

Mirai 僵尸网络恶意程序分析和监测数据研究

陈亚亮^{1,2}, 戴沁芸², 吴海燕², 魏征²

(1. 上海交通大学信息安全工程学院, 上海 200240;

2. 国家计算机网络应急技术处理协调中心上海分中心, 上海 201315)

摘要: 近年来, 随着物联网的兴起, 以僵尸网络为代表的恶意程序正在逐渐向物联网领域渗透, 已经出现利用物联网脆弱的安全防护进行传播并发动拒绝服务攻击的恶意代码。首先介绍了 Mirai 僵尸网络的整体架构, 对其受控端和控制端等多个组件的主要功能进行了研究; 然后对通过主动和被动方式获取的监测数据展开分析, 并在此基础上, 对 Mirai 僵尸网络恶意程序的监测发现和应对建议进行了讨论。

关键词: 僵尸网络; 恶意程序; Mirai; Shodan; TR-064

中图分类号: TP309.5

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00181

Research on the reverse analyses and monitoring data of Mirai malware botnet

CHEN Ya-liang^{1,2}, DAI Qin-yun², WU Hai-yan², WEI Zheng²

(1. School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240, China;

2. Shanghai Branch, Coordination Center of China, National Computer Network Emergency Response Technical Team, Shanghai 201315, China)

Abstract: In recent years, with the rapid development of Internet of things(IoT), malwares have come into Internet of things, and botnet is the typical one. Malwares spreading through IoT vulnerable devices have emerged. The overall structure of Mirai botnet and the function of its components were introduced, such as bots and C&C server. The monitoring data obtained through active and passive way were analyzed. Based on that, the discovery methods and response modes on such kind of botnet malwares were discussed.

Key words: botnet, malware, Mirai, Shodan, TR-064

1 引言

僵尸网络是由大量被僵尸程序感染的受控端设备(Bot)和由攻击者管理的控制服务器(C&C)组成的攻击网络。僵尸网络恶意程序由来已久, 其融合了木马的植入和控制技术、蠕虫的大范围传播感染技术, 从历史上看, 可以将其分为以 IRC 协议^[1]进行通信的初创阶段、以 HTTP 和 P2P 进行通信的发展阶段、以 Domain Flux^[2]和 URL Flux^[3]等技术为代表的对抗阶段, 以及移动互联网设备和物联网为主要攻击目标的融合阶段。

Mirai 僵尸网络恶意程序是融合阶段的重要代表, 该恶意程序及其变种直接导致了 2016 年底美国和德国的大规模网络瘫痪。

为了掌握 Mirai 僵尸网络的攻击态势, 遏制其在中国境内的蔓延, 国家计算机网络应急技术处理协调中心上海分中心(简称“上海互联网应急中心”)在国家计算机网络应急技术处理协调中心(简称“国家互联网应急中心”)的指导下深度参与上海地区 Mirai 僵尸网络的应急处置工作。本文结合国家互联网应急中心及上海互联网应急中心应急支撑体系前期的技术积累及工作,

收稿日期: 2017-06-13; 修回日期: 2017-06-29。通信作者: 陈亚亮, dcreg2013@163.com

从源代码及样本、变种演化情况、多方监测数据等多个维度展开分析,并结合处置方式提出应对建议。

1.1 攻击情况概述

2016年10月21日上午,美国互联网域名解析服务商 Dyn 公司遭遇大规模拒绝服务攻击,攻击流量高达 1.2 Tbit/s,造成包括 Twitter、Facebook、Paypal、GitHub、华尔街日报网站在内的大量网站域名无法被正确解析,从而导致用户无法登录系统或访问站点。这一事件的元凶之一,就是被称为 Mirai 的僵尸网络。

2016年11月28日,德国电信遭遇大范围网络故障,约 90 万台路由器无法联网。德国电信确认问题后,要求设备供应商提供新的固件升级包,建议用户断电重启路由器,并安装固件升级包,德国电信还采取了一系列的过滤措施保证升级过程不受攻击影响。该攻击为 Mirai 恶意程序变种导致,在相关感染的样本中发现了与 Mirai 僵尸网络恶意程序相同的代码。

1.2 事件时间线

2016年8月31日,安全博客 MalwareMustDie 发布了一篇关于 Mirai 恶意程序的逆向分析报告^[4],Mirai 僵尸网络第一次进入公众视野。

