



BLUEHAT
SECURITY ABOVE ALL ELSE

Getting “In Tune” with an Enterprise: Detecting Microsoft Intune Lateral Movement

Brett Hawkins (@h4wkst3r)

Adversary Services, IBM X-Force Red

Agenda

1. Introduction
2. Background
3. Intune Offensive Use Cases
4. Detecting and Preventing Intune Lateral Movement
5. Conclusion

Blog Post



SecurityIntelligence

Getting “in tune” with an enterprise: Detecting Intune lateral movement



Light

Dark

September 4,
2024

By [Brett Hawkins](#)
13 min read

[Adversary Services](#)

[X-Force](#)

Organizations continue to implement cloud-based services, a shift that has led to the wider adoption of [hybrid identity environments](#) that connect on-premises Active Directory with Microsoft Entra ID (formerly Azure AD). To manage devices in these hybrid identity environments, Microsoft Intune (Intune) has emerged as one of the most popular device management solutions. Since this trusted enterprise platform can easily be integrated with on-premises Active Directory devices and services, it is a prime target for attackers to abuse for conducting lateral movement and code execution.

This research will give a background on Intune, how it is being used within organizations and show how to use this cloud-based platform to deploy

Introduction

Who am I?

Public Security Research:

<https://h4wkst3r.github.io>



Current Role

Capability Lead,
Adversary Services

IBM X-Force Red



Conference Speaker

Black Hat (US&EU),
DerbyCon, Wild West
Hackin' Fest, BSides,
Hackers Teaching Hackers



Open-Source Tool

Author

SharPersist,
InvisibilityCloak, SCMKit,
ADOKit

Research Drivers

[Research](#) [Threat intelligence](#) [Microsoft Incident Response](#) [Threat actors](#) · 17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

By [Microsoft Incident Response](#)
[Microsoft Threat Intelligence](#)



Threat actors
abuse of device
management
(Octo Tempest)



Lack of research on Win32
App Deployment




Adoption of hybrid
identity architecture




Lack of detection rules
for abuse of Intune for
lateral movement

What is new in this research?




User created Intune Windows app or PowerShell scri..


Incident number 34

 Unassigned

Owner

 New

Status

 High

Severity


Description

This rule will trigger when a user has created a PowerShell script or Windows app in Intune, and has also initiated a device restart for a device within 24 hours. This can be evident of misuse or abuse by a threat actor to force a device to run a script or application.


Alert product names

- Microsoft Sentinel


Evidence

 1

Events

 1

Alerts

 0

Bookmarks

Last update time

07/30/24, 09:04 AM


Creation time

07/30/24, 09:04 AM

Entities (0)

-

Tactics and techniques

 Execution (0)



C2 Payload deployment via Win32 Apps



New Sentinel Detection Rules for abuse of Intune for Lateral Movement



New observations to trigger scripts or Windows Apps to run on Intune managed devices

Prior Work

Andy Robbins (@_wald0)

[Death from Above: Lateral Movement from Azure to On-Prem AD](#)

Chris Thompson (@_Mayyhem)

[Maestro: Abusing Intune for Lateral Movement over C2](#)

