

Q

8

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



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



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

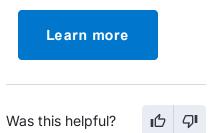
Framework: MITRE ATT&CKTM

- 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 Execution of File Written or Modified with Network Connection by Microsoft Office »

ElasticON events are back!

Learn about the Elastic Search Al Platform from the experts at our live events.





The Search Al Company

Follow us











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

Execution of COM object via Xwizard | Elastic Security Solution [8.15] | Elastic - 31/10/2024 19:53

https://www.elastic.co/guide/en/security/current/execution-of-com-object-via-xwizard.html

<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.