2016年9月30日,Hackforums 的论坛用户“Anna-senpai”放出了 Mirai 的源码^[5],称受感染的物联网设备正在被缓慢清理,其手上的僵尸网络规模已经下降到 30 万台主机。

2016年10月21日,美国域名服务商 Dyn 遭受大规模 DDoS 攻击,造成包括 Twitter、Facebook 在内的多家美国网站无法被正确解析,进而造成半个美国的网络瘫痪。

2016年11月7日,安全研究员 Kenzo 发布了一个针对 7547 端口上路由器等设备的 TR-069/TR-064 相关的安全公告^[6]。

2016年11月28日,德国电信累积约 90 万个路由器遭受 Mirai 僵尸网络新变种的攻击,网络大面积瘫痪。

2017年2月8日,俄罗斯杀毒软件制造商 Dr. Web 发布了 Windows 版本的 Mirai 恶意程序的分析报告^[7],该变种可以感染 Windows 平台主机微软主机和嵌入式 Linux 系统的物联网设备。

1.3 影响范围及危害

由于 Mirai 僵尸网络恶意程序影响范围广、潜在危害大,该恶意程序在未来的 1~2 年会一直得到广泛关注。

Mirai 僵尸网络恶意程序的攻击目标包括所有主流的操作系统,从嵌入式设备的 Linux 操作系统到桌面服务器的 Windows 操作系统,覆盖面广泛。攻击向量也从最先的单纯弱口令扫描逐渐演化到利用应用漏洞进行攻击。无论是从攻击目标看,还是从攻击范围看,Mirai 僵尸网络恶意程序的影响范围都是巨大的。

随着物联网的兴起,拒绝服务攻击作为一种传统的互联网攻击手段,正在逐渐向物联网领域渗透。根据 Gartner 公司的统计^[8],2016年,全球物联网设备数量为 63.8 亿台,预计 2020 年将达到 204 亿台。而 Mirai 僵尸网络规模仅利用 3×10^4 余台受控端发出的攻击流量就能达到 1 Tbit/s 的攻击流量,如果未来大规模的物联网设备感染类似恶意程序,形成僵尸网络,造成的攻击流量足以令全球互联网瘫痪。

2 恶意程序分析

本节依据恶意程序制作者通过网络论坛发布并上传到 Github 的源代码,对 Mirai 僵尸网络恶意程序代码进行静态分析,同时编译部分代码并模拟运行,对动态运行结果进行跟踪,最终整合动态和静态分析情况,完成对 Mirai 僵尸网络恶意程序的分析。

2.1 原始恶意程序分析

2.1.1 整体架构

Mirai 僵尸网络恶意程序的运行结构可以分为 3 部分:Bot 僵尸网络受控端、Loader 加载服务器、C&C 僵尸网络控制服务器,如图 1 所示,其主要功能如下。