Links to prior work
provided in appendix
slides and blog post

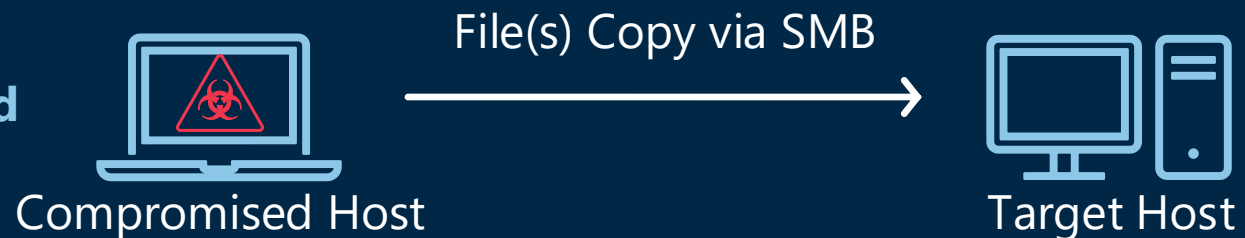


Background

Common Windows Lateral Movement Techniques

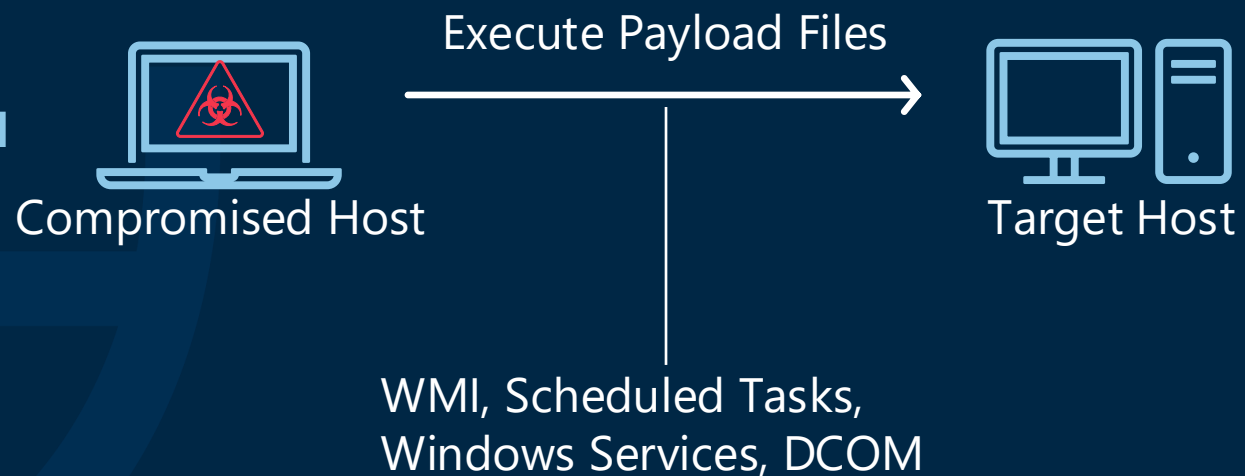
1

Transfer Payload

