Mirai botnet and DDoS attacks
security note

Nokia Threat Intelligence Labs

October 2016

This Security Note summarizes what is currently known about the Mirai Botnet(s) that has/have been responsible for recent massive Distributed Denial of Service (DDoS) attacks, including the:

- 600Gbps attack against the Brian Krebs web site (September 2016)
- 1.5Tbps attack against a French web hosting provider (October 2016)
- Attack against DynDNS that disrupted Internet service (21 October 2016)
Botnet prevention, detection and remediation

The botnet source code was released in late September and is now available to the hacker community not only experiment with it, but also to create botnets to launch attacks. Given such dangerous code, it was inevitable that a major DDoS attack would be launched against the internet infrastructure.

The Nokia NetGuard Endpoint Security (NES) product allows service providers to detect which devices are infected. The infections can be remediated by rebooting the device, logging into it, and resetting the password. The NES product can also detect the command-and-control (C&C) sites and build an IP black list that can be used to block communication with those sites. As a result, service providers can prevent devices in their networks from participating in the attacks by blocking the C&C. The large-scale attacks are difficult to prevent because they are being launched from infected devices on hundreds of carrier networks around the globe.

As is often the case, the security industry has attributed these attacks to other malware that may or may not be related to the Mirai attacks. The malware includes:

- Shellshock
- Bashlite
- Gafgyt

The malware uses different attack vectors and can also target IoT devices.

Distinguishing features

The Mirai botnet and associated DDoS attacks have a number of distinguishing features from previous botnets.

Mirai targets IoT devices

The Mirai botnet targets any device with a public internet IP address that can be accessed using Telnet or SSH. The botnet actively scans for any internet accessible devices that have Telnet or SSH services open to the internet. This means that the botnet targets residential gateways, home routers, as well as a host of IoT devices, such as video cameras, smart meters, DVRs, and Mifi gateways. The botnet uses brute force password guessing to access these devices and install the bot software.

In our mobile deployments, we have seen a variety of compromised devices. Many of these are mobile Mifi devices. Even so, we are also seeing infection on devices based on a variety of mobile chipsets. These chipsets include Telit and Gemalto that are built into mobile IoT devices, such as cars and video cameras.

The following table lists the infected device types in one of the NES deployments.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sierra Wireless</td>
<td>MC8790V</td>
<td>9657</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>MC8790</td>
<td>7704</td>
</tr>
<tr>
<td>NetComm Wireless Limited</td>
<td>NWL-10</td>
<td>7606</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>USB316</td>
<td>1972</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>MC8775</td>
<td>1691</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>MC8795V</td>
<td>1100</td>
</tr>
<tr>
<td>HUAWEI Technologies Co Ltd</td>
<td>EM820W</td>
<td>985</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>MC8775V</td>
<td>980</td>
</tr>
<tr>
<td>u-blox AG</td>
<td>LISA-U200</td>
<td>795</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>AirCard 320U</td>
<td>709</td>
</tr>
<tr>
<td>NetComm Wireless Limited</td>
<td>3G10WVT</td>
<td>691</td>
</tr>
<tr>
<td>NetComm Wireless Limited</td>
<td>NTC-6200-02</td>
<td>619</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>Q26 Extreme</td>
<td>519</td>
</tr>
<tr>
<td>Ericsson AB</td>
<td>F5521gw</td>
<td>476</td>
</tr>
<tr>
<td>Telit Communications SpA</td>
<td>HE910-EUD, HE910-EUR</td>
<td>471</td>
</tr>
<tr>
<td>Gemalto M2M GmbH</td>
<td>PLS8-E</td>
<td>470</td>
</tr>
<tr>
<td>NetComm Wireless Limited</td>
<td>NTC-140W-02</td>
<td>468</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>MC8704</td>
<td>449</td>
</tr>
<tr>
<td>SIMCOM Wireless Solutions Co Ltd</td>
<td>SIM5320E</td>
<td>427</td>
</tr>
</tbody>
</table>
From third-party reports, approximately 80 percent of the bots are DVRs manufactured by Dahua Technology. These are not usually deployed in mobile networks, so the NES product is not able to see them. The following table is sourced from a Brian Krebs article, and lists the devices targeted by the Mirai password guessing routine.

---

From third-party reports, approximately 80 percent of the bots are DVRs manufactured by Dahua Technology. These are not usually deployed in mobile networks, so the NES product is not able to see them. The following table is sourced from a Brian Krebs article, and lists the devices targeted by the Mirai password guessing routine.

---

Hangzhou Xiongmai Technology, a vendor behind DVRs and internet-connected cameras, said on Sunday that security vulnerabilities involving weak default passwords in its products were partly to blame.3

Bot rallying behaviour

The mechanism used by a bot to contact its command and control (C&C) system is known as its “rallying strategy”. The Mirai rallying strategy is different from most previous botnets. Instead of the bots having to find the C&C server, the C&C server finds them. In fact, the attacker knows where all the bots are, and how to contact them. This enables attackers to shift the C&C site anytime they want.

