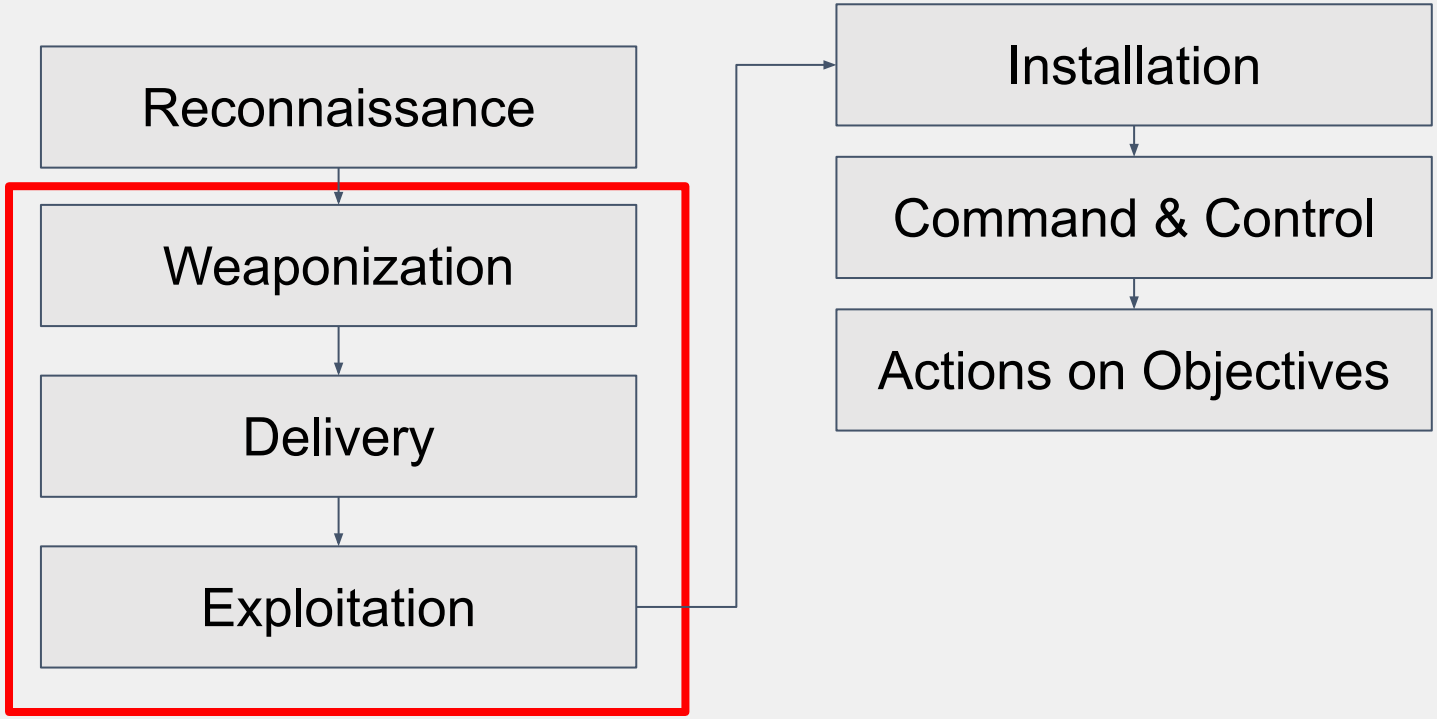
Gaining RCE with files

And what to do about it

Attacks in 2025


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

MITRE - Focus of this presentation



Phishing
Initial Access

Attacker Goals

What do attackers want?

Execute **their** code
on **your** system

Attacker Goals

What do attackers want?

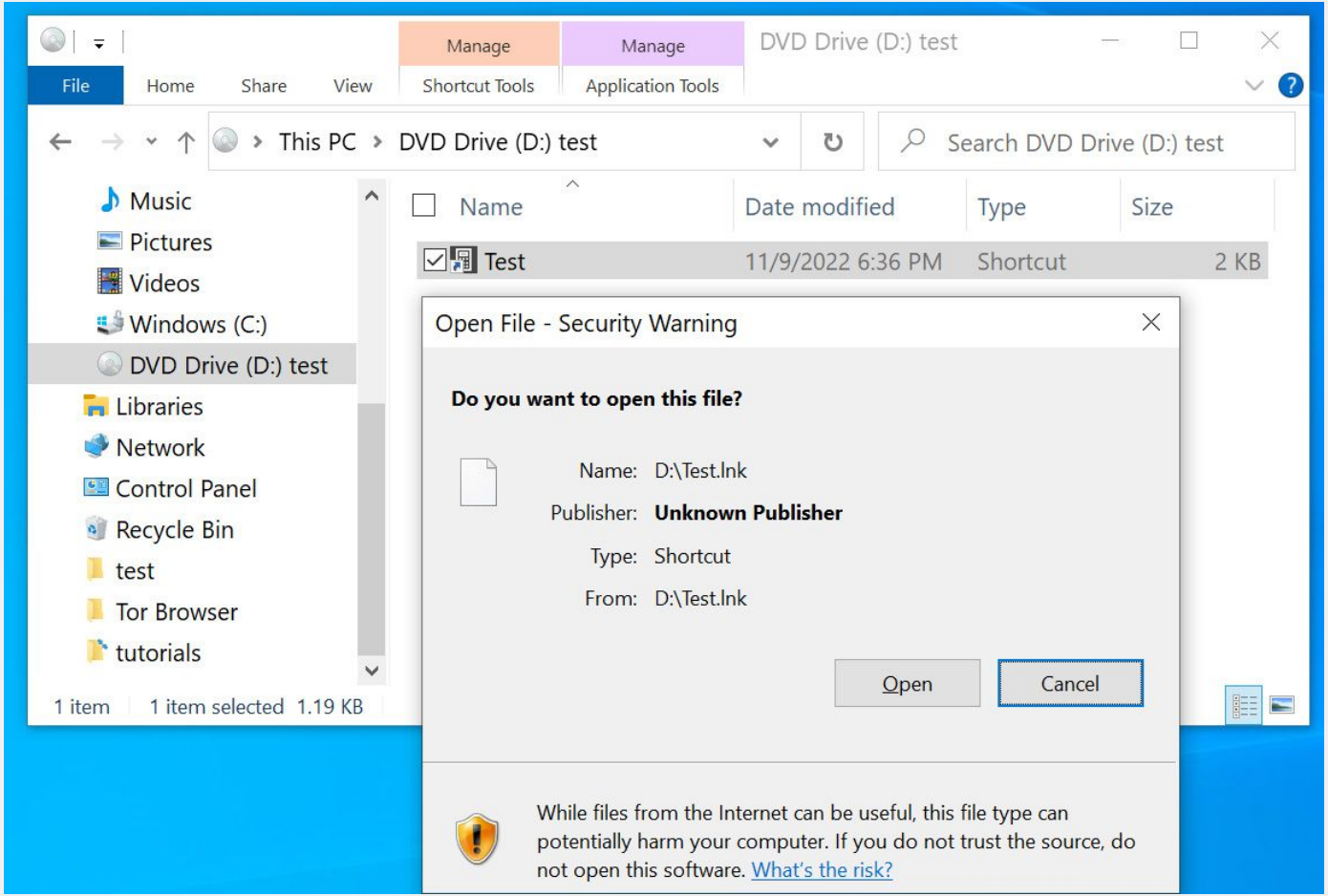
Requirements:

- Cheap
- Compatible with most users
- Easy to use
- Easy to mutate

Make victim **click an exe**

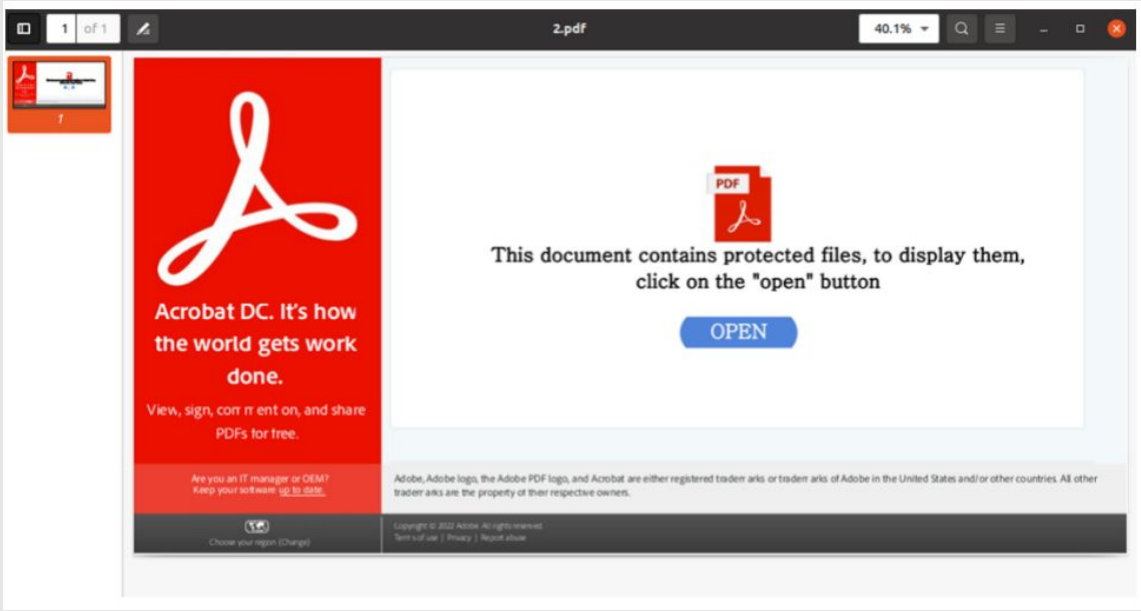
Initial Access
Remote Code Execution
Exploiting

Initial access with .lnk in .iso



Initial Access: PDF -> ZIP -> LNK -> rundll32.exe -> DLL

PDF
→ ZIP
→ LNK → CMD (rundll32.exe)
→ Qbot DLL



Initial Access Chains - Qbot

HTML Attachment → Password-Protected Zip → IMG → LNK → CMD → Qbot DLL
HTML Attachment → Password-Protected Zip → IMG → LNK → Qbot DLL
HTML Attachment → Password-Protected Zip → VHD → LNK → CMD → Qbot DLL
HTML Attachment → Password-Protected Zip → VHD → LNK → Qbot DLL

PDF Attachment → Actor-Controlled URL → Password-Protected Zip → ISO → WSF → Qbot DLL
PDF Attachment → Actor-Controlled URL → Password-Protected Zip → IMG → LNK → Qbot DLL

Zip Attachment→ OneNote File → HTA → CURL → Qbot DLL
URL → Zip → OneNote File → HTA → CURL → Qbot DLL
PDF Attachment → Actor-Controlled URL → Zip → ISO → LNK → CMD → EXE → Qbot DLL
PDF Attachment → OneDrive URL → JavaScript File → PowerShell → Qbot DLL

OneNote Attachment → WSF → Jscript → PowerShell → Qbot DLL
OneNote Attachment → HTA → CURL → Qbot DLL
OneNote Attachment → CMD → PowerShell → Qbot DLL
OneNote Attachment → CHM → PowerShell → Qbot DLL

Attack Chain Components

Delivery / Container

- What the user sees (presentation)
- .zip, .iso, .doc, .pdf

Execution / Trigger

- Initial RCE
- .lnk, .vbs, .bat, .exe

Staging

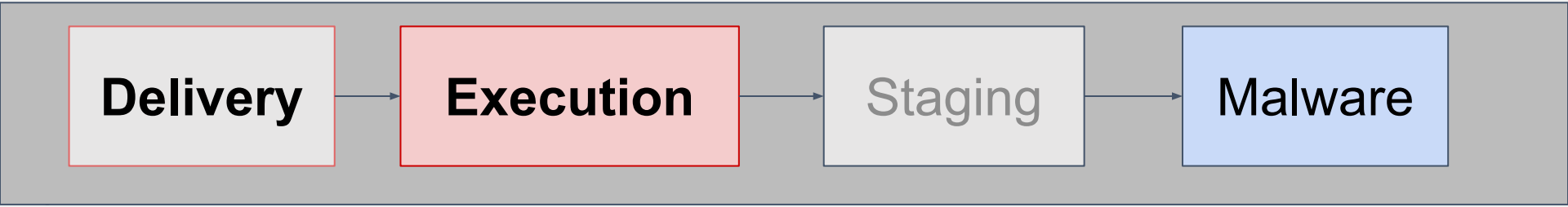
- Lots of different code executions
- .bat, .vbs, .js, .exe, rundll, curl, bits-transfer, …
- More download, persistence

Malware / Payload

- The actual C2 malware RAT
- Usually downloaded
- .exe, .dll

Initial Access Chains - Qbot

HTML Attachment → Password-Protected Zip → IMG → LNK → CMD → Qbot DLL
HTML Attachment → Password-Protected Zip → IMG → LNK → Qbot DLL
HTML Attachment → Password-Protected Zip → VHD → LNK → CMD → Qbot DLL
HTML Attachment → Password-Protected Zip → VHD → LNK → Qbot DLL



URL → Zip → OneNote File → HTA → CURL → Qbot DLL
PDF Attachment → Actor-Controlled URL → Zip → ISO → LNK → CMD → EXE → Qbot DLL
PDF Attachment → OneDrive URL → JavaScript File → PowerShell → Qbot DLL

OneNote Attachment → WSF → Jscript → PowerShell → Qbot DLL
OneNote Attachment → HTA → CURL → Qbot DLL
OneNote Attachment → CMD → PowerShell → Qbot DLL
OneNote Attachment → CHM → PowerShell → Qbot DLL

Example 1: Email -> ZIP -> VBS

https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

Hi There,

Please take a peek at the document contained in the one way link down below.

ONE-WAY LINK

Passcode: W1289

Hav

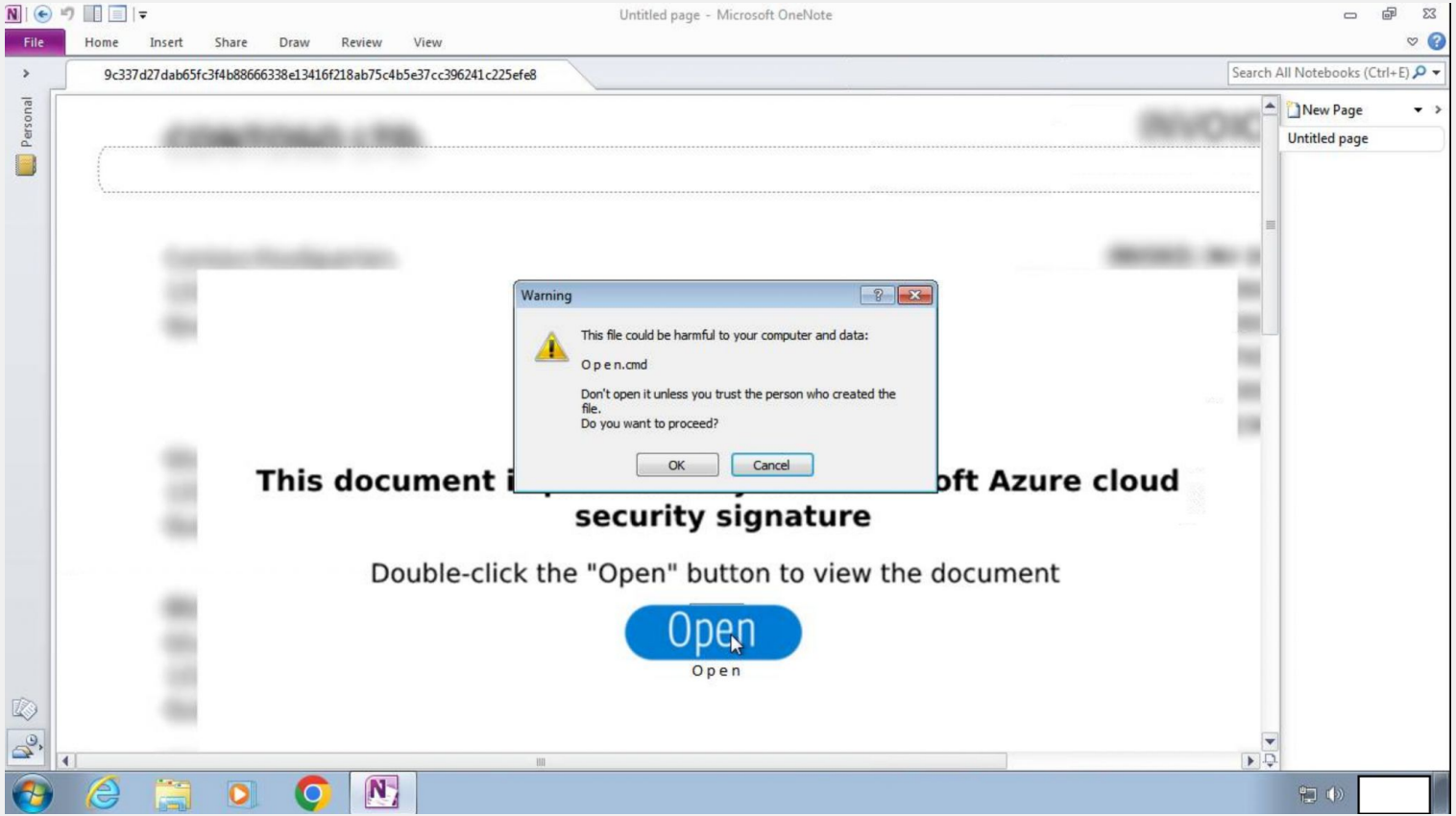
Document[2023.10.11_08-07].vbs

Readme[2023.10.11_08-07].txt

```
You can discover the pitch followed below, attached
with this particular email message. Please remember
to give it a read and of course email or give me a
call in case any questions arise.
```

Example 2: Email -> PDF -> CMD

https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/



Example 3: Email -> ZIP -> JS

https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/

Confirm Forest City account status - Mozilla Thunderbird

File Edit View Go Message Tools Help

From Gloria Z. Drewes <no-reply@astragale-bien-etre.info>

To

Date Wed, 18 Jan 2023 21:56:25 +0300

Subject **Confirm Forest City account status**

Dear Customer,

I have sent you the documents regarding your account status, please download file.