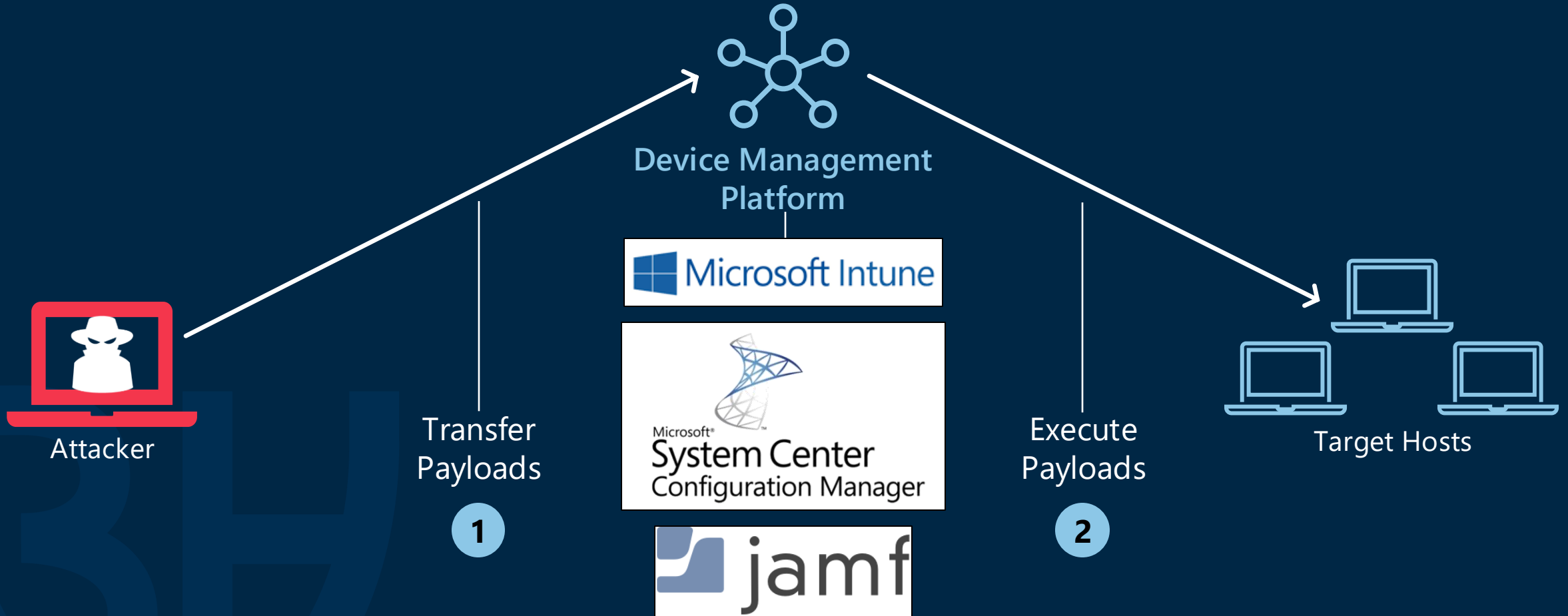


2

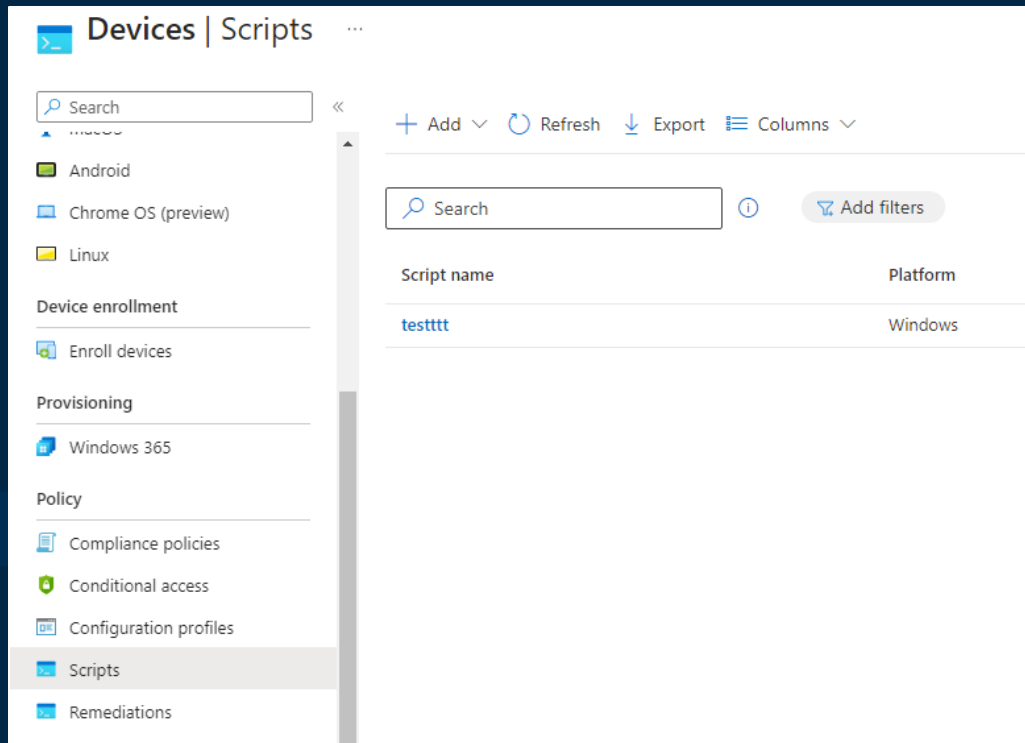
Execute Payload



Using Device Management Platforms for Lateral Movement



Intune Deployment Scripts and Applications



