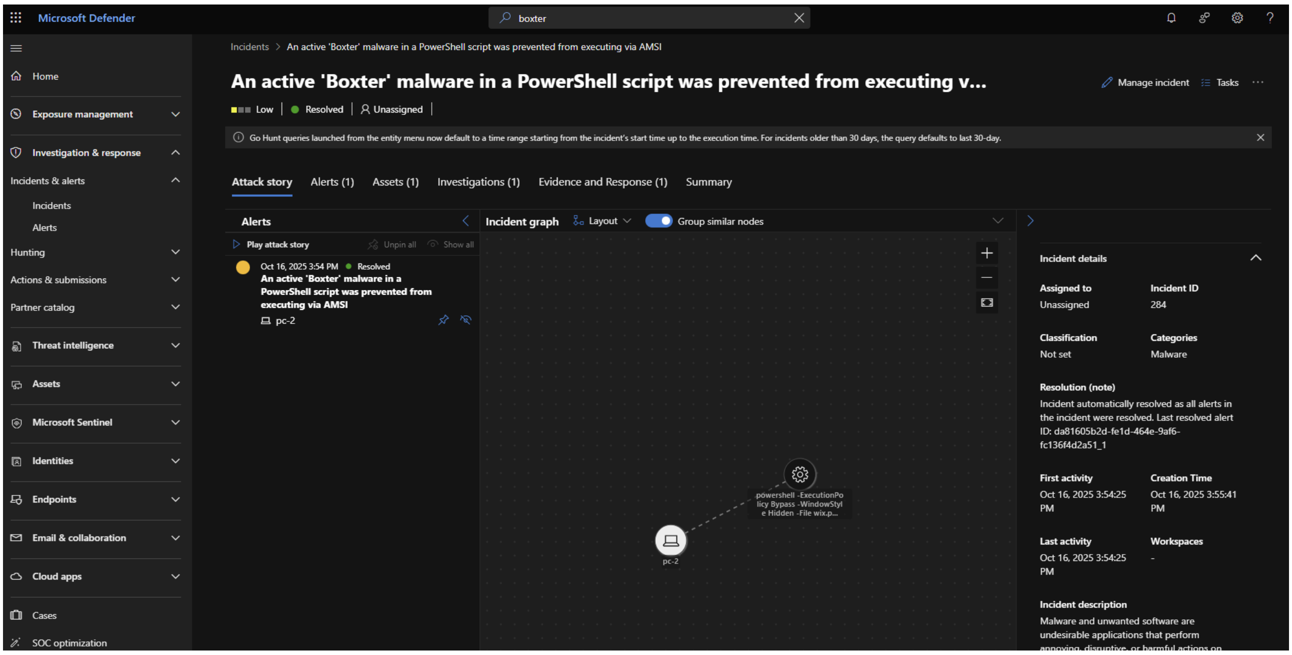
📁 Incident Metadata

Case Type:	SMB Attack
Reported by:	Microsoft Defender
Analyst:	Haydar AKYÜREK
Date:	2025-10-24
Severity:	🔴 **High**
Status:	✅ Closed
Decision:	✅ **True Positive**

📜 Incident description:

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.
A malware is considered active if it is found running on the machine or it already has persistence mechanisms in place. Active malware detections are assigned higher severity ratings.
Because this malware was active, take precautionary measures and check for residual signs of infection.



An active 'Boxter' malware in a PowerShell script was prevented from executing v...

Low | Resolved | Unassigned |

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Oct 16, 2025 3:54 PM ● Resolved
An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI
pc-2

Incident details

Assigned to
Unassigned

Incident ID
284

Classification
Not set

Categories
Malware

Resolution (note)
Incident automatically resolved as all alerts in the incident were resolved. Last resolved alert ID: da81605b2d-fe1d-464e-9af6-fc136f4d2a51_1

