WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

TECHNICAL INTELLIGENCE REPORT

Actor Type: II-III
Serial: TIR-19-140-001
Country: all
Report Date: 20190520
Industries: All

Mirai Clusters

Summary

Mirai is a self-propagating malware that infects networked devices and turns them into remotely controlled bots. Targets include devices in the Internet of Things (IoT) such as IP cameras and home routers and access is achieved with either software exploits or via authentication with factory default credentials. Mirai is frequently updated to include new exploits making it difficult to mitigate.

This report provides cluster trending on infrastructure over the past several weeks from this report date.

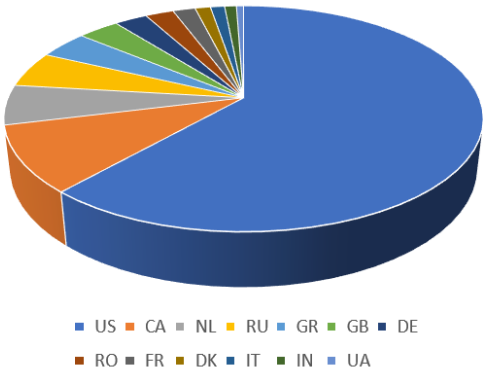
Details

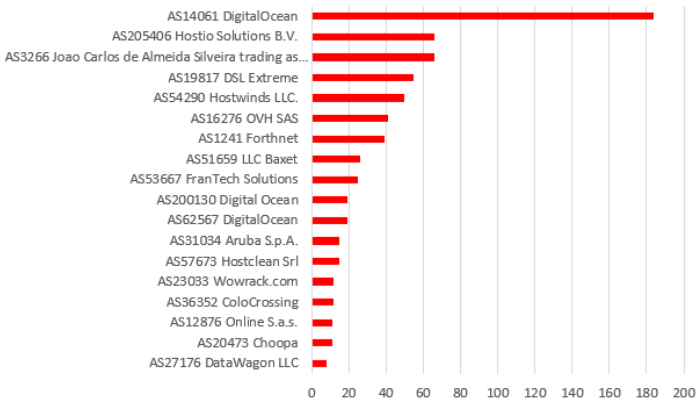
In January 2019, Palo Alto reported 11 new exploits leveraged by Mirai, making a total of 27. The variant was characterized by its inclusion of a variety of exploits for different embedded devices such as network storage devices, network video recorders (NVRs) and IP cameras. Also found were additional exploits for devices typically leveraged by businesses including targeting WePresent WiPG-1000 Wireless Presentation systems, and in LG Supersign TVs. [1]

In May 2019, Wapack Labs performed an inventory of recent Mirai specimens on Virus Total. A total of 29K malware specimens were observed during the period spanning from early March to mid-May 2019. Analysis of distribution points or ITW (In-the-wild) revealed over 73 domains and 1219 IP addresses. A comprehensive indicator list is provided as a companion document to this product.

[1] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

Of the 1200 Mirai distribution nodes, the vast majority are geolocated to the US, with Digital Ocean listed as the ASN. Digital Ocean is US cloud infrastructure provider headquartered in New York and as of 2018 was the 3rd largest hosting company in terms of web-facing computers.[2] It is unclear why they are a prime host for Mirai distribution points however it is most likely a result of a combination of a large volume of web-facing computers and unpatched servers.

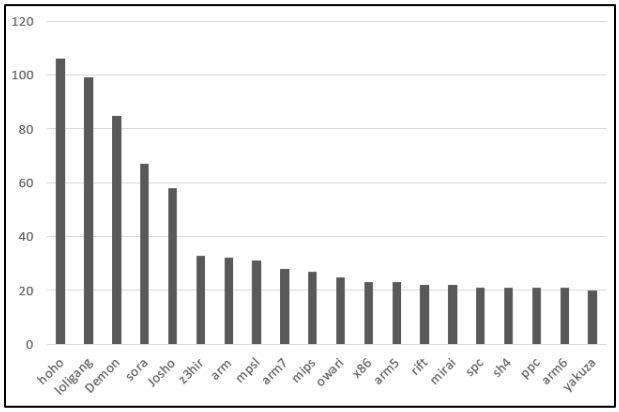


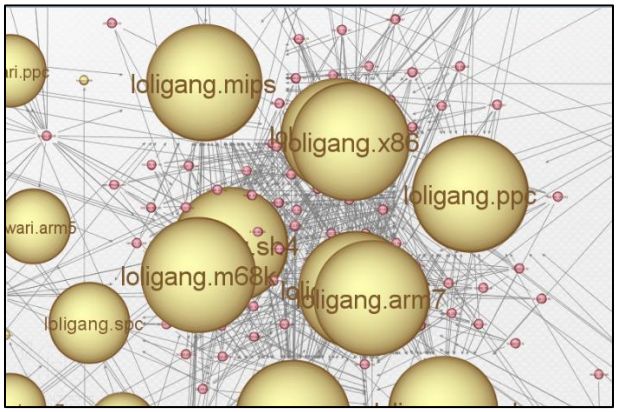


Figures 1. & 2., Geolocation and ASN Breakdown – Mirai Distribution Points

Examination of the Mirai distribution URLs exposed a number of clusters group by malware filenames. For example, filenames hoho and loligang comprised the largest of the clusters.

