





Sign in

 elastic / detection-rules


Public


 Notifications


 Fork 498


 Star 2k


<> Code

 Issues 145

 Pull requests 22

 Actions

 Security



 Insights

[New Rule] DNS-over-HTTPS Enabled by Registry #1371

New issue

 Closed

 #1379

 austinsonger opened on Jul 20, 2021

Description

Identifies when a user enables DNS-over-HTTPS. This can be used to hide internet activity or be used to hide the process of exfiltrating data. With this enabled organization will lose visibility into data such as query type, response and originating IP that are used to determine bad actors.

Required Info

Target indexes

winlogbeat-*, "logs-endpoint.events.*", "logs-windows.*"

Platforms

Windows

Optional Info

Query

Assignees

No one assigned

Labels

Rule: New

community

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

```
registry where event.type in ("creation", "change") and
  (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
registry.data.strings: "1") or
  (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\DnsO
registry.data.strings: "secure")
```

NOTE: Going to expand this query for the other browsers

New fields required in ECS/data sources for this rule?

Related issues or PRs

False Positives

-
-

MITRE

Tactic	Technique ID	Technique Name	Sub-Technique Name

References

- <https://www.tenforums.com/tutorials/151318-how-enable-disable-dns-over-https-doh-microsoft-edge.html>
- <https://chromeenterprise.google/policies/?policy=DnsOverHttpsMode>

  austinsonger added **Rule: New** on Jul 20, 2021

  austinsonger mentioned this on Jul 23, 2021

 [\[New Rule\] DNS-over-HTTPS Enabled by Registry #1379](#)

 botelastic on Sep 19, 2021

This issue has been automatically marked as stale because it has not had recent activity. It will be closed if no further activity occurs. Thank you for

your contributions.


 **botelastic** added **stale** on Sep 19, 2021

 **austinsonger** on Sep 19, 2021 Contributor Author ...

Just keeping this active.

 **botelastic** removed **stale** on Sep 19, 2021

 **brokensound77** added **community** on Sep 30, 2021

 **w0rk3r** closed this as completed in [#1379](#) on Oct 16, 2021

[Redacted content]

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)