New Mirai Variant Launches 54 Hour DDoS Attack against US College

incapsula.com/blog/new-mirai-variant-ddos-us-college.html

March 29, 2017

Update (3/30/2017):
Following a media inquiry, we drilled down into our data and discovered that 56 percent of all IPs used in the attack belonged to DVRs manufactured by the same vendor. We have contacted the vendor with an offer to share our information and assist with resolving the issue.

Since the Mirai malware was discovered last August, we've seen it used in a number of high profile DDoS attacks, including the September assault on cybersecurity expert Brian Krebs and October's takedown of Dyn DNS services.

Given the success of those attacks, along with the public availability of the Mirai source code, it was clearly only a matter of time before botnet herders began experimenting with new versions of the malware.

Last December, we wrote about a variant that exploited a TR-069 network router protocol vulnerability to infect TalkTalk Telecom home routers. And earlier this year we saw the emergence of a repurposed Windows botnet capable of spreading Mirai bots to Linux systems.

One thing the above variants have in common is they've mostly been used to launch network layer DDoS attacks. A few weeks ago, however, what could be another version of Mirai–this one more adept at launching application layer assaults–popped up on our radar.

Attack Description

The attack, which started on February 28 and ran for 54 hours straight, targeted one of our customers, a US college.

The average traffic flow came in at over 30,000 RPS and peaked at around 37,000 RPS—the most we've seen out of any Mirai botnet. In total, the attack generated over 2.8 billion requests.

Mirai_variant_request

Based on a number of signature factors, including header order, header values and traffic sources, our client classification system immediately identified that the attack emerged from a Mirai-powered botnet.

Our research showed that the pool of attacking devices included those commonly used by Mirai, including CCTV cameras, DVRs and routers. While we don't know for sure, open telnet (23) ports and TR-069 (7547) ports on these devices might indicate that they were exploited by known vulnerabilities.

We also noticed that the DDoS bots used in the attack were hiding behind different user-agents than the five hardcoded in the default Mirai version. This–and the size of the attack itself–led us to believe that we might be dealing with a new variant, which was modified to launch more elaborate application layer attacks.

Overall, in the course of the attack, we spotted the following 30 user-agent variants:

```
Mozilla/5.0 (Windows NT 6.0; rv:13.0) Gecko/20100101 Firefox/13.0.1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:13.0) Gecko/20100101 Firefox/13.0.1
Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.11 (KHTML, like Gecko)
Chrome/20.0.1132.47 Safari/536.11
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.56 Safari/536.5
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/534.57.2 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.2
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.57.2 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.2
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.1 (KHTML, like Gecko)
Chrome/13.0.782.112 Safari/535.1
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.56 Safari/536.5
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.11 (KHTML, like Gecko)
Chrome/20.0.1132.57 Safari/536.11
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1
Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.02
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.11 (KHTML, like Gecko)
Chrome/20.0.1132.47 Safari/536.11
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727;
.NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Mozilla/5.0 (Linux; U; Android 2.2; fr-fr; Desire_A8181 Build/FRF91)
App3leWebKit/53.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/534.57.5 (KHTML, like
Gecko) Version/5.1.7 Safari/534.57.4
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0) Gecko/20100101 Firefox/13.0.1
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML,
like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.56 Safari/536.5
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; MRA 5.8 (build 4157); .NET
CLR 2.0.50727; AskTbPTV/5.11.3.15590)
```

We also saw attack traffic originating from 9,793 IPs worldwide:

mirai_variant_map

Out of these, over 70 percent are located in following ten countries:

Country	% of botnet IPs
United States	18.4%

Israel	11.3%
Taiwan	10.8%
India	8.7%
Turkey	6%
Russia	3.8%
Italy	3.2%
Mexico	3.2%
Colombia	3.0%
Bulgaria	2.2%

Less than a day after the initial assault ended, another one began that lasted for an hour and a half with an average traffic flow of 15,000 RPS.

Based on our experience, we expect to see several more bursts before the offender(s) finally give up on their efforts.

Afterthoughts

Ever since the Mirai source code was made public last year, we’ve seen offenders continue to evolve the malware’s capabilities to expand its range and launch more elaborate and impactful assaults.

Looking at the bigger picture, this variant of Mirai might be a symptom of the increased application layer DDoS attack activity we saw in the second half of 2016.

That said, with over 90 percent of all application layer assaults lasting under six hours, an attack of this duration stands in a league of its own.

Try Imperva for Free

Protect your business for 30 days on Imperva.

Start Now