关于 Mirai 变种 Miori 僵尸网络大规模传播的风险提示

本报告由国家互联网应急中心（CNCERT）与奇安信科技集团股份有限公司（奇安信）共同发布。

一、 概述

近期，CNCERT 和奇安信共同监测发现一个新的且在互联网上快速传播的 DDoS 僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以 IP 数计算）最多已超过 1 万、且每日会针对多个攻击目标发起攻击，给网络空间带来较大威胁。该僵尸网络为 Mirai 变种，包括针对 mips、arm、x86 等 CPU 架构的样本，由于该僵尸网络样本均以 miori 命名，我们将其命名为 Mirai_miori。在 2 个月的时间中，我们捕获到 Mirai_miori 僵尸网络样本至少迭代过 3 个版本，具有 9 个传播源，涉及 6 个 C2 服务器，传播方式主要为弱口令爆破以及 1 day 和 N day 漏洞。Mirai_miori 僵尸网络出现以来所投递的样本变动很小，运营者将主要精力投入到漏洞搜集利用以及更换 C2 服务器上。

二、 僵尸网络分析

（一）相关样本分析

本文选取 V2 ARM CPU 架构的样本为主要的分析对象，

样本的基本信息如下：

文件名	miori
MD5	bfb42bb1a4b0278bf2550e943a6c9f9e
文件格式	ELF 32-bit LSB executable ARM
C2	2.56.56.162

1、样本运行后在控制台上输出以下内容“your device just got infected to a bootnoot”，并修改进程名为" "

```
v24 = ((int (__fastcall *)(int, int *))sub_C4F0)(1, &v67);
_libc_write(1, v24, v67);
_libc_write(1, "\n", 1);
encode(1u);
strcpy(v61, "  ");
memset(&v61[3], 0, 97);
v25 = prctl(15, v61);
```

图 1　样本运行信息

2、遍历/proc/目录下的文件，结束掉指定进程。

```
_GI_strcpy(v32, "/proc/");
_GI_strcat(v32, v9);
_GI_strcat(v32, "/maps");
_GI_strcpy(v30, "/proc/");
_GI_strcat(v30, v9);
_GI_strcat(v30, "/exe");
_GI_strcpy(v33, "/proc/");
_GI_strcat(v33, v9);
_GI_strcat(v33, "/comm");
_GI_strcpy(v29, "/proc/");
_GI_strcat(v29, v9);
_GI_strcat(v29, "/cwd");
v11 = _GI_readlink(v30, v31, 63);
```

图 2　结束指定进程

3、Mirai_miori 变种对 mirai 的上线机制进行了修改。第一个包是固定四字节\x03\x00\x02\x01，第二个包是样本运行参数长度+运行参数，缺省为\x00，一般在 shell 脚本里指定，

之后每 60s 发送固定 2 字节心跳包\x00\x00，若 10 秒内有收到 C2 下发的非心跳指令，则心跳包间隔时间会相应增加。

```
    else
    {
      v48 = strlen(v62);
      LOBYTE(v68[0]) = v48;
      dword_1A2E4 = ((int (__fastcall *)(int))get_localaddr)(v48);
      _libc_send(dword_1A024, &unk_11760, 4, 0x4000);
      _libc_send(dword_1A024, v68, 1, 0x4000);
      if ( LOBYTE(v68[0]) )
        _libc_send(dword_1A024, v62, LOBYTE(v68[0]), 0x4000);
    }
  }
}
while ( dword_1A024 == -1
```

