Bring Your Own Policy:

Weaponizing ADMX for Cloud-to-On-Prem Lateral Movement.

(Part of Altered Security Hacker Summer 2026)

About Us

Security Researcher @ Altered Security

- LinkedIn - linkedin.com/in/hduseja
- Overall 7.5+ years of hands-on experience in Information Security.
- Strong passion for Enterprise Cloud Security, and Red Teaming.
- Spends days researching attack vectors in Azure, Intune, Entra ID, Hybrid Identity and M365 services with implementable defenses.

About Us

Vishal Raj

Security Researcher @ Altered Security

- LinkedIn - linkedin.com/in/vishal-raj007
- Focus on identifying and exploiting misconfiguration in modern cloud environments.
- Proactively research AI Red Team techniques to evaluate its attack surfaces.
- Active technical blogger sharing practical research and attack scenarios.

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like

ALTERED SECURITY

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Free Labs and Challenges	redlabs.enterprisesecurity.io

What is Hacker Summer ?

- Altered Security’s month-long Red Teaming event.
  - Research blogs and webinars on Red Teaming for on-prem, Azure and AI.
  - Call for papers.
  - Discounts and giveaways.

Webinar Ground Rules

- You can ask questions on redlabs channel (#general) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.
- To ensure a smooth experience, participants are not allowed to use their microphone.
- Please maintain professional conduct and a respectful atmosphere throughout the webinar.

Preamble

Source: https://pbs.twimg.com/media/HDxSclcbEAE0SNx.jpg

Understanding Azure

- Azure is Microsoft’s comprehensive cloud computing platform offering extensive IaaS, PaaS and SaaS solution.
- It allow organizations to build, deploy and manage compute, storage and networking via its global data centers.
- It offers high availability, enterprise-grade security, seamless scalability, and pay-as-you-go pricing to optimize performance and costs for business workloads.

Understanding Entra ID

- Microsoft Entra ID is a cloud-native identity and access (IAM) management platform designed to provide governance, authentication, authorization, and access to its users across Azure, Microsoft 365, Intune and many of the external SaaS solutions.

- It delivers key capabilities including single sign-on (SSO), multi-factor authentication (MFA), conditional access policies, and seamless hybrid identity integration to secure user access across applications.

Microsoft Intune

- Microsoft Intune is a separately licensable cloud-based Endpoint Management suite, that is part of the same Microsoft Cloud ecosystem as Azure and Entra ID.

- It allows organizations to securely manage devices - including laptops, desktops, smartphones, and tablets - across multiple operating systems, including Windows, macOS, Linux, Android, and iOS, from a single management interface.

Microsoft Intune

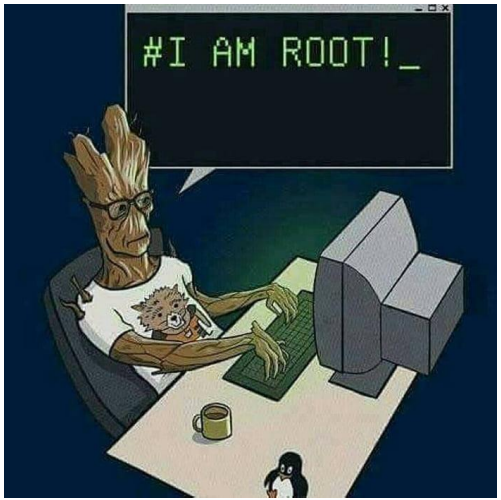
- It supports three management modes: MDM, MAM, and a combination of both. Our focus for today will be on Mobile Device Management (MDM) mode.

- Through MDM, administrators can perform:
  - Device Compliance.
  - Device Configuration.
  - Endpoint Security.
  - Managed Device Actions.
  - Device Updates.

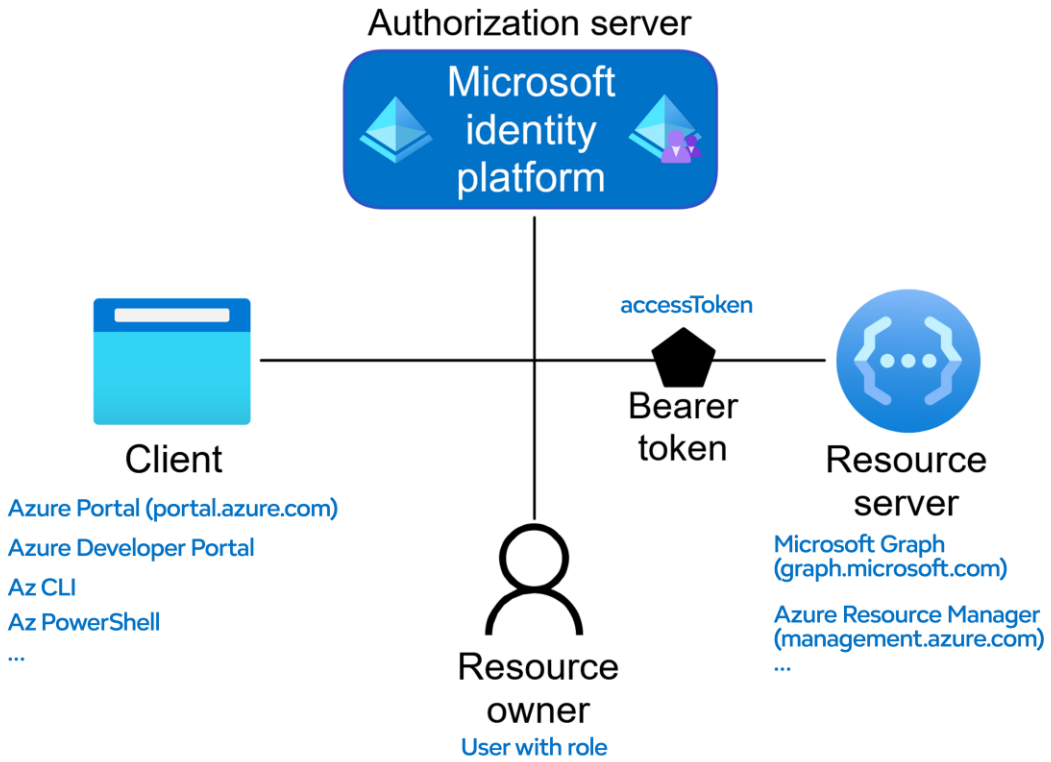
Inherent Risk of Intune as an MDM solution

