Suricata - Feature #121
Alert on domain name look up, capture traffic for corresponding IP
03/12/2010 07:25 PM - Dave Smith

| Status:   | New                  |
| Priority: | Low                  |
| Assignee: | Community Ticket     |
| Category: |                      |
| Target version: | TBD                |
| Effort:   | medium               |
| Difficulty: | medium           |

Description
It'd be handy to have the ability to capture traffic involving an IP address found in DNS responses for a known bad domain. As far as I know, no other IDS product does this.

As an example, say I have an IDS sensor at my border router. A workstation on my network looks up badguy.com, and receives a DNS response for address 4.5.6.7.

As I know badguy.com is a botnet command and control host, and that any communication with 4.5.6.7 will therefore be of security interest, I want to have all traffic involving that IP address recorded (possibly for x minutes after the DNS request or until the IP in the DNS response changes) to see what data has gone out to that command and control host, especially if it contains data that will help me quickly identify the infected workstation, that I can use to find the infected box and clean it up.

History

#1 - 04/06/2011 07:38 AM - Victor Julien
- Assignee set to Anonymous

#2 - 07/04/2012 03:41 AM - Victor Julien
- Target version set to TBD

I guess such a thing would start with a DNS protocol decoder.

#3 - 04/29/2015 04:01 AM - Andreas Moe
Dont we do DNS protocol decoding? seeing that we can log DNS activity? Or is this more of a scenario where we could write "alert dns..."

#4 - 07/17/2018 08:15 AM - Victor Julien
- Effort set to medium
- Difficulty set to medium

#5 - 02/23/2019 10:07 PM - Andreas Herz
- Assignee set to Community Ticket