Microsoft-365-Defender-Hunting-Queries/Delivery/Gootkit-malware.md at master · microsoft/Microsoft-365-Defender-Hunting-Queries

By endisphotic

Archived: 2026-04-05 21:31:16 UTC

Latest commit

Mar 1, 2021

This query was originally published on Twitter, by @MsftSecIntel.

Gootkit is malware that started life as a banking trojan, and has since extended its capabilities to allow for a variety of malicious activities.

The query helps find events related to Gootkit downloads and command-and-control behavior.

Query

```
AlertInfo | where Title =~ "Suspected delivery of Gootkit malware"
// Below section is to surface active follow-on Command and Control as a result of the above behavio
// only file create events where the malware may be present but has not yet been executed.
////
// Get alert evidence
| join AlertEvidence on $left.AlertId == $right.AlertId
// Look for C2
| join DeviceNetworkEvents  on $left.DeviceId == $right.DeviceId
| where InitiatingProcessFileName =~ "wscript.exe" and InitiatingProcessCommandLine has ".zip" and I
| summarize by RemoteUrl, RemoteIP , DeviceId, InitiatingProcessCommandLine, Timestamp,
InitiatingProcessFileName, AlertId, Title, AccountName
```

Category

This query can be used to detect the following attack techniques and tactics (see MITRE ATT&CK framework) or security configuration states.

Technique, tactic, or state	Covered? (v=yes)	Notes
Initial access		
Execution		

Technique, tactic, or state	Covered? (v=yes)	Notes
Persistence		
Privilege escalation		
Defense evasion		
Credential Access		
Discovery		
Lateral movement		
Collection		
Command and control	v	
Exfiltration		
Impact		
Vulnerability		
Exploit		
Misconfiguration		
Malware, component		
Ransomware		

Contributor info

Contributor: Microsoft 365 Defender team