- In an enterprise environment, Microsoft Intune provides administrators the capability to deploy and execute management scripts directly on Intune enrolled corporate devices.
- It allows deployment of **`PowerShell`** scripts (on Windows) and **`Shell`** scripts (on macOS/Linux).

- These scripts run under the highest administrative privileges, typically as **`LOCALSYSTEM`** on Windows or **`root`** on macOS/Linux respectively.
- While essential for modern non-interactive endpoint operations, this introduces a direct, high-impact pipeline for an attacker to bypass several roadblocks using the cloud management plane and execute script directly onto target endpoints.



OAuth Flow

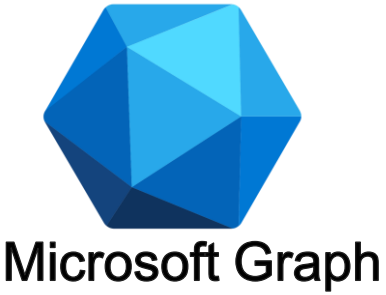

Authorization server
Microsoft identity platform
accessToken
Bearer token
Client
Azure Portal (portal.azure.com)
Azure Developer Portal
Az CLI
Az PowerShell
...
Resource owner
User with role
Resource server
Microsoft Graph (graph.microsoft.com)
Azure Resource Manager (management.azure.com)
...

Different Types of Tokens

Token Type	
Access Token	
Refresh Token	
Primary Refresh Token	

Inner workings of Intune

- Behind the scenes, Microsoft Graph acts as the primary API surface powering majority of the Intune operations.
- Compromising a first-party application from Microsoft with access to the Microsoft Graph permissions **`DeviceManagementConfiguration.ReadWrite.All`** or **`DeviceManagementScripts.ReadWrite.All`** in its scope, grants an attacker the authority to inject and execute malicious scripts onto all or targeted devices.