Bot 僵尸网络受控端:实现反调试、隐藏自身进程、设置初始的域名端口值、设置默认弱口令、网络连接及 DDoS 攻击功能。

Loader 加载服务器:登录被爆破的脆弱主机,加载并运行引导程序,下载 Mirai 主程序实现恶意程序的植入。

C&C 僵尸网络控制服务器:对成功感染的 Bot

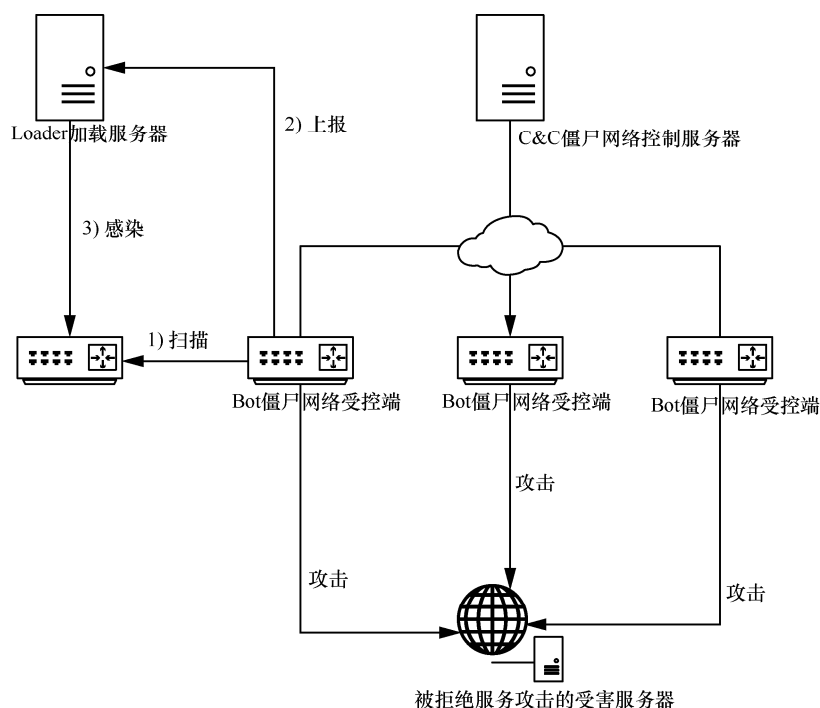


图 1 Mirai 僵尸网络恶意程序整体架构

进行监控，僵尸网络使用者通过控制接口向 Bot 下发攻击指令，控制僵尸网络发动 DDoS 攻击。

2.1.2 僵尸网络受控端分析

僵尸网络受控端的主要功能是扫描潜在开放 Telnet 网络服务的设备，将成功破解的设备地址、用户名、密码等信息上报给攻击者，接受 C&C 僵尸网络控制服务器的命令发起攻击，其代码划分为以下几个模块。

1) 主函数模块

主函数模块主要完成防止设备重启、防止多实例运行、受控端上线并保持连接等功能。

Mirai 僵尸网络恶意程序的感染目标主要为物联网的嵌入式设备，因此恶意程序无法将自身写入设备固件中，只能存在于内存中，一旦设备重启，恶意程序就会消失。嵌入式设备重启功能主要通过“看门狗”程序^[9]实现，在设备正常运行时，需要不断向该程序发送确认消息；而运行异常时，通过向该程序发送控制指令，即可命令设备重启。Mirai 僵尸网络恶意程序通过向“看门狗”程序发送控制码 0x80045704 防止设备异常重启。

Mirai 恶意程序会尝试绑定并监听 48101 端口，如果失败，便会关闭已经使用此端口的进程并重新尝试，从而形成一种互斥机制，防止同一

个设备上运行多个实例，这也是检测是否感染 Mirai 恶意程序的重要方法。

在完成独占运行、攻击初始化等步骤后，Bot 僵尸网络受控端会连接 C&C 僵尸网络控制服务器，在僵尸网络中上线；未收到控制服务器的攻击指令时，Bot 默认每隔 60 s 与控制服务器沟通一次。

2) attack 模块

attack 模块主要用于解析 C&C 控制服务器下发的攻击命令并发动拒绝服务攻击，具体攻击函数如表 1 所示。

表 1 攻击函数		
攻击函数	发包方式	源 IP 地址情况
attack_udp_generic	原始套接字发包	伪造源 IP
attack_udp_vse	原始套接字发包	伪造源 IP
attack_udp_dns	原始套接字发包	真实源 IP
attack_udp_plain	完整协议栈发包	真实源 IP
attack_tcp_syn	原始套接字发包	伪造源 IP
attack_tcp_ack	原始套接字发包	伪造源 IP
attack_tcp_stomp	原始套接字发包	真实源 IP
attack_gre_ip	原始套接字发包	伪造源 IP
attack_gre_eth	原始套接字发包	伪造源 IP
attack_app_http	完整协议栈发包	真实源 IP

3) scanner 模块

scanner 模块主要功能是扫描其他可能受感染的设备，具体流程为：首先生成随机 IP，然后随机选择字典中的用户名密码组合进行 telnet 登录测试，如果扫描的随机 IP 有回应，则建立正式连接，并上报成功的扫描结果，表 2 展示字典中的用户名密码组合。

表 2 用户名密码组合

用户名/密码	用户名/密码	用户名/密码
root/x3511	admin/1111	root/zlxx.
root/vizxv	root/666666	root/7ujMko0vizxv
root/admin	root/password	root/7ujMko0admin
admin/admin	root/1234	root/system
root/888888	root/klv123	root/ikwb
root/xmhdipc	Administrator/admin	root/dreambox
root/default	service/service	root/user
root/juantech	supervisor/supervisor	root/realtek
root/123456	guest/guest	root/0
root/54321	guest/12345	admin/111111
support/support	guest/12345	admin/1234
root/(none)	admin1/password	admin/12345
admin/password	administrator/1234	admin/54321
root/root	666666/666666	admin/123456
root/12345	888888/888888	admin/7ujMko0admin
user/user	ubnt/ubnt	admin/1234
admin/(none)	root/klv1234	admin/pass
root/pass	root/Zte521	admin/meinsm
admin/admin1234	root/hi3518	tech/tech
root/1111	root/jvbzd	mother/fucker
admin/smcadmin	root/anko	

