



# Ransomware Resistance

Protective Measures with Low Effort and High Impact



# About Me

- Florian Roth
- Head of Research @ Nextron Systems
- IT Sec since 2000, Nation State Cyber Attacks since 2012
- THOR Scanner
- Twitter @cyb3rops
- Open Source Projects:
  - Sigma (Generic SIEM Rule Format)
  - LOKI (Open Source Scanner)
  - APT Groups and Operations Mapping
  - Antivirus Event Analysis Cheat Sheet
  - ...



# Ransomware Overview Spreadsheet – Prevention Tab

## ■ Public Google Document

Ransomware Overview   Wird gespeichert...

Datei Bearbeiten Ansicht Einfügen Format Daten Tools Add-ons Hilfe Letzte Änderung am 17. April von Nader Zaveri

100% € % .0 .00 123 Roboto Co... 11 B I S A

	A	B	C	D	E	F	G
	No	Measure	Type	Description	Complexity*	Effectiveness*	Impact*
3	1	Backup and Restore Process	Recovery	Make sure to have adequate backup processes on place and frequently test a restore of these backups ("Schrödinger's backup - it is both existent and non-existent until you've tried a restore")	Medium	High	Low
4	2	Windows Defender Ransomware Protection	GPO	Windows Defender includes a security feature called "Ransomware Protection" that allows you to enable various protections against ransomware infections. This feature is disabled by default in Windows 10. It can be activated via GPO and has the name "Controlled Folder Access". (see the links)	Low	High	Low
5	3	Block Macros	GPO	Disable macros in Office files downloaded from the Internet. This can be configured to work in two different modes: A.) Open downloaded documents in 'Protected View' B.) Open downloaded documents and block all macros	Low	High	Low
6	4	Block Windows Binary Access to Internet	GPO	Use Windows Firewall policies to block binaries access to the so called "Remote Scope". These binaries include powershell.exe, bitsadmin.exe, certutil.exe, regsrv32.exe, mshta.exe, msbuild.exe, hh.exe, makecab.exe, ieexec.exe, extract.exe, expand.exe (see the links for details)	Low	High	Low
7	5	Filter Attachments Level 1	Mail Gateway	Filter the following attachments on your mail gateway: .386, .ace, .acm, .acv, .ade, .adp, .adt, .ani, .app, .arc, .arj, .asd, .asp, .avb, .ax, .bas, .bat, .boo, .btm, .cab, .cbt, .cdr, .cer, .chm, .cla, .cmd, .cnv, .com, .cpl, .crt, .csc, .csh, .css, .dll, .drv, .dvb, .email, .exe, .fon, .fxp, .gms, .gvb, .hlp, .ht, .hta, .html, .htt, .inf, .ini, .ins, .iso, .isp, .its, .jar, .job, .js, .jse, .ksh, .lib, .lnk, .maf, .mam, .maq, .mar, .mat, .mau, .mav, .maw, .mch, .mda, .mde, .mdt, .mdw, .mdz, .mht, .mhtml, .mhtml, .mpd, .mpt, .msc, .msi, .mso (except oledata.mso), .msp, .mst, .nws, .obd, .obj, .obt, .obz, .ocx, .ops, .ovl, .ovr, .pcd, .pci, .perl, .pgm, .pif, .pl, .pot, .prf, .prg, .ps1, .pub, .pwz, .qpw, .reg, .sbf, .scf, .scr, .sct, .sfx, .sh, .shb, .shs, .shtml, .shw, .smm, .svg, .sys, .td0, .tlb, .tmp, .torrent, .tsk, .tsp, .tt6, .url, .vb, .vbe, .vbs, .vbx, .vom, .vsmacro, .vss, .vst, .vsw, .vwp, .vxd, .vxe, .wbk, .wbt, .wlz, .wk,	Low	Medium	Low

<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/>

# Protection

the preservation from injury or harm

# Resistance

the ability not to be affected by something, especially adversely

# Resilience

the capacity to recover quickly from difficulties; toughness

# Protection (implies previous Detection)

Antivirus, Sandboxes and EDRs to detect and avert threats

# Resistance

basic methods of separation and blocking to protect from new and unknown threats

# Resilience

fast and easy recovery from occurred incidents

# Ransomware Kill Chain

	Delivery	Infection	Propagation
Methods	Phishing Emails Vulnerabilities (SMBv1) Brute Force (RDP)	Malicious Document Dropper/Downloader	Network Scanning Extracted Credentials
Protection	Security Awareness Trainings Multi-Factor-Authentication	Antivirus EDR	IPS
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Resistance	Firewalling Email Filters Patch Management	Policies Execution Prevention	Firewalling (OS level) Network Segregation User Account Segregation

