AKAMAI THREAT ADVISORY

Satori Mirai Variant Alert

Version: V002

Date: December 6, 2017

Akamai

1.0 / Summary / Akamai, along with industry peers, has identified an updated variant of Mirai (Satori) that has activated within the past 24 hours and is rapidly growing. In the past 24 hours, Akamai has observed more than 650,000 unique IP addresses, confirming with peers in the industry seeing comparable numbers. This activity expands beyond the brute-force type of attack seen with Mirai exploit activity previously, adding exploits that target multiple vulnerabilities:

1. One new undisclosed vulnerability in Huawei Home Gateway and CPE devices
2. Existing CVE-2014-8361
3. Previous list of vulnerabilities on IoT and CPE devices

Much of the scanning activity is sourced from Mirai nodes, in the most recent Wproot/Mroot and login variant, from the end of November. The admin/CentryL1nk login variant seems to be concentrated in devices located in Egypt, Ecuador, Tunisia, Argentina, and Colombia.

Akamai is working with industry peers to investigate, mitigate, and remediate the activities around this malware system. When appropriate, Akamai will add new rules to our security solutions.

Akamai recommends that our customers take the actions described in the Recommendations section as soon as possible, to mitigate risk of a DDoS attack from this botnet. Consultations with Akamai SEs and NAMs would help determine if Akamai's solutions and tools would be able to assist.

2.0 / Recommendations / The main threat vectors for Satori are the infections of devices inside networks and then the use of the infected devices for malicious activities.

- Efforts to track down infected devices, mitigating their impact, and then remediation are prudent for all networks to explore.
- Review of the security tools deployed to protect services from attacks launched by Satori is recommended. DoS attacks would be one of the expected uses, but not the only use.

Kona Customers. Akamai recommends customers verify that their Kona WAF rules are set to deny and the following provisions are in place:

- Place the origin behind Site Shield to block direct-to-origin attacks.
- Implement rate controls sitewide. Akamai recommends settings of 40 requests/second for bursting and 20 requests/second for average to mitigate http floods.

3.0 / Findings Summary / On December 5, 2017, 0200Z, Akamai's infrastructure logged a dramatic increase in scanning activity destined for ports TCP 37215 and TCP 52869 (visualization included below).

Prior to this time, scanning activity to those ports was minimal with a large increase in scanning observations after 0200Z (Figures 1, 2).