PowerShell Scripts:
Script file with .ps1 extension



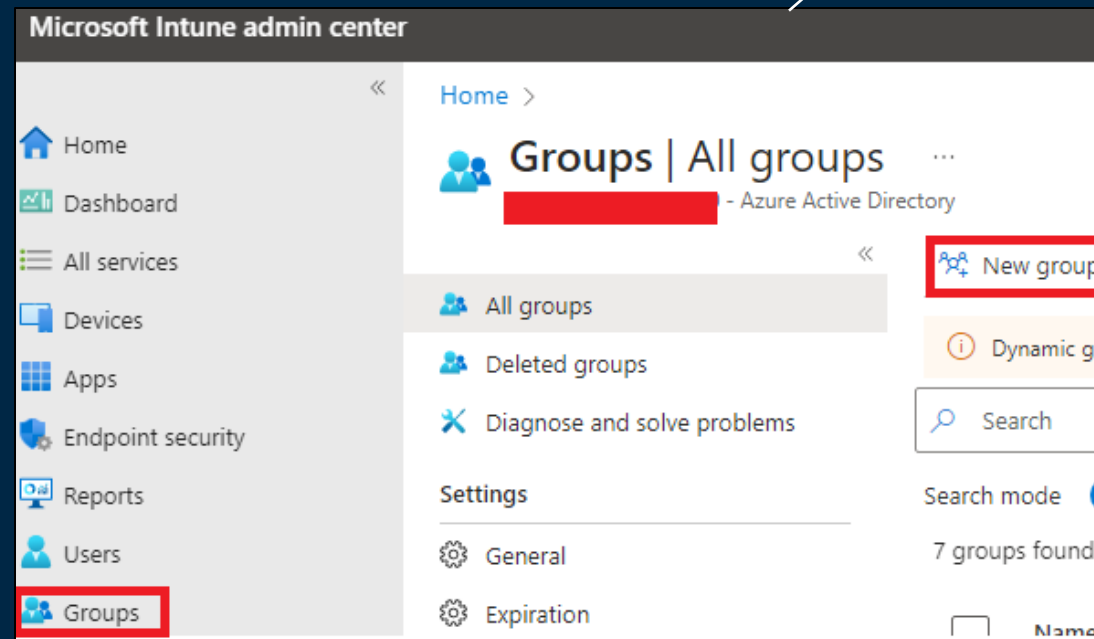
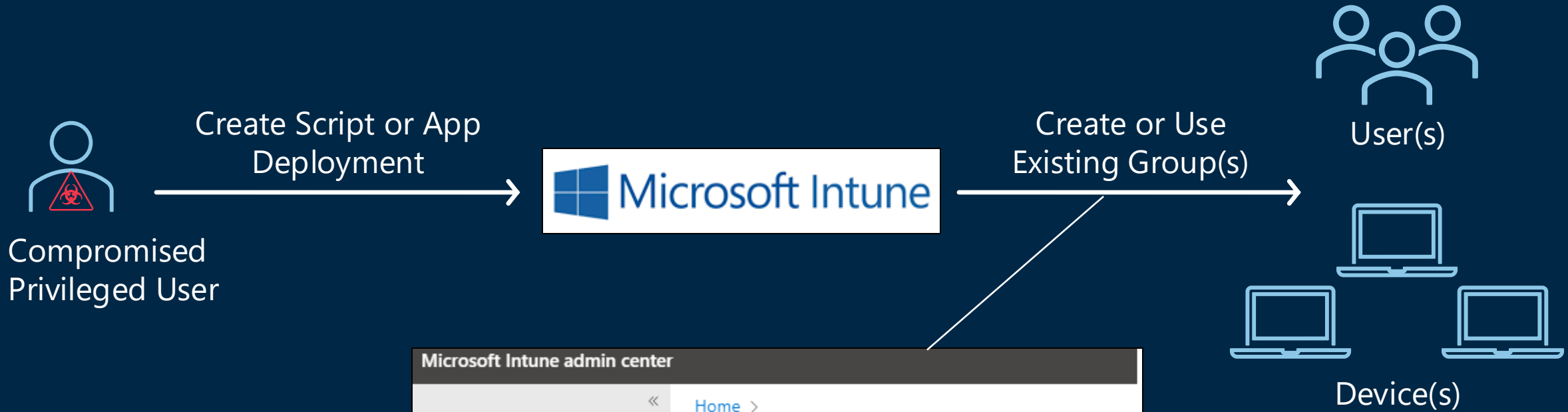
Line of Business (LOB) Apps:
MSI Files, Secure App Packages (.appx, .appxbundle)



