Suricata - Feature #4649

Autonomous System Number (ASN) support similar to GeoIP

08/26/2021 02:55 PM - Brandon Murphy

Status: New
Priority: Normal
Assignee:
Category:
Target version:
Effort:
Difficulty:
Label:

Description
Request is to introduce a new keyword which leverages the MaxMind GeoIP ASN database similar to that of the current "geoip" keyword.

The keyword should also allow for negations.

This keyword is useful for detecting host name impersonation such as the following:

http.host; content: ".azure.com"; endswith; asn:!dst,398656,398575;

The optional "org" argument could allow the AS Organization to be inspected instead of the AS number itself, useful with an org has many different ASNs

http.host; content: ".azure.com"; endswith; asn:!dst,org Microsoft Corporation;

I provide the above only as examples, I'm not too concerned about the specific keyword format.

Documentation on the GeoIP ASN Database can be found here - https://dev.maxmind.com/geoip/docs/databases/asn?lang=en

History

#1 - 09/07/2021 04:13 PM - Michael Tremer
Hello Brandon,

Victor made me aware of this ticket when we were discussing integrating the IPFire Location database into suricata (https://location.ipfire.org).

We have this data available in the database and querying is fast so that we could easily implement this.

Matching the ASN is absolutely no problem.

The organization is probably not so easy, because we cannot always rely on the string. They change often and use different abbreviations ("Inc.", or "Ltd." vs "Limited"). Making this work reliably is probably going to be difficult.

#2 - 09/09/2021 01:34 PM - Brandon Murphy

They change often and use different abbreviations ("Inc.", or "Ltd." vs "Limited"). Making this work reliably is probably going to be difficult.

I would imagine these are localized to specific organizations though. While Github might always use "Github Inc." I would be surprised if they vary from that. Additionally, much like the GeoIP feature supports multiple countries treated as a logical OR, perhaps we can do the same here and allow the signature writer to cover those variants?

#3 - 09/21/2021 05:44 PM - Michael Tremer
I have submitted a draft pull request for the geoip implementation. If that receives good feedback and is being merged I would be happy to consider adding ASN support into the module:

https://github.com/OISF/suricata/pull/6398

#4 - 10/04/2021 09:50 AM - Michael Tremer
I had a look at what data we have in our database. For "GitHub Inc." it looks like this:

```
root@michael:/build/location-database# git grep -i github
database.txt:name: GITHUB
```

Workable I would say. However Google looks like this:

```
root@michael:/build/location-database# git grep -i google
database.txt:name: GOOGLE-FIBER
database.txt:name: GOOGLE
database.txt:name: GOOGLE-PRIVATE-CLOUD
database.txt:name: GOOGLE-FIBER
database.txt:name: GOOGLE-PRIVATE-CLOUD
database.txt:name: GOOGLE-PRIVATE-CLOUD
database.txt:name: GOOGLE-PRIVATE-CLOUD
database.txt:name: GOOGLE-PRIVATE-CLOUD
database.txt:name: GOOGLE-PRIVATE-CLOUD
```

These are taken from the text dump of the IPFire Location database.

Maybe Google is a bad example since it is such a large organisation which has grown through acquisitions and had to merge it all together in one way or another.

Here are some more:

```
root@michael:/build/location-database# git grep -i facebook
database.txt:name: FACEBOOK
database.txt:name: FACEBOOK-CORP
database.txt:name: FACEBOOK-OFFNET
```

```
root@michael:/build/location-database# git grep -i linkedin
database.txt:name: LINKEDIN
database.txt:name: LINKEDIN
database.txt:name: LINKEDIN
database.txt:name: LINKEDIN
database.txt:name: LINKEDIN
database.txt:name: LINKEDIN
database.txt:name: Linkedin Singapore Pte. Ltd
```

```
root@michael:/build/location-database# git grep -i netflix
database.txt:name: NETFLIX-ASN
```

```
root@michael:/build/location-database# git grep -i akamai
database.txt:name: AKAMAI
```
I would not consider it practical to match regular expressions to have the option for "OR" or a lot of flexibility in general. Matching ASNs only would be a deterministic way that is performing well with loads of traffic.

Would you be able to sponsor this feature?

#5 - 02/14/2022 03:46 PM - Brandon Murphy
- Tracker changed from Bug to Feature