elastic

Start free trial

Contact Sales

Platform Solutions Customers Resources Pricing Docs

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

Execution of COM object via Xwizard

edit

Windows Component Object Model (COM) is an inter-process communication (IPC) component of the native Windows application programming interface (API) that enables interaction between software objects or executable code. Xwizard can be used to run a COM object created in registry to evade defensive counter measures.

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://lolbas-project.github.io/lolbas/Binaries/Xwizard/
- http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/

Tags:

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

Version: 311

Rule authors:

- Elastic

Rule license: Elastic License v2

Rule query

edit

```
process where host.os.type == "windows" and event.ty
 (process.name : "xwizard.exe" or ?process.pe.origin
 (
   (process.args : "RunWizard" and process.args : "{
   (process.executable != null and
     not process.executable : ("C:\\Windows\\SysWOW6
   )
 )
```

Framework: MITRE ATT&CK^{TM}

- Tactic:
    - Name: Execution
    - ID: TA0002
    - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:
    - Name: Inter-Process Communication
    - ID: T1559
    - Reference URL: https://attack.mitre.org/techniques/T1559/
- Sub-technique:
    - Name: Component Object Model
    - ID: T1559.001
    - Reference URL: https://attack.mitre.org/techniques/T1559/001/

« Execution from a Removable Media with Network Connection

Execution of File Written or Modified by Microsoft Office »

Was this helpful? 👍 👎

About us

About Elastic

Leadership

DE&I

Blog

Newsroom

Join us

Careers

Career portal

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

Partners

Find a partner

Partner login

Request access

Become a partner

Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

Trademarks Terms of Use Privacy Sitemap