Windows App (Win32):
Compressed format with .intunewin extension

Intune Offensive Use Cases

User and Host Targeting



Ad-Hoc Triggering



Cobalt Strike Beacon via Intune Win32 App

Demo

C:\Demo>

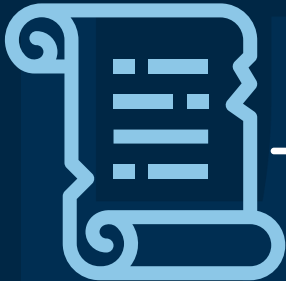
**Creating Intune
package**

Detecting and Preventing Intune Lateral Movement

Intune Logging - Azure



Auditable Event



Audit Log

IntuneAuditLogs schema

Log Stream



Operations of Interest



Audit Log
IntuneAuditLogs
schema



createDeviceManagementScript
DeviceManagementScript

Create PowerShell Script

Create MobileApp

Create Windows App

Delete MobileApp

Delete Windows App

deleteDeviceManagementScript
DeviceManagementScript

Delete PowerShell Script

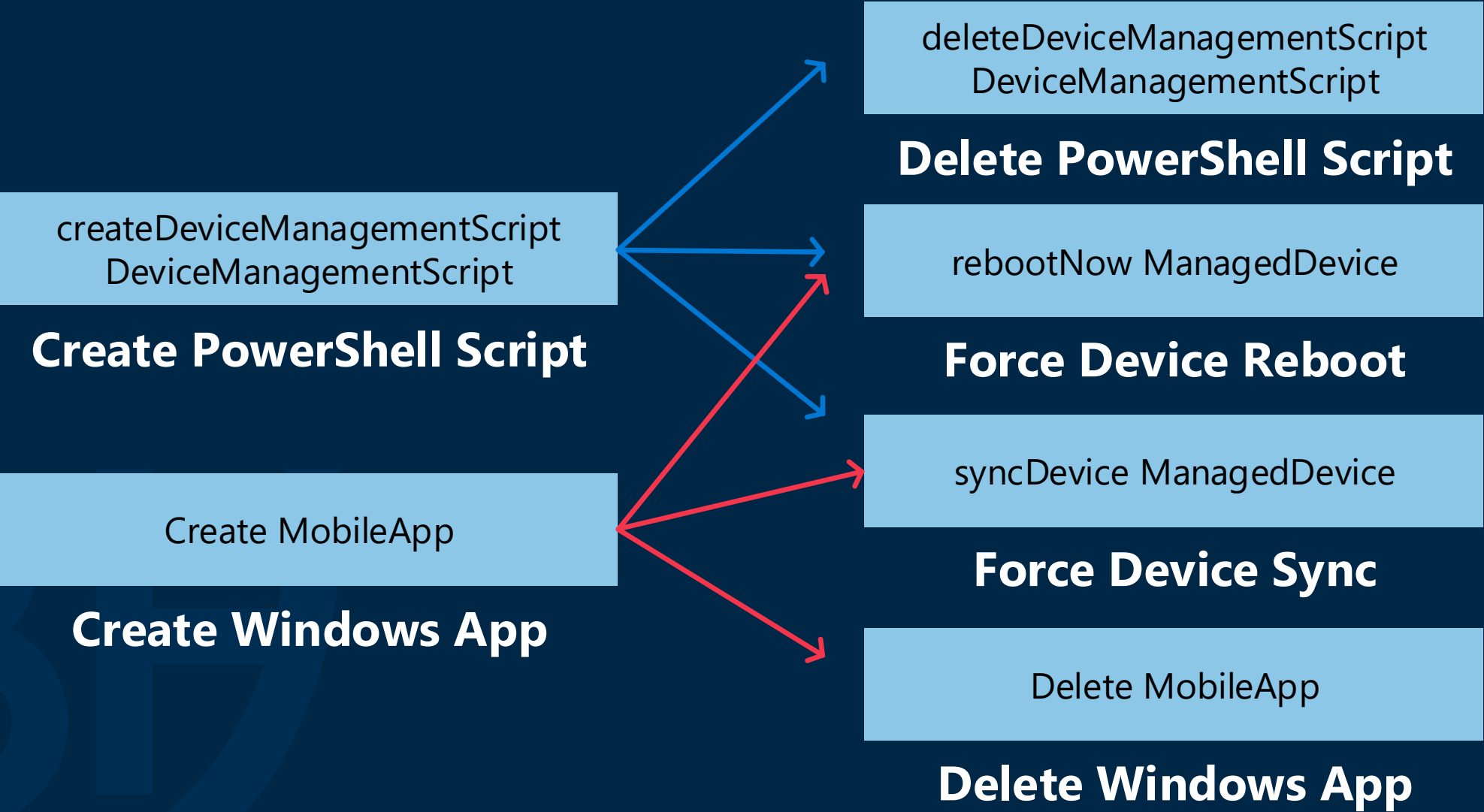
rebootNow ManagedDevice

Force Device Reboot

syncDevice ManagedDevice

Force Device Sync

Potential Malicious Combinations of Operations



New Microsoft Sentinel Rules



Rule #1: User created PowerShell script or Windows application

Rule #2: User created and deleted PowerShell script

Rule #3: User created and deleted Windows application

Rule #4: User created PowerShell script or Windows application and forced a device restart

Rule #5: User created PowerShell script or Windows application and forced a device sync

New Microsoft Sentinel Rules

main

1 Branch

0 Tags

Go to file

Code

h4wkst3r

adding ADO KQL queries

9e46001 · 3 weeks ago

3 Commits

AzureDevOps	adding ADO KQL queries	3 weeks ago
MicrosoftIntune	initial push	3 weeks ago
README.md	adding ADO KQL queries	3 weeks ago

README

KQL-Queries

Collection of defensive KQL queries