# Ransomware Kill Chain – Industry Focus

	Delivery	Infection	Propagation
Methods	Phishing Emails Vulnerabilities (SMBv1) Brute Force (RDP)	Malicious Document Dropper/Downloader	Network Scanning Extracted Credentials
Protection	Security Awareness Trainings Multi-Factor-Authentication	Antivirus EDR	IPS
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Resistance	Firewalling Email Filters Patch Management	Policies Execution Prevention	Firewalling (OS level) Network Segregation User Account Segregation

**Industry Focus**

**This is what we'll look at**



# Protective Measures

1. Backup and Restore Process
2. Windows Defender Ransomware Protection
3. Block Macros
4. Block Windows Binary Access to Internet
5. Filter Attachments Level 1
6. Filter Attachments Level 2
7. Use Web Proxies
8. Block Executable Downloads
9. Enforce UAC Prompt
10. Remove Admin Privileges
11. Restrict Workstation Communication
12. Sandboxing Email Input
13. Execution Prevention
14. Change Default "Open With" to Notepad
15. Restrict program execution
16. Sysmon
17. VSSAdmin Rename
18. Disable WSH
19. Folder Redirection
20. Remove Backup Server from Domain
21. Multi-Factor-Authentication (MFA)

*Low  
Complexity  
Measures*

**Effort**

**20%**

**80%**

**Effect**

**80%**

**20%**



# Low Complexity Measures

Measures that have a low complexity of implementation, minimal influence on business critical processes and don't require a lot of previous research or expertise

# High Complexity Measures

## Examples

# High Complexity: Filter Attachments

- Where can I get a good and curated list of problematic extensions?
- Do we have critical business processes that depend on one or more of these extensions?
- How and where can we block them?

Measure	Type	Description
Filter Attachments Level 1	Mail Gateway	Filter the following attachments on your mail gateway: .386, .ace, .acm, .acv, .ade, .adp, .adt, .ani, .app, .arc, .arj, .asd, .asp, .avb, .ax, .bas, .bat, .boo, .btm, .cab, .cbt, .cdr, .cer, .chm, .cla, .cmd, .cnv, .com, .cpl, .crt, .csc, .csh, .css, .dll, .drv, .dvb, .email, .exe, .fon, .fxp, .gms, .gvb, .hlp, .ht, .hta, .html, .htt, .inf, .ini, .ins, .iso, .isp, .its, .jar, .job, .js, .jse, .ksh, .lib, .lnk, .maf, .mam, .maq, .mar, .mat, .mau, .mav, .maw, .mch, .mda, .mde, .mdt, .mdw, .mdz, .mht, .mhtm, .mhtml, .mpd, .mpt, .msc, .msi, .mso (except oledata.mso), .msp, .mst, .nws, .obd, .obj, .obt, .obz, .ocx, .ops, .ovl, .ovr, .pcd, .pci, .perl, .pgm, .pif, .pl, .pot, .prf, .prg, .ps1, .pub, .pwz, .qpw, .reg, .sbf, .scf, .scr, .sct, .sfx, .sh, .shb, .shs, .shtml, .shw, .smm, .svg, .sys, .td0, .tlb, .tmp, .torrent, .tsk, .tsp, .tt6, .url, .vb, .vbe, .vbs, .vbx, .vom, .vsmacro, .vss, .vst, .vsw, .vwp, .vxd, .vxe, .wbk, .wbt, .wlz, .wk, .wml, .wms, .wpc, .wpd, .ws, .wsc, .wsf, .wsh
Filter Attachments Level 2	Mail Gateway	Filter the following attachments on your mail gateway: (Filter expression of Level 1 plus) .doc, .xls, .rtf, .docm, .xlsm, .pptm, .bin

# High Complexity: Block program executions

- Which programs should we white-list?
- Is there a list of legitimate programs that we use in our organisation?
- Who maintains that list?
- Where do we apply the restrictions?  
(Workstations, Admin Workstations, Systems of Support Staff, Servers, Admin Jump Server)