[2] https://en.wikipedia.org/wiki/DigitalOcean





Figures 2. & 3., Mirai Filename Clusters

The following are example URLs with 'hoho' and 'loligang' filenames. The filename clusters also use identical URI stems, for example /lmaoWTF/ was the commonly observed path in the loligang cluster.

- http://107.172.122.231/bins/hoho.sh4
- http://167.99.62.191/bins/hoho.arm7
- http://138.197.105.67/bins/hoho.ppc
- http://178.128.247.3/lmaoWTF/loligang.arm6
- http://52.234.231.142/lmaoWTF/loligang.ppc
- http://198.12.97.84/lmaoWTF/loligang.arm5

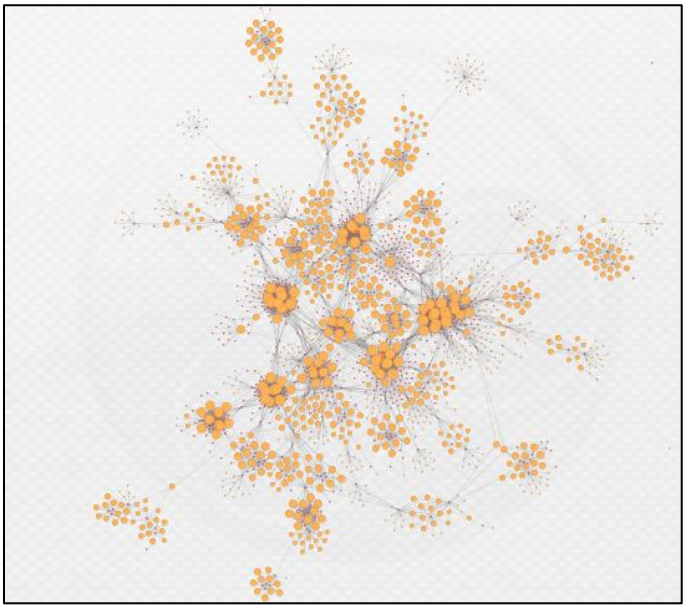


Figure 4. Mirai Clusters

The top distribution paths are as follows:

- /bins/
- /lmaoWTF/
- /sh/
- /Demon.sparc/
- /mips/

Wapack Labs performed additional trending against Mirai endpoints using Shodan scanning data. One of data points analyzed was tags with the most common being 'cloud'. Many also contained database tags which may be a reflection of new exploits targeting devices leveraged by businesses. The 3rd most common tag was 'scanner' which is expected given how Mirai performs scanning in order to identify vulnerable devices.

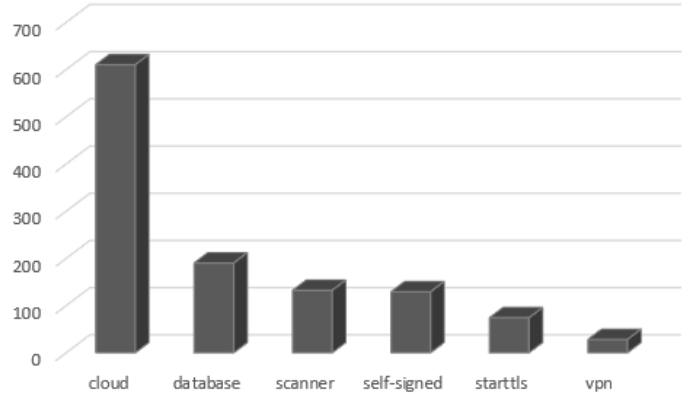


Figure 5. Mirai Tags - Shodan

Top data products identified by Shodan for Mirai endpoints included OpenSSH, Apache httpd, and MySQL.

