

Much of the new mirai variant that scans port 7547 has been covered by various sources.

In this blog, we will not repeat such known facts, and we are just going to list a few observations that we have seen so far.


Mirai First Hit and Capability Assessment

All the mirai samples so far inherit a coding issue so we can distinguish between a true mirai scanner and a regular scanner.

The following table lists first seen time of “old” mirai and the “new” ones that hit our honeypot.

You can see the variant on port 7547 first shown up on 2016-11-26 21:27:23, and first observed for the variant on port 5555 was one day after on 2016-11-27 17:04:02(all GMT +8).

!



Daily bot activity (blue and red lines on the rightmost are the two new variants)

According to the current trend, the bot growth rates of the four ports are:

!



Currently, the growth rate of the bot on port 7547 has far exceeded the number of bots on port 23/2323.

The total number of bots on current port 7547 has already exceeded 30,000.

Bot growth rate on port 7547, per 10 minutes:

The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.

On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.

In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the geographical distribution of the existing mirai botnet.

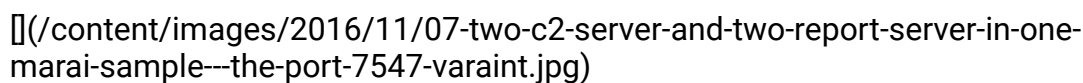
We provide various statistics and data downloads of Mirai-infected devices at <http://data.netlab.360.com/mirai-scanner> for researchers.

For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.

The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet

The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)

!

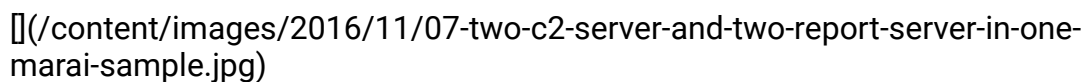
 (/content/images/2016/11/07-two-c2-server-and-two-report-server-in-one-mirai-sample---the-port-7547-varaint.jpg)

It is noteworthy the exact combination, both C2s and report servers had previously been embedded in the “old” mirai sample that we saw a while ago on 2016-11-09.

Detail of the sample of 2016-11-09 variant:

CRC32: 2BD6603A MD5: EF713BDD7B06097447A25F4B35C738F6 SHA-1: 44D9C6A682E48DFA86BACDBD68F11A1F3CB78D07

!

 (/content/images/2016/11/07-two-c2-server-and-two-report-server-in-one-mirai-sample.jpg)

Bot Overlap

In other words, the operator of new variant on port 7547 and the previous mirai operator are very likely the same group of people.

The following diagram shows the overlap of all the bots we captured in our honeypot that have scanned port 23/2323/5555/7547.

We can see that:

96.4% of the Mirai Bots scan port 23 or port 2323.

Among them, 79% only scan port 23 and 6.4% only scan 2323, 11% scan both port 23 and 2323.

About 3.1% of the Mirai bots only scan port 7547.

The infection speed is amazing considering that Mirai’s propagation on this port started only three days ago.

No more than 0.1% of the bots show other cross-scanning behaviors among the

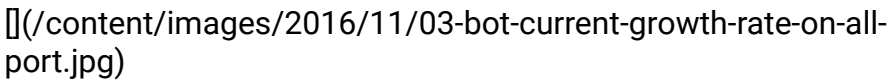
four-ports, which is still quite rare.

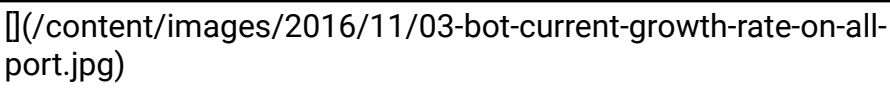
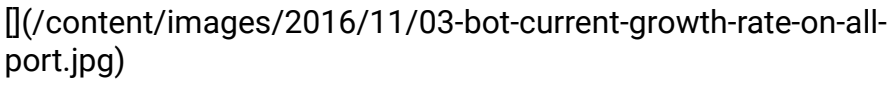
Infected Device Breakdown

All together we have logged 46,653 IPs that were infected with this new 7547 variants, and we tried to ID these known infected IPs by sending out requests that emulate tr064|tr069 protocol so we would be able to get accurate device info.

The following is a breakdown of the infected device lists from 5976 IPs that response us.

(The majority of the sources might have that port blocked by mirai, or device reboot, or IP changing, or various network issues).