First activity
Oct 16, 2025 3:54:25 PM

Creation Time
Oct 16, 2025 3:55:41 PM

Last activity
Oct 16, 2025 3:54:25 PM

Workspaces
-

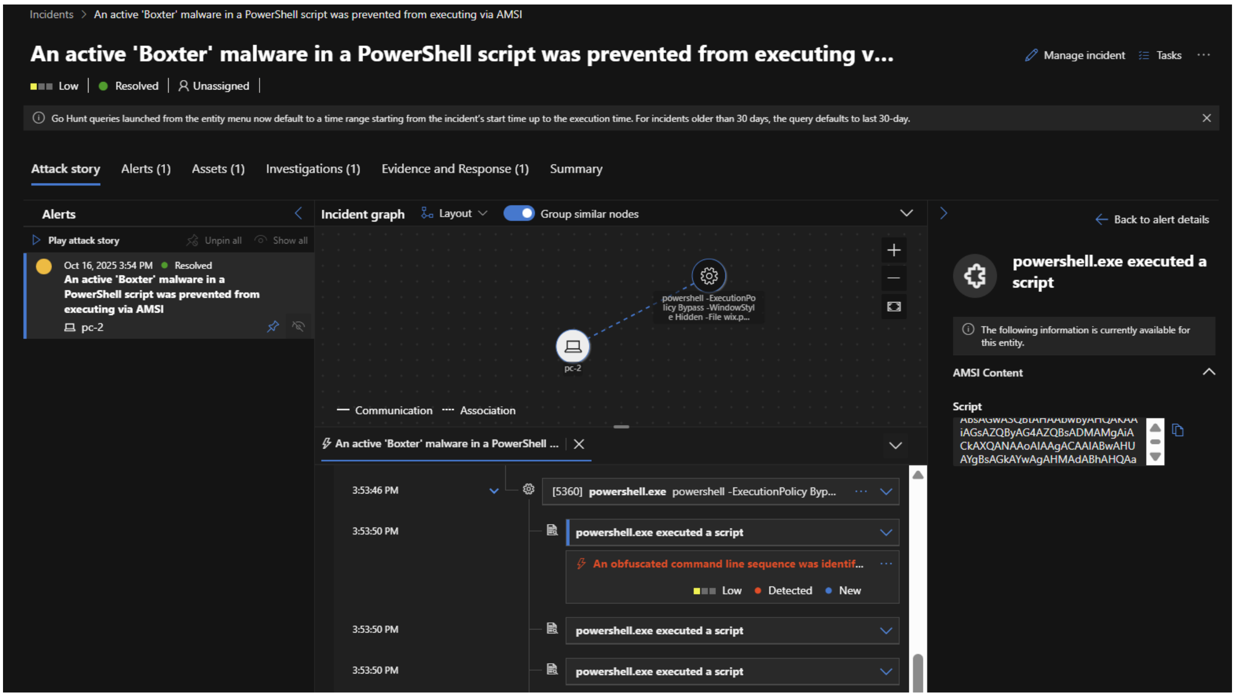
Incident description
Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on

🔍 Microsoft Defender Incident Analysis Notes

1. The wix.ps1 file is executed with the command: `powershell -ExecutionPolicy Bypass -WindowStyle Hidden -File wix.ps1`.

Here, `-WindowStyle Hidden` runs the PS1 file hidden, and `-ExecutionPolicy Bypass` allows it to bypass that security protection.

2. Here we see an obfuscated script that is causing the alarm:



Incidents > An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI

An active 'Boxter' malware in a PowerShell script was prevented from executing v...

Manage incident · Tasks · ···

Low | ● Resolved | Unassigned |

ⓘ Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Attack story · Alerts (1) · Assets (1) · Investigations (1) · Evidence and Response (1) · Summary

Alerts

Play attack story · Unpin all · Show all

Oct 16, 2025 3:54 PM ● Resolved
An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI
pc-2

Incident graph · Layout · Group similar nodes

powershell -ExecutionPolicy Bypass -WindowStyle Hidden -File wix.p...
pc-2
Communication
Association

An active 'Boxter' malware in a PowerShell ...

3:53:46 PM — [5360] **powershell.exe** powershell -ExecutionPolicy Byp...