Best regards,

Gloria Z. Drewes
2705 Woodrow Way, Livingston, TX, 77351
Phone: +1-(946)-895-5149
Fax: +1-(885)-526-4370

Distributor for USA: Forest City

VAT Reg. USA 489665771

1 attachment: 98181772.zip 7.8 KB

Save

98181772.zip 7.8 KB

98181772.zip

Extract

File Home Share View Compressed Folder Tools

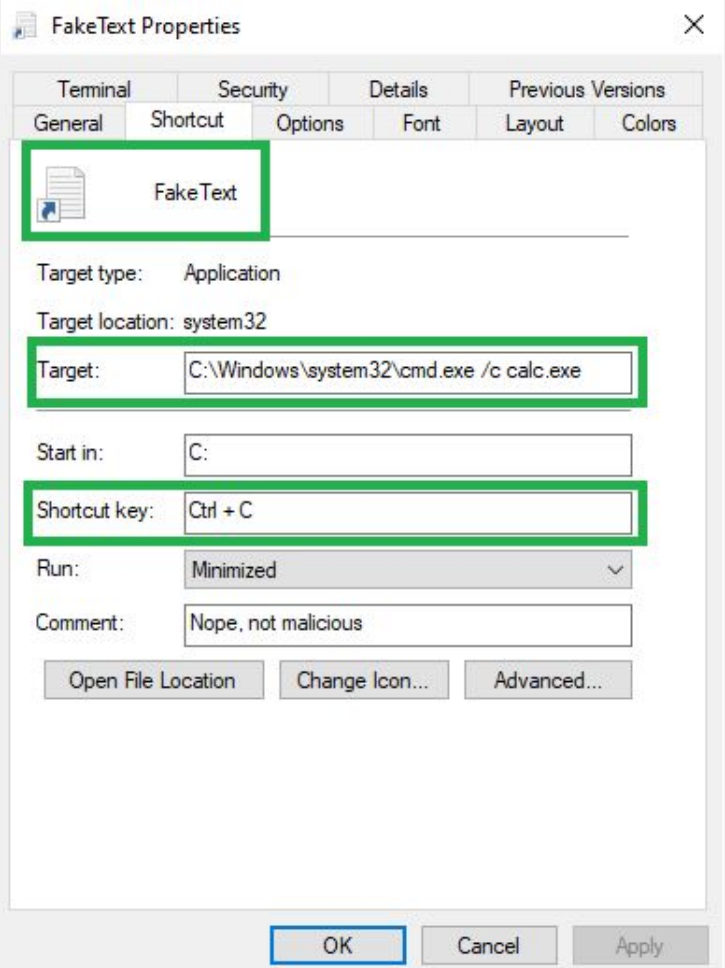
« pid-8920 › 98181772.zip

Search 98181772.zip

Name	Type	Size	Date modified
2326.js	JavaScript File	29 KB	1/13/2023 2:23 PM

1 item

Example 4



.lnk: Windows Link File

Can point to any file - including EXE
.. powershell.exe

Phishing = Password Fishing

What about sending malicious **files (or links to files)?** MalSpam?

IAFD - Initial Access via File Delivery
TMD - Targeted Malware Delivery
DIC - Delivery-based initial compromise

Execbait
SpearRCE
RCE Delivery
Malware Drop

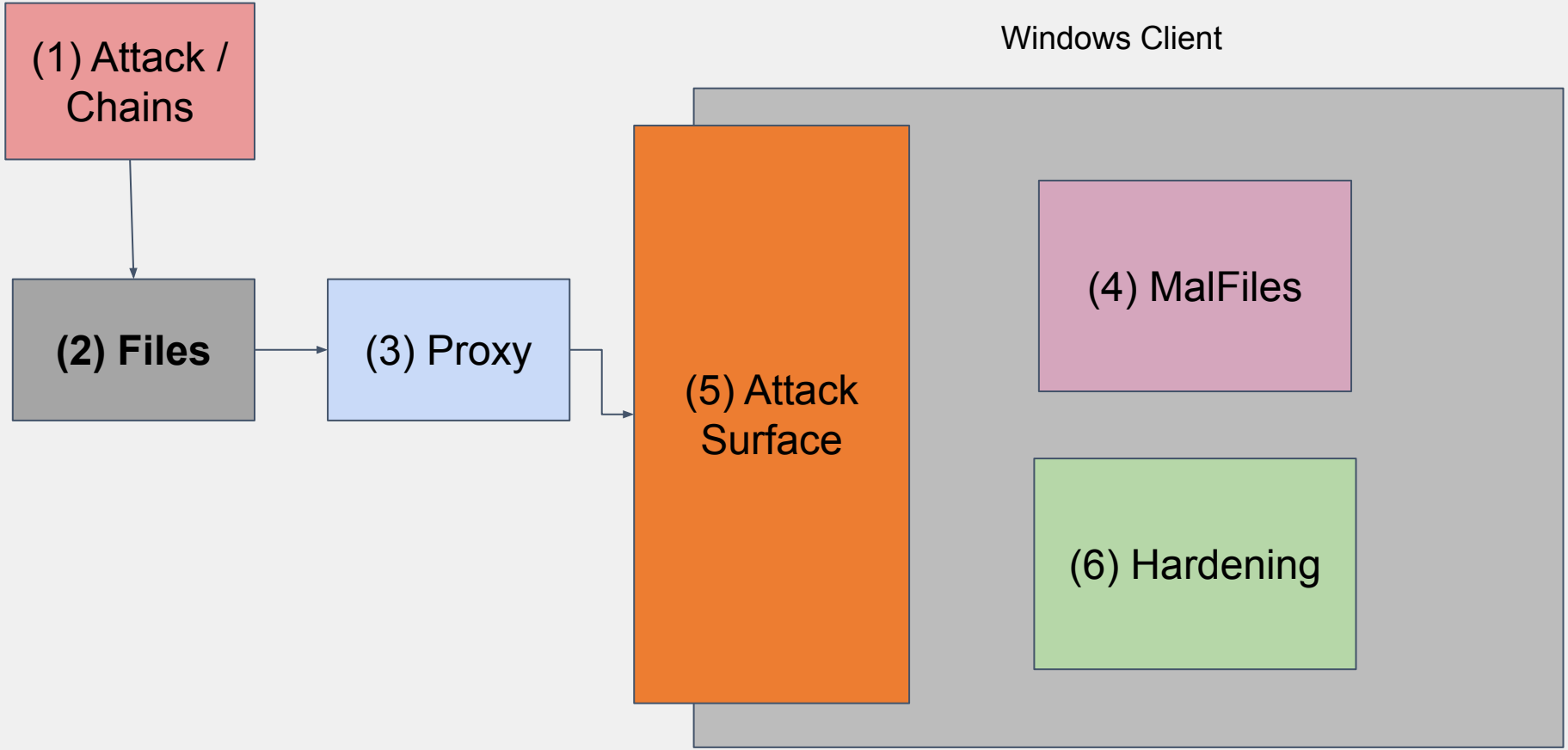
Philex (File + Exploit)
FEX (File-Executed Exploit)

From ChatGPT

Gaining RCE with files

And what to do about it

What are files?


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

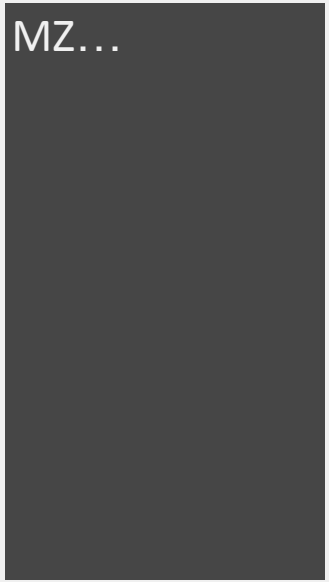
Files

Files are **unstructured data** (byte array)
with a name (invented with UNIX)

How we know whats inside?

- **Filename**
- **Magic bytes**
- **Content Type**

virus.exe



virus.**exe**

MZ…

Filename Extension

Used by **Windows**

- .docx: MS Office
- .zip: A archive
- .xml: Text

virus.exe

Magic Bytes

Used By **Linux**

MZ, ELF, #!/bin/bash

```
$ hexdump -C --length 16 /bin/bash
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|

$ file /bin/bash
/bin/bash: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, stripped
```

virus.exe

MZ…

Content Type

Used by **browsers** & apps to describe data blobs (think in a database, or HTTP)

Based on file extension, magic bytes?

`.csv`	Comma-separated values (CSV)	`text/csv`
`.doc`	Microsoft Word	`application/msword`
`.docx`	Microsoft Word (OpenXML)	`application/vnd.openxmlformats-officedocument.wordprocessingml.document`

File Type Identification

File Extension

virus.exe

MZ…

Magic Bytes

virus.exe

MZ…

Content-Type

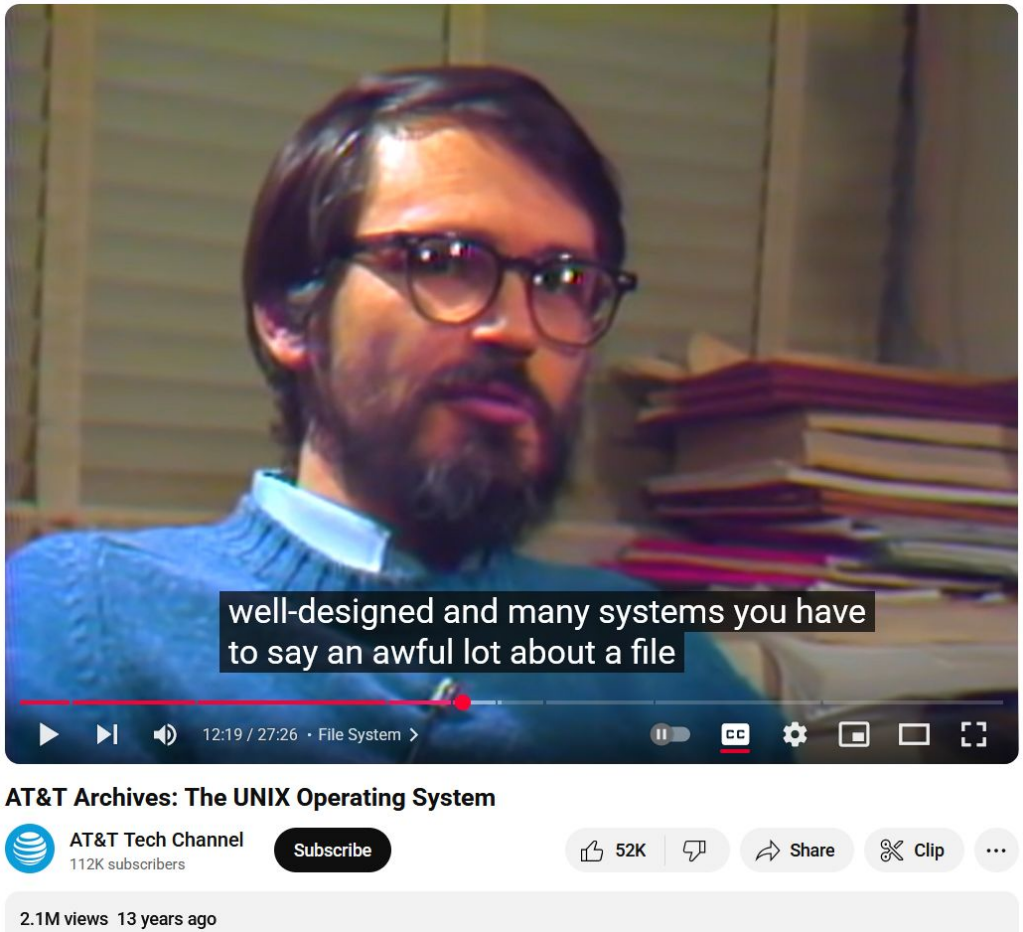
application/executable

virus.exe

the reasons the system (UNIX) works as well as it does is that the file system is well-designed ..

In many systems you have to say an awful lot about a file before you can do anything with it you have to say **where** it is and **how big** it is and **what kind of information** it's going to that's going to be in it all kinds of things that are basically utterly completely irrelevant

here you don't have to do any of that a file is as big as it is **it doesn't matter where it is as long as you know what it's called**

