Matching a long list of tls.fingerprint fields is extremely CPU intensive

The suricata-update script comes with some useful rule sources, like the sslbl.abuse.ch. It is basically around 3000 rules with malicious certificate's fingerprints.

This list alone, when combined with the ET Pro ruleset makes the CPU usage on my sensor go from 6% to 60% and even 100% on as little as 400Mbit/sec of traffic.

This sensor is way oversized - Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz x 2 so 24 cores tuned to perfection. Removing just those 3000 rules dropped the CPU usage to as little as 6%. I repeated the test thrice (just so I could say thrice, because I never get to say thrice).

Feel free to tell me the engine works like designed and it's just abused here, and the intelligence framework / datasets should be used instead. In this case let's move it to suricata-update so people don't experience problems by default.

This is Suricata version 4.1.5 RELEASE

38d55ce9367216ce4c8347559bc3b153faafae5/; sid:920200862; rev:1;
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (ZeuS C&C)"; tls.fingerprint:"7c:fd:2c:56:08:47:7d:34:c2:a3:9e:0a:74:3a:20:52:dc:de:94:d1"; reference:url, sslbl.abuse.ch/ssl-certificates/sha1/7cfd2c5608477d34c2a39e0a743a2052dced94d1/; sid:920201260; rev:1);
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (ZeuS C&C)");
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (ZeuS C&C)");
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (ZeuS C&C)");
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (ZeuS MITM)");
+alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL certificate detected (Zloader C&C)");

History

#1 - 10/20/2019 08:50 PM - Andreas Herz
- Tracker changed from Bug to Support
- Assignee set to Community Ticket
- Target version set to Soon