

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Learn more and customize

Reject

Accept

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-opa-plugin-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

ElasticON events are back!
Learn about the Elastic Search AI Platform from the experts at our live events.

Learn more

Was this helpful?



Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Rule query



```
process where host.os.type == "windows" and event.type == "start"
  (process.name : "xwizard.exe" or ?process.pe.original_file_name
  (
    (process.args : "RunWizard" and process.args : "{*}") or
    (process.executable != null and
      not process.executable : ("C:\\Windows\\SysWOW64\\xwizard.exe"
    )
  )
)
```

Framework: MITRE ATT&CK™

- 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 »



The Search AI Company

Follow us



About us

- About Elastic
- Leadership
- DE&I
- Blog
- Newsroom

Partners

- Find a partner
- Partner login
- Request access
- Become a partner

Trust & Security

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Investor relations

- Investor resources
- Governance
- Financials
- Stock

EXCELLENCE AWARDS

- Previous winners
- ElasticON Tour
- Become a sponsor
- All events

[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 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.