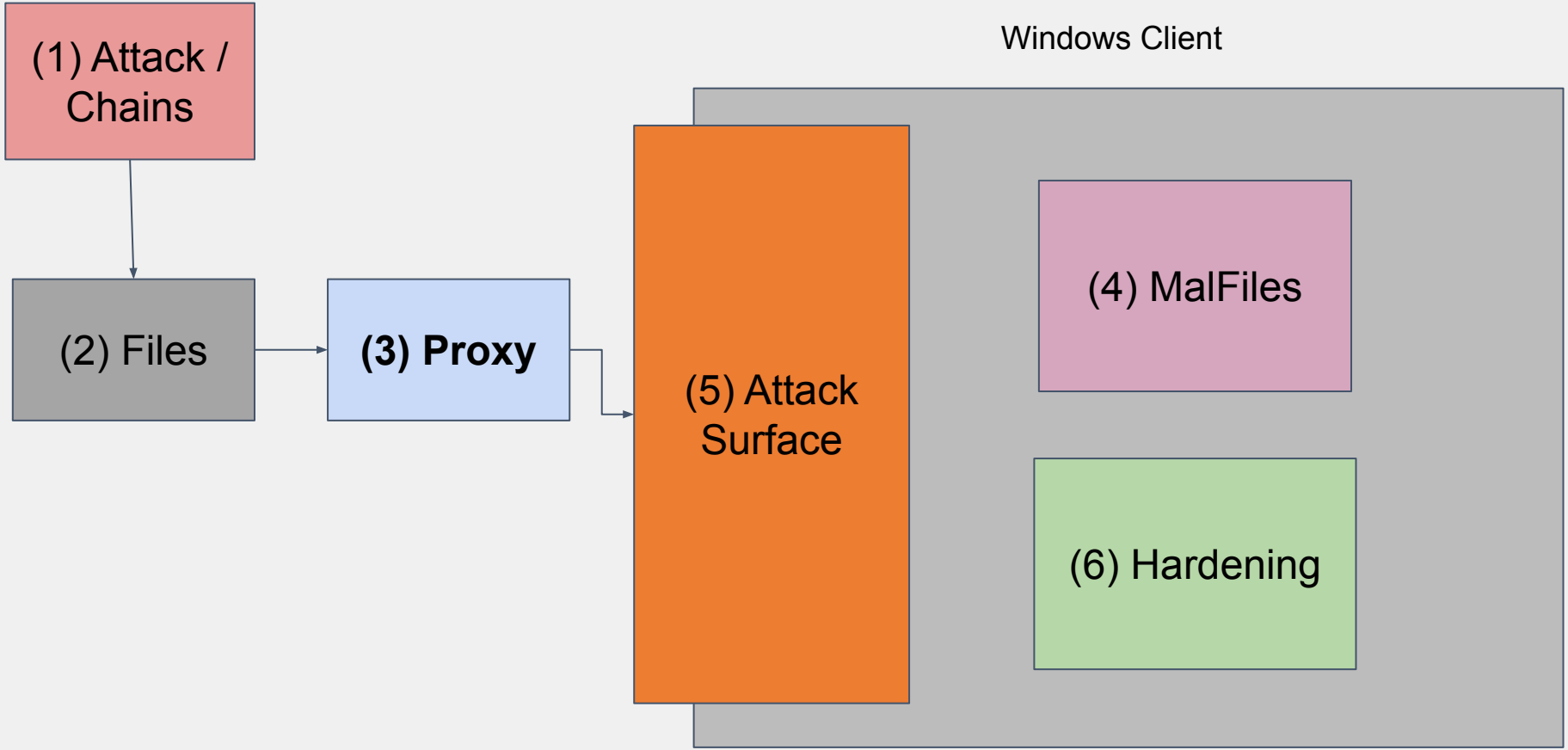


Brian W. Kernighan

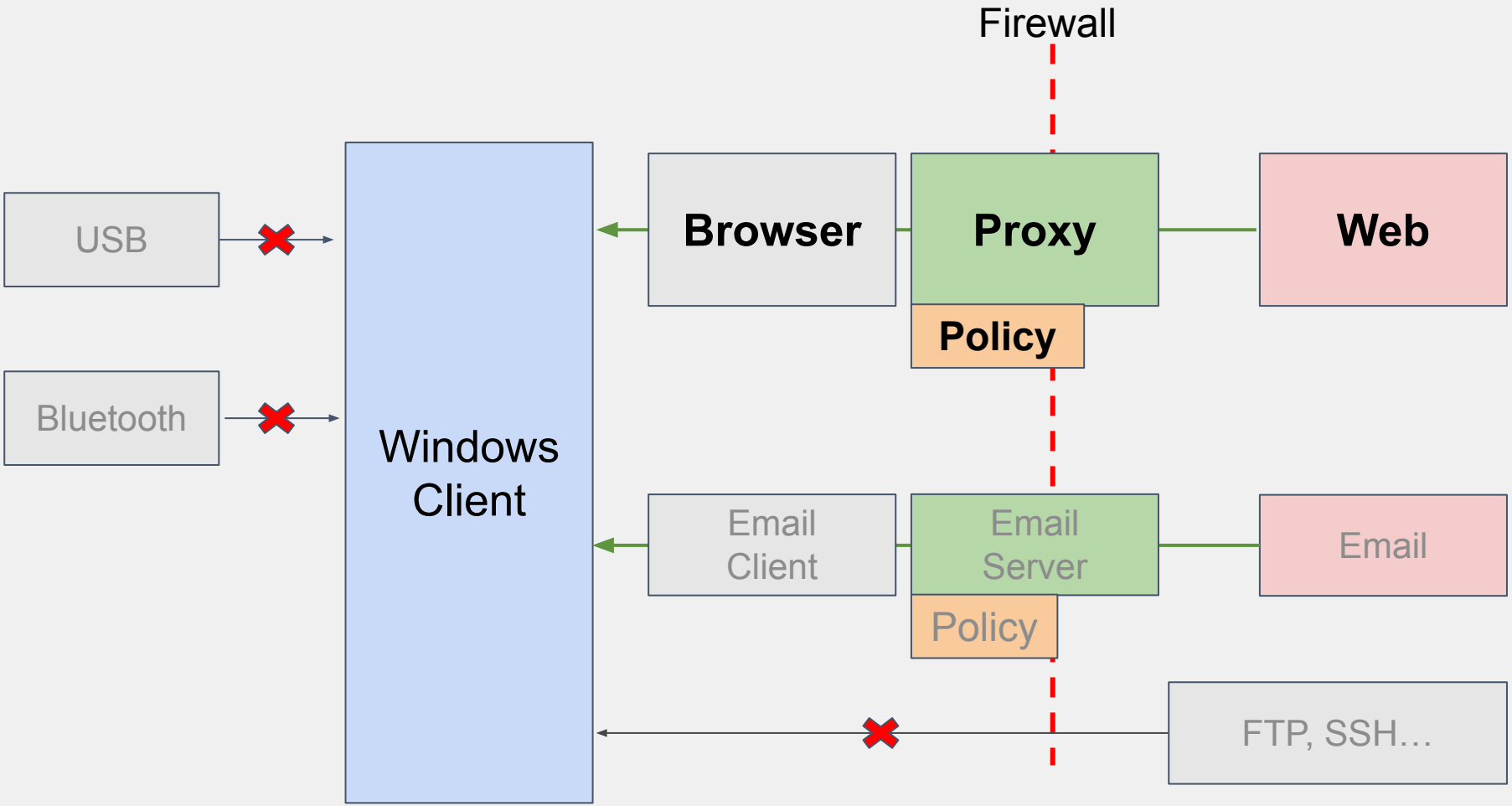
Gaining RCE with files

And what to do about it

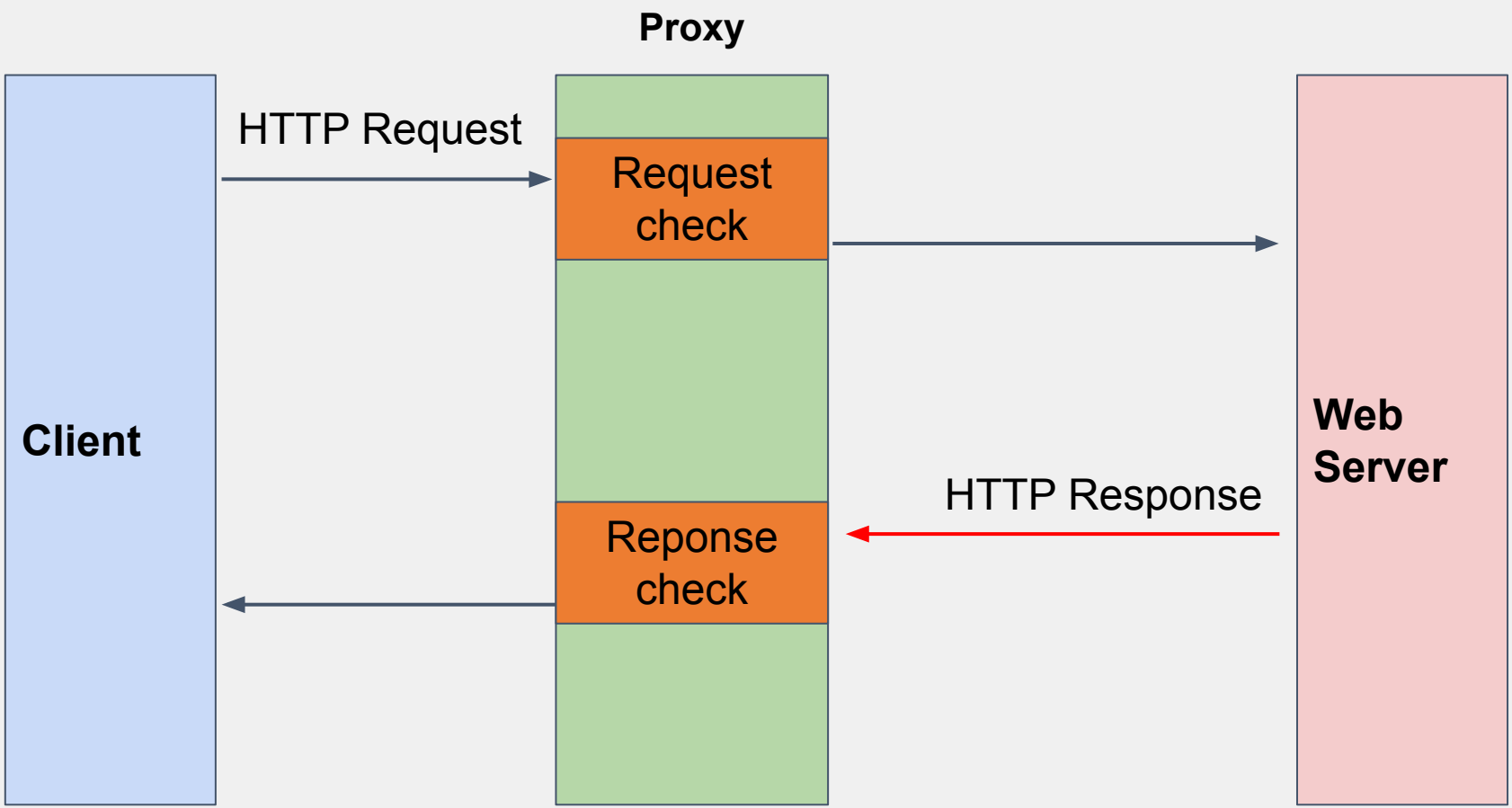
Content Filter


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

How files reach a client



Proxy Content Filter



File Download: HTTP Response Header

Request:

```
HTTP/1.1 GET mega.com/download/381
```

Response:

```
HTTP/1.1 200 OK
Content-Disposition: attachment; filename=test.svg
Content-Type: image/svg+xml


<data…>
```

File Download via HTTP - Request & Response

General

Request URL: https://calibre-ebook.com/downloads/demos/demo.docx

Request Method: GET

Status Code: 200 (from disk cache)

Remote Address: 166.78.105.155:443

Referrer Policy: origin

Response Headers

accept-ranges: bytes

content-length: 1311881

content-type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

date: Thu, 07 Apr 2022 17:40:27 GMT

etag: "51c3cbe8-140489"

last-modified: Fri, 21 Jun 2013 03:43:36 GMT

server: nginx

demo (1).docx

demo.docx

Proxy / Content Filter should protect Windows Client against malicious files

Request:

```
HTTP/1.1 GET /data/file.txt
```

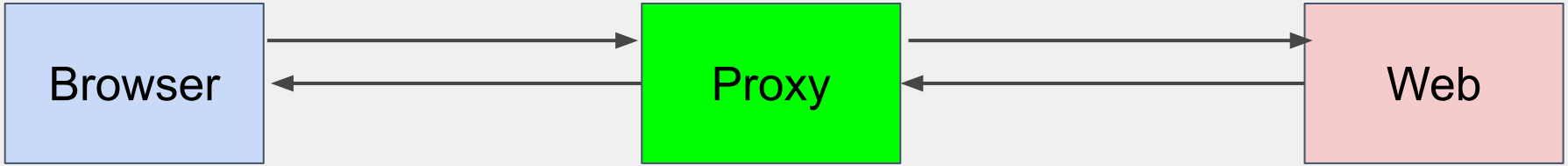
Response:

```
HTTP/1.1 200
Content-Disposition: attachment,
                     filename=file.txt
Content-Type: application/text
Data: Bytes
```

Proxy / Content Filter should protect Windows Client against malicious files

Request:

```
HTTP/1.1 GET /data/file
```



Response:

```
HTTP/1.1 200
Content-Disposition: attachment,
                     filename=file.exe
Content-Type: image/svg+xml
Data: Bytes
```

What filename will the browser choose?

- file?
- file.exe?
- file.svg?
- file.txt?

Browser decides!

Request:

```
HTTP/1.1 GET /data/file
```

Response:

```
HTTP/1.1 200
Content-Disposition: attachment,
                     filename=file.exe
Content-Type: image/svg+xml
Data: Bytes
```

Middleboxes dont know what the endpoints are doing

Proxy vs Chrome/Firefox/IE11

Whis information will the browser use to give the file a filename?

Attacks:

- *Confusion by HTTP header*
  - *Missing or added quotes, whitespaces*
  - *Multiple “Content-Disposition” headers lolz*
- *Confusion with filename*
  - *URL filename or “Content-Disposition” filename?*
  - *Broken “Content-Disposition” header?*
- *Content-Type does not match magic bytes*
- *Content-Type does not match file extension*

Content-Filter Misconfiguration: Filter by Content Type

Content-Filter blocks **.exe** files via **Content-Type?**

```
Content-Type: "application/vnd.microsoft.portable-executable"
```

Instead use:

```
Content-Type: "application/octet-stream"
```

Two primary MIME types are important for the role of default types:

- `text/plain` is the default value for textual files. A textual file should be human-readable and must not contain binary data.
- `application/octet-stream` is the default value for all other cases. An unknown file type should use this type. Browsers pay a particular care when manipulating these files, to protect users from software vulnerabilities and possible dangerous behavior.

Content Filter: What to filter To Protect Windows?

File filtering rules based on	Manageable by proxy?	Relevant for Windows?	Bypass if filtered by?
Magic Bytes	Easy	Not really	No
Content Type	Easy	No	Yes octet/stream
File extension	Hard	**Yes**	Likely

HTML SMUGGLING

- JavaScript in an HTML file
- “Creates” a file on the fly (base64 decode)
- Browser shows a download dialog

Issue: File Download with JavaScript

file.html:

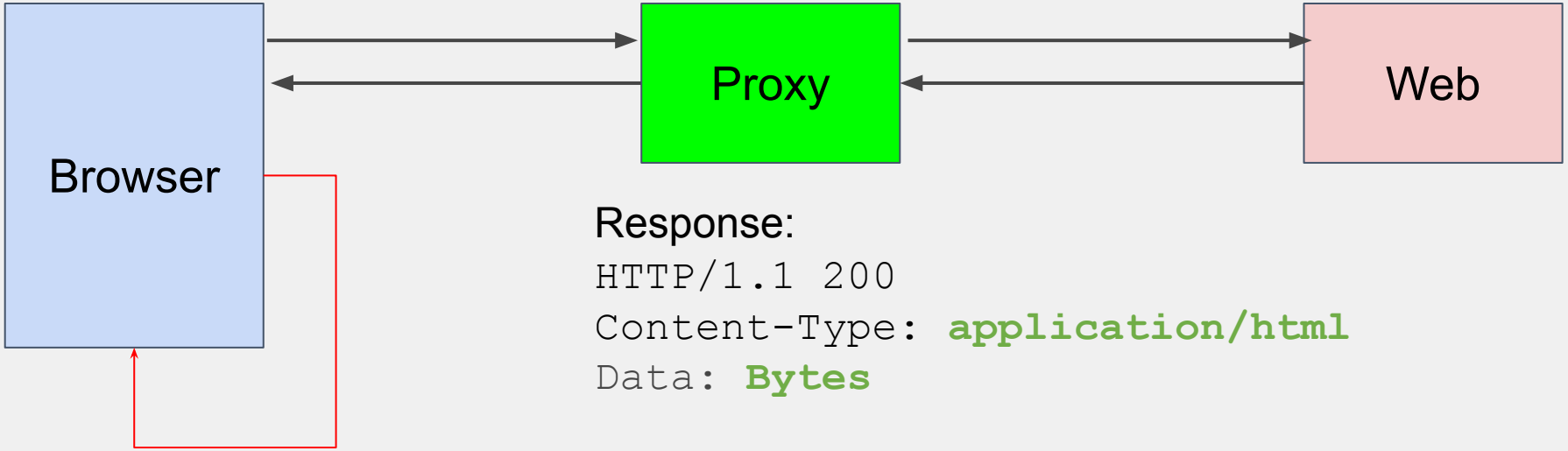
```
function download_txt() {
  var textToSave = document.getElementById('txt').innerHTML;
  var hiddenElement = document.createElement('a');

  hiddenElement.href = 'data:attachment/text,' + encodeURI(textToSave);
  hiddenElement.target = '_blank';
  hiddenElement.download = 'myFile.txt';
  hiddenElement.click();
}

document.getElementById('test').addEventListener('click', download_txt);
```

https://stackoverflow.com/questions/24898044/is-possible-to-save-javascript-variable-as-file

Proxy / Content Filter should protect Windows Client against malicious files

Request:

```
HTTP/1.1 GET /data/htmlsmuggling.html
```



Response:

```
HTTP/1.1 200
Content-Type: application/html
Data: Bytes
```

Browser presents
File Download Dialog

Content Filter Conclusion

Making a content-filter filter the right files is hard

Combination of:

- Mime-type filtering
- File-extension filtering
- Magic-bytes filtering

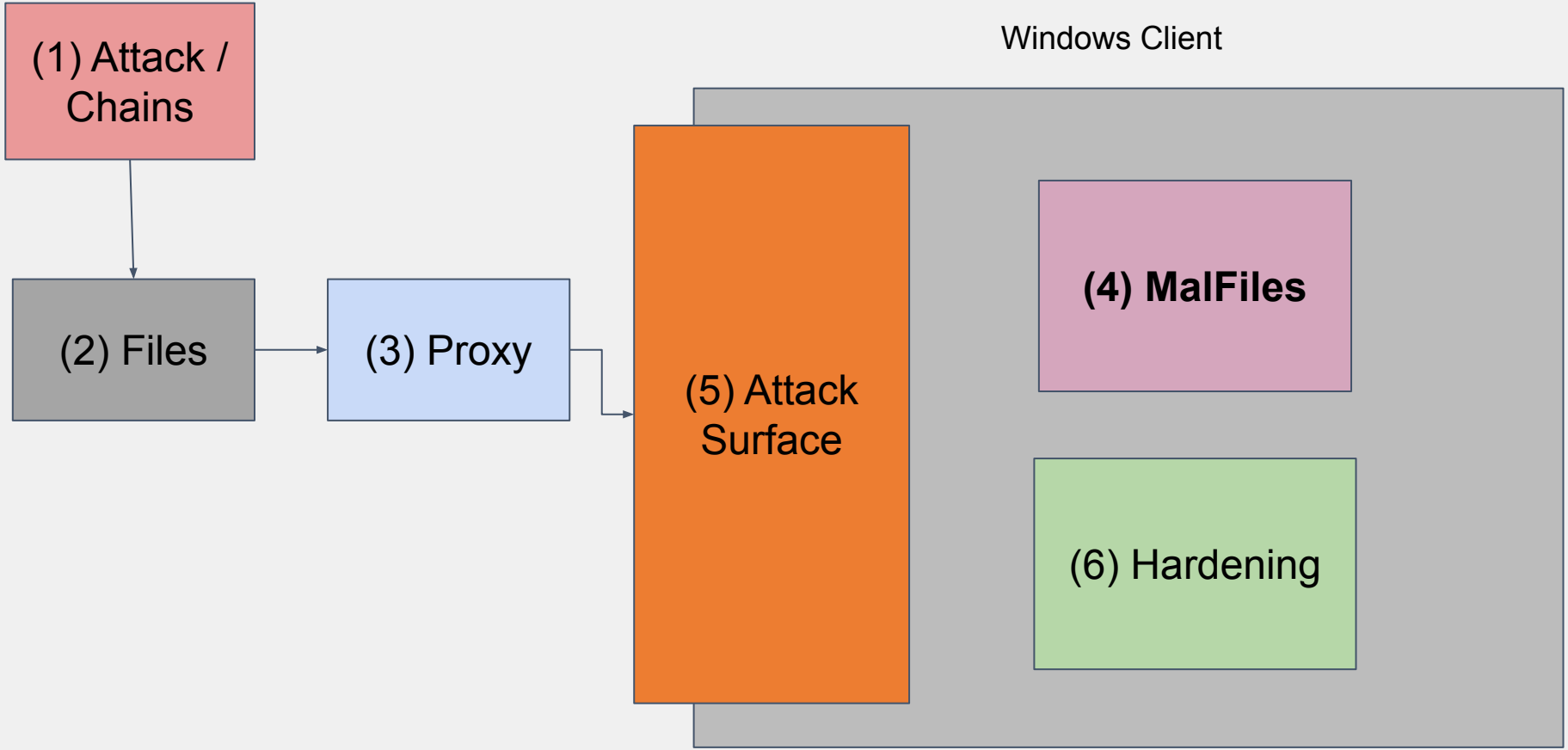
And is completely bypassed with HTML smuggling…

- Browser / Web
- Outlook / Email attachments
- Teams?