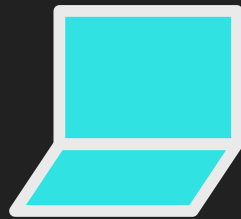
15	Restrict program execution	GPO	Block program executions (AppLocker)
----	----------------------------	-----	--------------------------------------

# Low Complexity Measures

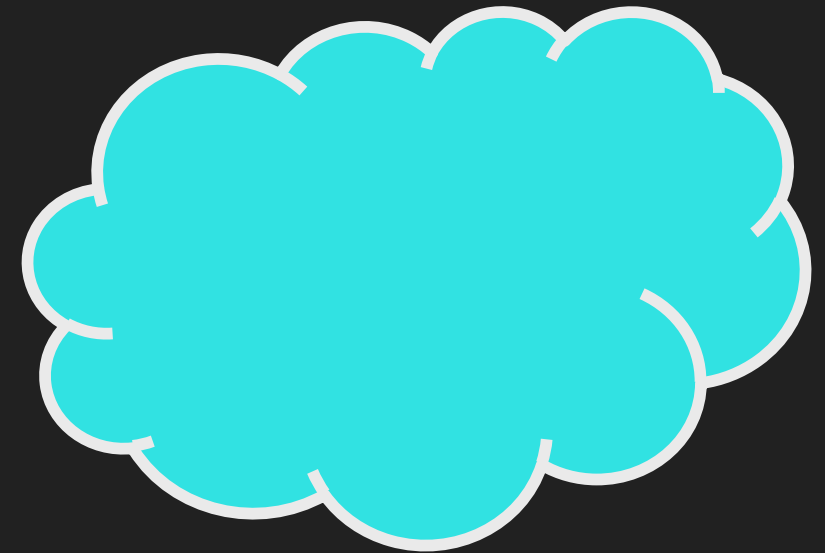
1. Backup and Restore Process
2. Windows Defender Ransomware Protection
3. Block Macros
4. Block Windows Binary Access to Internet
5. Filter Attachments Level 1
6. Filter Attachments Level 2
7. Use Web Proxies
8. Block Executable Downloads
9. Enforce UAC Prompt
10. Remove Admin Privileges
11. Restrict Workstation Communication
12. Sandboxing Email Input
13. Execution Prevention
14. Change Default "Open With" to Notepad
15. Restrict program execution
16. Sysmon
17. VSSAdmin Rename
18. Disable WSH
19. Folder Redirection
20. Remove Backup Server from Domain
21. Multi-Factor-Authentication (MFA)