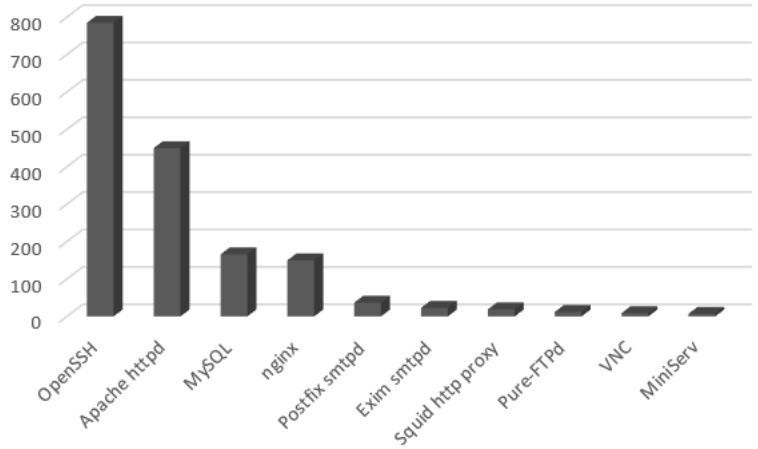


Figure 6. Dataproducts - Shodan

Conclusion

Mirai remains the leading malware currently targeting IoT devices. In 2016, Mirai's source code was leaked resulting in a massive uptick of IOT botnets and a competitive landscape where variants would apply patches to prevent other malware from taking over their bots. Additionally, the public source code allowed for the development of more sophisticated variants, such as Satori and Reaper.

As long as there continues to be vulnerabilities and exploits for IOT devices, then malware such as Mirai can be expected to take advantage. This is exacerbated by the fact that many networked devices require manual updates, which result in infrequent patching and consequently expose more vulnerable devices and allow for larger botnets.

Indicators:

The following are indicators. A comprehensive list is available via the Wapack API or in CTAC.

Indicator	Type	Kill_Chain_Phase	First_Seen	Last_Seen	Comments	Report_Reference	Attribution
139.59.34.206	IP	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
http://139.59.34.206/d/xd.mpsl	URL	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
205.185.113.25	IP	Delivery	5/4/2019	5/4/2019		TIR-19-140-001	Mirai
http://205.185.113.25/l/5akCM	URL	Delivery	5/4/2019	5/4/2019		TIR-19-140-001	Mirai
185.244.25.135	IP	Delivery	4/30/2019	4/30/2019		TIR-19-140-001	Mirai
http://185.244.25.135/nope/daddyscum.ppc	URL	Delivery	4/30/2019	4/30/2019		TIR-19-140-001	Mirai
178.62.32.28	IP	Delivery	4/25/2019	4/25/2019		TIR-19-140-001	Mirai
http://178.62.32.28/zehir/z3hir.arm5	URL	Delivery	4/25/2019	4/25/2019		TIR-19-140-001	Mirai
94.177.247.231	IP	Delivery	5/4/2019	5/8/2019		TIR-19-140-001	Mirai
http://94.177.247.231/lmaoWTF/poogang.x86	URL	Delivery	5/4/2019	5/8/2019		TIR-19-140-001	Mirai

178.156.202.249	IP	Delivery	4/26/2019	4/26/2019		TIR-19-140-001	Mirai
http://178.156.202.249/qtmzbn	URL	Delivery	4/26/2019	4/26/2019		TIR-19-140-001	Mirai
178.128.247.3	IP	Delivery	4/22/2019	4/30/2019		TIR-19-140-001	Mirai
http://178.128.247.3/lmaoWTF/loligang.arm6	URL	Delivery	4/22/2019	4/30/2019		TIR-19-140-001	Mirai
52.234.231.142	IP	Delivery	4/30/2019	5/5/2019		TIR-19-140-001	Mirai
http://52.234.231.142/lmaoWTF/loligang.ppc	URL	Delivery	4/30/2019	5/5/2019		TIR-19-140-001	Mirai
173.0.52.108	IP	Delivery	5/8/2019	5/8/2019		TIR-19-140-001	Mirai
http://173.0.52.108/yakuza.mpsl	URL	Delivery	5/8/2019	5/8/2019		TIR-19-140-001	Mirai
134.209.16.229	IP	Delivery	4/28/2019	4/29/2019		TIR-19-140-001	Mirai
http://134.209.16.229/bins/arm.light	URL	Delivery	4/28/2019	4/29/2019		TIR-19-140-001	Mirai
159.89.202.9	IP	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
http://159.89.202.9/zehir/z3hir.arm5	URL	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
165.227.111.138	IP	Delivery	4/24/2019	4/25/2019		TIR-19-140-001	Mirai
http://165.227.111.138/bins/hoho.sh4	URL	Delivery	4/24/2019	4/25/2019		TIR-19-140-001	Mirai
162.243.164.86	IP	Delivery	4/28/2019	4/29/2019		TIR-19-140-001	Mirai
http://162.243.164.86/hehe.spc	URL	Delivery	4/28/2019	4/29/2019		TIR-19-140-001	Mirai
188.166.25.58	IP	Delivery	4/24/2019	4/24/2019		TIR-19-140-001	Mirai
http://188.166.25.58/sh	URL	Delivery	4/24/2019	4/24/2019		TIR-19-140-001	Mirai
185.244.25.81	IP	Delivery	5/1/2019	5/1/2019		TIR-19-140-001	Mirai
http://185.244.25.81/sh4	URL	Delivery	5/1/2019	5/1/2019		TIR-19-140-001	Mirai