Gaining RCE with files

And what to do about it

Malicious File Types


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

Which files to filter?

Summing Up On File Formats

» Plenty Ways To Skin A Cat - nightmare for Detection Engineers & Threat Hunters

» Below a list of 87+ extensions that we can weaponize, meaning they pose *actual* risk:

Word

1. docm
2. doc
3. docx
4. dot
5. dotm
6. rtf

Excel

7. xls
8. xlsm
9. xlam
10. xlsx
11. xlsb
12. xla
13. xlt
14. xltm
15. slk

Publisher

16. chm
17. scf ← Exotics
18. url
19. csproj
20. inf
21. ics
22. pub

PowerPoint

23. one — OneNote
24. ppa
25. ppam
26. pptm
27. ppsm
28. pot
29. potm
30. pps
31. pptx

Visio

32. vdw
33. vsd
34. vsdm
35. vss
36. vssm
37. vstm
38. vst

MS Project

39. library-ms
40. settingscontent-ms
41. mpd
42. mpp
43. mpt
44. mpw
45. Mpx

WSH, COM, HTML

46. vbs
47. vbe
48. hta
49. sct
50. wsf
51. wsc
52. xsl
53. vbe
54. js
55. jse
56. html
57. svg

Containers

58. mde → MS Access
59. accde
60. zip
61. 7z
62. iso
63. img
64. cab
65. pdf
66. vhd
67. vhdx
68. wim

Executables

69. exe
70. scr
71. ocx
72. cpl
73. wll
74. xll
75. msi
76. msix
77. appx
78. bat
79. ps1
80. cmd
81. sh
82. Lnk

ClickOnce & VSTO

83. application
84. config
85. manifest
86. deploy
87. vsto

Mariusz Banach / mgeeky

Modern Initial Access and Evasion Tactics
Desperate Infection Chains

WarCon 2022, X33fcon23

https://mgeeky.tech/
https://github.com/mgeeky

Malicious File Extension - Past Prediction

BUY	HOLD	SELL
CHM	LNK	Office Macros
EXE + DLL Sideloading	ISO, IMG	VBS*, HTA
MSI	CPL	EXE
MSIX, APPX	XLL	OneNote
ClickOnce, VSTO	WSF, JS	
Complex Chains	XSL	
HTML Smuggling		
ZIP, 7zip, GZ,		

Your recommendations for 2023

* VBScript gets obsoleted and will be available for opt-in install someday

MalFiles Categorization

Directly Executables

Will execute your code when clicked

.exe / .com
.bat
.vbs
.js

Execution as a feature

Will execute code when opened by app

.docm
.xlsm
.svg

Container

Contain or link to files

.zip / .iso*
.docx
.one
.html
.pdf

Which file types to filter?

File filter:

- Blacklist?
  - Based on threat landscape? (CTI)

- Whitelist?
  - Based on company usecases
  - Should be an official policy
    - E.g. signed by the CISO
  - How to handle exceptions?
  - Containers uh-oh

Which file types to filter?

What about non **initial-access** files like:

- .dll
- .ps1

Filter or no filter?

“Instructions:
Download the .txt file, rename to .exe, and doubleclick”

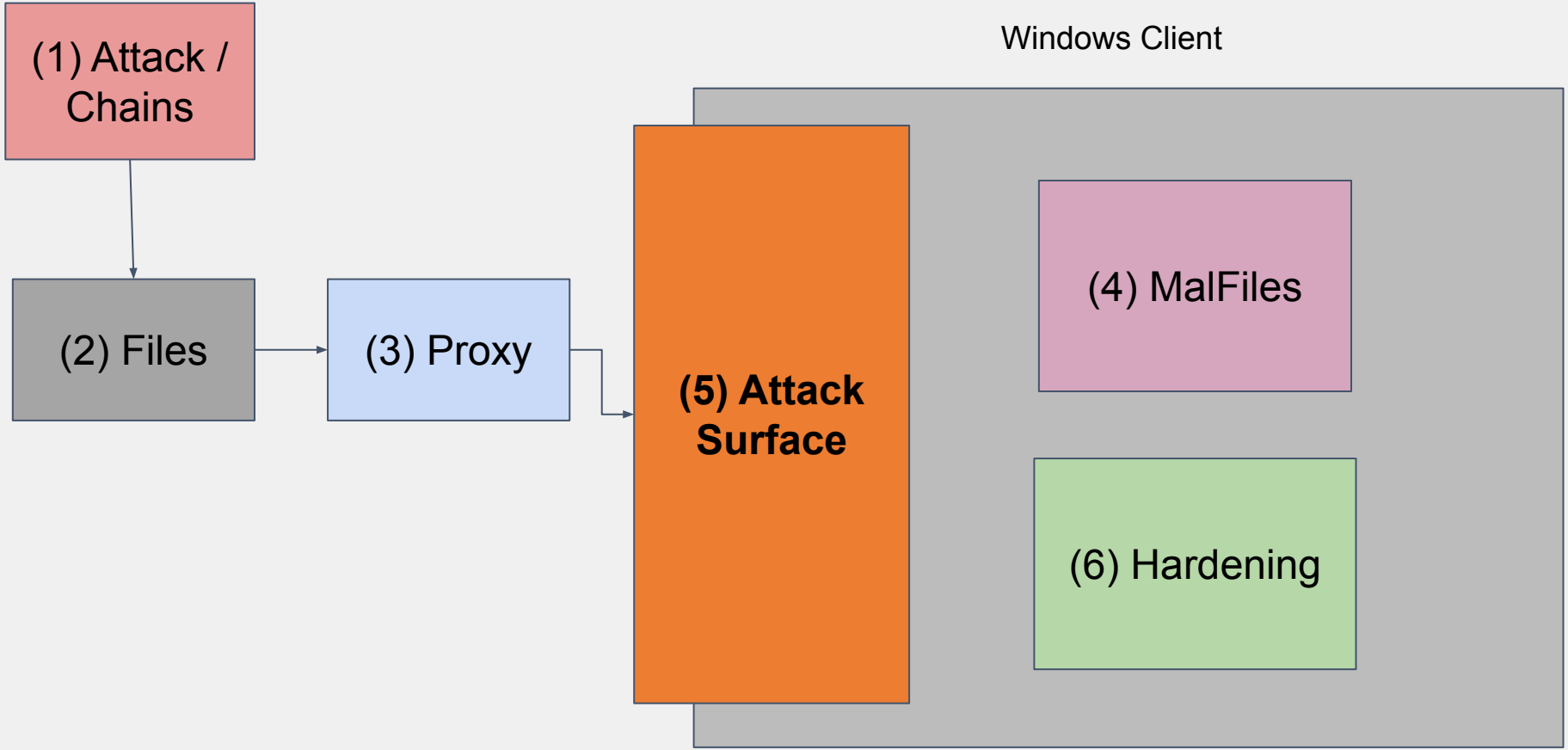
With RCE, can do en/decryption of future files, via authenticated HTTP. Content filter is blind.
If you already do have initial access, there’s no stopping you (like HTML Smuggling).

Filtering non-initial access files doesnt hurt, but doesnt help so much either.

Gaining RCE with files

And what to do about it

Attack Surface


(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

Which Files To Block?

Badfiles lists

badfiles.ch

Relaunch to update

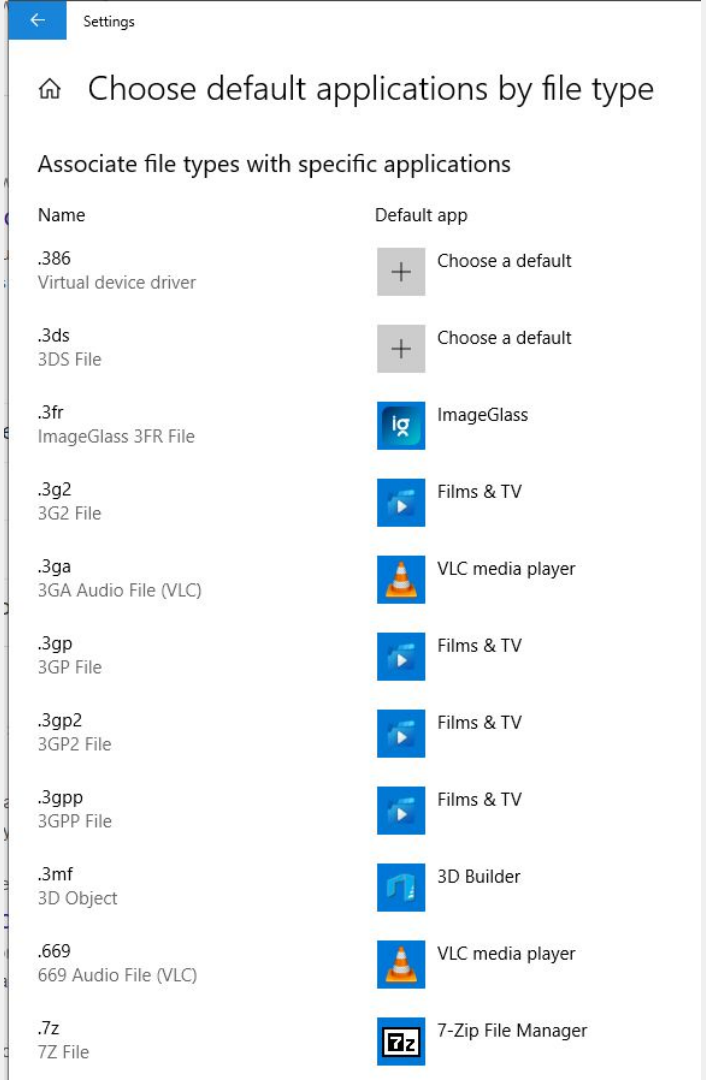
badfiles Extensions Windows About

Extension	Category	Exec	MITRE InitialAccess	MITRE Execution	Notes	Builtin
.7z	Archive	true				
.accda	Office					
.accdb	Office					
.accde	Office					
.accdr	Office					
.ace	Archive	true				
.ade	Office				Can contain scripts and execute actions within Access.	
.adp	Office				Similar to .ade, can contain and execute scripts within Access.	
.app	System	true			It's an application bundle on macOS. If malicious, it can introduce harmful software to the system.	true
.appinstaller	System	true			Used to install apps. Potentially harmful if sourced from untrusted locations.	true
.application	System	true			ClickOnce applications can execute code when deployed.	true
.appref-ms	System	true			A pointer to a ClickOnce application. Can cause the referenced application to be run.	true
.appx	System	true			Can be used to install potentially malicious Windows apps.	true
.appxbundle	System	true			Bundle of APPX packages. Can install potentially malicious apps.	true
.arj	Archive	true				

Windows: File Association

(Ignores magic bytes)

- .docx: Start Office
- .zip: Start zip
- .xml: Start Visual Studio (pls nonono!)



Waasa - List Windows File Associations

Waasa

File View Options Content Filter

Extension	DoubleClicl	Judgem	App Name	U\	Executable Path	Executable Args	ContentFil
.adt	recommenc		Media Player	X	C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2308.3.0_x64__8wekyb3d8bbwe\		
.adts	recommenc		Media Player	X	C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2308.3.0_x64__8wekyb3d8bbwe\		
.all	exec		Windows Security	X	C:\Program Files\WindowsApps\Microsoft.SecHealthUI_1000.25873.9001.0_x64__8wekyb3d8bbwe\SecHealthUI.e		
.amr	exec		Media Player	X	C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2308.3.0_x64__8wekyb3d8bbwe\		
.amv	exec		VLC media player		C:\Program Files\VideoLAN\VLC\vlc.exe	"--started-from-file" "%1"	
.androidproj	exec		Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"%1"	
.aob	exec		VLC media player		C:\Program Files\VideoLAN\VLC\vlc.exe	"--started-from-file" "%1"	
.ape	exec		VLC media player		C:\Program Files\VideoLAN\VLC\vlc.exe	"--started-from-file" "%1"	
.appcontent-ms	exec		Windows Shell Common Dll				
.appinstaller	exec	Bad	App Installer	X	C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.21.2771.0_x64__8wekyb3d8bbwe\AppInstaller.e		
.application	exec	Bad	ClickOnce Application Deployment Support Libr		C:\Windows\System32\rundll32.exe	"C:\Windows\System32\dfshim.dll,...	
.appref-ms	exec	Bad	ClickOnce Application Deployment Support Libr		C:\Windows\System32\rundll32.exe	"C:\Windows\System32\dfshim.dll,...	
.appx	exec	Bad	App Installer	X	C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.21.2771.0_x64__8wekyb3d8bbwe\AppInstaller.e		
.appxbundle	exec	Bad	App Installer	X	C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.21.2771.0_x64__8wekyb3d8bbwe\AppInstaller.e		
.ari	exec		Photos	X	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\		
.arw	exec		Photos	X	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\		
.asa	exec		Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"/dde"	
.asax	exec	Careful	Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"/dde"	
.asd	exec	Bad	Word		C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	"/n" "%1" "/o" "%u"	
.asf	recommenc		Media Player	X	C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2308.3.0_x64__8wekyb3d8bbwe\		
.ashx	exec	Careful	Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"/dde"	
.asm	exec		Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"/dde"	
.asmx	exec		Microsoft Visual Studio 2022		C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe	"/dde"	
.avci	exec		Paint		C:\Program Files\WindowsApps\Microsoft.Paint_11.2304.33.0_x64__8wekyb3d8bbwe\PaintApp\mspaint.exe	"%1"	
.avi	exec		VLC media player		C:\Program Files\VideoLAN\VLC\vlc.exe	"--started-from-file" "%1"	
.b4s	exec		VLC media player		C:\Program Files\VideoLAN\VLC\vlc.exe	"--started-from-file" "%1"	

Autoloaded file with gathered data: gathered_data.json

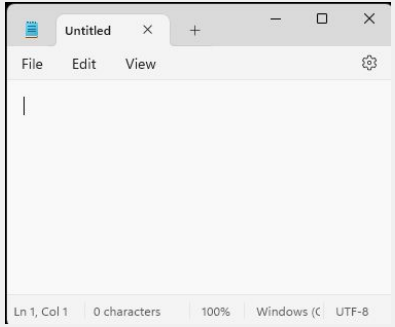
https://github.com/dobin/waasa using **shlwap** windows API

Windows Application Attack Surface

.jfif	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.jpe	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.jpeg	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.jpg	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.js	exec	Bad	Microsoft ® Windows Based Script Host	C:\Windows\System32\WScript.exe
.JSE	exec		Microsoft ® Windows Based Script Host	C:\Windows\System32\WScript.exe
.json	exec		Microsoft Visual Studio 2022	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe
.jsonld	exec		Microsoft Visual Studio 2022	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe
.jsproj	exec		Microsoft Visual Studio 2022	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe
.jsx	exec		Microsoft Visual Studio 2022	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe
.jxr	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.k25	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.kdc	exec		Photos	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2023.11090.12017.0_x64__8wekyb3d8bbwe\PhotosApp
.less	exec		Microsoft Visual Studio 2022	C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\devenv.exe