4) killer 模块

killer 模块主要有 2 个作用：一是查找特定端口对应的进程并将其关闭，然后占用该端口；二是查找特定进程的对应路径，并删除文件。

2.1.3 加载服务器分析

Bot 僵尸网络受控端扫描后的结果会发送到扫描结果接收服务器，经处理后将具体设备信息以特定格式传递给 Loader 加载服务器，对设备实施感染，感染过程主要包括以下几步。

1) 通过待感染节点的 telnet 用户名和密码成

功登录。

2) 执行“/bin/busybox ps”命令，根据返回结果关闭某些特殊进程。

3) 执行“/bin/busybox cat /proc/mounts”，根据返回结果切换到可写目录。

4) 如果发现可用于读写的文件目录，进入该目录并将“/bin/echo”复制到该目录，文件更名为 dvrHelper，并开启所有用户的读写执行权限。

5) 执行“/bin/busybox cat /bin/echo”，通过返回结果解析“/bin/echo”这个 ELF 文件的头部判断体系架构，即其中的 e_machine 字段。

6) 根据不同的体系架构，选择一种方式上传对应的恶意程序文件。

7) 执行恶意程序并清理。

2.1.4 僵尸网络控制服务器分析

C&C 僵尸网络控制服务器的主要功能是向僵尸网络管理员提供管理界面，向付费用户提供登录界面和发动快速攻击的应用接口。

图 2 展示了管理员和付费用户登录僵尸网络控制台的业务流程。

管理员登录成功后可以添加用户、设置分配给普通用户的受控端数量、发动攻击；普通用户登录成功后只可以发动攻击。

付费用户还可以通过 telnet 访问 101 端口的应用接口发动快速攻击。

2.2 变种恶意程序分析

2.2.1 技术背景

一般分配 TR-069 协议（CPE WAN management protocol）给互联网上的 TCP/7547 端口，ISP 利用该协议对用户侧设备进行远程管理^[10]，完成诸如服务开通、功能设定、系统检测等运维操作。

然而，7457 端口同时还可以运行 TR-064 协议（LAN-side CPE configuration），该协议允许用户通过 LAN 侧的管理软件对 ISP 提供的路由器进行配置。

TR-069 协议和 TR-064 协议分别运行在路由器的 WAN 口和 LAN 口。当路由器的 WAN 口允许接收并响应 TR-064 协议请求时，会导致严重的安全漏洞，攻击者可以通过互联网远程配置该路由器，配置命令包括获取设备信息、获取 Wi-Fi