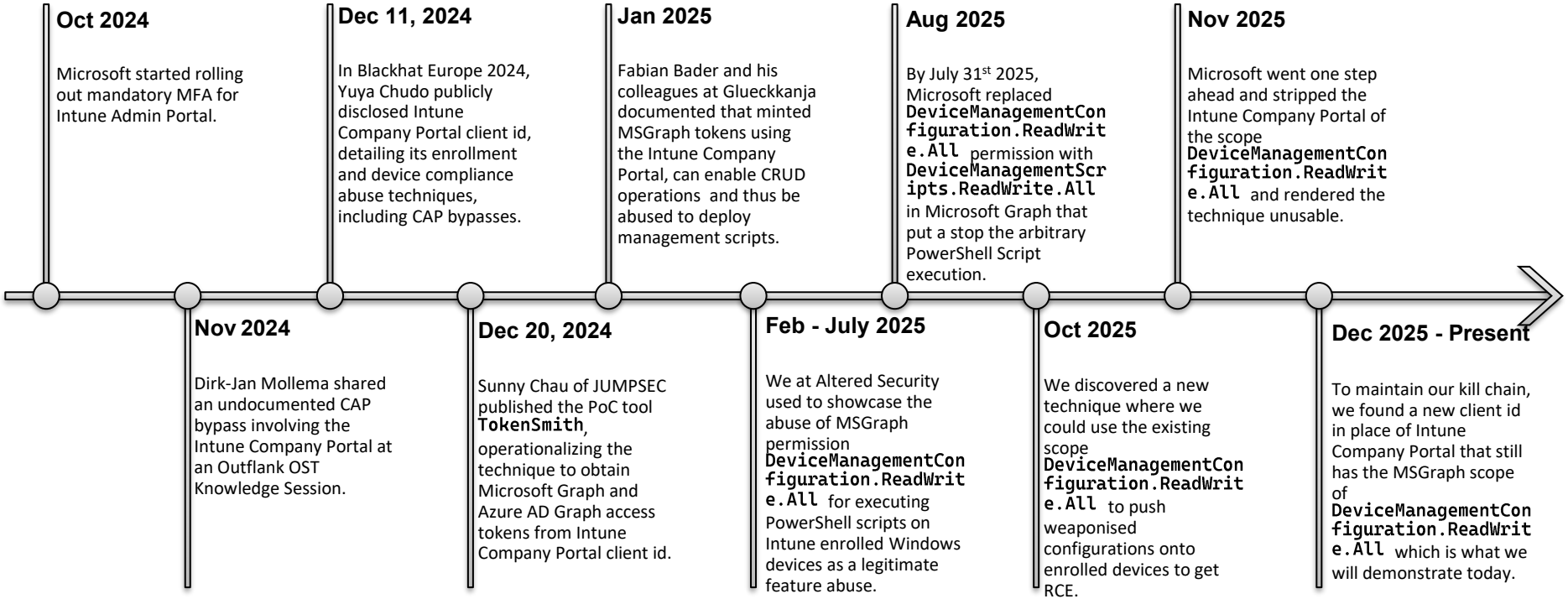


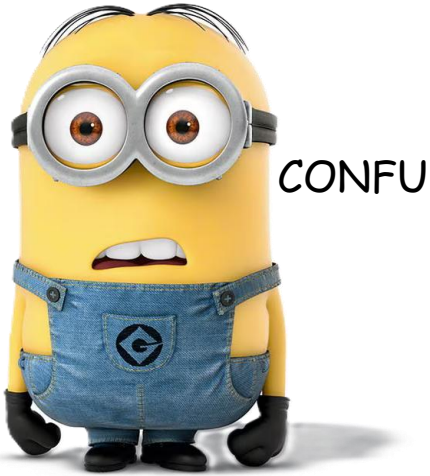

```
  "scp": "CloudPC.Read.All CloudPC.ReadWrite.All DeviceManagementApps.ReadWrite.All DeviceManagementCloudCA.Read.All
DeviceManagementCloudCA.ReadWrite.All DeviceManagementConfiguration.ReadWrite.All
DeviceManagementManagedDevices.PrivilegedOperations.All DeviceManagementManagedDevices.ReadWrite.All
DeviceManagementRBAC.ReadWrite.All DeviceManagementScripts.ReadWrite.All DeviceManagementServiceConfiguration.ReadWrite.All
Directory.AccessAsUser.All User.Read.All",
```

Intune Abuse that worked till Oct 2024

PlatformScript_Demo.mp4

Historical Context





CONFUSED ???

Intune Company Portal

Previously, as explained in earlier demo, PRT cookie was used to provide us with GUI Access of Intune Portal.

Microsoft brought MFA to Intune Portal, so even with PRT cookie, GUI Access was not possible.

The researcher community found a workaround that uses Graph API Calls using Intune Company Portal App Id with its scope "`DeviceManagementConfiguration.ReadWrite.All`", for scripts execution.

To prevent scripts execution, Microsoft swapped "`DeviceManagementConfiguration.ReadWrite.All`" with "`DeviceManagedScripts.ReadWrite.All`", that Intune Company Portal didn't had in its scope.

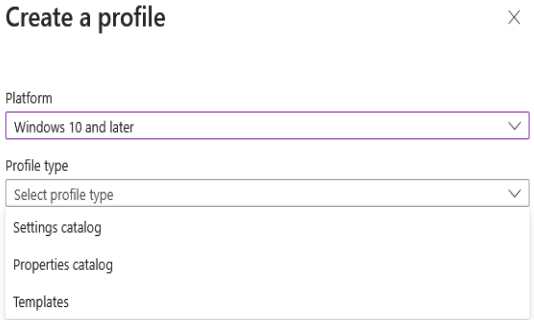
We found a new workaround to get RCE w/o using platform scripts using the existing scope "`DeviceManagementConfiguration.ReadWrite.All`".

Then Microsoft removed "`DeviceManagementConfiguration.ReadWrite.All`" permission from the scope of Intune Company Portal App.

We found a different App Id that had the permission "`DeviceManagementConfiguration.ReadWrite.All`" to ensure that our RCE method w/o scripts is maintained.

Device Configuration Policies

- The scope '**DeviceManagementConfiguration.ReadWrite.All**' is used to create Device Configuration Policies to configure and apply Windows settings for enrolled devices through Intune profile types.

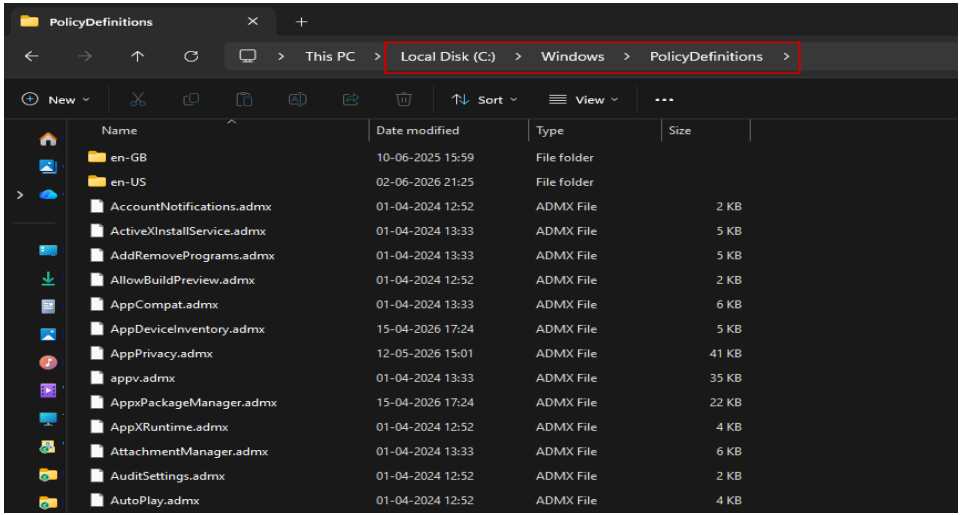


- Many of these settings are backed by Windows Configuration Service Providers (CSPs) that satisfy most administration requirements. However, what about settings that are not exposed through the existing catalogs or templates?