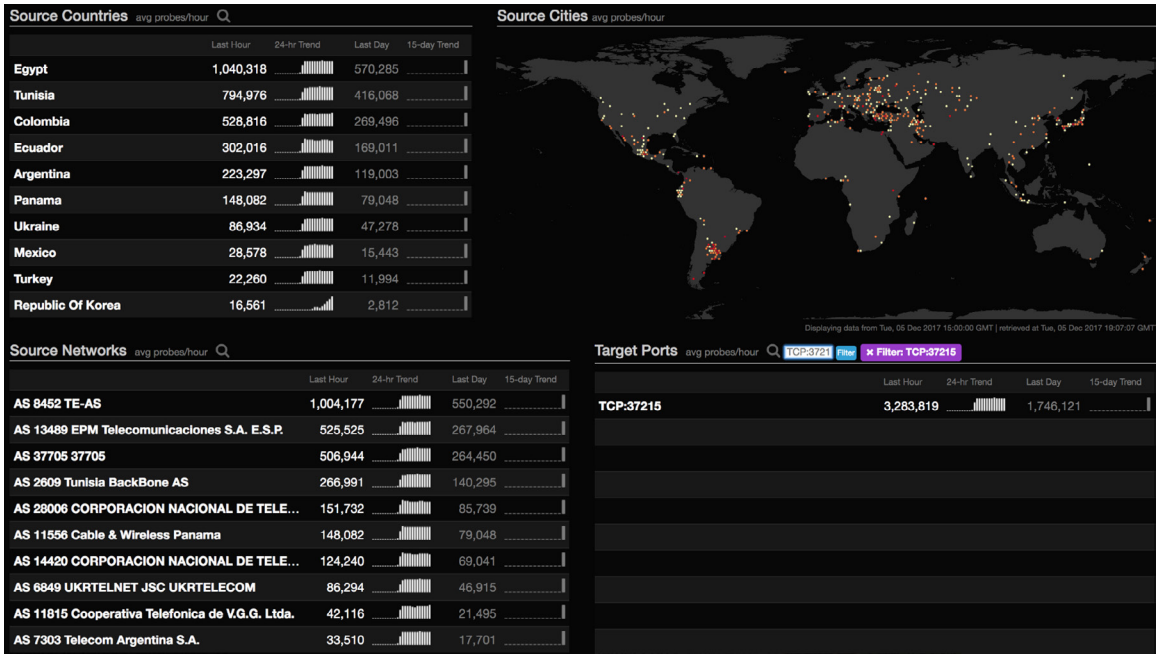

Figure 1: Scanning Activity (packets), TCP 37215

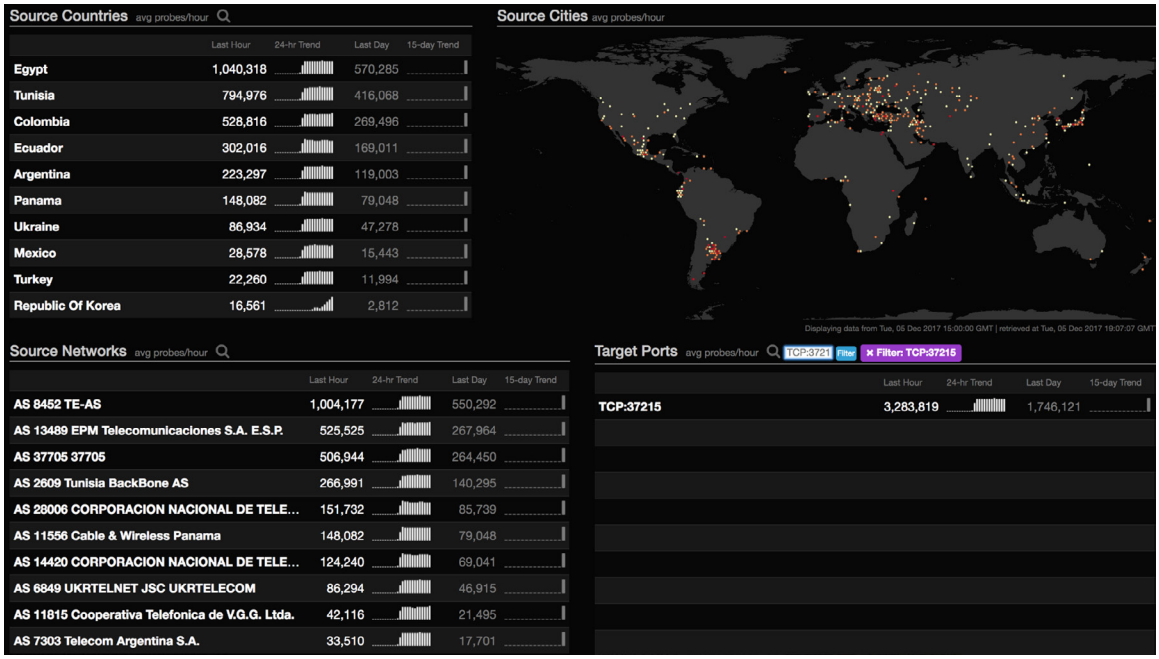

Figure 2: Scanning Activity (packets), TCP 52869

Akamai has corroborated these observations with industry peers working together to investigate this surge of activity. A TLP:WHITE example was issued by 360 Netlab (Ref: http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/):

> **About 12 hours ago** (2017-12-05 11:57 AM GMT+8), we noticed a new version of Satori (a mirai variant which we named Satori), starting to propagate very quickly on port 37215 and 52869. This new variant has two significant differences from known mirai variants:
>
> - The bot itself now does NOT rely on loader|scanner mechanism to perform remote planting, instead, bot itself performs the scan activity. This worm like behavior is quite significant.
>
> - Two new exploits, which work on port 37215 and 52869 have been added, see below for more details. Due to the worm like behavior, we all should be on the lookout for the port 37215 and 52869 scan traffic. (For those who don't have the visibility, feel free to check out our free Scanmon system for port 37215 and 52869, or ISC port pages for 37215 and 52869.

To highlight the above statement, Satori is based on Mirai, but does not rely on brute-forcing login combinations in order to infect its targets. Satori utilizes an unpublished exploit to target specific devices similar to the Reaper botnet.

Associated Binaries

```
df9c48e8bc7e7371b4744a2ef8b83ddf   b
a7922bce9bb0cf58f305d17ccbc78d98   okiru.mipsel
37b7c9831334de97c762dff7a1ba7b3f   okiru.arm7
e1411cc1726afe6fb8d09099c5fb2fa6   okiru.x86
cd4de0ae80a6f11bca8bec7b590e5832   okiru.x86
7de55e697cd7e136dbb82b0713a01710   okiru.mips
797458f9cee3d50e8f651eabc6ba6031   okiru.m68k
353d36ad621e350f6fce7a48e598662b   okiru.arm
8db073743319c8fca5d4596a7a8f9931   okiru.sparc
0a8efeb4cb15c5b599e0d4fb9faba37d   okiru.powerpc
08d48000a47af6f173eba6bb16265670   okiru.x86_64
e9038f7f9c957a4e1c6fc8489994add4   okiru.superh
```

Malware delivery IPs

```
95.211.123.69
77.73.69.177
172.93.97.219
165.227.220.202
198.7.59.177
```

Current C2

```
95.211.123.69:7645
```

This C2 was first null routed by the community taking action against Satori, then removed by the organization for which it was hosted (2017-12-06). We expect new C2s to be used as this incident evolves.

Distraction C2

```
109.206.187.130:23 (Believed to be distraction for threat researchers)
```

4.0/ Malware Analysis (x86) /

VirusTotal: https://www.virustotal.com/#/url-analysis/u-ae9fd49dc90f8e360597c0b0950
7255e33ce9cb0209b75adaa230b3243961dfa-1512498951

Detux: https://detux.org/report.php?sha256=f9a4c6857bb3a4feebb232c54e6ecff
d3742ce598b48e975d675b38232b8e30e

Hybrid Analysis: https://www.hybrid-analysis.com/sample/f9a4c6857bb3a4feebb232
c54e6ecffd3742ce598b48e975d675b38232b8e30e?environmentId=300

Do you have questions, comments, or feedback about this report? Please contact **sirt@akamai.com**