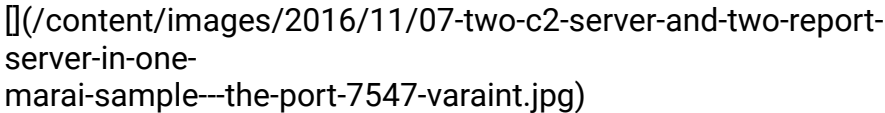
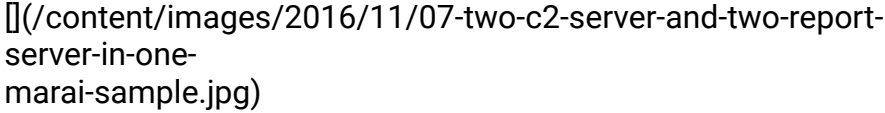
ID	Name	Identified Sentence
T1046	Network Service Scanning	Much of the new mirai variant that scans port 7547 has been covered by various sources.
T1065	Uncommonly Used Port	<p>The following table lists first seen time of “old” mirai and the “new” ones that hit our honeypot.</p> <p>You can see the variant on port 7547 first shown up on 2016-11-26 21:27:23, and first observed for the variant on port 5555 was one day after on 2016-11-27 17:04:02(all GMT +8).</p> <p>!</p>
T1043	Commonly Used Port	<p>The following table lists first seen time of “old” mirai and the “new” ones that hit our honeypot.</p> <p>You can see the variant on port 7547 first shown up on 2016-11-26 21:27:23, and first observed for the variant on port 5555 was one day after on 2016-11-27 17:04:02(all GMT +8).</p> <p>!</p>
T1065	Uncommonly Used Port	<p></p> <p>Currently, the growth rate of the bot on port 7547 has far exceeded the number of bots on port 23/2323.</p>

T1046	Network Service Scanning	<p></p> <p>Currently, the growth rate of the bot on port 7547 has far exceeded the number of bots on port 23/2323.</p>
T1043	Commonly Used Port	<p></p> <p>Currently, the growth rate of the bot on port 7547 has far exceeded the number of bots on port 23/2323.</p>
T1048	Exfiltration Over Alternative Protocol	<p>The total number of bots on current port 7547 has already exceeded 30,000.</p> <p>Bot growth rate on port 7547, per 10 minutes:</p> <p>The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.</p> <p>On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.</p> <p>In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the geographical distribution of the existing mirai botnet.</p> <p>We provide various statistics and data downloads of Mirai-infected devices at http://data.netlab.360.com/mirai-scanner for researchers.</p> <p>For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.</p> <p>The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet</p>

		<p>The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)</p> <p>!</p>
T1065	Uncommonly Used Port	<p>The total number of bots on current port 7547 has already exceeded 30,000.</p> <p>Bot growth rate on port 7547, per 10 minutes:</p> <p>The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.</p> <p>On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.</p> <p>In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the geographical distribution of the existing mirai botnet.</p> <p>We provide various statistics and data downloads of Mirai-infected devices at http://data.netlab.360.com/mirai-scanner for researchers.</p> <p>For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.</p> <p>The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet</p> <p>The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)</p> <p>!</p>
T1046	Network Service Scanning	<p>The total number of bots on current port 7547 has already exceeded 30,000.</p>

		<p>Bot growth rate on port 7547, per 10 minutes:</p> <p>The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.</p> <p>On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.</p> <p>In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the geographical distribution of the existing mirai botnet.</p> <p>We provide various statistics and data downloads of Mirai-infected devices at http://data.netlab.360.com/mirai-scanner for researchers.</p> <p>For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.</p> <p>The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet</p> <p>The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)</p> <p>!</p>
T1008	Fallback Channels	<p>The total number of bots on current port 7547 has already exceeded 30,000.</p> <p>Bot growth rate on port 7547, per 10 minutes:</p> <p>The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.</p>

		<p>On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.</p> <p>In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the geographical distribution of the existing mirai botnet.</p> <p>We provide various statistics and data downloads of Mirai-infected devices at http://data.netlab.360.com/mirai-scanner for researchers.</p> <p>For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.</p> <p>The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet</p> <p>The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)</p> <p>!</p>
T1043	Commonly Used Port	<p>The total number of bots on current port 7547 has already exceeded 30,000.</p> <p>Bot growth rate on port 7547, per 10 minutes:</p> <p>The figure shows that, bot's growth rate quickly reached a peak, and smoothly maintained at a high level.</p> <p>On the other hand, from the perspective of the backbone network, the scan on port 7547 began to rise sharply in the evening of 2016-11-26.</p> <p>In terms of the geographical distribution of the newly infected bot, Brazil is still far ahead of the others, which is consistent with the</p>