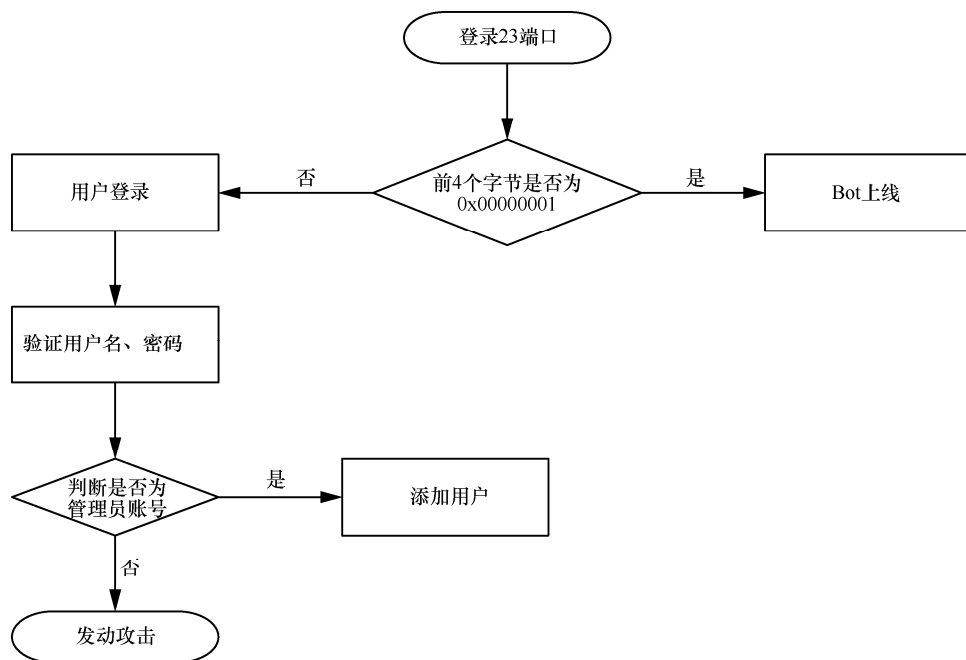


图2 登录僵尸网络控制台流程

密码、获取 SSID 和 MAC 地址、设置 NTP 服务器。

而 TR-064 协议在设置 NTP 时间服务器时存在命令注入漏洞, 攻击者通过发送符合 TR-064 协议格式要求的数据分组, 可以执行任意命令, 如 “busybox iptables -I INPUT -p tcp --dport 80 -j ACCEPT”。

2.2.2 变种特点

在德国电信断网事件的捕获样本中发现了与 Mirai 相同的代码, 但该变种也有自己的特征。

1) 利用 7547 端口进行传播

对随机生成的 IP 地址进行扫描, 并向目标主机发送包含攻击代码的数据分组, 攻击代码的主要功能是下载针对不同平台的恶意代码。

2) 绑定并监听 31517 端口

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。

3) 精简弱口令列表

对弱口令列表进行精简, 通过 3 组弱口令进行 telnet 弱口令扫描。

2.2.3 后续演进情况

1) 使用域名生成算法

2016 年 12 月 9 日, 奇虎 360 公司 Netlab 网络安全研究实验室发现部分利用 TR-064 协议漏洞传播的 Mirai 恶意程序变种样本中包含域名生

成算法^[11], 用于生成 CNC 僵尸网络控制服务器备用域名, 其主要特征如下。

① 使用 3 个顶级域名: online/tech/support。

② L2 域名固定长度 12 字符, 每个字符在 “a” ~ “z” 随机选择。

③ 域名仅由月、日和硬编码的种子字符串确定。

④ 每天只生成一个域名, 因此最多存在 365 个 DGA 域名。

⑤ DGA 域名仅在硬编码的 C2 域名无法解析时使用。

2) 感染 Windows 平台

2017 年 2 月 6 日, 俄罗斯杀毒软件制造商 Dr. Web 捕获了 Windows 版本的 Mirai 恶意程序, 可以感染 Windows 平台微软主机和嵌入式 Linux 系统的物联网设备, 主要扫描如下端口: 22、23、135、445、1433、3306、3389。

除 3389 以外的所有端口, 均会执行配置文件中的相关命令, 如添加数据库用户、获取恶意程序、写入文件等。

3 数据获取及分析

本节阐述上海互联网应急中心通过主动和被动这 2 种方式获取 Mirai 僵尸网络监测数据, 并对受控端和控制端分别展开数据分析。

3.1 数据获取

Mirai 僵尸网络监测发现的方式分为主动监测与被动监测。

主动监测数据可以利用 Mirai 扫描模块中的特征值,通过检查 SYN 包的包头,从 TCP/23 端口的扫描流量中识别出 Mirai 恶意程序发出的扫描流量。这类监测数据的主要来源为上海互联网应急中心应急服务支撑单位的上报数据。

被动监测数据则是利用国家互联网应急中心某技术平台,将 Mirai 僵尸网络通信流量中指纹特征配入系统,开展相应监测。具体指纹特征包括端口特征和报文特征,端口特征指 Mirai 恶意程序会监听 48101 端口,报文特征如表 3 和表 4 所示。

表 3 Bot 上线报文特征

发送方	协议	数据
Bot	telnet	\x00\x00\x00\x01
CNC	tcp	ack
Bot	telnet	\x00
CNC	tcp	ack

表 4 心跳链接报文特征

发送方	协议	数据
Bot	telnet	\x00\x00
CNC	telnet	\x00\x00
Bot	tcp	ack

3.2 主动监测数据分析

3.2.1 受控端监测情况

1) IP 地址统计

奇虎 360 公司 Netlab 网络安全研究实验室开放数据项目 (Netlab open data project) 建立了 Mirai 僵尸网络监测页面,实时呈现 Mirai 僵尸网络的发展演变情况。