3:53:50 PM — **powershell.exe executed a script**

An obfuscated command line sequence was identif...
Low ● Detected ● New

3:53:50 PM — **powershell.exe executed a script**

3:53:50 PM — **powershell.exe executed a script**

Back to alert details

powershell.exe executed a script

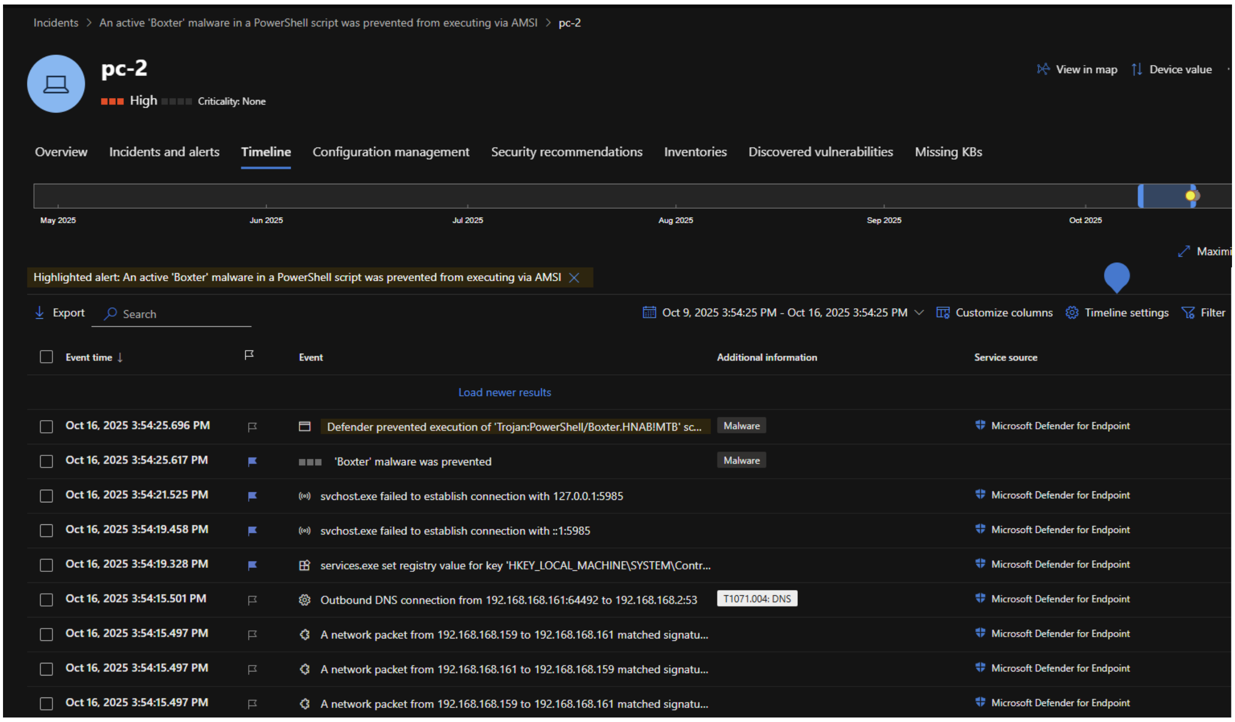
ⓘ The following information is currently available for this entity.

AMSI Content

Script

AbsAGwASQBtAHAAbwByAHQAKAA
iAGsAZQByAG4AZQBsADMAMgAiA
CkAXQANAAoAIAAgACAAIABwAHU
AYgBsAGkAYwAgAHMAdABhAHQAa

3. Powershell.exe is running and then this obfuscated script appears. We can see that the Wix.ps1 file originated from msiexec.exe. This executable is used to run MSI files. Here, we need to find what invoked the msiexec process that created this wix.ps1 file.
4. We clicked “See in Timeline” and started investigating this.



Incidents > An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI > pc-2

pc-2

High · Criticality: None

View in map · Device value

Overview · Incidents and alerts · Timeline · Configuration management · Security recommendations · Inventories · Discovered vulnerabilities · Missing KBs

