

Tailored: Windows Host Firewall Tampering

Incident Description

- This incident involves the changes of firewall settings.
- As reported by: [Event ID 2003 — Firewall Rule Processing | Microsoft Learn](#)

KQL

```
Event
| where EventLog == "Microsoft-Windows-Windows Firewall With Adv
| where EventID == 2003
```

Tactics and Techniques: Defense Evasion

- [Impair Defenses: Disable or Modify System Firewall, Sub-technique T1562.004 - Enterprise | MITRE ATT&CK®](#)

Initial Response Actions

- Verify the authenticity of the alert or report.
- Identify the altered settings.
- Determine how the settings were altered.
- Assess the potential impact of the incident.

Containment and Recovery

- Revoke access to the firewall from the affected user or application immediately if unintended, otherwise skip to the documentation phase.

- Check for any other unauthorized access to the firewall and revoke it if necessary.
- Monitor other affected systems for any suspicious activity related to the incident.
- Identify the root cause of the incident and take corrective actions to prevent similar incidents from occurring in the future.

Document Findings and Close out Incident

- Example:

Tailored: Windows Host Firewall Tampering

Incident ID 78

Refresh
 Delete incident
 Logs
 Tasks
 Activity log

High

Severity

Closed

Status

Joshua Guz...

Owner

Workspace name

law-soc

Description

--

Alert product names

- Microsoft Sentinel

Reason for closing

FalsePositive - Inaccurate data

I am closing this as a false positive because, this alert triggered due to altering the firewall settings in order to perform a vulnerability scan with Qualys to see how much information I could get with Windows Defender on versus off.

Evidence

18

Events

6

Alerts

0

Bookmarks

Last update time

2/6/2024, 2:19:01 PM

Creation time

2/2/2024, 12:33:26 PM

Entities (1)

WindowsVM

Tactics and techniques

Defense Evasion

Incident workbook

Incident Overview

Analytics rule

Tailored: Windows Host Firewall Tampering

Incident Team

-

Tags

+

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insi...

Investigate

Overview

Entities

Incident timeline

Search

Add

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Feb 2 12:26:32

Tailored: Windows Host Firewall Tampering

High | Detected by Microsoft Sentinel | Tactics:

Similar incidents

Severity	Incident ID	Title
High	77	Tailored: Windows Host Firewall Tampering
Low	76	Test Brute Force Attempt - Windows
Medium	70	Tailored: Brute Force ATTEMPT - MS SQL Server
Medium	75	Tailored: Brute Force ATTEMPT - Windows
Low	74	Test Brute Force Attempt - Windows

- Reason for closing in the example: I am closing this as a false positive because, this alert triggered due to altering the firewall settings in order to perform a vulnerability scan with Qualys to see how much information I could get with Windows Defender on versus off.