- To configure such settings, Intune administrators can use one of two approaches:
  - Custom Templates.
  - Administrative Templates.

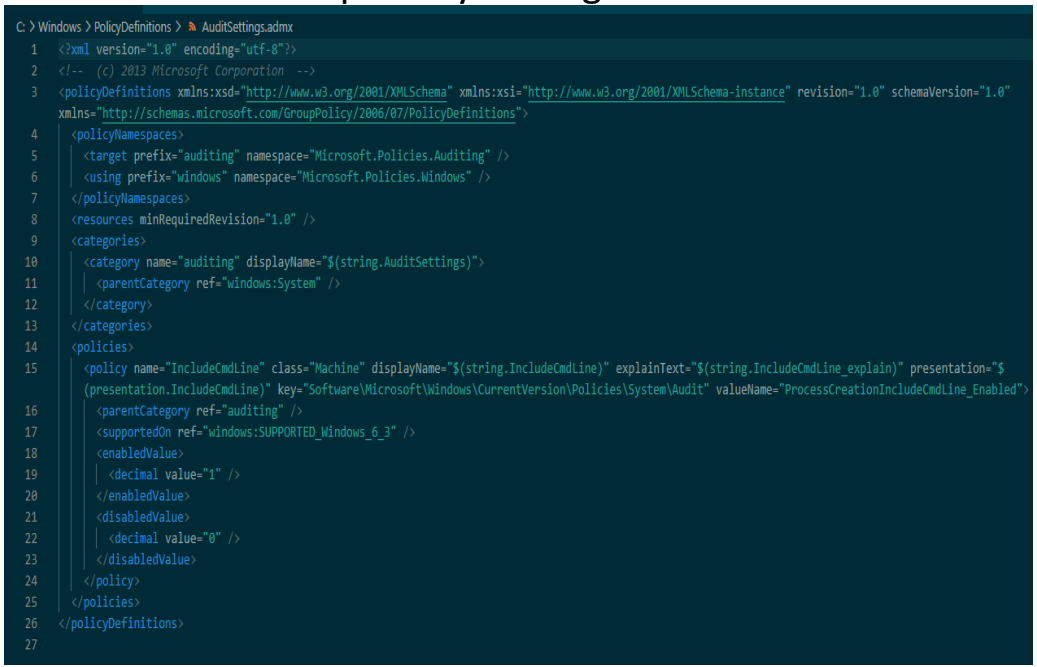
Administrative Templates

- Administrative Templates are based on policy definitions. Many of these definitions are built into Windows and are located in the C:\Windows\PolicyDefinitions folder. However, administrators can also import custom ADMX (Administrative Templates XML) files into Intune to expose additional policy settings beyond the traditionally available ones on enrolled devices.



ADMX File Format

- An ADMX file is an XML-formatted document that contains policy definitions to configure Windows Group Policy settings.

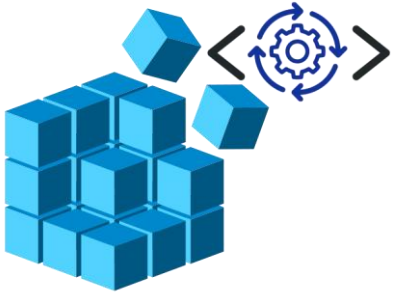


- After a custom ADMX file is imported into Intune, each policy setting is exposed as an individual configuration item within its corresponding policy category.

- Administrators can then configure them to apply Local Group Policy under both Computer Configuration or User Configuration in Windows.

Possible Scenarios for ADMX Abuse

- By virtue of their underlying Group Policy implementation, ADMX templates can be used to modify registry keys and values, within the registry hive.



- One well-documented MITRE ATT&CK technique (T1547.001 – Registry Run Keys / Startup Folder) involves abusing Windows Registry Run and RunOnce keys to achieve automatic code execution during user logon.

Limitations of ADMX

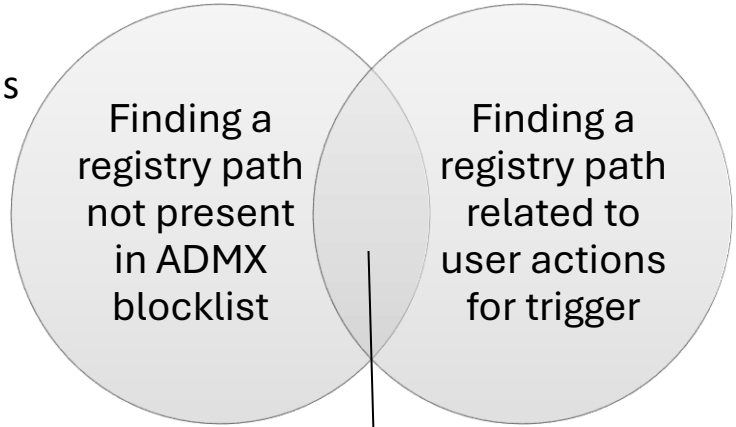
- However, by default, sensitive paths within the registry hive (HKLM, HKCU) are not allowed to be modified.