图 3　上线机制

4、DDoS 攻击方法，样本内置了 8 种 DDoS 攻击，部分 DDoS 攻击复用了 mirai 的源码。

攻击方法名称	含义	特点
tcp_stomp	ack flood 攻击变体	高 BPS
tcp_syn	半开连接攻击，耗尽服务器资源	高 BPS
tcp_ack	在 tcp 连接建立之后，发送带有 ack 标志位的数据包。	高 BPS
udp_plain	udp flood 攻击变体	高 BPS
gre_ip	修改的 greeth flood	高 BPS
gre_eth	基于 GRE 协议的洪水攻击	高 BPS
udp_ves	基于 UDP 的洪水攻击	针对受 OVH 保护的服务器
tcp_plain	修改的 tcp flood	高 BPS
tcp_stomp	ack flood 攻击变体	高 BPS

```
{
  add_attack(0, tcp_stomp);
  add_attack(7, tcp_plain);
  add_attack(6, udp_ves);
  add_attack(4, gre_ip);
  add_attack(3, udp_plain);
  add_attack(1, tcp_syn);
  add_attack(2, tcp_ack);
  add_attack(5, gre_eth);
  return 1;
}
```

图 4　攻击方式

（二）传播方式分析

Mirai_miori 变种可以分为三个版本，运营者通过增加漏洞数量并积极利用 1 day 漏洞来扩大僵尸网络规模。以 CVE-2022-29591 漏洞为例，该漏洞首次披露于今年 5 月 10 日，我们在 5 月 17 日即捕获到该漏洞利用的流量，可见该僵尸网络运营人员对新漏洞具有较高的敏感性并具有一定的漏洞利用能力。

V1 版本	内容	备注
样本自传播方式	telnet 爆破 23，2323	XOR 加密，密钥：0x62
传播源服务器攻击方式	telnet 爆破 23，2323	
	ssh 爆破 22，2222	
	CVE-2017-9100	
	CVE-2017-17215	
	CVE-2019-11399	
C2	142.93.229.199	
传播源	142.93.229.199 37.0.11.168	
传播时间推测	2022 年 4 月 6 日至 5 月 17 日	

V2 版本	内容	备注
样本自传播方式	telnet 爆破 23，2323	XOR 加密，弱口令增多，密钥不变
	ssh 爆破 22，2222	

传播源服务器攻击方式	telnet 爆破 23，2323	
	CVE-2017-9100	
	CVE-2022-29591	
	D-Link DIR-823G v1.02 B05 命令注入漏洞	
	CVE-2019-11399	
	Hadoop Yarn REST API 未授权漏洞利用	
	Android Debug Bridge 5555	
C2	2.56.56.162 142.93.229.199 46.19.137.50 195.58.38.253 31.7.58.162	
传播源	2.56.56.162 185.28.39.119 46.19.137.50 195.58.38.253 194.31.98.205 31.7.58.162	
传播时间推测	2022 年 4 月 13 日至今	

V3 版本	内容	备注
样本自传播方式	telnet 爆破 23，2323	XOR 加密，弱口令增多，密钥改为 0x3
传播源服务器攻击方式	ssh 爆破 22，2222	
	CVE-2022-22965	
	telnet 爆破 23，2323	
	NetCore 53413 后门漏洞	
	CVE-2022-29591	
	CVE-2017-9100	
	CVE-2017-17215	
	CVE-2022-29464	
	D-Link DIR-823G v1.02 B05 命令注入漏洞	
	CVE-2021-35395	
	Hadoop Yarn REST API 未授权漏洞利用	
C2	179.43.156.214	
传播源	179.43.156.214	
传播时间推测	2022 年 4 月 28 日至今	