***Communication  
Restrictions***

# “Worst” Practice Communication

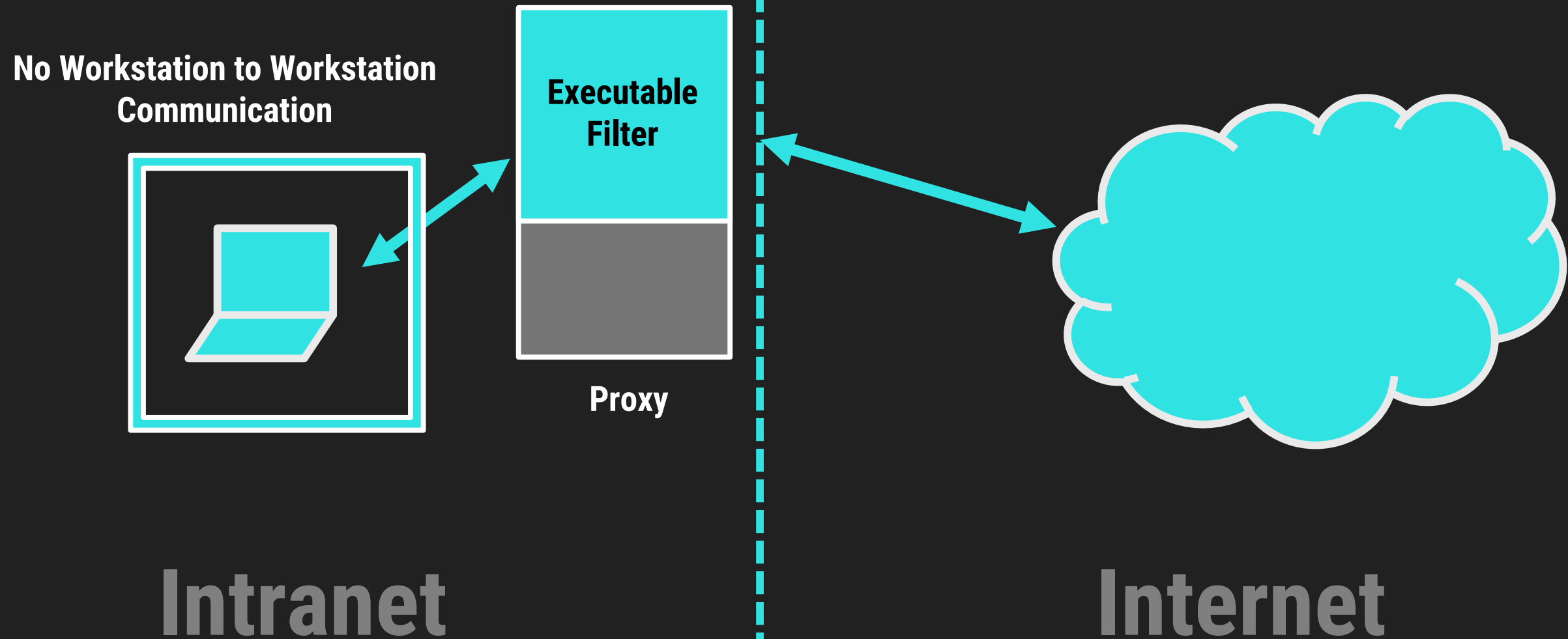