截至 2017 年 3 月 31 日,根据该监测页面提供的信息,通过统计 Mirai 僵尸网络恶意程序及其变种的扫描行为,累计发现 Bot 受控端 IP 地址 2 291 661 个,其中,中国排名第一,Bot 受控端 IP 地址共计 456 026 个。

从 Bot 受控端的活跃情况来看,2017 年 3 月 31 日当日的活跃扫描 IP 为 9 329 个,且自 2017 年 1 月 25 日起,当日活跃扫描 IP 均在 2×10^4 个以下。

2) 感染设备情况

知道创宇 ZoomEye 平台^[12]对公开的 Mirai 僵尸网络扫描数据列表中 62 961 个独立 IP 地址的 Banner 信息进行了统计,选取 Dyn 公司遭到攻击前后 2016 年 7 月 18 日和 10 月 25 日这 2 个时间点,分析得出感染 Mirai 僵尸网络的设备端口、设备类型、运行服务等情况。

Mirai 僵尸网络主要扫描攻击端口为 23,检索该端口在 Dyn 公司遭到攻击前后的变化情况,发现在 62 961 个独立 IP 地址中,8 454 个 IP 地址的 23 端口被关闭,1 010 个地址的端口被打开,整体趋势与 Mirai 恶意程序关闭 23 端口的行为特征相符。

1 898 个 IP 可以识别出准确的设备类型,主要感染设备为路由器、媒体设备和摄像头,排名前 10 的设备类型如表 5 所示。

表 5 排名前 10 的设备类型

设备类型	数量
Broadband router	698
Media device	406
Router	266
Webcam	243
WAP	219
Bridge	24
Firewall	17
Printer	9
Storage-misc	5
Switch	5

识别出 270 种服务类型,主要服务类型为 uc-httpd、Busybox telnetd 和 Portable SDK for UPnP devices,排名前 10 的服务类型如表 6 所示。

表 6 排名前 10 的服务类型

服务类型	数量
uc-httpd	5 040
Busybox telnetd	2 884
Portable SDK for UPnP devices	1 364
gSOAP soap	1 269
Allegro RomPager	923
mini_httpd	546
Q-SEE DVR telnetd	533
Dropbear sshd	370
micro_httpd	342
SNMPv1 server	297

3) 潜在影响范围

重点考察 23 端口的 Banner 信息在 2016 年 7 月和 2016 年 10 月这 2 个时间点的变化情况, 可以发现 2016 年 7 月 18 日最多的 Banner 信息为“LocalHost login”和“(none) login”, 其数量变化情况如表 7 所示。

设备类型	7 月数量	10 月数量
LocalHost login	4 871	110
(none) login	1 357	360

由表 7 可以看到 Banner 数量大幅下降, 可以推断 23 端口的 Banner 信息为这 2 条的设备, 极有可能会感染 Marai 恶意程序, 如果以这 2 条 Banner 信息作为查询条件, 在 4 个常见的网络空间搜索引擎中进行搜索(截至 2017 年 4 月 9 日), 可以得到如表 8 所示地址数量。

类型	ZoomEye	Shodan	Censys	FOFA
LocalHost login	155 674	41 130	4 560 591	297
(none) login	1 859 616	415 615	30 525 889	26 108

因不同搜索引擎的扫描和数据处理机制存在差异, 如 ZoomEye 会对多次扫描得到的数据进行累计, 而 Shodan^[13]则会直接更新数据, Censys^[14]每周会对 23 端口进行扫描, FOFA^[15]建立时间最短, 导致上述统计的 IP 地址数量差异较大, 实际影响范围还需要在全量数据基础上做进一步核实验证。

3.2.2 控制服务器监测情况

根据奇虎 360 公司 Netlab 网络安全研究实验室开放数据项目的 Mirai C2 监测页面提供的信息, 截至 2017 年 4 月 9 日, 累计发现 C&C 控制服务器 IP 地址 204 个, 其中, 美国排名第一, C&C 控制服务器 IP 地址共计 43 个; 累计下发攻击命令 1 577 363 条, 攻击目标 11 748 个, 攻击方式排名前 3 的分别为 udp_flood、tcp_stomp 和 http_flood。

从活跃情况来看, 2017 年 3 月 31 日的活跃 CNC 控制服务器 IP 地址 16 个, 下发攻击命令 1 720 条, 且近 3 个月内的大部分时间控制服务器