运营者所使用的漏洞信息：

漏洞	简介
CVE-2017-9100	身份认证绕过漏洞，受影响设备为固件版本为 3.04 的 D-Link DIR-600M 设备。
CVE-2017-17215	华为 HG532 部分定制版本存在远程代码执行漏洞。攻击者通过向 37215 端口发送恶意数据包，成功利用可以导致远程代码执行。
CVE-2019-11399	命令注入漏洞，受影响设备 TRENDnet TEW-651BR 2.04B1、TEW-652BRP 3.04b01 和 TEW-652BRU 1.00b12 。
CVE-2021-35395	Realtek Jungle SDK v2.x 至 v3.4.14B 版本中存在缓冲区溢出漏洞。
CVE-2022-29591	缓冲区溢出漏洞，受影响设备 Tenda TX9 Pro 22.03.02.10。
CVE-2022-22965	远程代码执行，在 JDK 9+ 上运行的 Spring MVC 或 Spring WebFlux 应用程序都可能遭受攻击。
CVE-2022-29464	未经身份验证的无限制任意文件上传漏洞，允许未经身份验证的攻击者通过上传恶意 JSP 文件在 WSO2 服务器上获得 RCE。
D-Link DIR-823G v1.02 B05 命令注入漏洞	攻击者可以通过 POST 的方式往 /HNAP1 发送精心构造的请求，执行任意的操作系统命令。
Hadoop Yarn REST API 未授权漏洞利用	攻击者可以在未授权的情况下远程执行代码
NetCore 53413 后门漏洞	netcore/netis 路由器会默认监听 53413 端口（UDP），发送特定的字符串后，就可以获得 root 权限登录。
Android Debug Bridge 5555	5555 端口是安卓 adb 服务默认监听的端口，缺乏认证过程，允许攻击者远程执行代码。

各版本弱口令解密后内容如图 5 所示。

V1		V2		V3	
root		root		root	icatch99
default		root	root	root	Zte521
admin	admin	Admin	Admin	qbf77101	hexakisoctahedron
root	vizxv	admin	password	root	changeme
root	default	default		root	taZz@23
e8ehome	e8ehome	ubncT	ubncT	default	OxhlwSG8
e8telnet	e8telnet	root	123456	default	tlJwpbo6
root	ttnet	user	user	default	S2fGqNFs
admin	gpon	root	1234	root	
root	zte	admin	1234	root	root
telecomadmin	admintelecom	admin	admin	Admin	Admin
telnet	telnet	root	vizxv	admin	password
telnetadmin	telnetadmin	root	default	default	
support	support	e8ehome	e8ehome	ubnt	ubnt
root	1001chin	e8telnet	e8telnet	root	123456
admin	aquario	root	ttnet	user	user
default	default	admin	gpon	root	1234
adm		root	zte	admin	1234
root	taZz@23495859	telecomadmin	admintelecom	admin	admin
root	tsgoingon	telnet	telnet	root	vizxv
admin	admin123	telnetadmin	telnetadmin	root	default
root	GM8182	support	support	e8ehome	e8ehome
		root	1001chin	e8telnet	e8telnet
		admin	aquario	root	ttnet
		default	default	admin	gpon
		adm		root	zte
		root	taZz@23495859	telecomadmin	admintelecom
		root	tsgoingon	telnet	telnet
		admin	admin123	telnetadmin	telnetadmin
		root	GM8182	support	support
				root	1001chin
				admin	aquario
				default	default
				adm	adm
				root	taZz@23495859
				root	tsgoingon
				admin	admin123
				root	GM8182

图 5　各版本口令

三、 僵尸网络感染规模

通过监测分析发现，2022 年 4 月 6 日至 6 月 6 日 Mirai_miori 僵尸网络日上线境内肉鸡数最高达到 1.1 万台，累计感染肉鸡数达到 4.4 万。每日境内上线肉鸡数情况如下。