**Intranet**



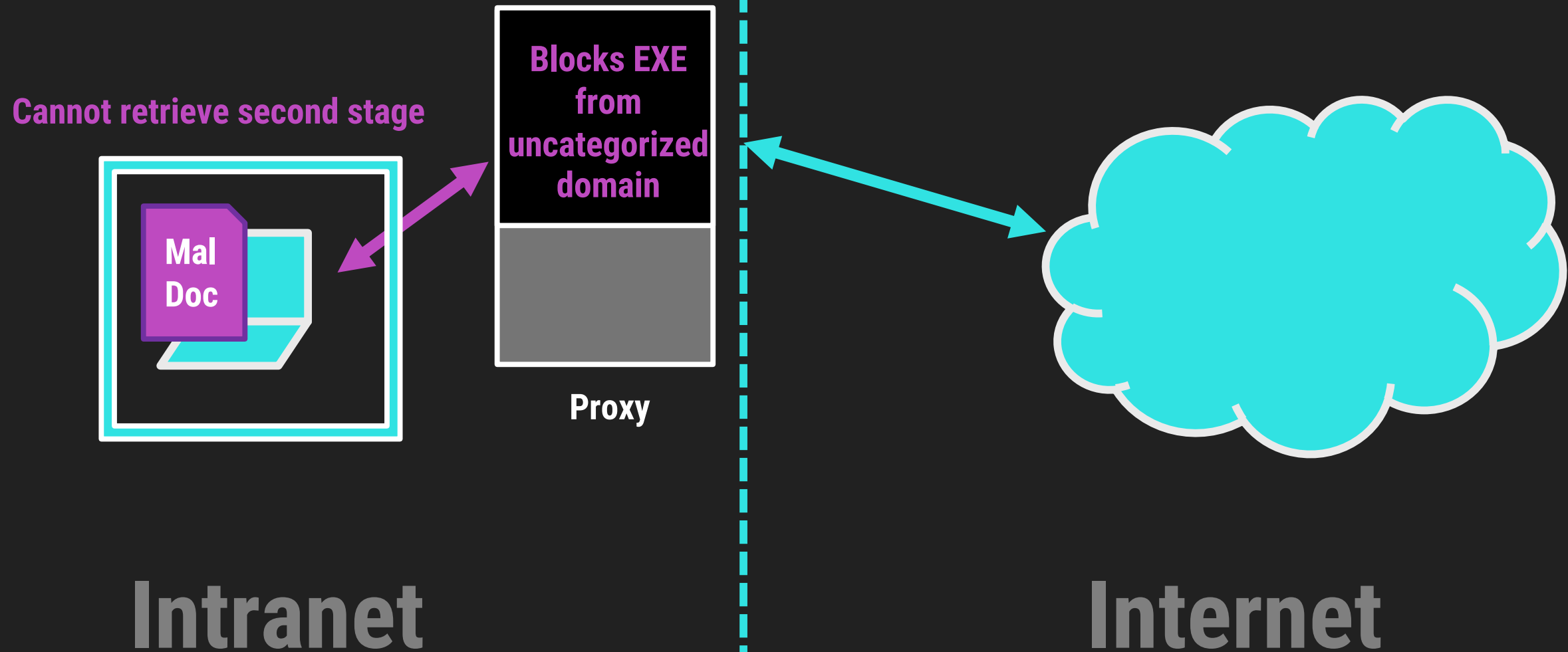
**Internet**

# Best Practice Communication