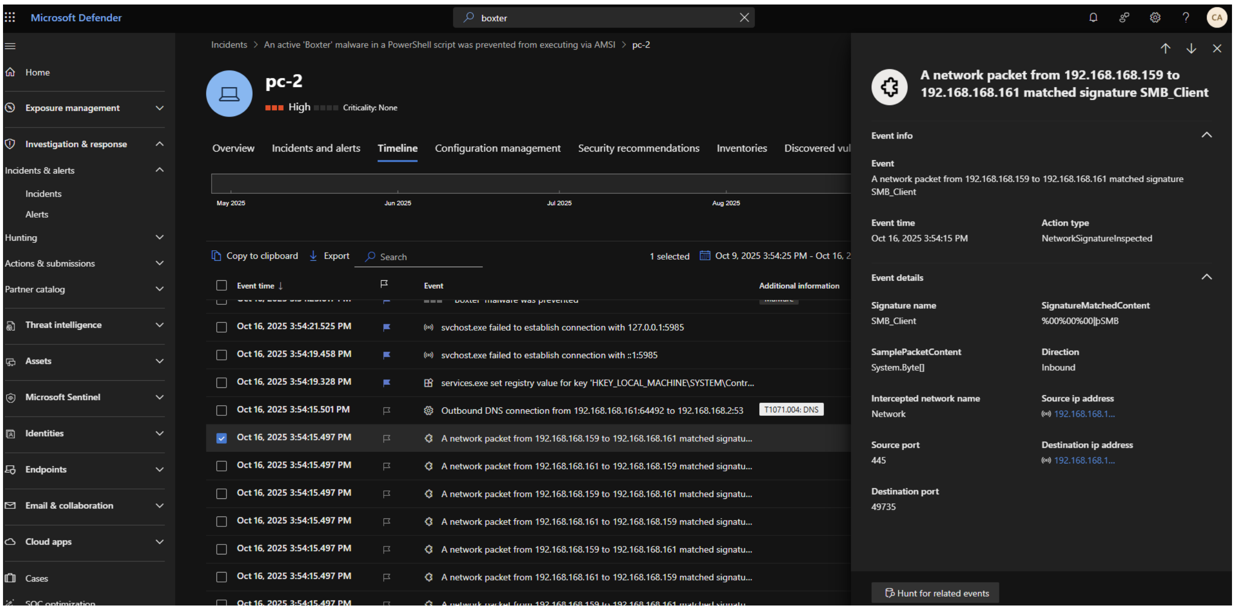
Highlighted alert: An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI

Export · Search · Oct 9, 2025 3:54:25 PM - Oct 16, 2025 3:54:25 PM · Customize columns · Timeline settings · Filter

Load newer results

Event time ↓	Event	Additional information	Service source
Oct 16, 2025 3:54:25.696 PM	Defender prevented execution of 'Trojan:PowerShell/Boxter.HNAB!MTB' sc...	Malware	Microsoft Defender for Endpoint
Oct 16, 2025 3:54:25.617 PM	'Boxter' malware was prevented	Malware	
Oct 16, 2025 3:54:21.525 PM	svchost.exe failed to establish connection with 127.0.0.1:5985		Microsoft Defender for Endpoint
Oct 16, 2025 3:54:19.458 PM	svchost.exe failed to establish connection with ::1:5985		Microsoft Defender for Endpoint
Oct 16, 2025 3:54:19.328 PM	services.exe set registry value for key 'HKEY_LOCAL_MACHINE\SYSTEM\Contr...		Microsoft Defender for Endpoint
Oct 16, 2025 3:54:15.501 PM	Outbound DNS connection from 192.168.168.161:64492 to 192.168.168.2:53	T1071.004: DNS	Microsoft Defender for Endpoint
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...		Microsoft Defender for Endpoint
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.161 to 192.168.168.159 matched signatu...		Microsoft Defender for Endpoint
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...		Microsoft Defender for Endpoint

5. We observed an SMB connection here. SMB is a protocol used for file sharing between devices on the same network. Wannacry also exploited a vulnerability in SMB. Here, we couldn't find more details about this communication.



Incidents > An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI > pc-2

pc-2

High Criticality: None

1 selected Oct 9, 2025 3:54:25 PM - Oct 16, 2

Event time ↓	Event	Additional information
Oct 16, 2025 3:54:21.525 PM	svchost.exe failed to establish connection with 127.0.0.1:5985	
Oct 16, 2025 3:54:19.458 PM	svchost.exe failed to establish connection with ::1:5985	
Oct 16, 2025 3:54:19.328 PM	services.exe set registry value for key 'HKEY_LOCAL_MACHINE\SYSTEM\Contr...	
Oct 16, 2025 3:54:15.501 PM	Outbound DNS connection from 192.168.168.161:64492 to 192.168.168.2:53	T1071.004: DNS
☑ Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.161 to 192.168.168.159 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.161 to 192.168.168.159 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.161 to 192.168.168.159 matched signatu...	
Oct 16, 2025 3:54:15.497 PM	A network packet from 192.168.168.159 to 192.168.168.161 matched signatu...	