When the ADMX policies are ingested, the registry keys to which each policy is written are checked so that known system registry keys, or registry keys that are used by existing inbox policies or system components, aren't overwritten. This precaution helps to avoid security concerns over opening the entire registry. Currently, the ingested policies aren't allowed to write to locations within the **System**, **Software\Microsoft**, and **Software\Policies\Microsoft** keys, except for the following locations:

- So, at this stage, the question that came to our mind was what can we do?

Improvise, Adapt and Succeed

- The Venn diagram alongside illustrates the our approach to find potential registry modification paths using ADMX as an attack vector for Intune enrolled Windows endpoint.



- At this stage, we found the registry path **`HKCU\Software\Classes\CLSID\{File-Explorer-UUID}\shell\opennewwindow\command`** which perfectly sits at the Intersection

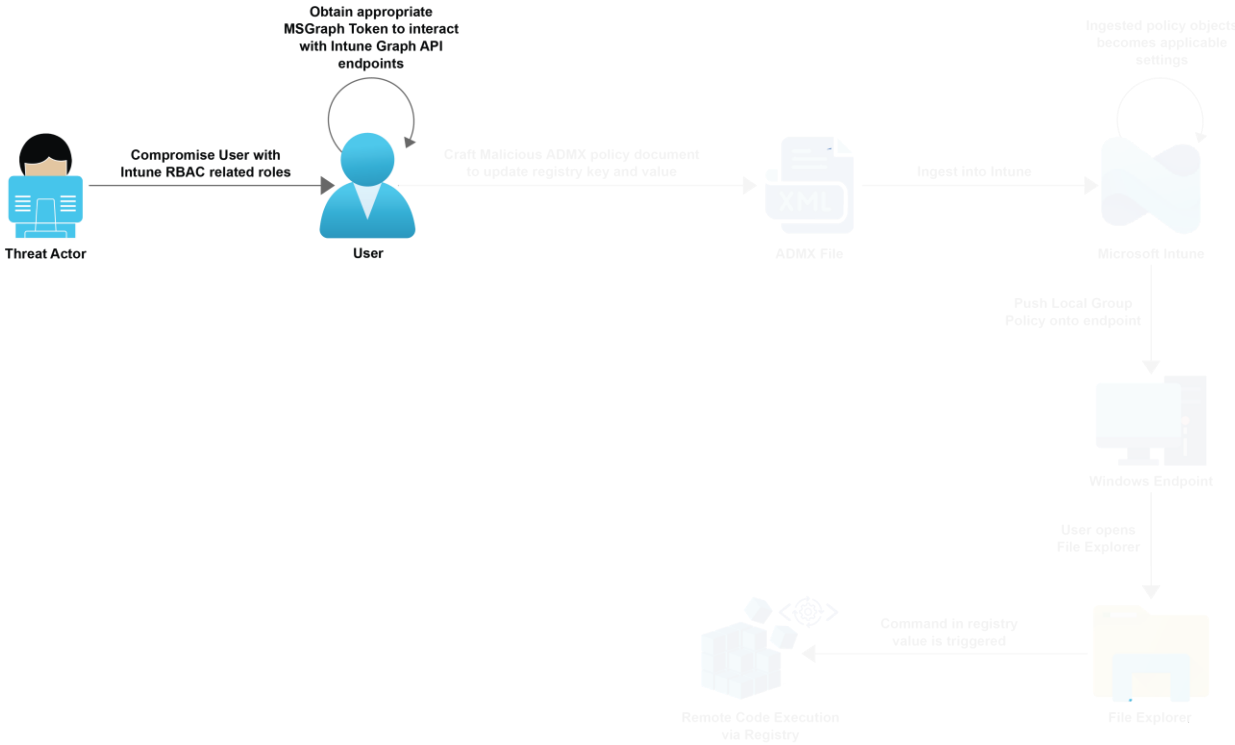

GET READY !!!
It's showtime...