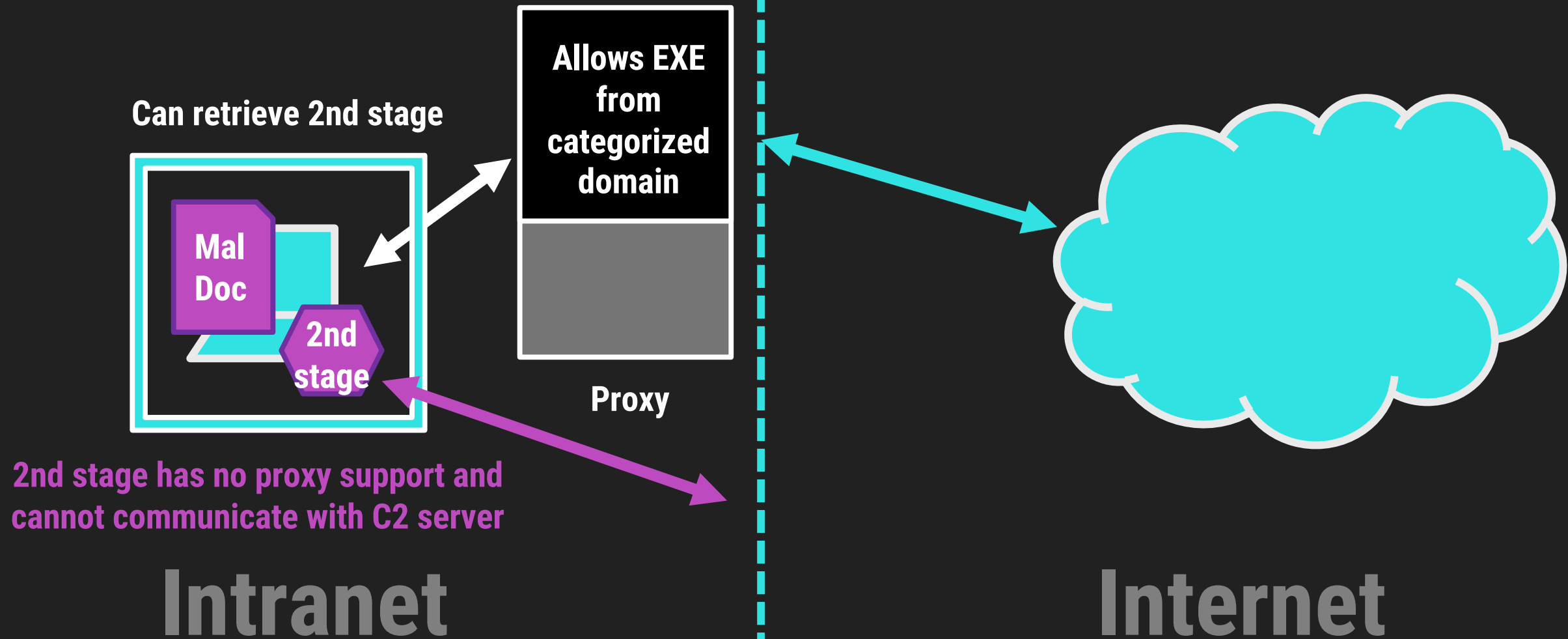




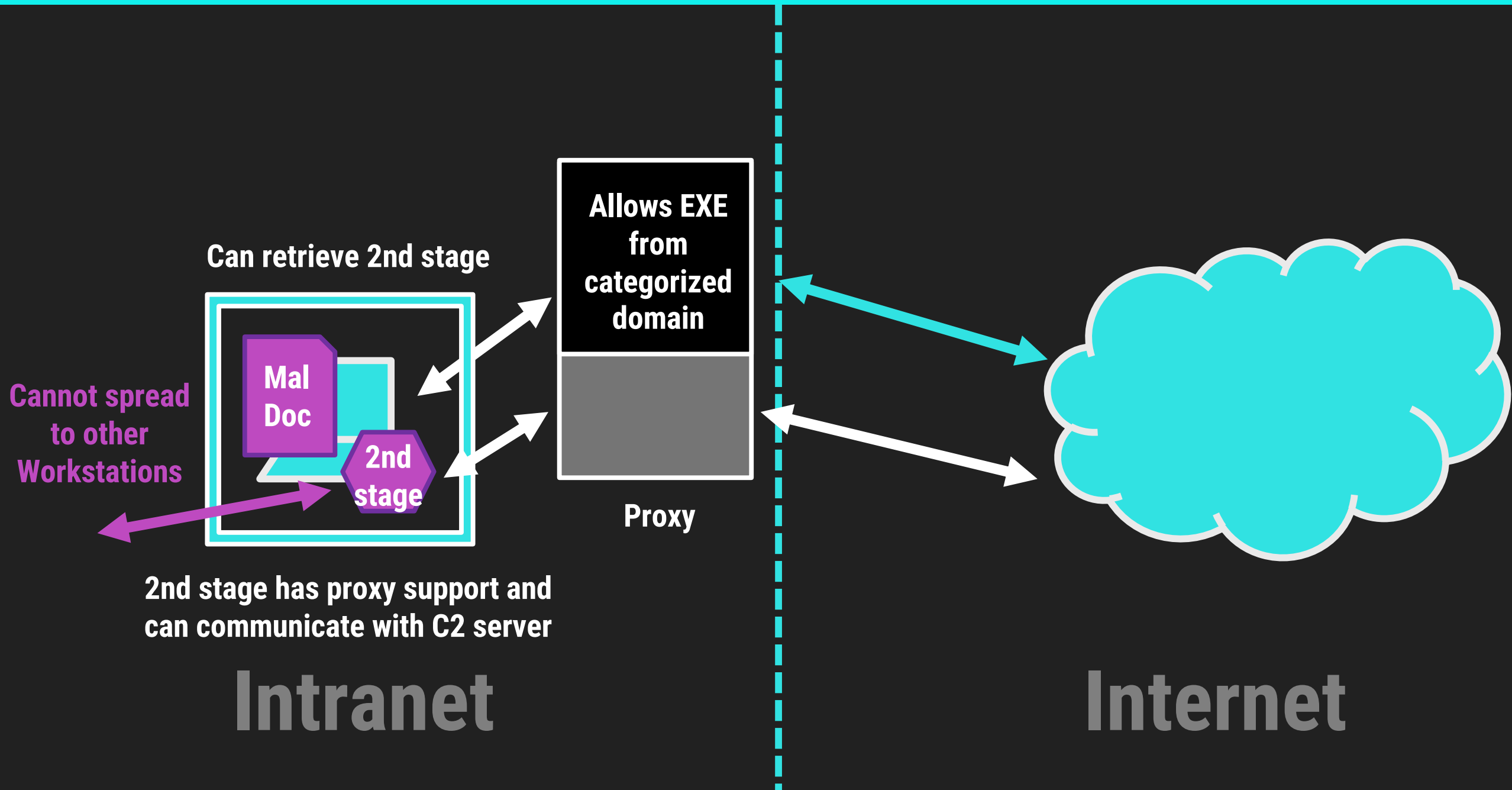
# Resistance 1 – Block Executable Downloads