IP 地址少于 20 个, 攻击命令少于 2 000 条。

3.3 被动监测数据分析

国家互联网应急中心利用某技术平台对 Mirai 僵尸网络数据进行排查, 发现受控端 IP 地址数据中涉及全国范围内的 IP 地址 5 681 个, 其中上海地区 IP 地址 210 个。

上海互联网应急中心按照国家互联网应急中心要求, 协调上海地区基础运营企业对 IP 地址的线路类型、是否为物联网设备等情况进行核查, 发现 80%以上 IP 地址的线路类型均为拨号用户。

同时, 利用技术手段对地址 telnet 端口的 Banner 信息进行查询, 得到 Banner 信息 70 条, 具体 Banner 信息情况如表 9 所示, 其中“XL_MINER_dddd login:”中的 dddd 为 4 位数字, “dvrds login:”可以确认为海康威视的监控设备。

Banner 信息	IP 地址数量	分布占比
XL_MINER_dddd login:	32	45.7%
dvrds login:	28	40.0%
(none) login:	2	2.9%
BUFFALO INC. LinkStation series login:	2	2.9%
192.0.0.64 login:	1	1.4%
F420Login:	1	1.4%
Hikvision login:	1	1.4%
M28x login:	1	1.4%
sdec login:	1	1.4%
sdha login:	1	1.4%

3.4 数据验证和挖掘

3.4.1 主被动数据重合性验证

上海互联网应急中心对奇虎 360 公司 Netlab 网络安全研究实验室公开的 Mirai 僵尸网络扫描数据进行定位, 确认上海地区 IP 地址 71 个, 其中上海电信地址 58 个、上海联通地址 12 个、上海移动地址 1 个。

与之前国家互联网应急中心的数据进行比对, 发现上海地区数据完全没有重合, 而全国数据也仅有 11 个 IP 地址重合。主被动数据重合度较低, 表明 2 种监测方式在原理机制、监测节点

等方面存在较大差异。

3.4.2 利用技术平台监测发现感染情况

上海互联网应急中心以 Mirai 僵尸网络利用 TR-064 漏洞传播的变种作为检测对象,该变种有扫描 7547 端口并开放 31517 端口的网络特征,本文选取国家互联网应急中心某技术平台上海地区某日的流量数据进行检索,具体排查步骤如下。

1) 查询目的端口为 7547 的流量数据,得到全天流量五元组数据 65 527 条,数据时间均在 22:44:52~23:59:59,时间分布较为聚集。

2) 筛选出源端口为 31517 的数据 2 条,如表 10 所示。

表 10 筛选出的 2 条流量数据				
源地址	目的地址	时间	源端口	目的端口
39.*.*.18	218.*.*.11	23:50:17	31517	7547
58.*.*.74	171.*.*.251	23:32:45	31517	7547

3) 分别提取源地址为 39.*.*.18 和 58.*.*.74 的流量记录,发现 58.*.*.74 有明显的扫描特征,涉及 554 个独立目的 IP 地址,后续如能结合报文数据,可以进一步确认该地址是否为感染 Mirai 恶意程序的变种。

4 应对建议

本文建议从技术和管理方面双管齐下,通过监测系统建设、威胁情报共享等多种方式积极应对 Mirai 僵尸网络。

在技术层面上,国家级应急支撑机构需要对系统监测和互联网公开数据进行关联分析,充分挖掘现有数据价值。同时,还建议积极申请资金,建立和完善恶意代码蜜罐捕获和分析系统。国家互联网应急中心作为协调机构,难以直接获取受害用户设备上的攻击样本,蜜罐系统^[16]可以成为获取恶意代码样本的重要渠道,为僵尸网络动态的实时监测提供重要手段。安全企业则应积极建立互联网网络空间搜索引擎,作为信息获取、漏洞排查的重要工具。

在管理层面上,建议国家级应急支撑机构牵头,参照国际现有标准,统一威胁情报格式,如:在 STIX 规范框架下,借助 CybOX 提供的词汇

描述威胁情报,并利用 TAXII 进行传输^[17],实现重要威胁情报自动化读取和汇总,推进网络安全威胁情报共享体系建设。各安全企业则结合自身实际业务能力,重点跟踪特定方向的威胁情报,形成企业特色,在此基础上实现情报共享。