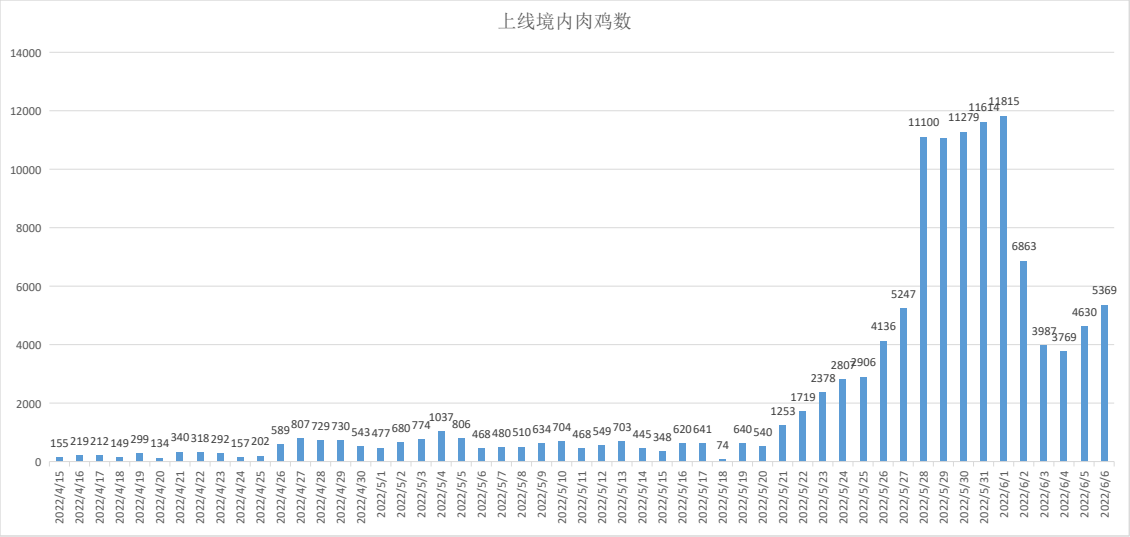
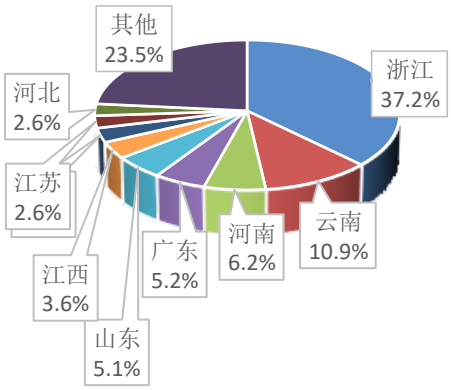


图 6 每日上线境内肉鸡数

Mirai_miori 僵尸网络位于境内肉鸡按省份统计，排名前三位的分别为浙江省（37.2%）、云南省（10.9%）和河南省（6.2%）；按运营商统计，电信占 79.7%，联通占 18.5%，移动占 0.7%。

肉鸡境内分布



肉鸡境内运营商分布

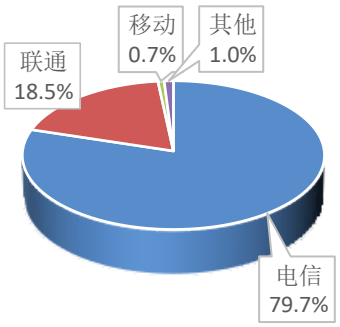


图 7 境内肉鸡按省份和运营商分布

四、 僵尸网络攻击动态

通过跟踪监测发现，Mirai_miori 僵尸网络自 2022 年 4 月 6 日出现起就一直对外发起 DDoS 攻击，后期随着控制规模扩大攻击行为日益活跃。攻击最猛烈的时候是 2022 年 5 月 30 日共对 323 个目标发起 DDoS 攻击，2022 年 5 月 29 日曾先后调动 2.5 千台肉鸡攻击某受害目标。其攻击事件趋势如下：

