Elastic Docs › Elastic Security Solution [8.15] › Detections and alerts › Prebuilt rule reference

Windows Service Installed via an Unusual Client

edit

Identifies the creation of a Windows service by an unusual client process. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-system.*
- logs-windows.*

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.x86matthew.com/view_post?id=create_svc_rpc
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4697
- https://github.com/atc-project/atomic-threat-coverage/blob/master/Atomic_Threat_Coverage/Logging_Policies/LP_0100_windows_audit_security_sys
- https://www.elastic.co/security-labs/siestagraph-new-implant-uncovered-in-asean-member-foreign-ministry

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Privilege Escalation
- Data Source: System

Version: 211

Rule authors:

- Elastic

Rule license: Elastic License v2

Setup

edit

Setup

The *Audit Security System Extension* logging policy must be configured for (Success) Steps to implement the logging policy with Advanced Audit Configuration:

```
Computer Configuration >
Policies >
Windows Settings >
Security Settings >
Advanced Audit Policies Configuration >
Audit Policies >
System >
Audit Security System Extension (Success)
```

Rule query

edit

```
configuration where host.os.type == "windows" and
  event.action == "service-installed" and
  (winlog.event_data.ClientProcessId == "0" or winlog.event_data.ParentProcessId ==
  not winlog.event_data.ServiceFileName : (
    "?:\\Windows\\VeeamVssSupport\\VeeamGuestHelper.exe",
    "?:\\Windows\\VeeamLogShipper\\VeeamLogShipper.exe",
    "%SystemRoot%\\system32\\Drivers\\Crowdstrike\\*-CsInstallerService.exe",
    "\"%windir%\\AdminArsenal\\PDQInventory-Scanner\\service-1\\PDQInventory-Scanne
  )
```

Framework: MITRE ATT&CK^{TM}

- Tactic:
  - Name: Privilege Escalation
  - ID: TA0004
  - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
  - Name: Create or Modify System Process
  - ID: T1543
  - Reference URL: https://attack.mitre.org/techniques/T1543/
- Sub-technique:
  - Name: Windows Service
  - ID: T1543.003
  - Reference URL: https://attack.mitre.org/techniques/T1543/003/

« Windows Script Interpreter Executing Process via WMI   Windows Subsystem for Linux Distribution Installed »

Learn more

Was this helpful?