Up till very recently, through the samples we had learned that the Mirai DGA seeds are all fixed to 0, as detailed in blog Now Mirai Has DGA Feature Built in, and were able to predict all corresponding DGA domains.

Surprisingly, although we have not see any related samples, just few days ago, our PassiveDNS based anomaly detect module captured some new domains that matches the characteristics of the mirai DGA algorithm but not belong to any seed 0 series.

The L2 domains conform to mirai DGA: 12 characters and a-y only.

But these domains do not belong to DGA seed 0 series.

This leads us to speculate that a new mirai variant and new DGA seed is emerging.

DGA Domains Generated With Non-zero DGA Seed

The new suspicious domain are listed below:

And the domains's query patterns are as follows:

A detailed study on these domains shows more findings:

The L2 domains conform to mirai DGA, 12 characters, a-y only.

But these domains does not belong to DGA seed 0 series.

All TLDs for these domains are fixed to .online , differing from previous TLDs of online / tech / support .

Maybe the author want just keep "online", but no more "tech support".

Of all the domains, the first seen starts almost strictly at 00:00:00 of the day, with the last seen almost always strictly ends at 00:00:00 on the next.

Those time window overlaps between the two consequential domains are very short, in minutes.

Considering such a strict time window control, we think one possible explanation is that those DNS queries were eventually launched by some mirai bots.

New DGA Seed 0x91 Brute-forced

Under the guidance of the precise mirai algorithm, we are pretty sure we are able to brute-force the new DGA seeds, no matter where it hides in the int32 4G space.

And the brute force did not take long before we cracked the new seed:

0x91

The new DGA seed is used to predict all the 2016-12 domains, as follows.

Note that almost all these domains are registered by mirai author, with the exception 18/19/27/29/30 on which the algorithm itself can not generated a functional DGA domain.

2016/12/08 pcrpxewicouh.online

2016/12/09 rwoywonuobcr.online

2016/12/10 liusqxocbedg.online

2016/12/11 ndoiabgxgmew.online

2016/12/12 hwjqtwkectlo.online

2016/12/13 mtoyrjnvlqdx.online

2016/12/14 ddfqdttkmoyv.online

2016/12/15 iaxjxyqjckqi.online

2016/12/16 nuuxndqlhiwb.online

2016/12/17 pxvmqwpemiif.online

2016/12/18 dfftxpajygxy

2016/12/19 fiotbgopgnxv

2016/12/20 shjwhbdgjyba.online

2016/12/21 xmjvlucdsegk.online

2016/12/22 irkbpugkwsir.online

2016/12/23 nwnrbhnesmtk.online

2016/12/24 wafunxdngsfc.online

2016/12/25 ydcvedrxcmym.online

2016/12/26 sggiyqadywsv.online

2016/12/27 ujmnvkyeltfv

2016/12/28 cmhewcvopvno.online

2016/12/29 hrjlyymassqx

2016/12/30 xsvftelyclfh

2016/12/31 dxukryyyqnhl.online

Open Questions

Although we can explain most of what we saw in our data, there are still some open questions.

We list them here with a hope to see feedback from the security community.

ID	Name	Identified Sentence
T1069	Permission Groups Discovery	This leads us to speculate that a new mirai variant and new DGA seed is emerging. DGA Domains Generated With Non-zero DGA Seed The new suspicious domain are listed below: And the domains's query patterns are as follows: A detailed study on these domains shows more findings: The L2 domains conform to mirai DGA, 12 characters, a-y only.
T1018	Remote System Discovery	This leads us to speculate that a new mirai variant and new DGA seed is emerging. DGA Domains Generated With Non-zero DGA Seed The new suspicious domain are listed below: And the domains's query patterns are as follows: A detailed study on these domains shows more findings: The L2 domains conform to mirai DGA, 12 characters, a-y only.
T1068	Exploitation for Privilege Escalation	Note that almost all these domains are registered by mirai author, with the exception 18/19/27/29/30 on which the algorithm itself can not generated a functional DGA domain. 2016/12/08 pcrpxewicouh.online 2016/12/09 rwoywonuobcr.online 2016/12/10 liusqxocbedg.online 2016/12/11 ndoiabgxgmew.online 2016/12/12 hwjqtwkectlo.online

		2016/12/13 mtoyrjnvlqdx.online 2016/12/14 ddfqdttkmoyv.online 2016/12/15 iaxjxyqjckqi.online 2016/12/16 nuuxndqlhiwb.online 2016/12/17 pxvmqwpemiif.online 2016/12/18 dfftxpajygxy 2016/12/19 fiotbgopgnxv 2016/12/20 shjwhbdgjyba.online 2016/12/21 xmjvlucdsegk.online 2016/12/22 irkbpugkwsir.online 2016/12/23 nwnrbhnesmtk.online 2016/12/24 wafunxdngsfc.online 2016/12/25 ydcvedrxcmym.online 2016/12/26 sggiyqadywsv.online 2016/12/27 ujmnvkyeltfv 2016/12/28 cmhewcvopvno.online 2016/12/29 hrjlyymassqx 2016/12/30 xsvftelyclfh 2016/12/31 dxukryyyqnhl.online Open Questions Although we can explain most of what we saw in our data, there are still some open questions.