5 结束语

僵尸网络一直是基础互联网网络安全运行的重大威胁,利用物联网设备开展攻击的 Mirai 僵尸网络已经造成多次严重的国家级互联网瘫痪事件。本文首先对 Mirai 僵尸网络恶意程序的运作机制进行了分析,然后通过数据分析呈现了其运行规模和具体特征,最后给出了针对 Mirai 僵尸网络恶意程序的应对建议。

参考文献:

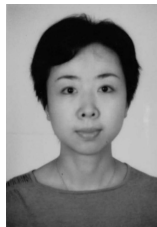
- [1] MCCARTY B. Botnets: big and bigger[J]. IEEE Security & Privacy, 2003, 1(4):87-90
- [2] STONE-GROSS B, COVA M, CAVALLARO L, et al. Your botnet is my botnet: analysis of a botnet takeover[C]//The 16th ACM Conference on Computer and Communication Security. 2009: 635-647.
- [3] CUI X, FANG B X, YIN L H, et al. Andbot: towards advanced mobile botnets[C]//The 4th Usenix Workshop on Large-scale Exploits and Emergent Threats. 2011: 11.
- [4] Linux/Mirai. How an old ELF malware is recycled[EB/OL]. <http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html>.
- [5] World's largest net: mirai botnet, client, echo loader, CNC source code released[EB/OL]. <https://hackforums.net/showthread.php?tid=5420472>.
- [6] Eir's D1000 modem is wide open to being hacked[EB/OL]. <https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/>.
- [7] Trojan.Mirai.1 [EB/OL].<https://vms.drweb.com/virus/?i=14934685&lng=en>.
- [8] Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016[EB/OL]. <http://www.gartner.com/newsroom/id/3598917>.
- [9] 汪胜聪, 滕勤, 左承基. 综述单片机控制系统的抗干扰设计[J]. 现代电子技术, 2003, 1: 7-9.
WANG S C, TENG Q, ZUO C J. Statement of an-ti-disturbance design in the micro-controller system[J]. Modern Electronic Technique, 2003, 1:7-9.
- [10] 吴春敏. 基于 TR-069 协议的远程配置管理终端的研究与实现[D]. 成都: 西南交通大学, 2006.
WU C M. Research and implementation of remote configuration management terminal base in TR-069 protocol[D]. Chengdu: Southwest Jiaotong University, 2006.
- [11] 张雪松, 徐小琳, 李青山. 算法生成恶意域名的实时检测[J]. 现代电信科技, 2013, 7: 3-8.
ZHANG X S, XU X L, LI Q S. The real-time detection of algo-

- rithmically generated malicious domain[J]. Modern Science & Technology of Telecommunications. 2013, 7: 3-8.
- [12] 钟馗之眼. 网络空间搜索引擎[EB/OL]. <https://www.zoomeye.org/>.
ZoomEye. Cyberspace Search Engine[EB/OL]. <https://www.zoomeye.org/>.
- [13] Shodan[EB/OL]. <https://www.shodan.io/>.
- [14] Censys[EB/OL]. <https://www.censys.io/>.
- [15] FOFA Pro .网络空间安全搜索引擎[EB/OL]. <https://fofa.so/>.
FOFA Pro. The cyberspace search engine[EB/OL]. <https://fofa.so/>.
- [16] FREILING F, HOLZ T, WICHERSKI G. Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks[C]//The 10th European Symposium on Research in Computer Security (ESORICS 2005). 2005: 319-335.
- [17] LI J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space[J]. Chinese Journal of Network and Information Security, 2016, 2(2):16-29.

作者简介:



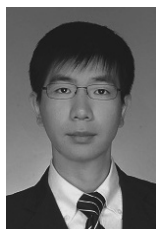
陈亚亮 (1988-), 男, 上海人, 国家计算机网络应急技术处理协调中心工程师, 主要研究方向为网络安全、移动互联网恶意程序。



戴沁芸 (1977-), 女, 湖北武汉人, 博士, 国家计算机网络应急技术处理协调中心高级工程师, 主要研究方向为网络安全、移动互联网。



吴海燕 (1989-), 女, 江苏启东人, 国家计算机网络应急技术处理协调中心工程师, 主要研究方向为网络安全。



魏征 (1986-), 男, 江苏苏州人, 国家计算机网络应急技术处理协调中心工程师, 主要研究方向为恶意程序分析。