# Resistance 2 – Enforce Web Proxy

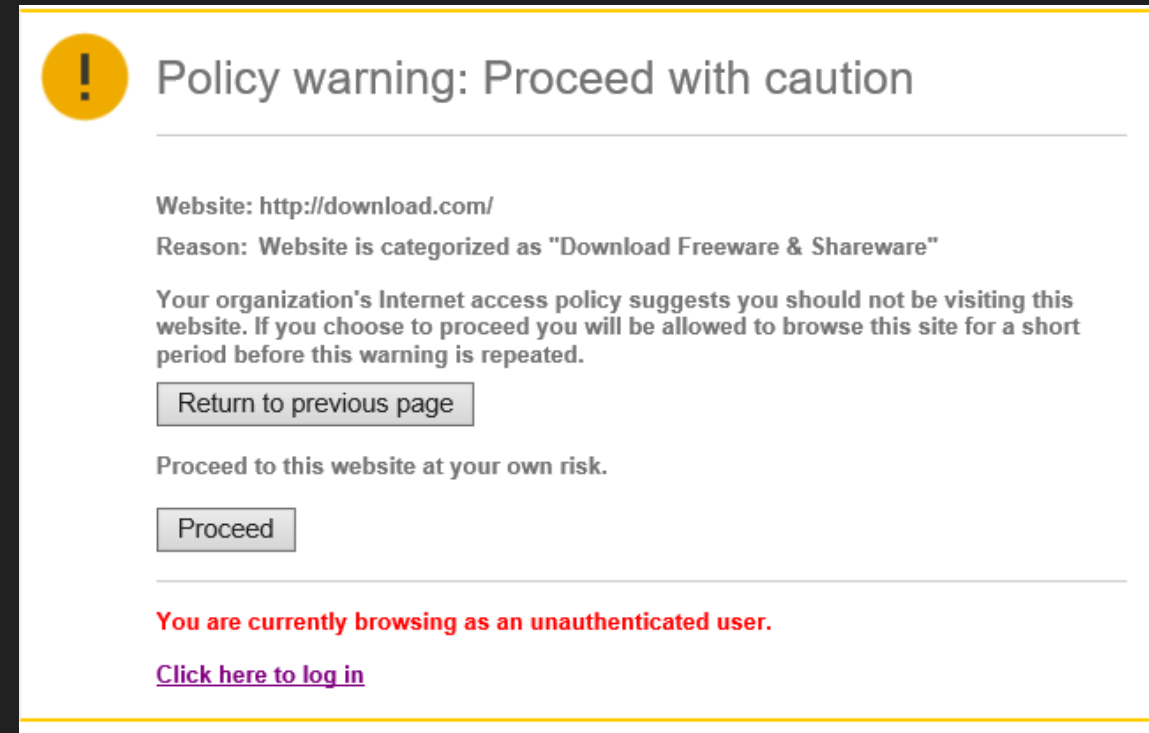


# Resistance 3 – Block Workstation to Workstation Communication



# Resistance Measures in Details

- Enforce Web Proxies
  - Level 1: from workstations on which humans open emails
  - Level 2: from all internal systems
- Block Executable Downloads
  - Level 1: from domains known as malicious (not recommended)
  - Level 2: Instead of blocking, show a splash page for downloads from uncategorized domains (recommended)
  - Level 3: from uncategorized domains
- Block Workstation to Workstation Communication
  - Network segregation is a requirement (allow connections to server segments, proxy, disallow to other client networks)
  - You can use the integrated Windows Firewall



# Resistance Measures Effects

- Block Executable Downloads  
(from uncategorized domains)
- Enforce Web Proxies
- Block Workstation to Workstation  
Communication

***averts ~90 percent\****

***averts ~60 percent\****

***greatly reduces  
impact\****

***\*of attacks***

# Many Experts Share My View

- I am not alone with that opinion
- Other experts in the industry have made the same experiences

 **SwiftOnSecurity** @SwiftOnSecurity 2d  
INCIDENT RESPONSE/RED TEAM:  
One Simple Trick to stopping an  
attack chain you've seen function, or  
would have worked if it was in place.  
75 43 290

 **markus neis**  
@markus\_neis

Replying to @SwiftOnSecurity

**Require Splash Page for New  
Domains/Uncategorized Domains  
on corporate Proxy and enforce  
Always-on VPN. Breaks most C2s**

1:59pm · 27 Jun 2020 · Twitter Web App

4 Replies 10 Retweets 51 Likes

Reply to @markus\_neis @SwiftOnSe...

 **Joe Slowik** @jfslowik 12h  
Replying to @markus\_neis @DrunkBinary...  
**This x100. Hell, just having a proxy  
with authentication does wonders.**  
7

# Challenges

- Many remote workers, especially due to the global pandemic
  - Bandwidth problems with VPN & corporate proxies
- A solid asset management is a requirement
  - You can't control / restrict / defend what you don't know
  - Affected systems are often the neglected and forgotten ones (embedded systems, POS devices, display systems, print servers etc.)





# Ransomware Resistance

Protective Measures with Low Effort and High Impact