A network packet from 192.168.168.159 to 192.168.168.161 matched signature SMB_Client

Event info

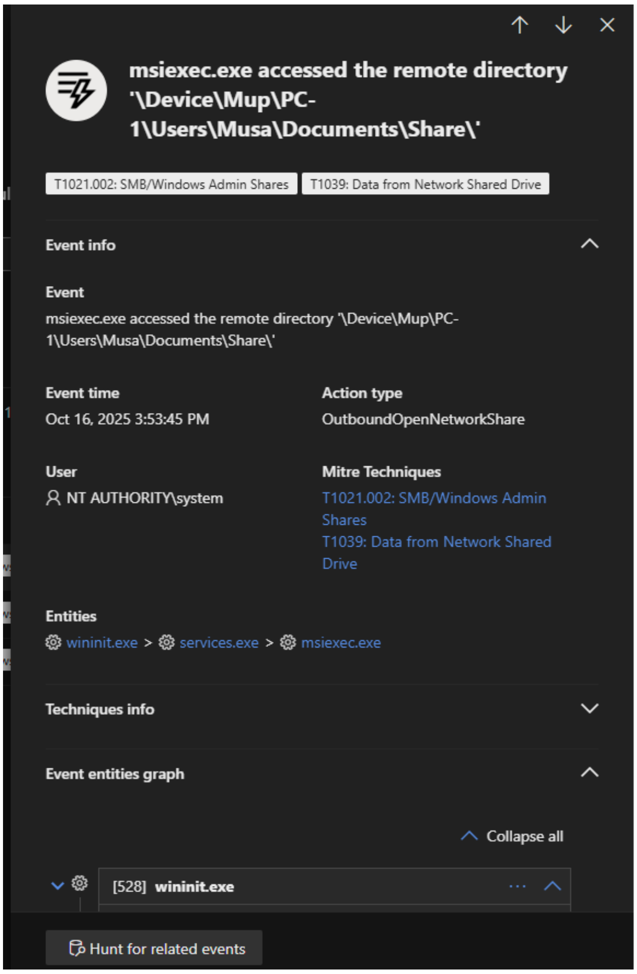
Event
A network packet from 192.168.168.159 to 192.168.168.161 matched signature SMB_Client

Event time: Oct 16, 2025 3:54:15 PM
Action type: NetworkSignatureInspected

Event details

Signature name: SMB_Client
SignatureMatchedContent: %00%00%00|þSMB
SamplePacketContent: System.Byte[]
Direction: Inbound
Intercepted network name: Network
Source ip address: 192.168.168.1...
Source port: 445
Destination ip address: 192.168.168.1...
Destination port: 49735

6. Continuing down, we saw that msiexec.exe accessed a file on another machine.



msiexec.exe accessed the remote directory '\Device\Mup\PC-1\Users\Musa\Documents\Share\'

T1021.002: SMB/Windows Admin Shares T1039: Data from Network Shared Drive

Event info

Event
msiexec.exe accessed the remote directory '\Device\Mup\PC-1\Users\Musa\Documents\Share\'

