Status Report #2

Chaitanya Achan, Philip Lundrigan, and Christian Schreiner

November 26, 2014

Infrastructure Setup *(Christian)*

- Progress: Christian integrated all of the pieces worked on so far onto the "production" server so we can start collecting a list of websites visited by the childrens' computers. Christian has set up remote access on this computer so other members of the group can work on this server without physically being at Christian's apartment. He has also been investigating automatic tools for mapping domain names (e.g. from the whitelist) to address ranges (usable by snort).
- Meeting expected goals/obstacles: We may run into difficulties with domain names not mapping 1-1 to internet addresses. For example, www.sears.com is a CNAME that eventually maps to e2272.b.akamaiedge.net. Akamai (and akamaiedge) is a web hosting operation that serves hundreds (or thousands) of websites. Loading webpages from *.sears.com requires loading many graphics and pagelets from other akamai servers, which are named in the akamai.com and akamaiedge.net domains. Thus, if the whitelist needs to contain www.sears.com, one must either allow ALL of Akamai's block of IP addresses, or lose a lot of webpage content from sears.com. If one allows all addresses in the block, one also allows webpages from all of the other sites that Akamai hosts, and at least some of them probably shouldn't be on the whitelist. Christian is investigating workarounds and mitigation strategies.
- Next steps: Next steps are to get BASE authentication working consistently and start generating web access logs that can become the starting point for the whitelist.

IDS setup and evaluation *(Phil)*

- Progress: I have finished writing a script that detects HTTP GET requests and sends TCP RST packets to stop the connection. His script ran into the same problems that Snort did – it was not fast enough to send the TCP

RST packet before the TCP response came. He has started debugging whether it is a problem with his system. One potential problem is that every test that has been done has been on the same computer. Maybe decoupling the Snort server and the computer that is getting blocked might help solve this problem.

- Meeting expected goals/obstacles: I reached my goal of creating a script that sent TCP reset packets to stop a TCP connection. However, since it doesn't work as well as we had hoped, we will have to figure out something else.
- Next steps: This coming week, I plan on testing Snort on the "production" server that Christian has set up.

Reporting setup and evaluation *(Chaitu)*

- Progress: I looked at the functionality BASE provides with the intent of getting domain names instead of IP addresses. It was determined that BASE does not inherently list domain names. One option we considered was to modify BASE to do a reverse DNS lookup. This was not the top choice as this also creates a small risk that we inadvertently introduce a bug in BASE.
- Meeting expected goals/obstacles: I would say we met the goal of determining what BASE provides, but we also found out that it does not provide all the information we would like to have. The option we are considering now is to use the list of IP addresses stored in the MySQL DB used by SNORT and BASE, as the input to a script that would do the reverse DNS lookup.
- Next steps: In the coming days, I am trying to refine the alerts generated by SNORT for just HTTP GET requests instead of for all TCP traffic. This would reduce the number of entries in the whitelist. I am also looking at developing the script for the reverse DNS lookup.