Applications

- [Azure DevOps](#)
- [Microsoft Intune](#)

About

Collection of defensive KQL queries

Readme

Activity

0 stars

1 watching

0 forks

Report repository

Releases

No releases published

Packages

No packages published

github.com/h4wkst3r/KQL-Queries

Setup Access Policy

The screenshot displays the Microsoft Intune admin center interface. On the left, the navigation pane includes links to Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration (highlighted with a red box), and Troubleshooting + support. The main content area is titled 'Home > Tenant admin' and features a 'Tenant admin | Multi Admin Approval' header with a key icon. Below the header is a search bar and a list of tenant administration options: Tenant status, Remote Help, Microsoft Tunnel Gateway, Cloud PKI, Connectors and tokens, Filters, Roles, Microsoft Entra Privileged Identity Management, Diagnostics settings, Audit logs, and Device diagnostics. At the bottom of this list, 'Multi Admin Approval' (with a key icon) is highlighted with a red box. On the right side of the main content area, there are tabs for 'All requests', 'My requests', and 'Access policies' (highlighted with a red box). Below the tabs, a description states: 'Access policies allow you to control which tasks and ad...'. Further down, there are '+ Create' and 'Refresh' buttons (both highlighted with red boxes), a 'Search by name' input field, and a message indicating 'Showing 0 to 0 of 0 records'. A table header with 'Name' and a sort icon is visible, followed by the text 'There are no policies to view'.