Event time: Oct 16, 2025 3:53:45 PM
Action type: OutboundOpenNetworkShare

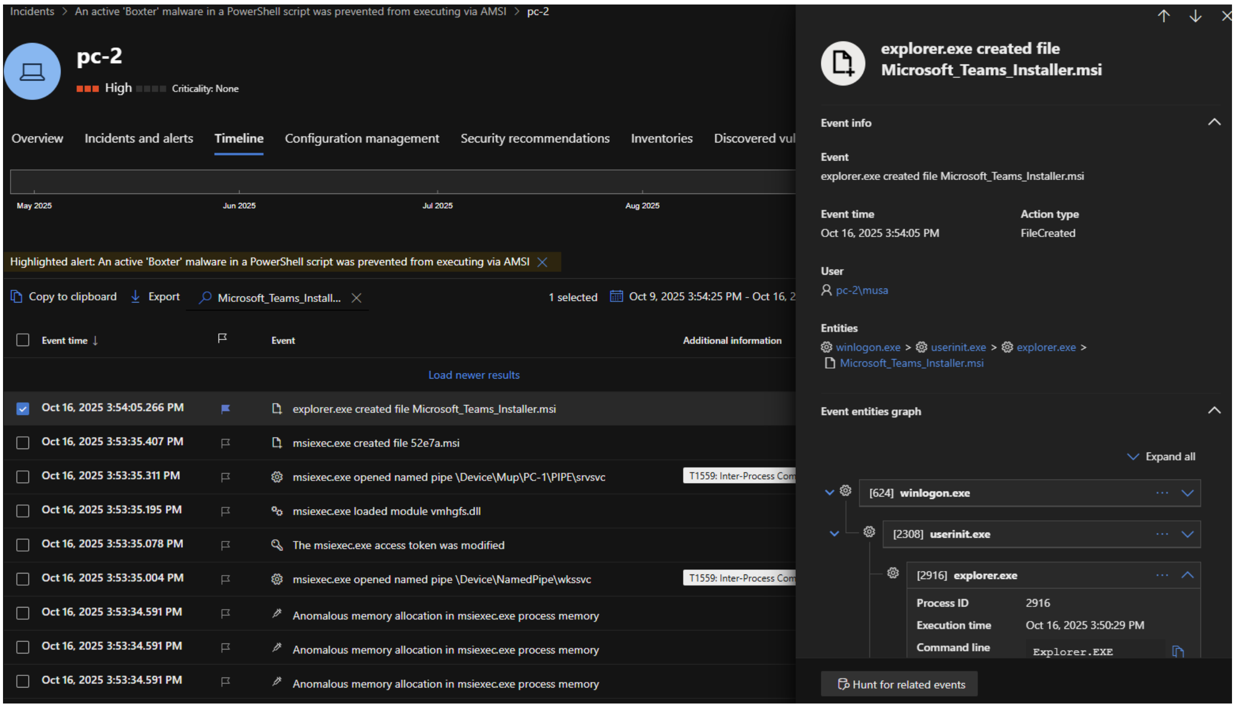
User
NT AUTHORITY\system
Mitre Techniques: T1021.002: SMB/Windows Admin Shares
T1039: Data from Network Shared Drive

Entities
wininit.exe > services.exe > msiexec.exe

[528] wininit.exe

7. We found that the MSI was executed from this path: `\\PC-1\Users\Musa\Documents\Share\Microsoft_Teams_Installer.msi`.

8. Below that we traced back to the initial creation of this MSI file.



Highlighted alert: An active 'Boxter' malware in a PowerShell script was prevented from executing via AMSI

	Event time ↓		Event	Additional information
☑	Oct 16, 2025 3:54:05.266 PM		explorer.exe created file Microsoft_Teams_Installer.msi	
□	Oct 16, 2025 3:53:35.407 PM		msiexec.exe created file 52e7a.msi	
□	Oct 16, 2025 3:53:35.311 PM		msiexec.exe opened named pipe \Device\Mup\PC-1\PIPE\srvsvc	T1559: Inter-Process Com
□	Oct 16, 2025 3:53:35.195 PM		msiexec.exe loaded module vmhgfs.dll	
□	Oct 16, 2025 3:53:35.078 PM		The msiexec.exe access token was modified	
□	Oct 16, 2025 3:53:35.004 PM		msiexec.exe opened named pipe \Device\NamedPipe\wkssvc	T1559: Inter-Process Com
□	Oct 16, 2025 3:53:34.591 PM		Anomalous memory allocation in msiexec.exe process memory	
□	Oct 16, 2025 3:53:34.591 PM		Anomalous memory allocation in msiexec.exe process memory	
□	Oct 16, 2025 3:53:34.591 PM		Anomalous memory allocation in msiexec.exe process memory	