Demonstration

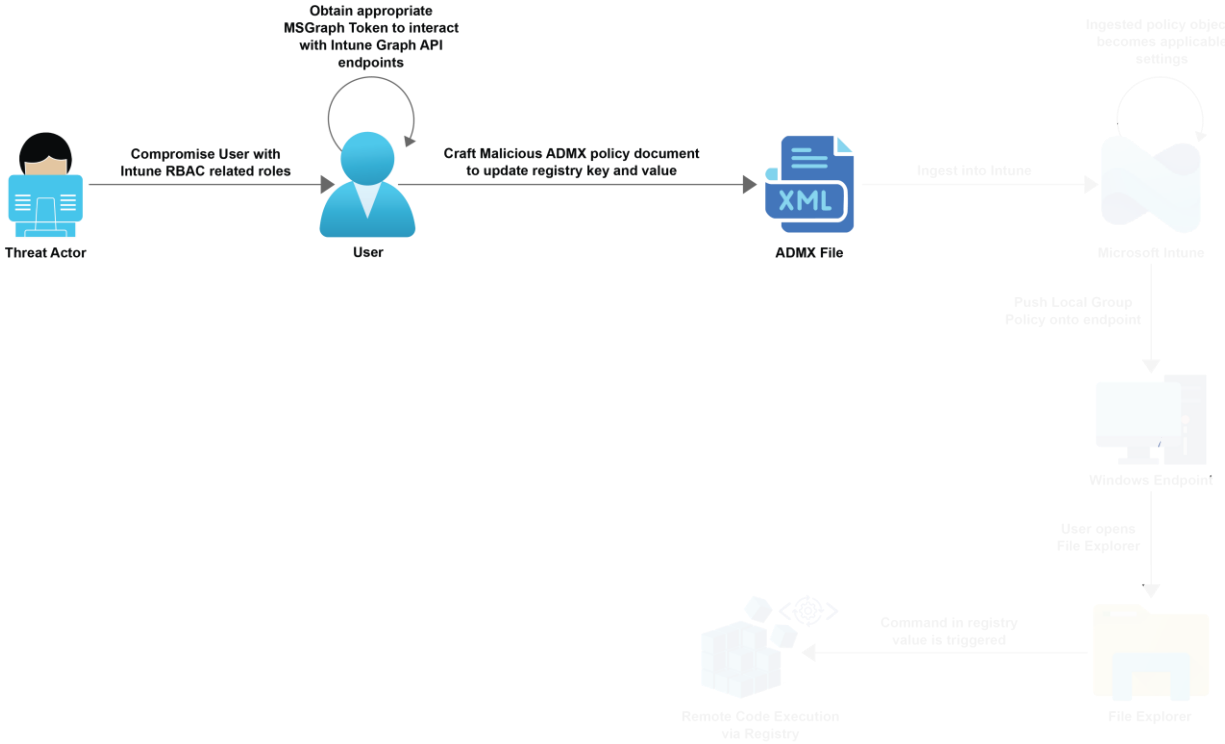
ADMX_Demo.mp4

In a nutshell

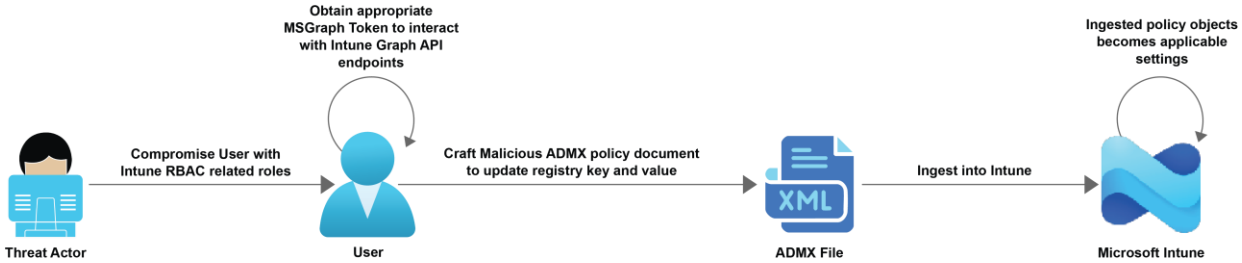
In a nutshell



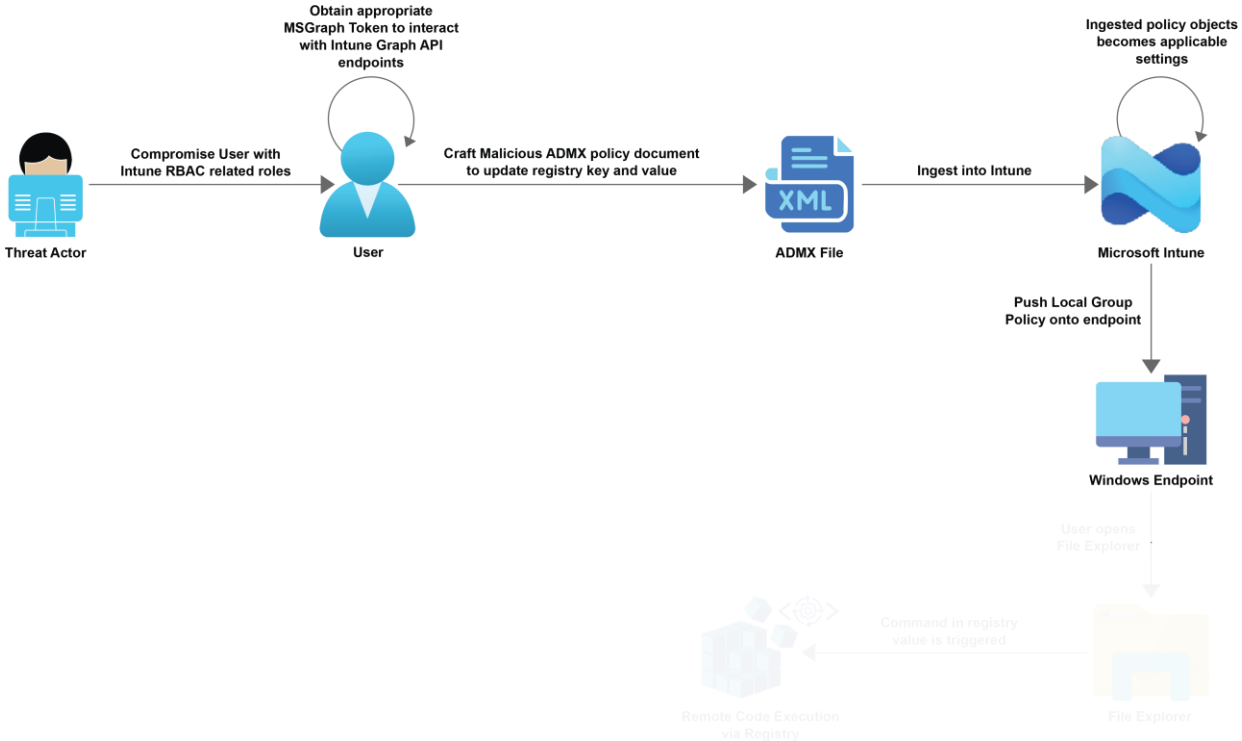
In a nutshell



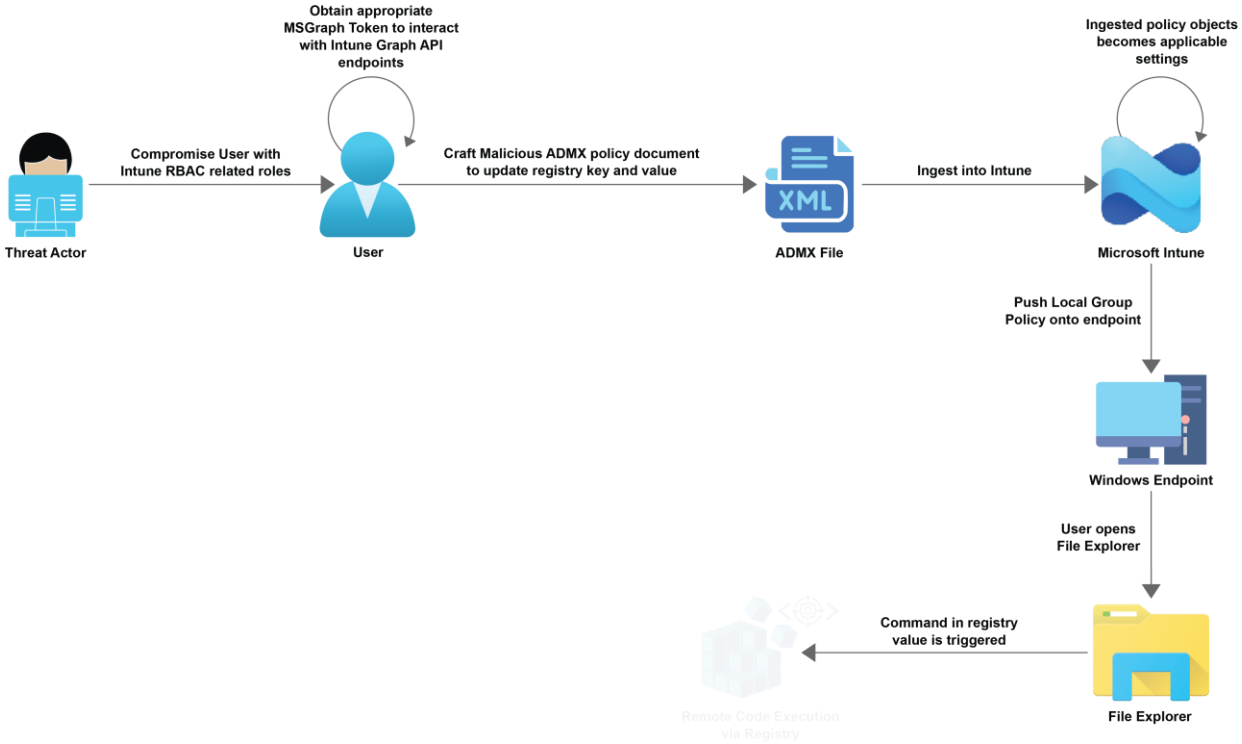
In a nutshell



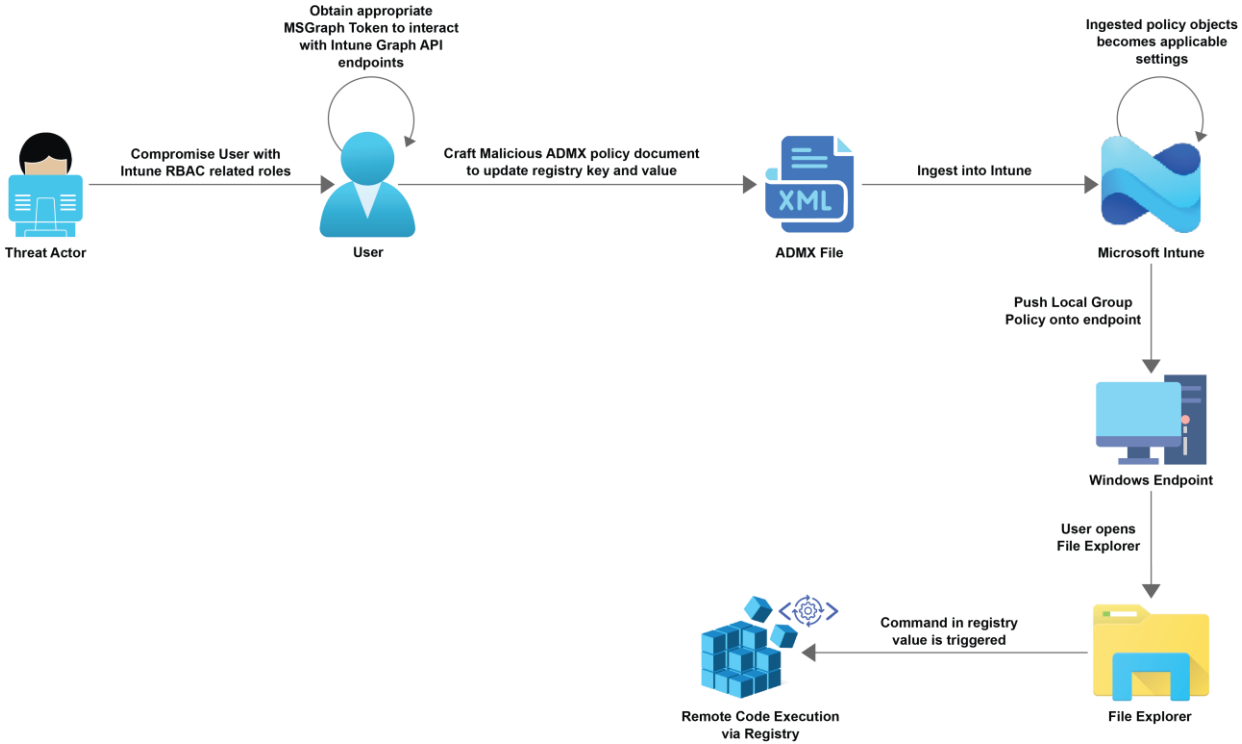
In a nutshell



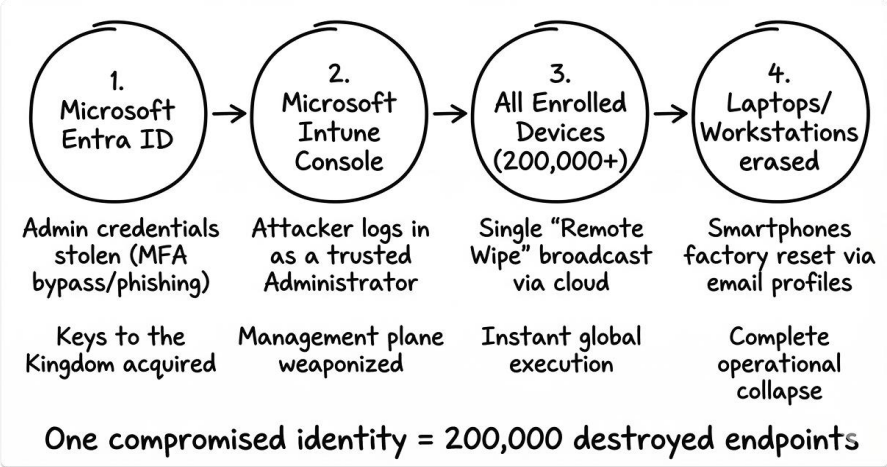
In a nutshell

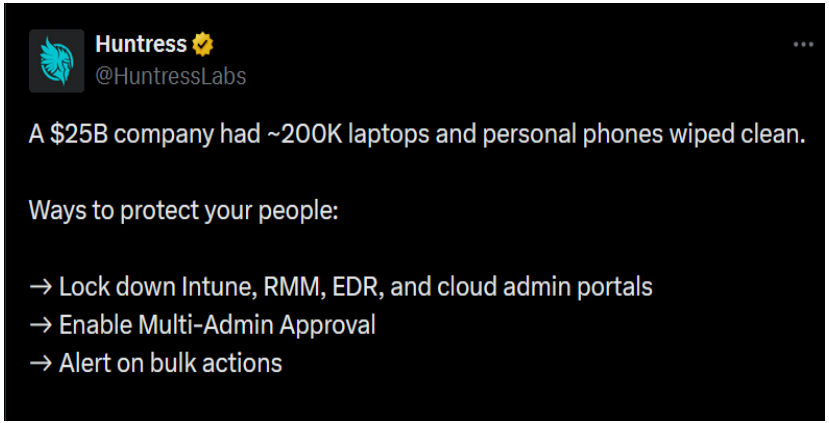


In a nutshell



The Stryker Attack – March 2026





Areas for Further Research

- Finding more registry paths that can be potentially abused via ADMX Local Group Policy document.
- Exploring the malicious application abuse via MAM (Mobile Application Management) mode of Intune.
- Examining Apple's Property List files (.plist) as mechanisms for deploying policy and configuration settings on macOS devices.
- Discovering ways to abuse Intune on Linux distributions.

Conclusion

- Microsoft recognized the Intune risk in 2024 and started a crack down by rolling out significant countermeasures, specifically clamping down on Microsoft Graph permissions for First-Party applications.
- We explored a novel approach that bypasses those exact countermeasures.
- We learned how a threat actor can take a Microsoft First-Party app with strictly limited Graph permissions, subvert it to deploy an ADMX policy, and cleanly drop an old-school registry persistence mechanism via Local Group Policy.

- Please provide feedback.
- Discord (#general channel for this webinar) - https://discord.com/invite/vcEwaRMwJe
- Red Team labs https://www.alteredsecurity.com/online-labs
- Bootcamps: https://www.alteredsecurity.com/bootcamps
- Free Azure Red Team Labs: https://redlabs.enterprisesecurity.io/