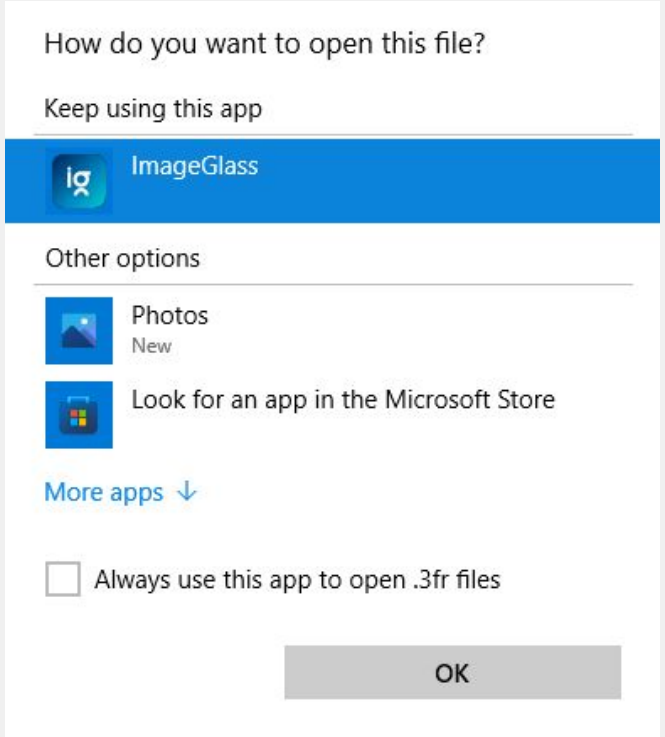
Social Engineering: What happens when clicking a file

Execute



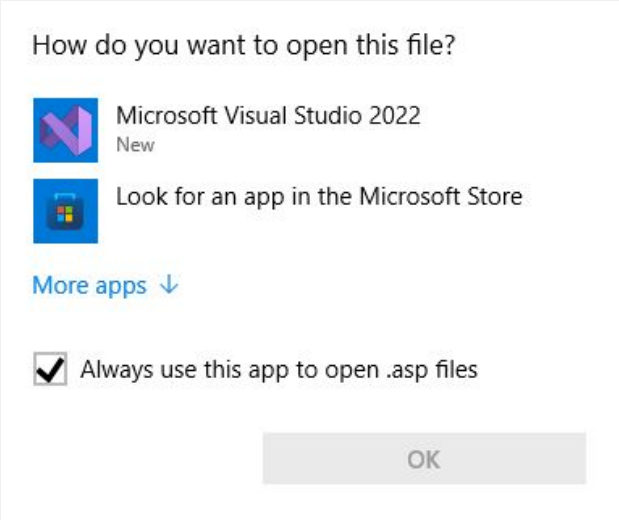
Best for IA

Show Recommended



Ok for IA

Show Selection



Bad for IA

Windows Application Attack Surface

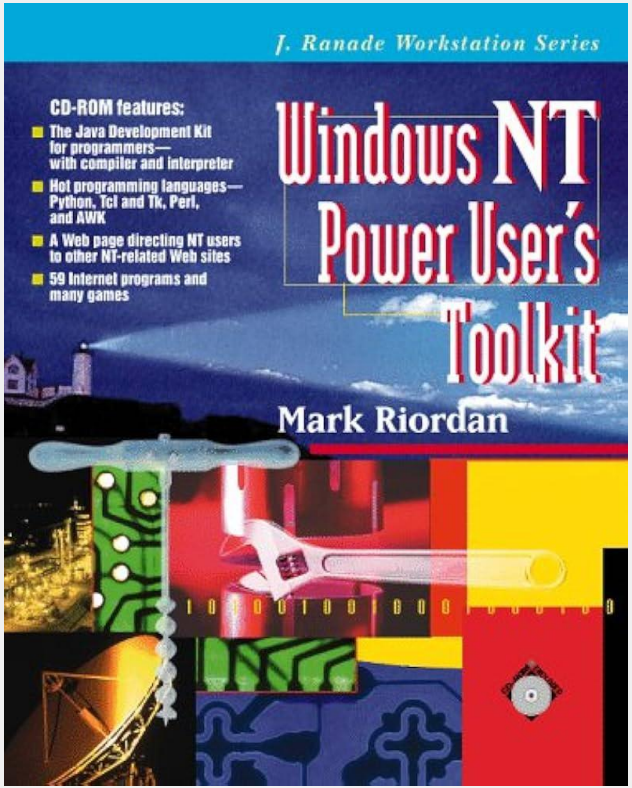
Increasing the attack surface:

- Install an application
- Replacing standard apps with 3rd party (Windows Zip to 7zip)

Because:

- Each installed application (which creates a file association) is part of the attack surface
- The more software you install, the more executable-features and vulnerabilities

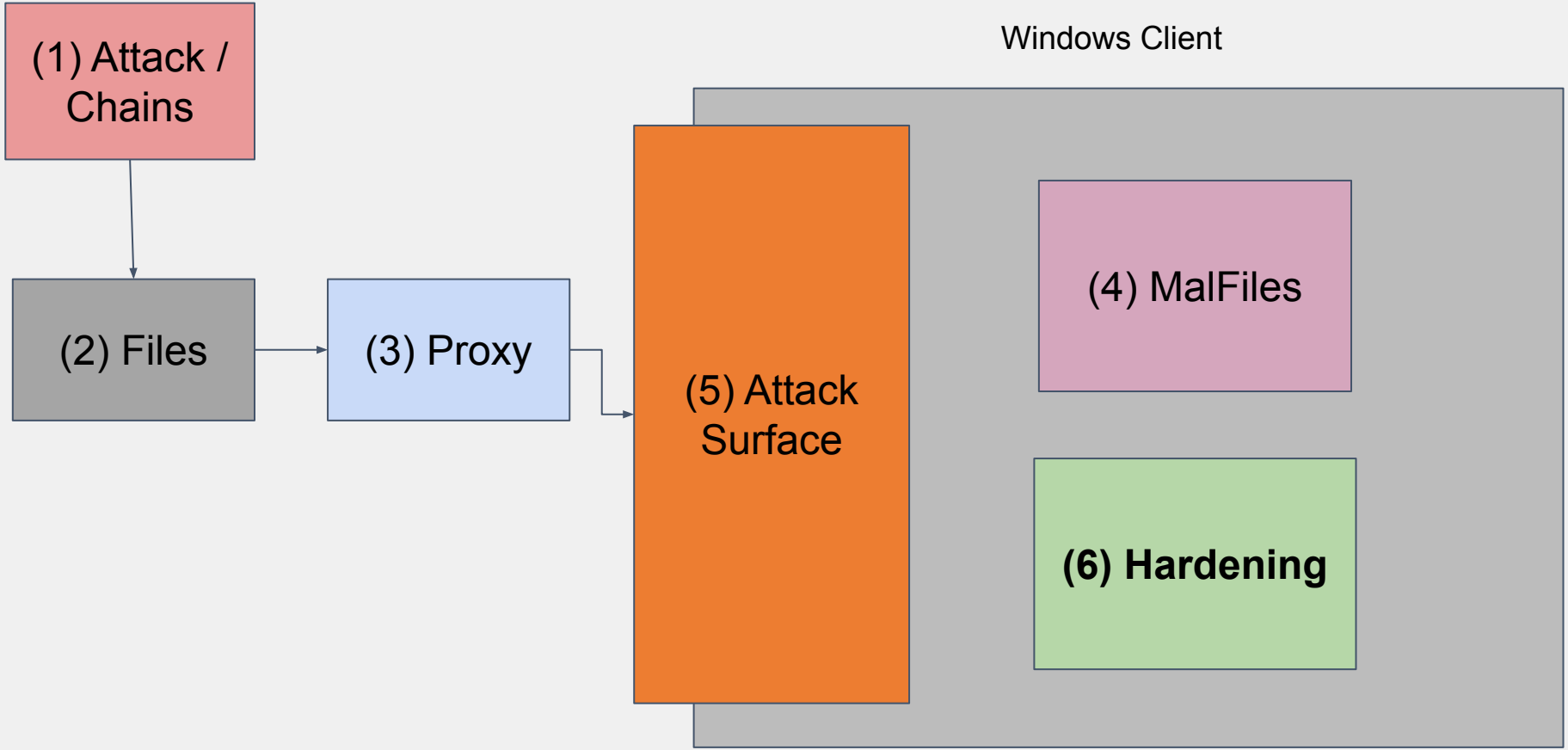
Dont be a “Power User” at work (or for security)



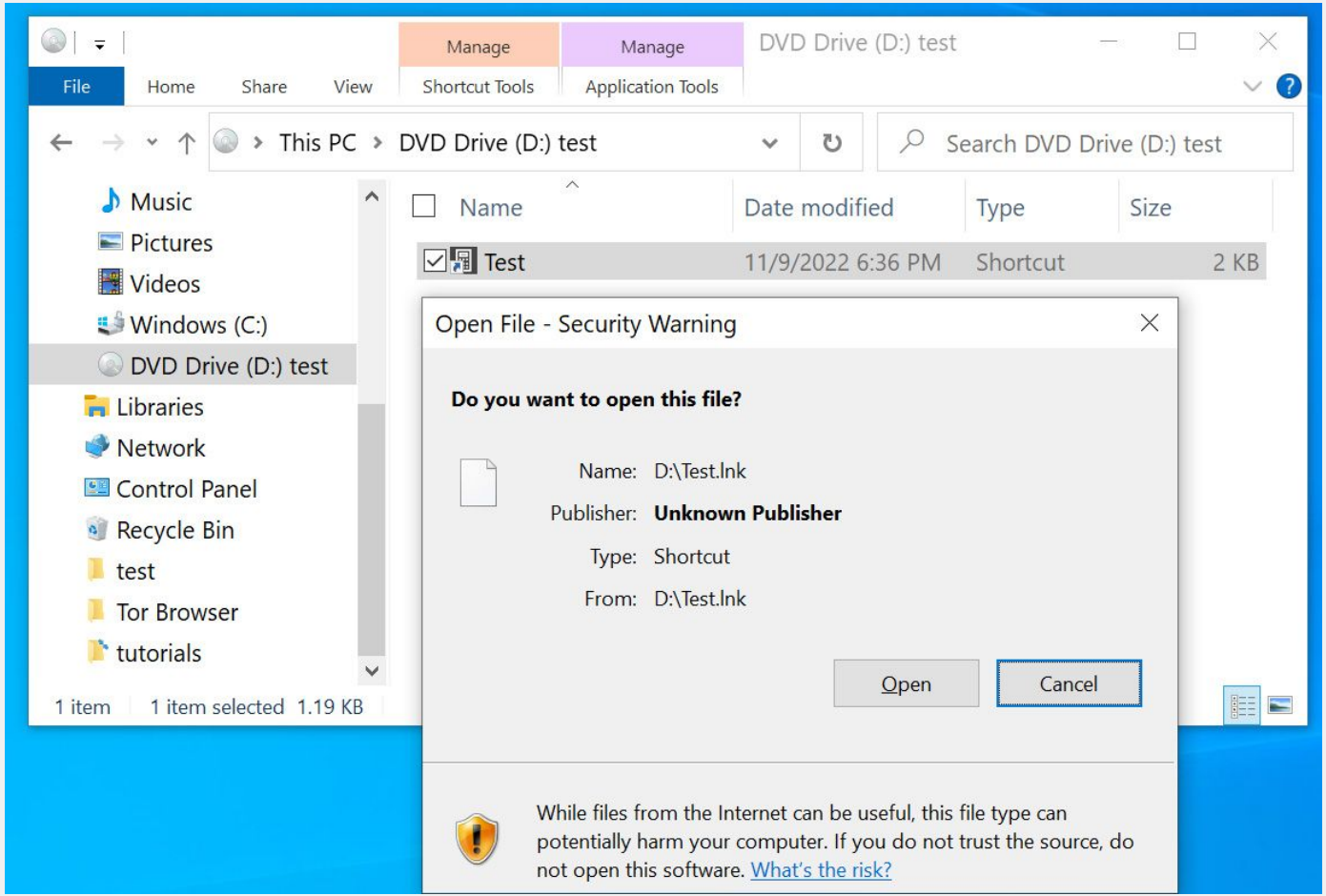
Gaining RCE with files

And what to do about it

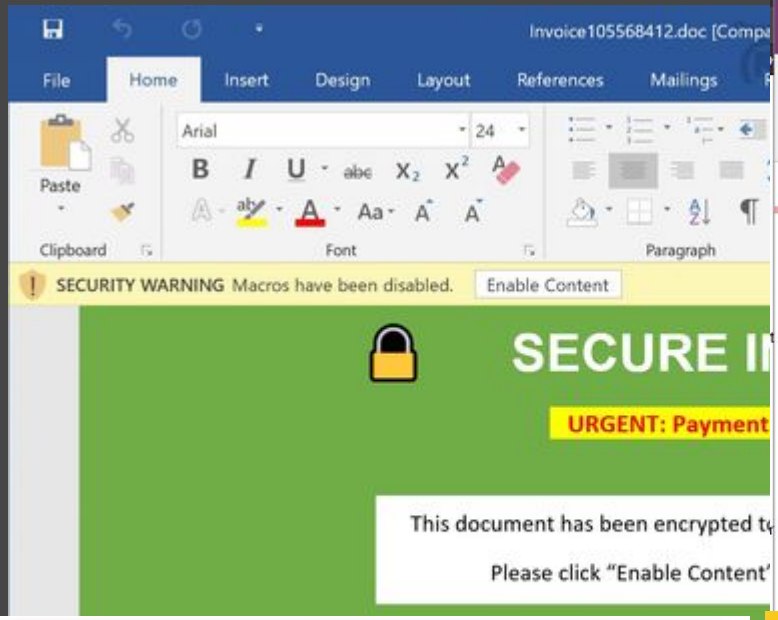
Hardening

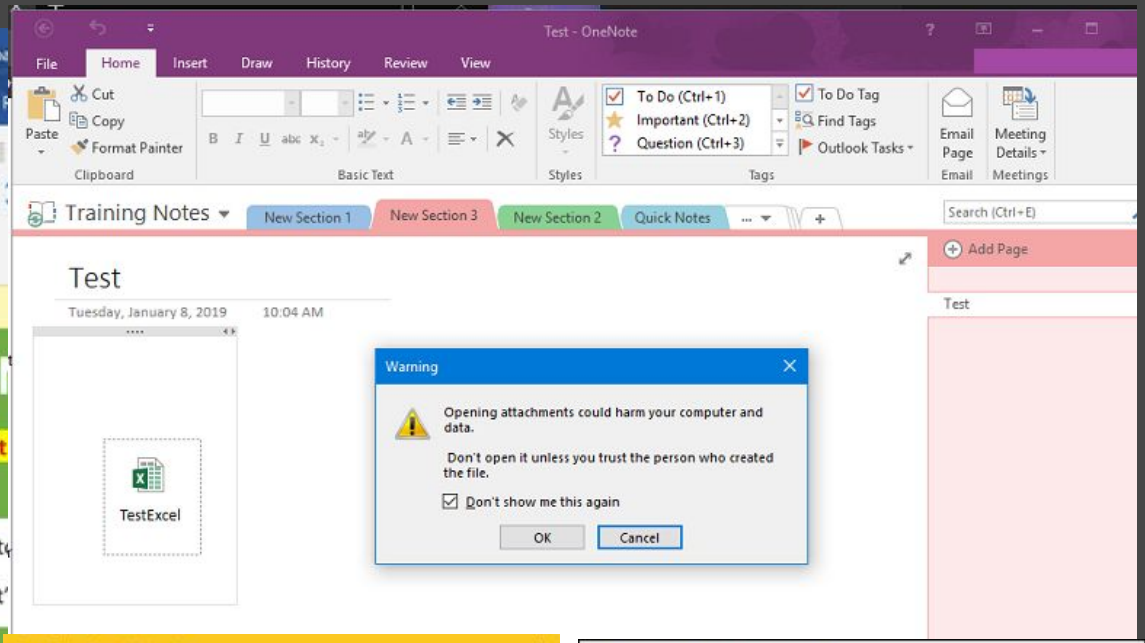

(1) Attack / Chains
(2) Files
(3) Proxy
Windows Client
(5) Attack Surface
(4) MalFiles
(6) Hardening

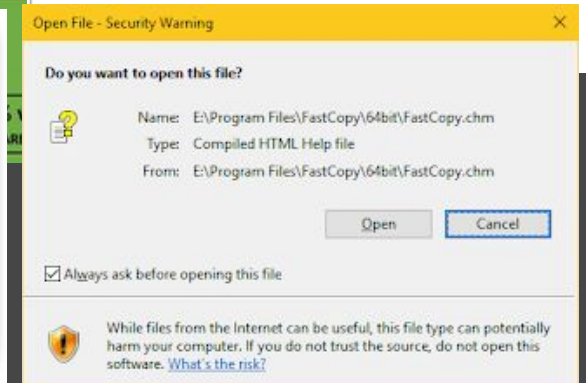
Last Line of Defense - Confirmation Dialog