explorer.exe created file Microsoft_Teams_Installer.msi

Event info

Event
explorer.exe created file Microsoft_Teams_Installer.msi

Event time: Oct 16, 2025 3:54:05 PM
Action type: FileCreated

User
pc-2\musa

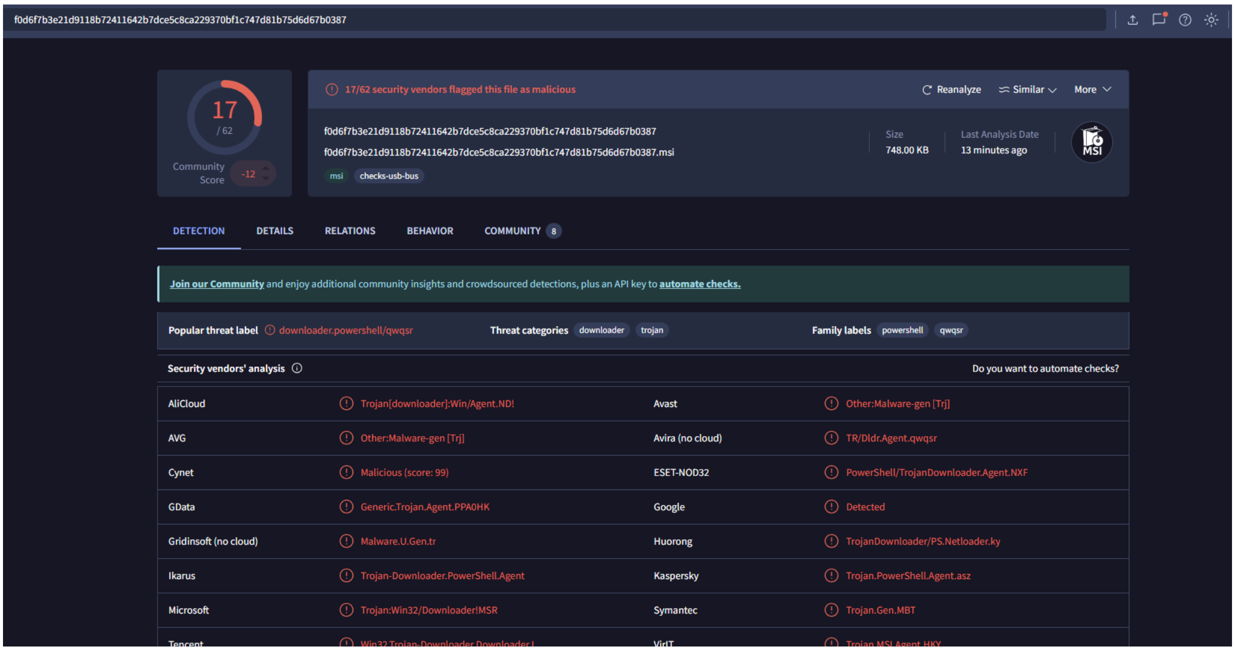
Entities
winlogon.exe > userinit.exe > explorer.exe > Microsoft_Teams_Installer.msi

Event entities graph

Expand all

[624] winlogon.exe
[2308] userinit.exe
[2916] explorer.exe
Process ID: 2916
Execution time: Oct 16, 2025 3:50:29 PM
Command line: `Explorer.EXE`

9. We also checked it on VirusTotal and confirmed it is indeed the file that triggered our alert. In the Behavior section we see the same process tree as on our host.



f0d6f7b3e21d9118b72411642b7dce5c8ca229370bf1c747d81b75d6d67b0387

17/62 security vendors flagged this file as malicious

f0d6f7b3e21d9118b72411642b7dce5c8ca229370bf1c747d81b75d6d67b0387
f0d6f7b3e21d9118b72411642b7dce5c8ca229370bf1c747d81b75d6d67b0387.msi
msi checks-usb-bus

Size: 748.00 KB
Last Analysis Date: 13 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: downloader.powershell/qwqsr
Threat categories: downloader, trojan
Family labels: powershell, qwqsr

Security vendors' analysis

Do you want to automate checks?

AliCloud	Trojan[downloader]:Win/Agent.ND!	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	Avira (no cloud)	TR/Dldr.Agent.qwqsr
Cynet	Malicious (score: 99)	ESET-NOD32	PowerShell/TrojanDownloader.Agent.NXF
GData	Generic.Trojan.Agent.PPA0HK	Google	Detected
Gridinsoft (no cloud)	Malware.U.Gen.tr	Huorong	TrojanDownloader/PS.Netloader.ky
Ikarus	Trojan-Downloader.PowerShell.Agent	Kaspersky	Trojan.PowerShell.Agent.asz
Microsoft	Trojan:Win32/Downloader!MSR	Symantec	Trojan.Gen.MBT
Tencent	Win32.Trojan-Downloader.Downloader.I	VirIT	Trojan.MSI.Agent.HKY

10. In conclusion, a file was executed from another machine. The affected machine needs to be re-imaged. We resolved the root cause on our own machine. Additionally, an extra investigation is required from the “Assets–Devices” section to determine how that file arrived on the other machine.

Decision: ✅ **True Positive**

🔧 Recommended Actions (SOC Level)

- Re-image the affected machine.
- Block or isolate the source host (\PC-1).
- Review SMB share permissions and disable unnecessary shares.
- Investigate how the MSI file was transferred to \PC-1.
- Check for similar indicators across the network.
- Update endpoint protection and run full scans.
- Document the incident and update detection rules.