Conhost Spawned By Suspicious Parent Process

Detects when the Console Window Host (conhost.exe) process is spawned by a suspicious parent process, which could be indicative of code injection.

Rule type: eql

Rule indices:

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

Severity: high

Risk score: 73

Runs every: 5m

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

Maximum alerts per execution: 100

References:

- https://www.fireeye.com/blog/threat-research/2017/08/monitoring-windows-console-activity-part-one.html

Tags:

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

Version: 310

Investigating Conhost Spawned By Suspicious Parent Process

The Windows Console Host, or `conhost.exe`, is both the server application for all of the Windows Console APIs as well as the classic Windows user interface for working with command-line applications.

Attackers often rely on custom shell implementations to avoid using built-in command interpreters like `cmd.exe` and `PowerShell.exe` and bypass application allowlisting and security features. Attackers commonly inject these implementations into legitimate system processes.

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.
- Investigate abnormal behaviors observed by the subject process, such as network connections, registry or file modifications, and any spawned child processes.
- 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.
- Retrieve the parent process executable and determine if it is malicious:
- Use a private sandboxed malware analysis system to perform analysis.
- Observe and collect information about the following activities:
- Attempts to contact external domains and addresses.
- File and registry access, modification, and creation activities.
- Service creation and launch activities.
- Scheduled task creation.
- Use the PowerShell `Get-FileHash` cmdlet to get the files' SHA-256 hash values.
- Search for the existence and reputation of the hashes in resources like VirusTotal, Hybrid-Analysis, CISCO Talos, Any.run, etc.

False positive analysis

- This activity is unlikely to happen legitimately. Benign true positives (B-TPs) can be added as exceptions if necessary.

Related rules

- Suspicious Process from Conhost - 28896382-7d4f-4d50-9b72-67091901fd26
- Suspicious PowerShell Engine ImageLoad - 852c1f19-68e8-43a6-9dce-340771fe1be3

Response and remediation

- Immediately block the identified indicators of compromise (IoCs).
- Inspect the affected systems for additional malware backdoors like reverse shells, reverse proxies, or droppers that attackers could use to reinfect the system.
- Remove and block malicious artifacts identified during triage.
- 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.
- Run a full antimalware scan. This may reveal additional artifacts left in the system, persistence mechanisms, and malware components.
- 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

edit

```
process where host.os.type == "windows" and event.type == "start
  process.name : "conhost.exe" and
  process.parent.name : ("lsass.exe", "services.exe", "smss.exe
                         "regsvr32.exe", "userinit.exe", "winin
  not (process.parent.name : "rundll32.exe" and
       process.parent.args : ("?:\\Windows\\Installer\\MSI*.tmp
                              "?:\\WINDOWS\\system32\\PcaSvc.dl
                              "?:\\WINDOWS\\system32\\davclnt.d
```

Framework: MITRE ATT&CK™

- 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/
- Tactic:
  - Name: Defense Evasion
  - ID: TA0005
  - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:

- Technique:
  - Name: Process Injection
  - ID: T1055
  - Reference URL: https://attack.mitre.org/techniques/T1055/

« Compression DLL Loaded by Unusual Process

Connection to Commonly Abused Free SSL Certificate Providers »