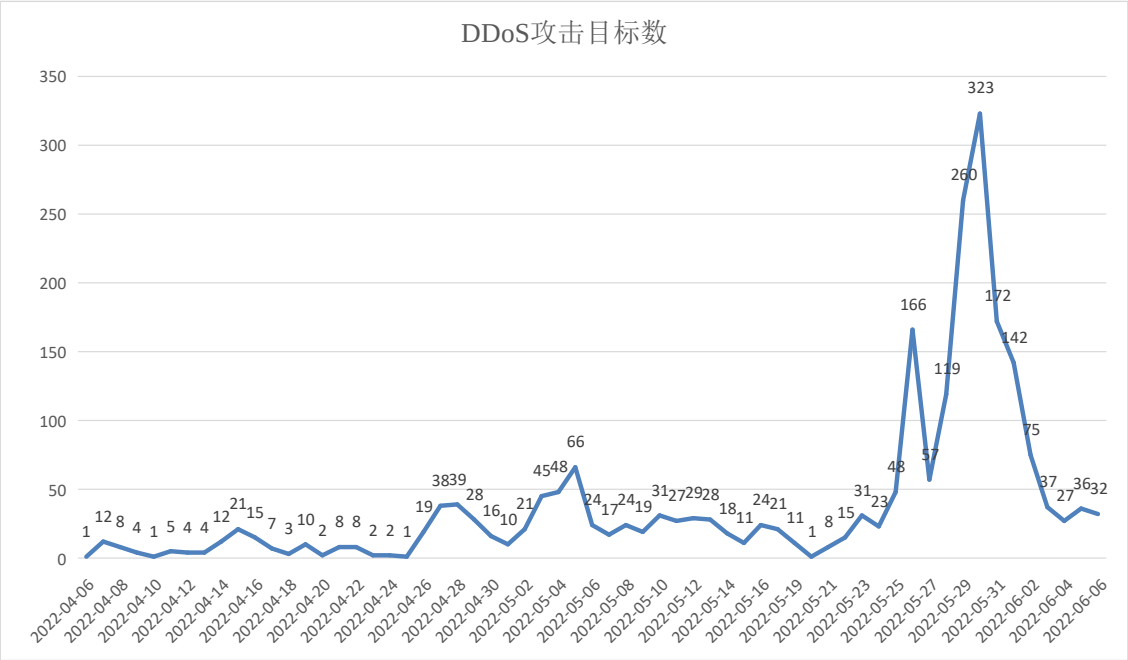


图 8 Mira_miori 变种僵尸网络攻击趋势

五、 防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：1、梳理已有资产列表，及时修复相关系统漏洞。2、不使用弱密码或默认密码，定期更换密码。