154.16.195.217	IP	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
http://154.16.195.217/algorithm_generator_un5329ej3e92jrj3/wh0_w4nt_s0m3_p4in.sh4	URL	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
103.60.14.156	IP	Delivery	5/2/2019	5/3/2019		TIR-19-140-001	Mirai
http://103.60.14.156/bins/yakuza.spc	URL	Delivery	5/2/2019	5/3/2019		TIR-19-140-001	Mirai
107.172.122.231	IP	Delivery	4/28/2019	4/28/2019		TIR-19-140-001	Mirai
http://107.172.122.231/bins/hoho.sh4	URL	Delivery	4/28/2019	4/28/2019		TIR-19-140-001	Mirai
198.12.97.84	IP	Delivery	4/9/2019	5/7/2019		TIR-19-140-001	Mirai
http://198.12.97.84/lmaoWTF/loligang.arm5	URL	Delivery	4/9/2019	5/7/2019		TIR-19-140-001	Mirai
194.147.34.126	IP	Delivery	5/3/2019	5/4/2019		TIR-19-140-001	Mirai
http://194.147.34.126/lmaoWTF/loligang.ppc	URL	Delivery	5/3/2019	5/4/2019		TIR-19-140-001	Mirai
157.230.242.52	IP	Delivery	4/23/2019	4/25/2019		TIR-19-140-001	Mirai
http://157.230.242.52/d/xb.spc	URL	Delivery	4/23/2019	4/25/2019		TIR-19-140-001	Mirai
5.196.247.7	IP	Delivery	5/7/2019	5/7/2019		TIR-19-140-001	Mirai
http://5.196.247.7/splintershell.eee	URL	Delivery	5/7/2019	5/7/2019		TIR-19-140-001	Mirai
134.209.158.135	IP	Delivery	4/27/2019	4/27/2019		TIR-19-140-001	Mirai
http://134.209.158.135/zehir/z3hir.m68k	URL	Delivery	4/27/2019	4/27/2019		TIR-19-140-001	Mirai
37.148.210.65	IP	Delivery	5/2/2019	5/2/2019		TIR-19-140-001	Mirai
http://37.148.210.65/lmaoWTF/loligang.mips	URL	Delivery	5/2/2019	5/2/2019		TIR-19-140-001	Mirai
185.244.25.85	IP	Delivery	4/28/2019	4/28/2019		TIR-19-140-001	Mirai
http://185.244.25.85/bins/spc	URL	Delivery	4/28/2019	4/28/2019		TIR-19-140-001	Mirai
35.201.141.13	IP	Delivery	5/6/2019	5/6/2019		TIR-19-140-001	Mirai
http://35.201.141.13/akbins/sh4.akira.ak	URL	Delivery	5/6/2019	5/6/2019		TIR-19-140-001	Mirai

140.82.37.11	IP	Delivery	4/23/2019	4/24/2019		TIR-19-140-001	Mirai
http://140.82.37.11/bins/sora.arm5	URL	Delivery	4/23/2019	4/24/2019		TIR-19-140-001	Mirai
46.166.185.58	IP	Delivery	5/3/2019	5/3/2019		TIR-19-140-001	Mirai
http://46.166.185.58/bins/frosty.sh4	URL	Delivery	5/3/2019	5/3/2019		TIR-19-140-001	Mirai
192.236.161.53	IP	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
http://192.236.161.53/bins/genisis.x86	URL	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
http://192.236.161.53/bins/orphic.x86	URL	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
134.209.156.37	IP	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
http://134.209.156.37/bins/orphic.x86	URL	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
68.183.86.110	IP	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
http://68.183.86.110/bins/orphic.x86	URL	Delivery	4/29/2019	5/8/2019		TIR-19-140-001	Mirai
167.99.62.191	IP	Delivery	4/25/2019	4/25/2019		TIR-19-140-001	Mirai
http://167.99.62.191/bins/hoho.arm7	URL	Delivery	4/25/2019	4/25/2019		TIR-19-140-001	Mirai
37.49.227.176	IP	Delivery	5/7/2019	5/8/2019		TIR-19-140-001	Mirai
http://37.49.227.176/Arceus.x86	URL	Delivery	5/7/2019	5/8/2019		TIR-19-140-001	Mirai
138.197.105.67	IP	Delivery	4/23/2019	4/25/2019		TIR-19-140-001	Mirai
http://138.197.105.67/bins/hoho.ppc	URL	Delivery	4/23/2019	4/25/2019		TIR-19-140-001	Mirai
205.185.120.241	IP	Delivery	4/26/2019	5/6/2019		TIR-19-140-001	Mirai
http://205.185.120.241/MasakiBins/spp.arm	URL	Delivery	4/26/2019	5/6/2019		TIR-19-140-001	Mirai
http://205.185.120.241/MasakiBins/telnet.arm	URL	Delivery	4/26/2019	5/6/2019		TIR-19-140-001	Mirai