Last Line of Defense - Confirmation Dialogs

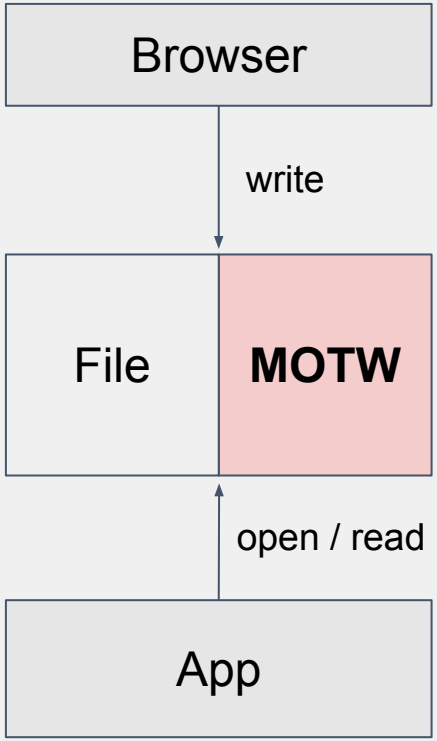






More Confirmation Dialogs with MOTW

- MOTW: Mark Of The Web
- Indicating files from “dangerous” location
- Set by:
  - the app which downloads the file (Browser usually)
- Stored in:
  - AFS (Alternative file stream)
- Interpreted by:
  - The opening App



- 0. Local computer
- 1. Local intranet
- 2. Trusted sites
- 3. Internet
- 4. Restricted sites

The evil bit RFC3514

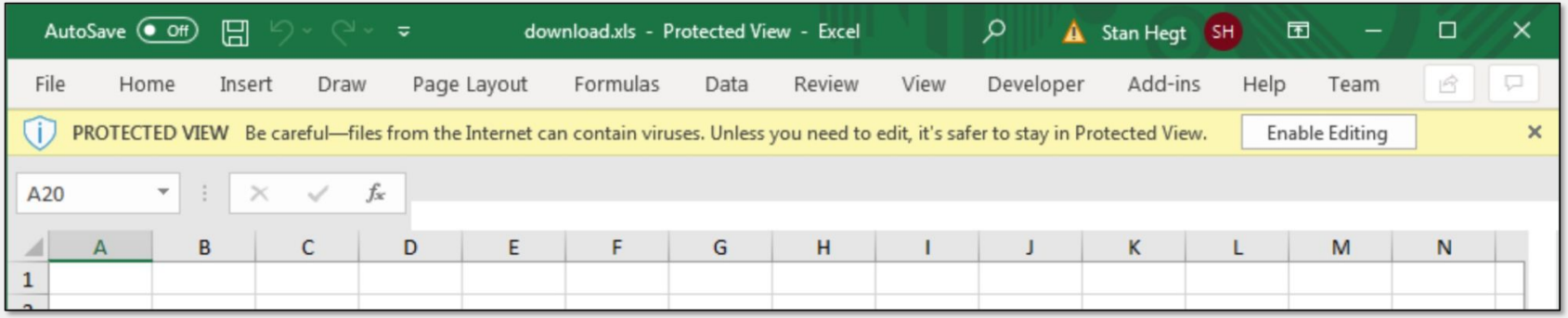
Administrator: Windows PowerShell

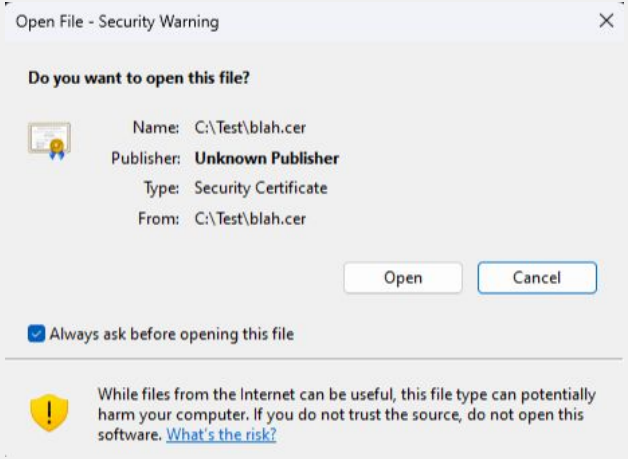
```
PS C:\Downloads\demo> Get-Item .\payload.doc -Stream *


   FileName: C:\Downloads\demo\payload.doc

Stream                    Length
------                    ------
:$DATA                    730624
Zone.Identifier               26


PS C:\Downloads\demo> Get-Content .\payload.doc -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
PS C:\Downloads\demo> _
```

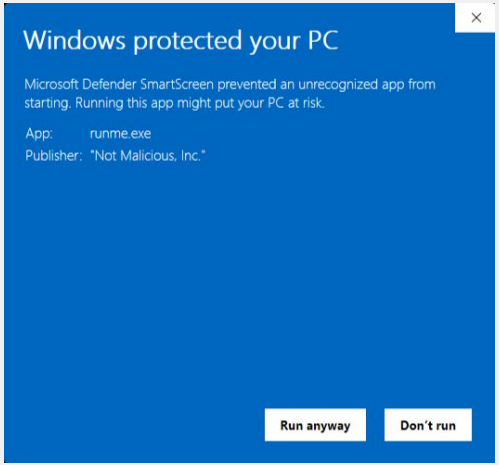
- 0. Local computer
- 1. Local intranet
- 2. Trusted sites
- 3. Internet
- 4. Restricted sites

https://www.outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/

Applications Interpreting MOTW





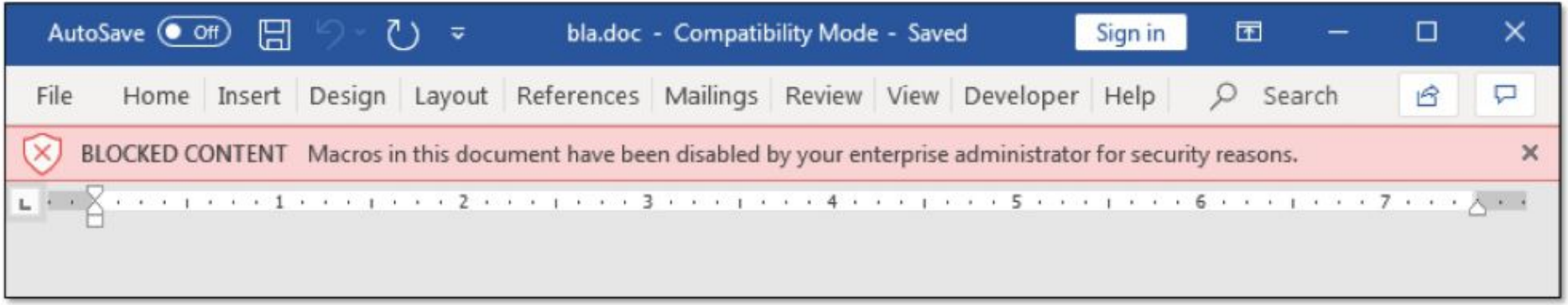


https://redcanary.com/threat-detection-report/techniques/mark-of-the-web-bypass/

Impact of MOTW

MS Office block macros downloaded from the internet

This feature was introduced in Office 2016 and later back-ported to Office 2013. If this setting is enabled, macros in MS Office files flagged with MOTW are disabled and a message is displayed to the user.



https://www.outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/

Getting rid of MOTW - Container

Archive Files as Container:

- ZIP / RAR / …
- ISO

Download .ZIP as MOTW
-> all contained files are MOTW

Archive Manager may skip MOTW for performance reasons

Comparison table of MOTW propagation support (as of 12 August 2024)

Name	Tested version	License	MOTW propagation	Enabled by default	Note
"Extract all" built-in function of Windows Explorer	Windows 11 23H2 Windows 10 22H2	proprietary	Yes ✔	Yes ✔	MOTW bypass vulnerabilities (fixed) *1
7-Zip	24.08	GNU LGPL	Yes ✔	No ✘ *2	
Bandizip	Standard Edition 7.36	freeware	Yes ✔	Yes ✔	MOTW bypass vulnerability (fixed) *3 Only for specific file extensions *4
CubeICE	3.4.0	freeware / proprietary	Yes ✔	Yes ✔	MOTW bypass vulnerability (fixed) *5

https://github.com/nmantani/archiver-MOTW-support-comparison

Application Hardening: Chrome Browser

Cant configure file download whitelist in Chrome **Enterprise :-(**

Chrome Enterprise and Education Help

Describe your issue

Setting the **DownloadRestrictions** policy blocks different subsets of these, depending on it's value:

- 0—Default. No special restrictions.
- 1—Blocks malicious files flagged by the Safe Browsing server and blocks all dangerous file types.
  Note: We only recommend setting this policy for organization units, browsers, or users that do not regularly incorrectly identify an entity, such as a file or a process, as malicious.
- 2—Blocks the following files:
  - Malicious files flagged by the Safe Browsing server.
  - Uncommon or unwanted files flagged by the Safe Browsing server.
  - All dangerous file types.

  Note: We only recommend setting this policy for organization units, browsers, or users that do not regularly incorrectly identify an entity, such as a file or a process, as malicious.
- 3—Blocks all downloads. Not recommended, except for special use cases.
- 4—**Recommended**. Blocks malicious files flagged by the Safe Browsing server but does not block dangerous file type.

Application Hardening: ASR / Office

ASR: Attack Surface Reduction

Some protections for the Office Suite

Like block Word from spawning processes

Weak and/or rarely used

-> Open internet files in guest vm

Polymorphic threats	Lateral movement & credential theft	Productivity apps rules	Email rules	Script rules	Misc rules
Block executable files from running unless they meet a prevalence (1,000 machines), age, or trusted list criteria	Block process creations originating from PSExec and WMI commands	Block Office apps from creating executable content	Block executable content from email client and webmail	Block obfuscated JS/VBS/PS/macro code	Block abuse of exploited vulnerable signed drivers [1]
Block untrusted and unsigned processes that run from USB	Block credential stealing from the Windows local security authority subsystem (lsass.exe)[2]	Block Office apps from creating child processes	Block only Office communication applications from creating child processes	Block JS/VBS from launching downloaded executable content	
Use advanced protection against ransomware	Block persistence through WMI event subscription	Block Office apps from injecting code into other processes	Block Office communication apps from creating child processes		
		Block Adobe Reader from creating child processes			

Microsoft Hardening OneNote

Microsoft Tightens OneNote Security by Auto-Blockir Extensions. Microsoft has announced plans to automat embedded files with "dangerous extensions" in OneNot reports that the note-taking service is being increasing malware delivery. 4 Apr 2023

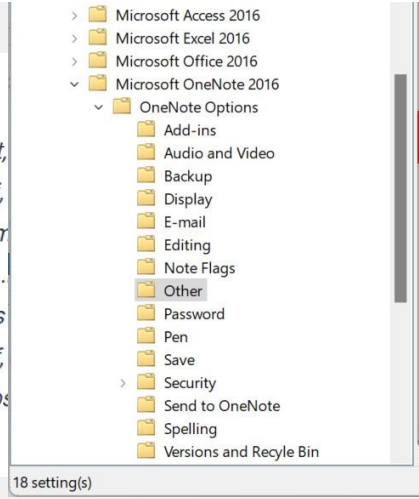
The Hacker News
https://thehackernews.com › Cybersecurity News

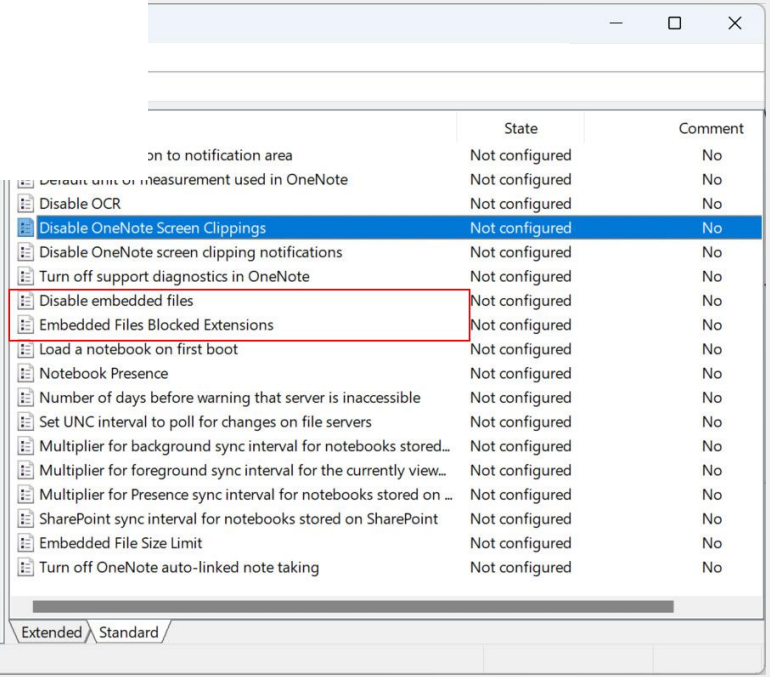
Microsoft Tightens OneNote Security by Auto-Blocking 120 ...

CLICK TO VIEW DOCUMENT

The list of 120 extensions is as follows -

.ade, .adp, .app, .application, .appref-ms, .asp, .aspx, .asx, .bas, .bat, .com, .cpl, .crt, .csh, .der, .diagcab, .exe, .fxp, .gadget, .grp, .hlp, .hpj, .jnlp, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .m .mdb, .mde, .mdt, .mdw, .mdz, .msc, .msh, .msh1, .msh2, .mshxml, . .mst, .msu, .ops, .osd, .pcd, .pif, .pl, .plg, .prf, .prg, .printerexport, .ps .psc2, .psd1, .psdm1, .pst, .py, .pyc, .pyo, .pyw, .pyz, .pyzw, .reg, .scf, .url, .vb, .vbe, .vbp, .vbs, .vhd, .vhdx, .vsmacros, .vsw, .webpnp, .webs and .xnk





	State	Comment
on to notification area	Not configured	No
Default unit of measurement used in OneNote	Not configured	No
Disable OCR	Not configured	No
Disable OneNote Screen Clippings	Not configured	No
Disable OneNote screen clipping notifications	Not configured	No
Turn off support diagnostics in OneNote	Not configured	No
Disable embedded files	Not configured	No
Embedded Files Blocked Extensions	Not configured	No
Load a notebook on first boot	Not configured	No
Notebook Presence	Not configured	No
Number of days before warning that server is inaccessible	Not configured	No
Set UNC interval to poll for changes on file servers	Not configured	No
Multiplier for background sync interval for notebooks stored...	Not configured	No
Multiplier for foreground sync interval for the currently view...	Not configured	No
Multiplier for Presence sync interval for notebooks stored on ...	Not configured	No
SharePoint sync interval for notebooks stored on SharePoint	Not configured	No
Embedded File Size Limit	Not configured	No
Turn off OneNote auto-linked note taking	Not configured	No