当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

六、 相关 IOC

样本 MD5：

fcedf135724d04d3299de41840da76a5

0294aa17e46586e7362cfde7e6f61e90

8ca06dff201e2efb1ef27282e875f720

09e16b247cb5d219252d2eb7185e4cd4

b1243cf53691dbccd3bcd5a5e2dea0ba

60ed67c5fd2c694cbed246c34f1996d4

bb3c7c16d1f045d9e0896dfe3558f794

549470175b5728bef241cd8318978071

2eb59f84503a5504463ea3d0acd21c98

135aab8d2ee4570d3d1f79b06df11202

1e06b8354d0d76b3e1c9f27794c6cc9e

452dc74070b167abb930ef3124ae9172

61fc0a2c42dab8730b074fa9c7ae7875

4d403169e481298767e7de263234094d

495c5cb7782ef8e8e2d0827302326226

c7072c10808b9f34daf54608c16b4165

44fd2a83044d5fe4e28d3d3f7109f7b2

bfb42bb1a4b0278bf2550e943a6c9f9e

93ef6d79bf74fb40a92a3577a2431194

fec708a45aee20dd22e2da807f3530d1

8ce0594eebe794f88f510c87cf1119dd

5bebe8d71b7bdc188efd3b451c27fb41

0225ecf57b8d91bc141c5ca22056016f

ba953ea2800ba05143b84e19bd810e1d

d3d96c71d604533fb9a3d3673f8bd641

88c2450f4158bc3ce8bc038c7923103c

2dc15f9aae304ecfc9aa9cad32dfd19c

683c7986e45b3b5c8840ef73144dfd30

23002f8a2d1900f0108bad51a1f1e124

3a155689509b91304f776015d1fc06cd

b37080f0f495d2e62aa377e4c291847e

39ea839c462d0248d9e7701843852685

b32a1c611ded2169cc5c6e281e5b4c0c

6844313d215b01dc1000e5d52090b6f7

c560ff207426cda72f15077ad841812e

4f87a057edf08576aef4232b87dd5481

9f98eacca243f3b4346e3d586efb91fb

下载链接：

http[:]//142.93.229.199/gaybub/miori.arm

http[:]//179.43.156.214/miori.arm

http[:]//185.28.39.119/gaybub/miori.arm

http[:]//185.28.39.119/gaybub/miori.mips

http[:]//185.28.39.119/miori.mips

http[:]//194.31.98.205/miori.arm

http[:]//194.31.98.205/miori.mips

http[:]//195.58.38.253/gaybub/miori.arm

http[:]//2.56.56.162/gaybub/miori.arm

http[:]//37.0.11.168/gaybub/miori.mips

http[:]//37.0.11.168/miori.arm

http[:]//46.19.137.50/c.sh

http[:]//46.19.137.50/gaybub/c.sh

http[:]//46.19.137.50/gaybub/miori.arc

http[:]//46.19.137.50/gaybub/miori.arm

http[:]//46.19.137.50/gaybub/miori.arm5

http[:]//46.19.137.50/gaybub/miori.arm6

http[:]//46.19.137.50/gaybub/miori.arm7

http[:]//46.19.137.50/gaybub/miori.i5

http[:]//46.19.137.50/gaybub/miori.i6

http[:]//46.19.137.50/gaybub/miori.m68k

http[:]//46.19.137.50/gaybub/miori.mips

http[:]//46.19.137.50/gaybub/miori.mipsl

http[:]//46.19.137.50/gaybub/miori.ppc

http[:]//46.19.137.50/gaybub/miori.sh4

http[:]//46.19.137.50/gaybub/miori.spc

http[:]//46.19.137.50/gaybub/miori.x86

http[:]//46.19.137.50/gaybub/sh

http[:]//46.19.137.50/gaybub/w.sh

http[:]//46.19.137.50/miori.arc

http[:]//46.19.137.50/miori.arm

http[:]//46.19.137.50/miori.arm5

http[:]//46.19.137.50/miori.arm6

http[:]//46.19.137.50/miori.arm7

http[:]//46.19.137.50/miori.i5

http[:]//46.19.137.50/miori.i6

http[:]//46.19.137.50/miori.m68k

http[:]//46.19.137.50/miori.mips

http[:]//46.19.137.50/miori.mipsl

http[:]//46.19.137.50/miori.ppc

http[:]//46.19.137.50/miori.sh4

http[:]//46.19.137.50/miori.spc

http[:]//46.19.137.50/miori.x86

http[:]//46.19.137.50/sh

http[:]//46.19.137.50/w.sh

http[:]//31.7.58.162/miori.mips

http[:]//31.7.58.162/miori.mpsl

http[:]//31.7.58.162/miori.x86

http[:]//31.7.58.162/miori.arm7

http[:]//31.7.58.162/miori.arm

http[:]//31.7.58.162/miori.sh4

http[:]//31.7.58.162/miori.arm6

http[:]//31.7.58.162/miori.arm5

http[:]//31.7.58.162/miori.ppc

http[:]//31.7.58.162/miori.arc

http[:]//31.7.58.162/miori.spc

http[:]//31.7.58.162/miori.i5

http[:]//31.7.58.162/miori.i6

http[:]//31.7.58.162/miori.m68k

http[:]//31.7.58.162/sh

http[:]//31.7.58.162/w.sh

http[:]//31.7.58.162/c.sh

控制 IP：

142.93.229.199

2.56.56.162

179.43.156.214

46.19.137.50

195.58.38.253

31.7.58.162