

Violations by a Single User Over a Session

Windows Service Installed via an Unusual Client

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

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

Pricing

Docs

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_sy

 https://www.elastic.co/security-labs/siestagraph-new-implant-uncovered-in-asean-memberforeign-ministry

Tags:

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

Version: 211

Rule authors:

Elastic

https://www.elastic.co/guide/en/security/current/windows-service-installed-via-an-unusual-client.html

AWS CLI Command with Custom Endpoint URL

AWS CloudTrail Log Created

Rule license: Elastic License v2

Setup

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



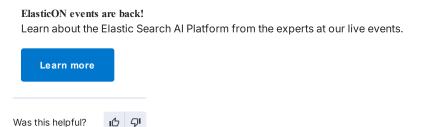
```
configuration where host.os.type == "windows" and
  event.action == "service-installed" and
  (winlog.event_data.ClientProcessId == "0" or winlog.event_data.ParentProcessId ==
  not winlog.event_data.ServiceFileName : (
    "?:\\Windows\\VeeamVssSupport\\VeeamGuestHelper.exe",
    "?:\\Windows\\VeeamLogShipper\\VeeamLogShipper.exe",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

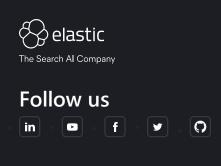
Framework: MITRE ATT&CKTM

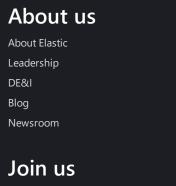
- Tactic:
 - · Name: Privilege Escalation
 - ID: TA0004
 - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
 - Name: Create or Modify System Process
 - ID: T1543
 - Reference URL: https://attack.mitre.org/techniques/T1543/
- · Sub-technique:
 - Name: Windows Service
 - ID: T1543.003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

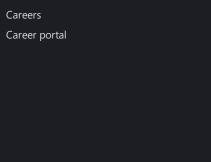
Windows Subsystem for Linux Distribution Installed »

[«] Windows Script Interpreter Executing Process via WMI









Find a partner Partner login Request access Become a partner Trust & Security Trust center EthicsPoint portal

Partners

Trust & Security Trust center EthicsPoint portal ECCN report Ethics email All ex

EXCELLENCE AWARDS

Investor relations

Previous winners
ElasticON Tour
Become a sponsor
All events

Investor resources

Governance

Financials

<u>Trademarks</u> <u>Terms of Use</u> <u>Privacy</u> <u>Sitemap</u> © 2024. Elasticsearch B.V. All Rights Reserved

Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.