Windows Firewall Disabled via PowerShell

Identifies when the Windows Firewall is disabled using PowerShell cmdlets, which can help attackers evade network constraints, like internet and network lateral communication restrictions.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.process-*
- logs-windows.forwarded*
- logs-windows.sysmon_operational-*
- endgame-*
- logs-system.security*
- logs-m365_defender.event-*
- logs-sentinel_one_cloud_funnel.*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References:

- https://docs.microsoft.com/en-us/powershell/module/netsecurity/set-netfirewallprofile?view=windowsserver2019-ps
- https://www.tutorialspoint.com/how-to-get-windows-firewall-profile-settings-using-powershell
- http://powershellhelp.space/commands/set-netfirewallrule-psv5.php
- http://woshub.com/manage-windows-firewall-powershell/

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Defense Evasion
- Tactic: Execution
- Resources: Investigation Guide
- Data Source: Elastic Endgame
- Data Source: Elastic Defend
- Data Source: System
- Data Source: Microsoft Defender for Endpoint
- Data Source: Sysmon
- Data Source: SentinelOne

Version: 310

Rule authors:

- Austin Songer

Investigation guide

Triage and analysis

Investigating Windows Firewall Disabled via PowerShell

Windows Defender Firewall is a native component that provides host-based, two-way network traffic filtering for a device and blocks unauthorized network traffic flowing into or out of the local device.

Attackers can disable the Windows firewall or its rules to enable lateral movement and command and control activity.

This rule identifies patterns related to disabling the Windows firewall or its rules using the `Set-NetFirewallProfile` PowerShell cmdlet.

Possible investigation steps

- Investigate the process execution chain (parent process tree) for unknown processes. Examine their executable files for prevalence, whether they are located in expected locations, and if they are signed with valid digital signatures.
- Identify the user account that performed the action and whether it should perform this kind of action.
- Contact the account owner and confirm whether they are aware of this activity.
- Investigate other alerts associated with the user/host during the past 48 hours.
- Inspect the host for suspicious or abnormal behavior in the alert timeframe.

False positive analysis

- This mechanism can be used legitimately. Check whether the user is an administrator and is legitimately performing troubleshooting.
- In case of an allowed benign true positive (B-TP), assess adding rules to allow needed traffic and re-enable the firewall.

Response and remediation

- Initiate the incident response process based on the outcome of the triage.
- Isolate the involved hosts to prevent further post-compromise behavior.
- Re-enable the firewall with its desired configurations.
- Investigate credential exposure on systems compromised or used by the attacker to ensure all compromised accounts are identified. Reset passwords for these accounts and other potentially compromised credentials, such as email, business systems, and web services.
- Review the privileges assigned to the involved users to ensure that the least privilege principle is being followed.
- Determine the initial vector abused by the attacker and take action to prevent reinfection through the same vector.
- Using the incident response data, update logging and audit policies to improve the mean time to detect (MTTD) and the mean time to respond (MTTR).

Rule query

```
process where host.os.type == "windows" and event.ac
  (process.name : ("powershell.exe", "pwsh.exe", "po
   process.args : "*Set-NetFirewallProfile*" and
   process.args : "*-Enabled*" and process.args : "*
   process.args : ("*-All*", "*Public*", "*Domain*",
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Defense Evasion
  - ID: TA0005
  - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:
  - Name: Impair Defenses
  - ID: T1562
  - Reference URL: https://attack.mitre.org/techniques/T1562/
- Sub-technique:
  - Name: Disable or Modify System Firewall
  - ID: T1562.004
  - Reference URL: https://attack.mitre.org/techniques/T1562/004/
- Tactic:
  - Name: Execution
  - ID: TA0002
  - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:

    - Name: Command and Scripting Interpreter
    - ID: T1059
    - Reference URL: https://attack.mitre.org/techniques/T1059/
- Sub-technique:
    - Name: PowerShell
    - ID: T1059.001
    - Reference URL: https://attack.mitre.org/techniques/T1059/001/

« Windows Event Logs Cleared

Windows Installer with Suspicious Properties »

About us

About Elastic

Leadership

DE&I

Blog

Newsroom

Join us

Careers

Career portal

Partners

Find a partner

Partner login

Request access

Become a partner

Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events