Template – Windows 10 active malware

[Link](https://endpoint.microsoft.com/#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/antivirus) to alert

**Description**

Think of Unknown/Uncommonly downloaded warnings as an early warning system for potentially undetected malware. There's generally a delay from the time new malware is released until it's identified. Not all uncommon programs are malicious, but the risk in the unknown category is much higher for the typical user.

**Classification**: Incident

**How to investigate**

[How Microsoft identifies malware and potentially unwanted applications - Windows security | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/criteria)

**Alert detail**

User:

Malware name:

Malware state:

Count:

Device:

Initial detection:

Category:

Severity:

**Remediation**

Perform a full scan of the device and remove the malware