Suricata - Feature #3192
POC advice for adding support for
09/24/2019 12:58 PM - Brian Jones

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>Support</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
https://www.joesandbox.com/analysis/177027/0/html
Connects to IPs without corresponding DNS lookups

History

#1 - 09/24/2019 01:02 PM - Brian Jones
Sorry, premature click of the enter key. Don't see a way to delete this. Please send help.

#2 - 09/24/2019 02:08 PM - Brian Jones
Posting anyway..
The pi-hole project has a cool new feature coming that will support whitelisting 100+ million domains.

https://github.com/pi-hole/FTL/pull/600
https://github.com/pi-hole/FTL/commit/822fb88d28a1ee1b582237b4b88ef82cc34bc089

On a small or medium size network, for example a call center, the admin may want to restrict the ability to "Connects to IPs without corresponding DNS lookups". An indicator that based on my google searches is only found on joesandbox reports (https://www.joesandbox.com/analysis/177027/0/html).

I know suricata has a great IP reputation feature, but I am looking for advice to create a proof of concept that more tightly couples these 3 things.
- DNS answers
- Reputation cache that can be inserted into from DNS answers and read from without having to reload rules.
- TCP flow or SYN tracking.

I should also mention that I am VERY aware of the false positives / false blocks that will occur by adding support for "Connects to IPs without corresponding DNS lookups". One idea to mitigate this is to consider the ASN number the ip address belongs to. If the ASN block is whitelisted, it will not be blocked.

The pi-hole project uses a sqlite database, but adds the whitelisted record into a cache. The advantage to this means that future DNS requests for a domain won't require making a SQL query because the domain is now in the cache. I don't think suricata currently supports anything like a real time IP reputation cache. That is my mine focus. Once I figure out that piece then I will worry about how to add DNS answers to it.

Additional relevant links
https://feodotracker.abuse.ch/mitigate/
https://github.com/pi-hole/FTL/issues/596

#3 - 09/24/2019 02:10 PM - Brian Jones
Brian Jones wrote:

Posting anyway..
The pi-hole project has a cool new feature coming that will support whitelisting 100+ million domains.

https://github.com/pi-hole/FTL/pull/600
https://github.com/pi-hole/FTL/commit/822fb88d28a1ee1b582237b4b88ef82cc34bc089

On a small or medium size network, for example a call center, the admin may want to restrict the ability to "Connects to IPs without corresponding DNS lookups". An indicator that based on my google searches is only found on joesandbox reports (https://www.joesandbox.com/analysis/177027/0/html).

I know suricata has a great IP reputation feature, but I am looking for advice to create a proof of concept that more tightly couples these 3 things.
- DNS answers
- Reputation cache that can be inserted into from DNS answers and read from without having to reload rules.
- TCP flow or SYN tracking.

I should also mention that I am VERY aware of the false positives / false blocks that will occur by adding support for "Connects to IPs without corresponding DNS lookups". One idea to mitigate this is to consider the ASN number the ip address belongs to. If the ASN block is whitelisted, it will not be blocked.

The pi-hole project uses a sqlite database, but adds the whitelisted record into a cache. The advantage to this means that future DNS requests for a domain won't require making a SQL query because the domain is now in the cache. I don't think suricata currently supports anything like a real time IP reputation cache. That is my mine focus. Once I figure out that piece then I will worry about how to add DNS answers to it.

Additional relevant links
https://feodotracker.abuse.ch/mitigate/
https://github.com/pi-hole/FTL/issues/596

#4 - 09/24/2019 08:24 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to Support

So you want to extend suricata to support that use case or do you want to use suricata in combination with other tools to achieve it?

#5 - 09/25/2019 01:58 PM - Brian Jones

Andreas Herz wrote:

So you want to extend suricata to support that use case or do you want to use suricata in combination with other tools to achieve it?

Most likely extend suricata to support the use case unless there is an affordable tool that I am not aware of.

First some quick background to help with context. If you read almost any malware report that depends on DNS, the malware is either using a known shady domain or using a domain that is not found in the top 10 or 100 million (https://www.domcop.com/top-10-million-domains). This means if my DNS system is on point, most DNS dependent malware will fail.

The problem now becomes how to stop previously unknown malware (no signatures) that don't need to do a domain lookup? --> "Connects to IPs without corresponding DNS lookup". User awareness training may be the best "solution" today, and of course the best protection against ransomware is to have good backups. But what if I don't want to spend every weekend restoring systems from tape backup? That means I need to figure out a way to alert or Hopefully, block malicious network traffic that is connecting directly via IP address.

I believe the file that would need to be modified is stream-tcp.c
https://github.com/OISF/suricata/blob/35bc73e4e2cb4865c06e0da7a05ea60f2966ee08/src/stream-tcp.c

It doesn't seem like the IP reputation known-good.list feature will work for this use case because adding new IP addresses to it quickly and hoping the rule-reload will be near real time is probably not likely.

For example. If a host on my network wants to connect to an IP that belongs to an ASN that is blocked (see https://feodotracker.abuse.ch/statistics/) but the domain is allowed by the DNS server, this connection should be allowed. In order to allow it, I need something like a sqlite + cache so that the local DNS server can notify stream-tcp.c that the IP address is good. This means the local DNS server determined the domain has a pagerank that is high and the domain is not on any of it's block lists.

If I am on the right track, my first priority is to figure out a way for stream-tcp.c to quickly do a cache lookup and then a sqlite lookup if the ip address is not in the cache. As I think about it, it would make sense to have a known-good and a know-bad cache so that future lookups for both good (DNS approved) and bad (no DNS history) will be fast. Any insight any of you can provide will be most appreciated.

#6 - 10/03/2019 07:23 PM - Brian Jones

After a lot of reading, bpf_map_lookup_elem looks really useful. Naive question.. On a POC IPS system with one rule, what are the pros and cons of attempting to store my rule in a bpf map? For my use case, bpf maps seem like a good way to allow external processes, such as a custom DNS code, to add records to the bpf map and provide a real time data store that suricata could read from to identify "Connects to IPs without corresponding DNS lookups" events. If you are familiar with the suricata code base, feel free to be blunt. I don't want to try to code something that would be painfully slow for reasons I am overlooking.

#7 - 09/05/2020 09:29 PM - Andreas Herz
- Tracker changed from Support to Feature
- Target version set to Support