http://205.185.120.241/MasakiBins/uchttpd.arm	URL	Delivery	4/26/2019	5/6/2019		TIR-19-140-001	Mirai
http://205.185.120.241/MasakiBins/ssh2.arm	URL	Delivery	4/26/2019	5/6/2019		TIR-19-140-001	Mirai
67.205.155.69	IP	Delivery	5/1/2019	5/1/2019		TIR-19-140-001	Mirai
http://67.205.155.69/bins/hoho.mips	URL	Delivery	5/1/2019	5/1/2019		TIR-19-140-001	Mirai
185.244.25.230	IP	Delivery	4/26/2019	4/26/2019		TIR-19-140-001	Mirai
http://185.244.25.230/sh	URL	Delivery	4/26/2019	4/26/2019		TIR-19-140-001	Mirai
ilililililililililil.hopto.org	Domain	Delivery	5/3/2019	5/8/2019		TIR-19-140-001	Mirai
http://ilililililililililil.hopto.org/shiina/shiina.ppc	URL	Delivery	5/3/2019	5/8/2019		TIR-19-140-001	Mirai
35.235.102.123	IP	Delivery	5/3/2019	5/8/2019		TIR-19-140-001	Mirai
http://35.235.102.123/shiina/shiina.ppc	URL	Delivery	5/3/2019	5/8/2019		TIR-19-140-001	Mirai
149.56.140.11	IP	Delivery	4/30/2019	5/2/2019		TIR-19-140-001	Mirai
http://149.56.140.11/mpsl	URL	Delivery	4/30/2019	5/2/2019		TIR-19-140-001	Mirai
185.244.25.188	IP	Delivery	4/18/2019	4/26/2019		TIR-19-140-001	Mirai
http://185.244.25.188/a8	URL	Delivery	4/18/2019	4/26/2019		TIR-19-140-001	Mirai
192.241.158.41	IP	Delivery	4/27/2019	5/4/2019		TIR-19-140-001	Mirai
http://192.241.158.41/pftp	URL	Delivery	4/27/2019	5/4/2019		TIR-19-140-001	Mirai
46.101.14.113	IP	Delivery	4/24/2019	4/24/2019		TIR-19-140-001	Mirai
http://46.101.14.113/bins/sora.x86	URL	Delivery	4/24/2019	4/24/2019		TIR-19-140-001	Mirai
185.22.153.36	IP	Delivery	4/26/2019	4/27/2019		TIR-19-140-001	Mirai
http://185.22.153.36/bins/owari.ppc	URL	Delivery	4/26/2019	4/27/2019		TIR-19-140-001	Mirai

165.22.84.107	IP	Delivery	5/6/2019	5/6/2019		TIR-19-140-001	Mirai
http://165.22.84.107/bins/hoho.mips	URL	Delivery	5/6/2019	5/6/2019		TIR-19-140-001	Mirai
http://159.89.202.9/zehir/z3hir.spc	URL	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
194.147.35.77	IP	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
http://194.147.35.77/zehir/z3hir.arm	URL	Delivery	4/29/2019	4/29/2019		TIR-19-140-001	Mirai
80.211.75.183	IP	Delivery	4/25/2019	4/26/2019		TIR-19-140-001	Mirai
http://80.211.75.183/zehir/z3hir.sh4	URL	Delivery	4/25/2019	4/26/2019		TIR-19-140-001	Mirai
139.59.10.88	IP	Delivery	5/7/2019	5/7/2019		TIR-19-140-001	Mirai

Additional Reporting: n/a

For questions or comments regarding this report, please contact the Lab directly by at 603-606-1246, or feedback@wapacklabs.com

---