

Disabling the Shield: AV Evasion Techniques

Incident Overview

Threat Type: Defense evasion and persistence through manipulation of endpoint protection policies and unauthorized administrative access

Time to Containment: 28 Minutes

This incident involved an attacker attempting to weaken endpoint defenses and establish administrative persistence within a cloud-hosted environment. By modifying antivirus exclusions and applying them across production Azure servers, the attacker aimed to create a blind spot in Microsoft Defender that could enable undetected malicious activity.

Before the attacker could leverage this access to deploy additional payloads or move laterally, Critical Start SOC analysts identified abnormal configuration changes and intervened.

Attack Characteristics: The attacker began by altering antivirus exclusion settings in Microsoft Defender, allowing specific file types such as .exe and wildcard file paths to bypass scanning.

These exclusions were then applied broadly across production Azure servers, effectively weakening endpoint protection controls and enabling potential malware execution without detection.

Shortly after the changes were deployed, the attacker created a new administrative account in the Defender portal, attempting to establish persistence and maintain remote control over security configurations.

This tactic is commonly used to disable or manipulate defenses prior to deploying additional malicious activity.

Alert Escalation: Suspicious Configuration Activity

Initial Vendor Severity: Configuration change alert

SOC Escalation: High priority due to policy manipulation and administrative account creation

Escalation Rationale

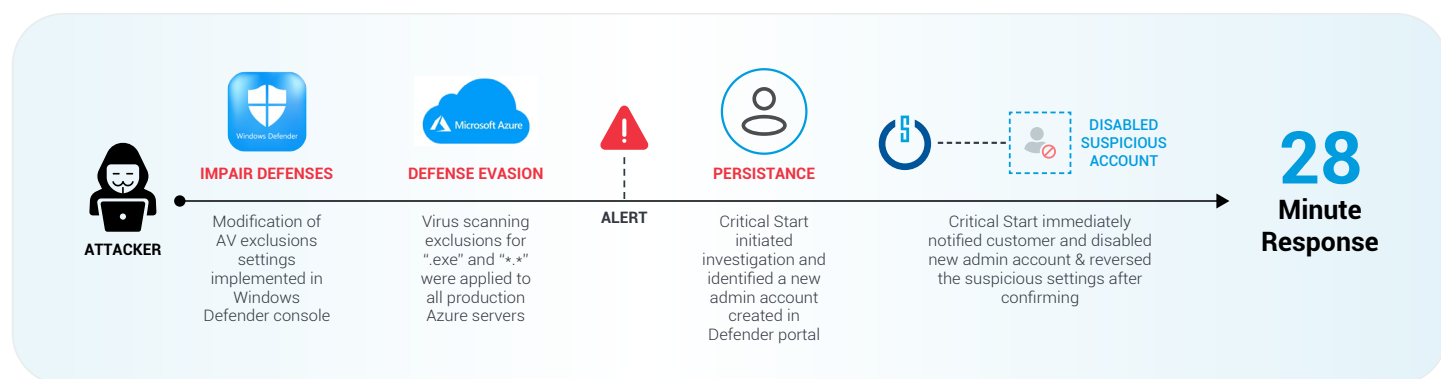
SOC analysts detected suspicious Defender configuration changes combined with the creation of a new privileged admin account. This pattern is strongly associated with defense evasion and persistence techniques, prompting immediate escalation and investigation.

Depth of Investigation

Critical Start analysts performed a multi-layer investigation that included:

- Reviewing Microsoft Defender policy modification logs
- Correlating configuration changes across Azure production servers
- Investigating newly created privileged accounts within the Defender portal
- Validating whether exclusions could allow execution of un-scanned binaries
- Confirming the attacker's ability to modify security configurations

This rapid investigation confirmed the attacker had successfully weakened defenses and created an administrative foothold.



Coordinated Cross-Platform Response

The SOC initiated an immediate response to neutralize the threat:

- Identified the unauthorized admin account created in the Defender portal
- Disabled the suspicious account and revoked administrative privileges
- Reversed malicious antivirus exclusion policies
- Restored Defender security controls across production servers
- Notified the customer and validated remediation actions in real time

This coordinated response prevented the attacker from using the weakened defenses to deploy malware or expand access.

Outcome

The attack was fully contained within 28 minutes.

By rapidly detecting abnormal configuration activity and removing the attacker's administrative access, the SOC prevented defense evasion from turning into a broader compromise.

This swift response restored security controls across the environment, eliminated the attacker's persistence mechanism, and ensured production Azure systems remained protected.