Setup Access Policy

Home > Tenant admin | Multi Admin Approval >

Create an access policy ...

1 Basics 2 Approvers 3 Review + create

Name * Approval for Scripts ✓

Description This is an access policy that will require approvers to approve a new script deployment.

Profile type * ⓘ Script ▼

i A script policy will limit actions on a script, such as Powershell scripts or remediation scripts. This could include create, edit, assign, and delete.

Home > Tenant admin | Multi Admin Approval >

Create an access policy ...

1 Basics 2 Approvers 3 Review + create

Name * Approval for Applications ✓

Description This is an access policy that will require approvers to approve a new app deployment

Profile type * ⓘ App ▼

i An app policy will limit actions on an application, such as mobile apps or built-in apps. This could include create, edit, assign, and delete.

Setup Access Policy cont.


[Home](#) > [Tenant admin | Multi Admin Approval](#) >

Create an access policy ...

✓ Basics **2** Approvers ③ Review + create

Members of groups you add here can approve requests that need more than one admin to approve

Included groups

 Add groups


Groups

Remove

Intune Approvers

Remove

Summary

 Before this resource can be created, it must be approved by another admin. Before you can submit this request, you must enter your business justification.

App information

App package file Dism.intunewin

Name Some App

Description

Publisher company

App Version --

Category --

Show this as a featured app in the No

Business justification *

[Previous](#)

[Submit for approval](#)

1

Enable MFA for privileged
Azure roles

2

Review privileged Azure
access on regular basis

3

Cloud-only accounts should
be used for privileged Azure
roles

Conclusion

Conclusion

01

Offense:

Device management systems provide stealthy lateral movement method

02

Defense:

Securing device management systems and administrators is critical

03

Defense:

Develop detection rules for device management system abuse

Acknowledgements

Thank You to the below people for feedback and support on this research

- Dave Cossa (@G0ldenGunSec)
- Ruben Boonen (@FuzzySec)
- Shawn Jones (@anthemtotheego)
- Valentina Palmiotti (@chompie1337)



Questions?

Twitter

- @h4wkst3r

Personal Website

- <https://h4wkst3r.github.io>

Blog Post

- <https://securityintelligence.com/x-force/detecting-intune-lateral-movement/>





Appendix – References 1

- <https://learn.microsoft.com/en-us/entra/identity/hybrid/whatis-hybrid-identity>
- https://twitter.com/_wald0
- <https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d>
- https://twitter.com/_Mayyhem
- <https://github.com/Mayyhem/Maestro>
- <https://defcon.org/html/defcon-32/dc-32-demolabs.html>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>
- <https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/choose-a-device-management-solution>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control>
- <https://learn.microsoft.com/en-us/mem/intune/apps/intune-management-extension>
- <https://learn.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>
- <https://jannikreinhard.com/2022/07/31/summary-of-the-intune-management-extension/>

Appendix – References 2

- <https://attack.mitre.org/tactics/TA0008/>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager>
- <https://www.cobaltstrike.com/>
- <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups>
- <https://github.com/dirkjanm/ROADtools>
- <https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-restart>
- <https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-sync>
- <https://securityintelligence.com/x-force/windows-features-dll-sideloading/>
- <https://hijacklibs.net/entries/microsoft/built-in/dismcore.html>
- <https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool>
- <https://www.anoopcnaair.com/intune-management-extension-deep-dive-level-300/>
- <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>

Appendix – References 3

- <https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/octo-tempest-hybrid-identity-compromise-recovery/ba-p/4166783>
- <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>
- <https://learn.microsoft.com/en-us/azure/sentinel/overview>
- <https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/multi-admin-approval>
- <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-secure-remote-workers>
- <https://twitter.com/G0ldenGunSec>
- <https://twitter.com/FuzzySec>
- <https://twitter.com/anthemtotheego>
- <https://twitter.com/chompie1337>
- <https://securityintelligence.com/x-force/detecting-intune-lateral-movement/>
- <https://github.com/h4wkst3r/KQL-Queries>