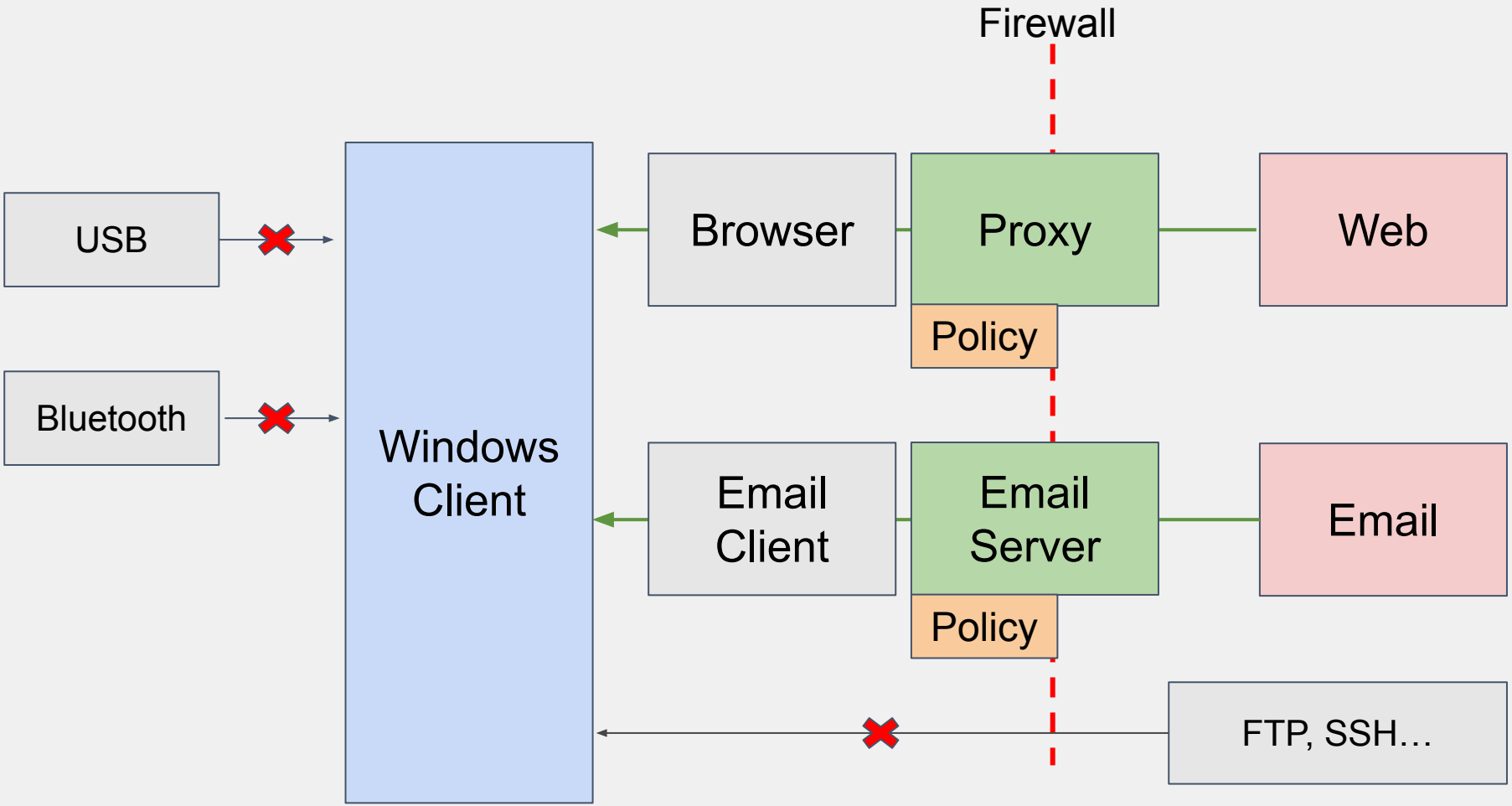
Extended | Standard

Gaining RCE with files

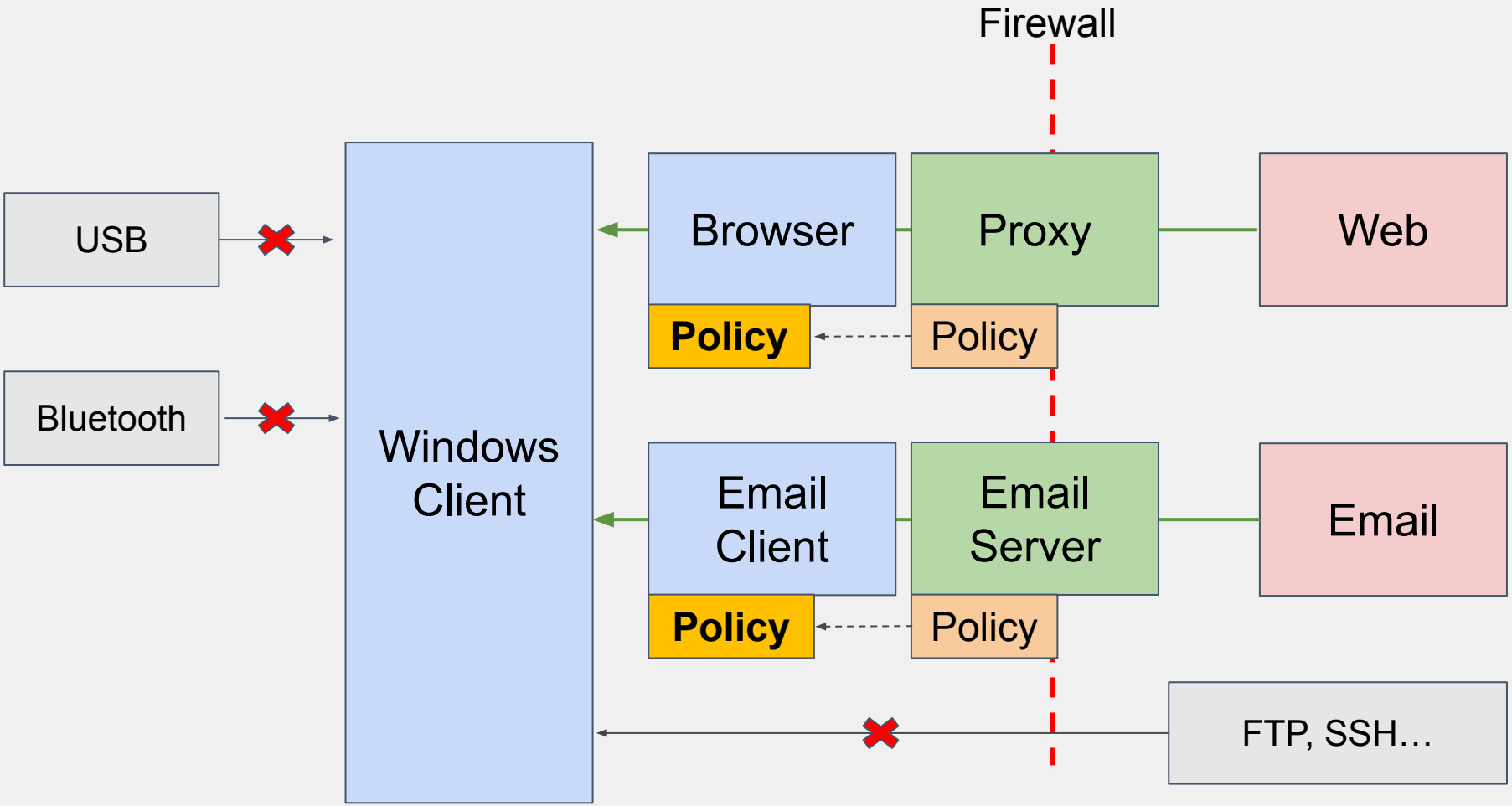
And what to do about it

Recommendations

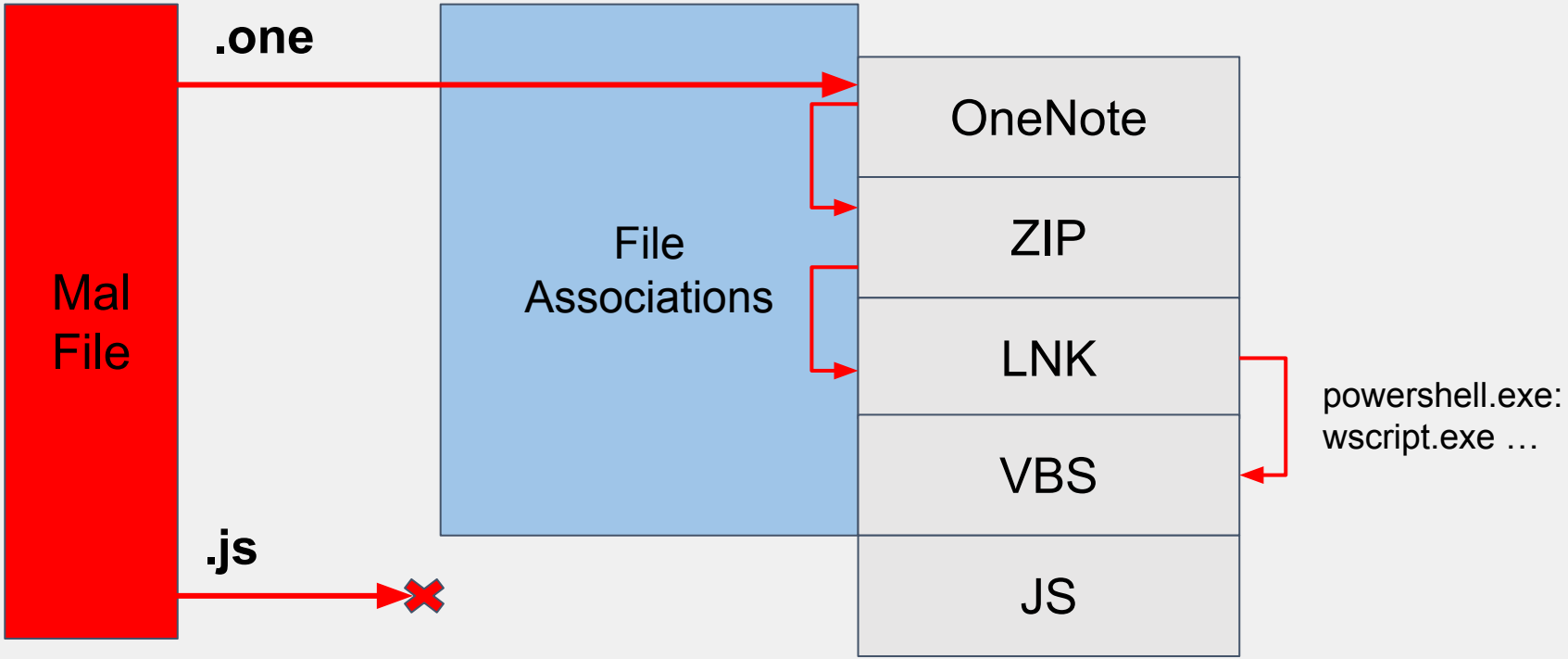
Restrict files reaching the client



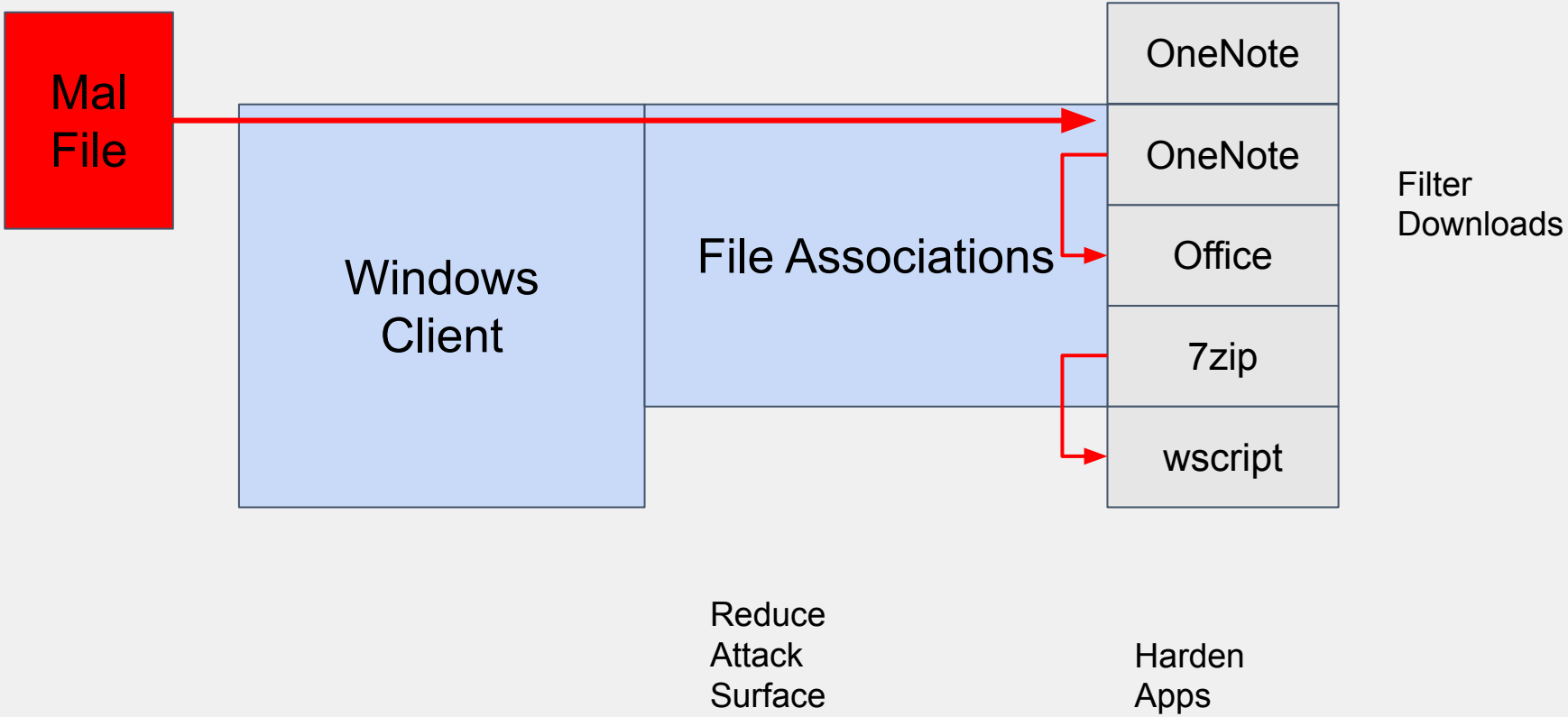
Zero Trust: Move File Download Policy to the apps



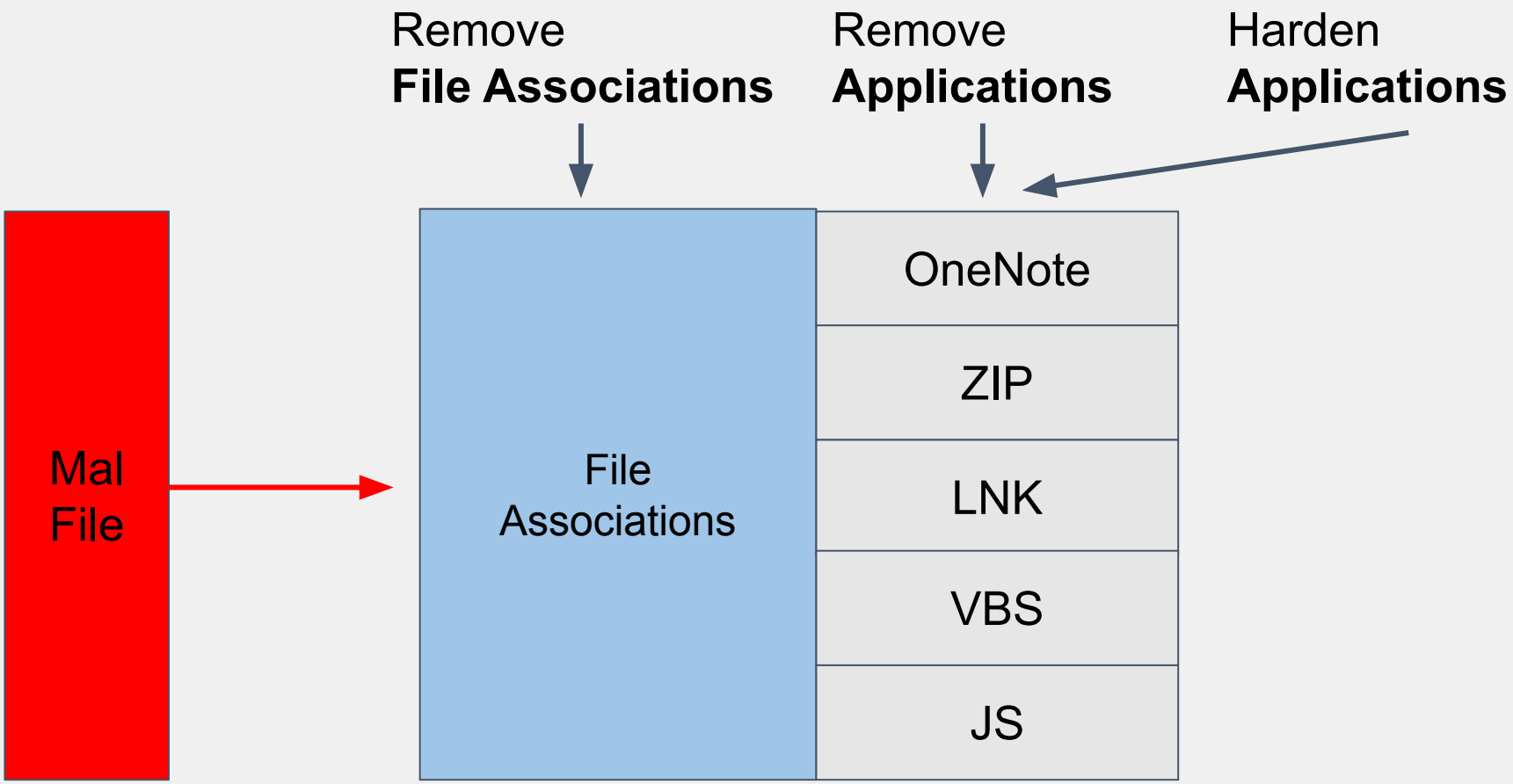
Reduce Attack Surface



How files reach a client



Reduce Attack Surface



Know files used typicall in current attacks

Know which files are used by the employees

Block ways where files can reach a client (block outgoing FTP)

Filter files with a whitelist (content filter)

Protect applications handling whitelisted files (ASR)

Cheap recommendations to protect against common initial access

- Remove commonly misused file type associations from Windows
  - .js, .vbs
  - .iso
  - .one

- Use a archive manager which supports MOTW
  - NOT 7zip
  - Windows zip is fine

- Activate as much of ASR as possible
  - Protects office applications like Word
  - Also double-check Office Word “Trust Center Settings”

Advanced recommendations:

- Decide for a browser
- Use **AppLocker** to block all other browsers
- Implement file download whitelist in the browser (Browser Plugin)

- File download policy for all other Apps communicating with the internet (**MS Teams**)
- Detect **HTML smuggling in emails**

How to make RedTeamers cry

Firewall ALL Traffic (including DNS)

Internet only via Proxy / Content Filter

- Require transparent proxy **authentication**
- Whitelist your last 3 browser **versions**

Result:

- Attackers dont have proxy support in their initial access chain
- Attackers dont configure their C2 beacon with a current user agent

SOC:

- Browser usage statistics
- Powershell usage statistics

The unreasonable effectiveness of content filters

- No proxy support in attack-chains
  - They all fail because they need direct internet access
- Domain (reputation) filtering reduces noise and increases attacker effort
- File filter work reasonably well against many common attacks
- Auditing, log files, incident reponse
- DLP Data Leakage Prevention (trivial to bypass but still effective)

Gaining RCE with files

And what to do about it

Practical Examples

Microsoft January Update - 159 CVE's- Possibly File Based Vulnerabilities

https://www.zerodayinitiative.com/blog/2025/1/14/the-january-2025-security-update-review

CVE-2025-21186	Microsoft Access Remote Code Execution Vulnerability	Important	7.8	Yes	No	RCE
CVE-2025-21366	Microsoft Access Remote Code Execution Vulnerability	Important	7.8	Yes	No	RCE
CVE-2025-21395	Microsoft Access Remote Code Execution Vulnerability	Important	7.8	Yes	No	RCE

Which types of extensions are blocked?