3 http://www.pcworld.com/article/3134039/hacking/chinese-firm-admits-its-hacked-products-were-behind-fridays-massive-ddos-attack.html
A Mirai bot spends most of its time scanning for new victims. When it locates one and manages to log in using the password guessing attack, it sends the IP address and userid/pw to the current C&C server. This stores the information in a database that contains the IP addresses and access credentials of all bots in the botnet. To move the C&C, the attacker simply starts up a new copy of itself in a different location, and uses the database to contacts all the bots, update their software, and give them their new orders.

Figure 1 Illustrates the botnet structure.¹

Figure 1. The botnet structure

Not for profit

- Unlike most recent botnets, the recent DDoS attacks appear to have no profit motive. The main objective is likely publicity. As such, it is a throwback to the virus and worm attacks of the 90s when hackers competed for notoriety by trying to infect the most devices.

¹ http://blog.level3.com/security/grinch-stole-iot/
• The Krebs attack was obviously targeted at a well-known network security blogger who would certainly generate publicity. It remains unclear, though, why OVH was the next target, but the event certainly made news. The Friday DDoS attack against DynDNS — again, with no financial gain in mind — was designed to cause the most damage to internet services.

• Moreover, at this point it is unclear whether one group is responsible for these attacks. The attacks might be the result of a number of competing hacker groups — each with a copy of the Mirai code, and each trying to out-do each other for the biggest impact.

The bot’s two functions: spread and attack

Unlike many bots, which separate the infection process from the attack side, Mirai combines these two functions into a single piece of code. Mirai bots do not sit idle waiting for instructions; they seek out new victims, working quietly in the background, 24/7. This is why Mirai is such a powerful threat. It has been reported that a Mirai botnet can grow to 130K in only one day.

The second function is, of course, the attack. Mirai has a powerful suite of attack capabilities. These include:

- **generic udp attack** - Straight up UDP flood
- **udp vsep attack** - Valve Source Engine query flood
- **udp dang attack** - DNS water torture
- **udp plain attack** - Plain UDP flood optimized for speed
- **tcp syn attack** - SYN flood with options
- **tcp ack attack** - ACK flood
- **tcp stomp attack** - ACK flood to bypass mitigation devices
- **gre ip attack** - GRE IP flood
- **gre Ethernet attack** - GRE Ethernet flood
- **http application attack** - HTTP layer 7 flood

These attack capabilities enable Mirai to deliver a variety of attacks — some directed at specific services, (such as DynDNS), and others for delivering a flood of traffic.
Botnet operation

The Mirai botnet has three operation phases.

Phase 1:
- Bot scans for vulnerable devices
- Brute force login against open Telnet and SSH ports

Phase 2:
- Infected device joins botnet and scans for other victims
- Reported to have created a 130K device botnet in one day

Phase 3:
- Botnet attacks victim

What the Nokia NetGuard Endpoint Security product detects

The NES product currently detects the scanning and brute force login attempts used by Mirai bots to add more victims. These capabilities enable us to identify the bots, because they are the ones that do the scanning. The infections can be remediated by rebooting the device, logging into it, and resetting the password.

The NES product can also detect C&C sites and build an IP black list used to block communication with those sites. As a result, service providers can prevent devices in their network from participating in the attacks by blocking the C&C. The full-scale attacks are difficult to prevent because they are launched from infected devices on hundreds of carrier networks around the globe.

The chart shows the spike in Telnet-failed login attempts that coincided with the Krebs and OVH attacks in October.
WGN can also detect excessive Telnet activity. The following chart is from one of their deployments.

Most TCP/23 flows are generated by Huawei MiFi or Dongles devices

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>E3531s-2</td>
<td>2G</td>
</tr>
<tr>
<td>E5531s-22</td>
<td>3G</td>
</tr>
<tr>
<td>E5151s-2</td>
<td>2G</td>
</tr>
</tbody>
</table>

We currently detect some of the generic attacks, (including SYS flood, UPD flood, DNS flood), but will shortly be adding signature specific to Mirai.
Impact on our customers

Surprisingly, the impact on many of our customers will be relatively small. This is because they use carrier-grade NAT that does not expose their users to scanning from the internet. Most mobile service providers use carrier-grade NAT, so their customer devices are not accessible from the internet. Even if these devices were vulnerable, they would not be subject to scanning and compromise.

It is important to note that, despite using NAT, carriers can be impacted when roaming users from carriers that don’t use NAT enter their network. However, the devices impacted by Mirai are unlikely to be roaming.

That said, when the internet becomes unusable due to these attacks, everyone suffers, even if they are not contributing to the problem.

Additional information