		<p>geographical distribution of the existing mirai botnet.</p> <p>We provide various statistics and data downloads of Mirai-infected devices at http://data.netlab.360.com/mirai-scanner for researchers.</p> <p>For those who have been using API to access our bot list, please re-download the data from 2016-11-26 and later to obtain updates for port 7547 and 5555 data.</p> <p>The New Variant Shares Some of the Infrastructure of the Existing Mirai Botnet</p> <p>The new mirai has two C2s (securityupdates.us, timeserver.host) and two report servers (rep.securityupdates.us, ntp.timeserver.host)</p> <p>!</p>
T1008	Fallback Channels	<p></p> <p>It is noteworthy the exact combination, both C2s and report servers had previously been embedded in the “old” mirai sample that we saw a while ago on 2016-11-09.</p> <p>Detail of the sample of 2016-11-09 variant:</p> <p>CRC32: 2BD6603A MD5: EF713BDD7B06097447A25F4B35C738F6 SHA-1: 44D9C6A682E48DFA86BACDBD68F11A1F3CB78D07</p> <p>!</p>
T1065	Uncommonly Used Port	<p></p> <p>Bot Overlap</p> <p>In other words, the operator of new variant on port 7547 and the previous mirai operator are very likely the same group of people.</p>

		<p>The following diagram shows the overlap of all the bots we captured in our honeypot that have scanned port 23/2323/5555/7547.</p> <p>We can see that:</p> <p>96.4% of the Mirai Bots scan port 23 or port 2323.</p>
T1046	Network Service Scanning	<p>[(/content/images/2016/11/07-two-c2-server-and-two-report-server-in-one-marai-sample.jpg)]</p> <p>Bot Overlap</p> <p>In other words, the operator of new variant on port 7547 and the previous mirai operator are very likely the same group of people.</p> <p>The following diagram shows the overlap of all the bots we captured in our honeypot that have scanned port 23/2323/5555/7547.</p> <p>We can see that:</p> <p>96.4% of the Mirai Bots scan port 23 or port 2323.</p>
T1008	Fallback Channels	<p>[(/content/images/2016/11/07-two-c2-server-and-two-report-server-in-one-marai-sample.jpg)]</p> <p>Bot Overlap</p> <p>In other words, the operator of new variant on port 7547 and the previous mirai operator are very likely the same group of people.</p> <p>The following diagram shows the overlap of all the bots we captured in our honeypot that have scanned port 23/2323/5555/7547.</p> <p>We can see that:</p> <p>96.4% of the Mirai Bots scan port 23 or port 2323.</p>
T1043	Commonly Used Port	<p>[(/content/images/2016/11/07-two-c2-server-and-two-report-server-in-one-marai-sample.jpg)]</p> <p>Bot Overlap</p> <p>In other words, the operator of new variant on port 7547 and the previous</p>

		<p>mirai operator are very likely the same group of people.</p> <p>The following diagram shows the overlap of all the bots we captured in our honeypot that have scanned port 23/2323/5555/7547.</p> <p>We can see that:</p> <p>96.4% of the Mirai Bots scan port 23 or port 2323.</p>
T1065	Uncommonly Used Port	Among them, 79% only scan port 23 and 6.4% only scan 2323, 11% scan both port 23 and 2323.
T1046	Network Service Scanning	Among them, 79% only scan port 23 and 6.4% only scan 2323, 11% scan both port 23 and 2323.
T1043	Commonly Used Port	Among them, 79% only scan port 23 and 6.4% only scan 2323, 11% scan both port 23 and 2323.
T1046	Network Service Scanning	About 3.1% of the Mirai bots only scan port 7547.
T1046	Network Service Scanning	<p>No more than 0.1% of the bots show other cross-scanning behaviors among the four-ports, which is still quite rare.</p> <p>Infected Device Breakdown</p> <p>All together we have logged 46,653 IPs that were infected with this new 7547 variants, and we tried to ID these known infected IPs by sending out requests that emulate tr064 tr069 protocol so we would be able to get accurate device info.</p>