The following extensions which will be blocked:

- accdb
- accde
- accdw
- accdt
- accda
- accdr
- accdu

Microsoft January Update - 159 CVE's- Possibly File Based Vulnerabilities

https://www.zerodayinitiative.com/blog/2025/1/14/the-january-2025-security-update-review

CVE-2025-21298	Windows OLE Remote Code Execution Vulnerability	Critical	9.8	No	No	RCE

- **CVE-2025-21298 - Windows OLE Remote Code Execution Vulnerability**

This bug rates a CVSS 9.8 and allows a remote attacker to execute code on a target system by sending a specially crafted mail to an affected system with Outlook. Fortunately, the preview pane is not an attack vector, but previewing an attachment could trigger the code execution. The specific flaw exists within the parsing of RTF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. As a mitigation, you can set Outlook to read all standard mail as plain text, but users will likely revolt against such a setting. The best option is to test and deploy this patch quickly.

Microsoft January Update - 159 CVE's- Possibly File Based Vulnerabilities

CVE-2025-21308	Windows Themes Spoofing Vulnerability	Important	6.5	Yes	No	Spoofing
CVE-2025-21178	Visual Studio Remote Code Execution Vulnerability	Critical	8.8	No	No	RCE
CVE-2025-21172	.NET and Visual Studio Remote Code Execution Vulnerability	Important	7.5	No	No	RCE
CVE-2025-21176	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2025-21354	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21362	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21187	Microsoft Power Automate Remote Code Execution Vulnerability	Important	7.8	No	No	RCE

Microsoft January Update - 159 CVE's- Possibly File Based Vulnerabilities

CVE-2025-21402	Microsoft Office OneNote Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21365	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21345	Microsoft Office Visio Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21356	Microsoft Office Visio Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21357	Microsoft Outlook Remote Code Execution Vulnerability	Important	6.7	No	No	RCE
CVE-2025-21361	Microsoft Outlook Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2025-21363	Microsoft Word Remote Code Execution Vulnerability	Important	7.8	No	No	RCE

https://www.zerodayinitiative.com/advisories/ZDI-24-1532/

This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation.

The specific flaw exists within the implementation of Zstandard decompression. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the current process.

7-Zip fixes bug that bypasses Windows MoTW security warnings, patch now

By Sergiu Gatlan

January 21, 2025 11:05 AM 2

A high-severity vulnerability in the 7-Zip file archiver allows attackers to bypass the Mark of the Web (MotW) Windows security feature and execute code on users' computers when extracting malicious files from nested archives.

7-Zip added support for MotW in June 2022, starting with version 22.00. Since then, it has automatically added MotW flags (special 'Zone.Id' alternate data streams) to all files extracted from downloaded archives.

This flag informs the operating system, web browsers, and other applications that files may come from untrusted sources and should be treated with caution.

Newly supported files

Windows 11 adds support for 11 file archives, including 7-Zip and RAR

By Sergiu Gatlan

October 29, 2023 10:09 AM 2

The updated list of supported archive types in Windows 11 now **adds .rar, .7z, .tar, .tar.gz, .tar.bz2, .tar.zst, .tar.xz, .tgz, .tbz2, .tzst, and .txz**, although support for password encrypted files is not yet available.

Redmond says it added the new file archive formats with the help of the open-source libarchive project, which means we will likely see other formats like LZH, LZH, and XAR.

https://www.bleepingcomputer.com/news/microsoft/windows-11-adds-support-for-11-file-archives-including-7-zip-and-rar/

CyberSec Trends

https://x.com/cyb3rops/status/1856973214687056188

Florian Roth ⚡
@cyb3rops

CyberSec Trends Q4/24 🔮

⬆️ EDR killers (vulnerable drivers)
⬆️ Auxiliary execution files .lnk .msc .rdp
⬆️ Abuse of legit remote access tools
⬆️ Token/cloud API abuse
⬆️ ADCS exploitation
⬆️ Fake CAPTCHAs: copy&paste PowerShell
⬆️ TA using systems out of EDR scope for persistence

.msc Attacks

In July 2022, Microsoft disabled macros by default in Office, causing threat actors to experiment with new file types in phishing attacks. The attackers first switched to ISO images and password-protected ZIP files, as the file types did not properly propagate Mark of the Web (MoTW) flags to extracted files.

After Microsoft fixed this issue in ISO files and 7-Zip added the option to propagate MoTW flags, attackers were forced to switch to new attachments, such as Windows Shortcuts and OneNote files.

Attackers have now switched to a new file type, Windows MSC (.msc) files, which are used in the Microsoft Management Console (MMC) to manage various aspects of the operating system or create custom views of commonly accessed tools.

```
      <String ID="8" Refs="2">Test</String>
      <String ID="23" Refs="2">Document</String>
      <String ID="24" Refs="1">Root</String>
      <String ID="38" Refs="2">Main</String>
      <String ID="39" Refs="1">res://apds.dll/redirect.html?target=javascript:eval("alert('GRIMRESOURCE')")</String>
    </Strings>
  </StringTable>
</StringTables>
```

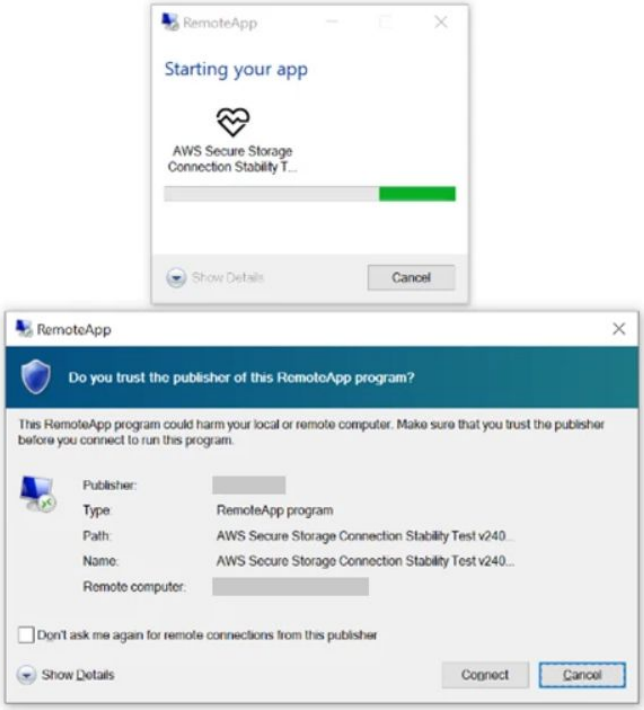
https://www.bleepingcomputer.com/news/security/new-grimresource-attack-uses-msc-files-and-windows-xss-flaw-to-breach-networks/

.rdp Attacks

https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

In this campaign, the malicious .RDP attachment contained several sensitive settings that would lead to significant information exposure. Once the target system was compromised, it connected to the actor-controlled server and bidirectionally mapped the targeted user's local device's resources to the server.

Resources sent to the server may include, but are not limited to, all logical hard disks, clipboard contents, printers, connected peripheral devices, audio, and authentication features and facilities of the Windows operating system, including smart cards.



macOS Gatekeeper bypass

Executive Summary

Unit 42 researchers have found that certain third-party utilities and applications pertaining to archiving, virtualization and Apple's native command-line tools do not enforce the quarantine attribute. This can pose a threat to the integrity of a security feature on macOS known as Gatekeeper, which is responsible for ensuring that only trusted software runs on the system. A bypass of Gatekeeper could leave the user unprotected from risky applications that may attempt to execute malicious content.

Many malware and adware families (such as CoinTicker, Shlayer and Bundlore) use the built-in utility curl to download their payload. In this way, they can **bypass Gatekeeper because curl does not set the quarantine attribute**.

These are the utilities and formats that we tested and found vulnerable:

- iZip: ZIP, TAR and 7Z
- Archiver: ARCHIVER, ZIP, TAR and 7Z
- BetterZip: ZIP, TAR and 7Z
- WinRAR: ZIP, TAR and 7Z
- 7z Utility: DMG, ZIP and 7Z

https://unit42.paloaltonetworks.com/gatekeeper-bypass-macos/

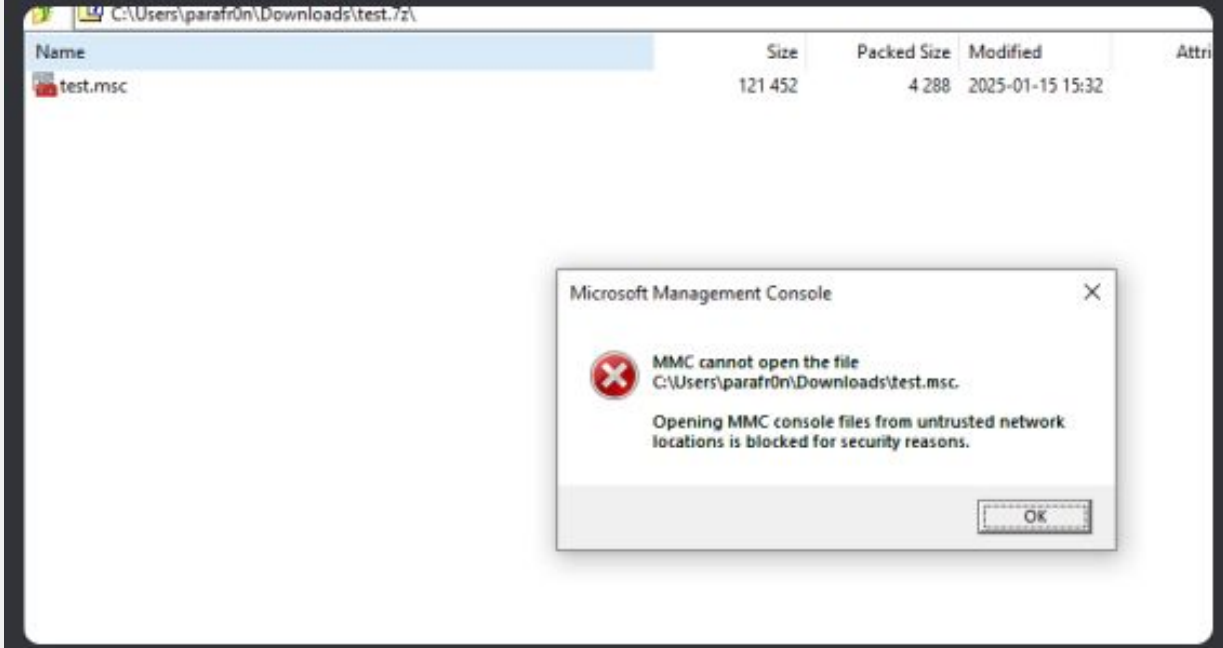
https://blog.sicuranext.com/breaking-down-multipart-parsers-validation-bypass/

TL;DR: Basically, all multipart/form-data parsers fail to fully comply with the RFC, and when it comes to validating filenames or content uploaded by users, there are always numerous ways to bypass validation.

```
POST /upload HTTP/1.1
Host: example.com
Content-Type: multipart/form-data; boundary=xxx

--xxx
Content-Disposition: form-data; name="foo"; filename="image.png"
Content-Type: image/png

... the image ...
--xxx--
```

Analyze Real Life Examples

mmc is motw'd now



3

that's your calc sample mgeeky

1

Gaining RCE with files

And what to do about it

Outro

To Proxy or not to Proxy?

- Many file types can be used for code execution, and therefore initial access
- Files Type is based on file extension (for Windows)
- Windows attack surface
    with WAASA

- Filtering files on Content filter is hard
- File filtering policy is hard
    badfiles.ch

- Windows hardening helps
  - MOTW
  - File association deassociation
  - ASR
  - 3rd party tools

References

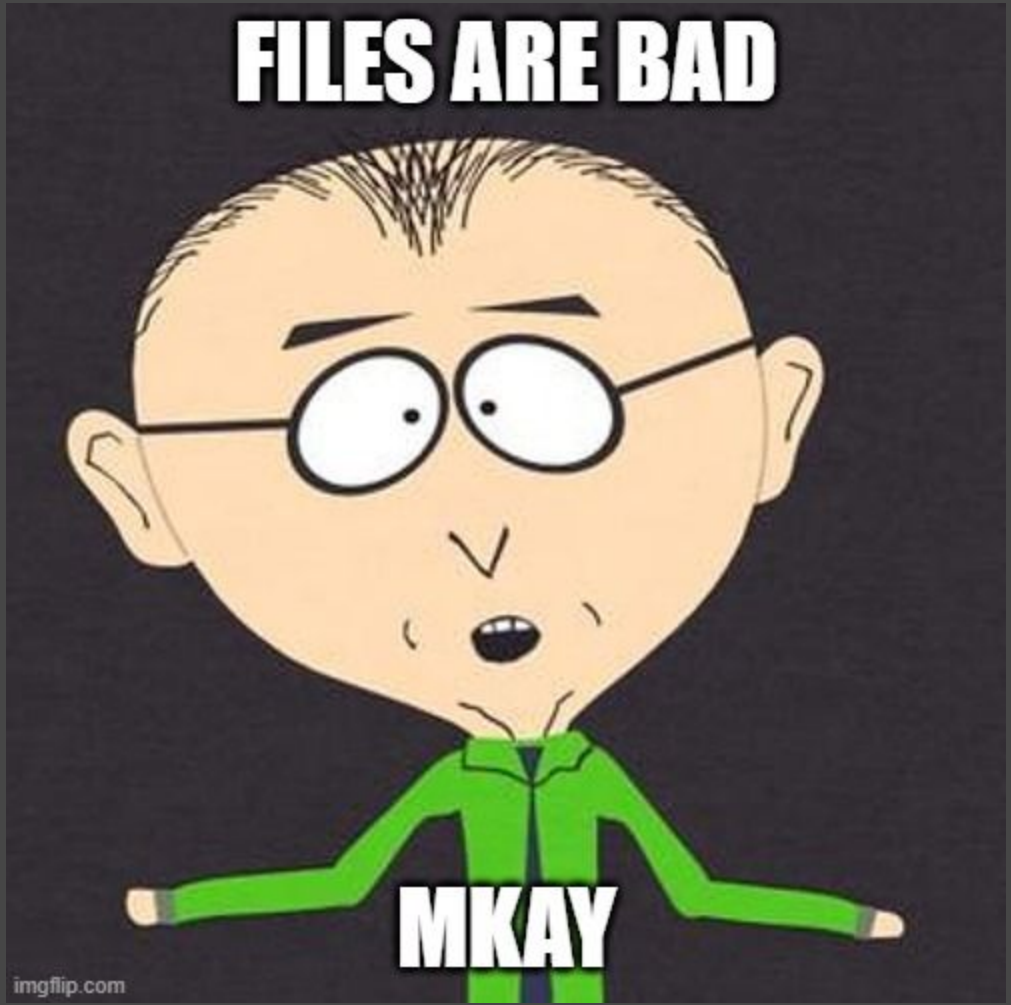
ACE FireFist - Attack Chain Emulation Development
Waasa - Windows Application Attack Surface Analyzer
Badfiles.ch

Mgeeky

Writeups to real life attack: thedfirreport.com

Ioprotect - content filter tests, attack chain emulation

Email protection (e.g HTML smuggling) - xorlab.ch (swiss)


FILES ARE BAD
MKAY
imgflip.com

Backup Slides

Lifetime of Malfiles

	Quality	Source
Delivery	Throw away Depends on target	Tools Manually
Execution	Straight forward	What others are doing
Staging	Often hilariously bad	Self made
Malware	High	Professional dev $$$

Content Type

Warning: Browsers use the MIME type, *not the file extension*, to determine how to process a URL, so it's important that web servers send the correct MIME type in the response's `Content-Type` header. If this is not correctly configured, browsers are likely to misinterpret the contents of files, sites will not work correctly, and downloaded files may be mishandled.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types

Microsoft recommends proxy bypass for Teams

- Reasonable (video streaming)

Zero trust gets rid of content filters altogether
Zero trust is a good thing!
But other measures have to be implemented instead (outgoing fw www only, application whitelisting, browser file download filtering)