关于 Mirai 变种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 2 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，在近 2 个月的时间中，我们捕获的该 Mirai 变种样本至少迭代过 4 个版本，通信协议都与 Mirai 基本一致，传播方式当前主要为 Telnet 口令爆破，历史上曾利用 Nday 漏洞进行传播。

二、 僵尸网络分析

（一）相关样本分析

本文选取最新的 V4 X86 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	gx86
MD5	02d163134e3b4eabe62497b81659c2db
文件格式	ELF 32-bit LSB executable, Intel 80386
C2	103.136.42.158:16100

1、样本运行时文件名必须为：GSec，否则结束进程并打印误导性声明。

```
v3 = sub_804D770(1, 0);
if ( !sub_80547CF(*v53, v3) )
{
  sub_804D880(1);
  sub_805302E(1, "established connection.\n", 0x18u);
  sub_8055FDB(1);
}
v4 = sub_80533D5("/etc/resolv.conf", (int)"w");
v5 = v4;
```

图 1　样本运行信息

2、该样本复用了部分 Gafgyt 家族代码，依据目标机器是否装 python 来修改进程名。

```
  __GI_fclose(v14);
  v15 = __GI_fopen("/usr/bin/python", (int)&unk_8057C77);
  if ( v15 )
  {
    __GI_fclose(v15);
    v16 = sub_8051A00(73, 0);
    prctl(15, v16, v49, a1, v52);
  }
}
else
{
  v35 = sub_8051A00(72, 0);
  prctl(15, v35, 0, 0, v52);
}
```

图 2　修改进程名

3、bot 端上线机制和 mirai 保持一致。

第一个包是固定四字节\x00\x00\x00\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。

```
  LOBYTE(v69) = sub_8052810(v63);
  dword_805C2E8 = sub_8052A80();
  __libc_send(dword_805A084, &unk_8057CEF, 4, 0x4000);
  __libc_send(dword_805A084, &v69, 1, 0x4000);
  if ( (_BYTE)v69 )
    __libc_send(dword_805A084, v63, (unsigned __int8)v69, 0x4000);
}


le ( dword_805A084 == -1
  || !_bittest(&readfds.__fds_bits[(unsigned int)dword_805A084 >> 5], dword_8
 = 0;
 = (_DWORD *)sub_80532A2();
1 = 0;
 = __libc_recv(dword_805A084, &v69, 2, 16386);
```

图 3　上线机制

4、DDoS 攻击方法

包含针对 Layer4 和 Layer7 层的攻击，包括典型的 mirai DDoS 攻击方法。

表 1 攻击方法说明

攻击方法名称	含义	特点
gudp	修改的 UDP FLOOD，Layer4	高 BPS
ovh_bypass	基于 UDP 的 Layer7 层攻击	针对受 OVH 保护的服务器
greeth	基于 GRE 协议，有效攻击载荷在 Layer2 层	高 BPS
plaintcp	修改的 TCP FLOOD，Layer4	高 BPS

greip	修改的 greeth FLOOD	高 BPS，PPS
std	修改的 UDP FLOOD	高 BPS

```
switch ( result )
{
  case 1:
    return attack_method_gudp(a1, a2, a3, a4);
  case 2:
    return udp_ovh_bypass(a1, a2, a3, a4);
  case 3:
    return attack_method_greeth(a1, a2, a3, a4);
  case 4:
    return attack_method_plaintcp(a1, a2, a3, a4);
  case 5:
    return udp_ovh_bypass(a1, a2, a3, a4);
  case 6:
    return attack_method_greip(a1, a2, a3, a4);
}
if ( result > 6 )
{
  if ( (rand_next(result) & 1) == 0 )
    return attack_method_gudp(a1, a2, a3, a4);
  result = attack_method_std(a1, a2, a3, a4);
}
```

图 4　攻击方式

（二）传播方式分析

在该 Mirai 变种僵尸网络 V1 至 V4 版本的变化中，传播模式里彻底剔除了漏洞传播模块，并且弱口令列表有多个版本，可以推测僵尸网络控制者认为口令爆破效果更好，因此更加青睐这种传播方式。

V1 版本	内容	备注
样本自传播方式	Telnet 爆破 23、2323	明文存储口令
	NVMS-9000 DVR RCE	

传播源服务器攻击方式	Telnet 爆破 23、2323	
C2	46.175.146.159	
传播源	107.174.137.24	
传播时间推测	2022-04-06 至 2022-04-21	

V2 版本	内容	备注
样本自传播方式	Telnet 爆破 23、2323	口令加密，数量增加，包含特殊口令
	NVMS-9000 DVR RCE	
传播源服务器攻击方式	Telnet 爆破 23、2323	
C2	103.136.42.158	
传播源	107.174.137.24	同 V1 版本
传播时间推测	2022 年 4 月 21 日左右	

V3 版本	内容	备注
样本自传播方式	Telnet 爆破 23、2323	数量增加，包含特殊口令
传播源服务器攻击方式	Telnet 爆破 23、2323	
	CVE-2022-22965	Spring4Shell（194.31.98.186），5 月初停止
C2	103.136.42.158	
传播源	194.31.98.186、107.174.137.24	
传播时间推测	2022 年 5 月 13 日左右	

V4 版本	内容	备注
样本自传播方式	Telnet 爆破 23、2323	多个版本，口令数量不同，包含特殊口令
传播源服务器攻击方式	Telnet 爆破 23、2323	
C2	103.136.42.158	
传播源	194.31.98.230、103.136.41.159、5.255.101.44	与 V3 版本传播源 IP 不同
传播时间推测	2022 年 4 月 27 日开始，至今活跃	

在各版本口令解密后内容如图 5 所示。

v1		v2		v3		v4-var1		v4-var2	
admin	admin	admin	888888	default	12345	user	888888	admin	\
admin	tlJwpbo6	root	2010vesta	ftp	\	f~i!b@e#r$h%o^m*esuperadmin	s(f)u_h+g|u	root	Fireitup
guest	12345	root	2011vesta	ftp	ftp	awnfibre	fibre@dm!n	root	Pon521
nobody	tmadmin	user	user1234	guest	123456	trueadmin	admintrue	support	\
root	\	telecomadmin	nE7jA%5m	telnetadmin	telnetadmin	rootmet	m3trOr00t	root	root621
telnetadmin	telnetadmin	user	888888	user	user	telecomadmin	NWTF5x%RaKSmVbD	root	root
default	\	admin	esuper	root	123456	telecomadmin	NWTF5x%	default	default
root	vizxv	awnfibre	fibre@dm!n	bin	bin	admin	\	admin	BrAhMoS@15
guest	guest	trueadmin	admintrue	root	xc3511	admin	1234	root	123456
!!Huawei	@HuaweiHgw	rootmet	\	root	cxlinux	admin	12345	ftp	ftp
user	user	telecomadmin	NWTF5x%RaKSmVbD	root	icatch99	admin	h@32LuyD	user	\
ftp	ftp	telecomadmin	NWTF5x%	root	12345	admin	chzhdpl	root	vizxv
bin	\	admin	\	root	admin	admin	BrAhMoS@15	guest	12345
daemon	daemon	admin	12345	superadmin	Is$uper@dmin	admin	1q2w3e	root	\
root	xc3511	admin	h@32LuyD	root	zlxx.	telnetadmin	\	default	12345
ftp	\	admin	chzhdpl	root	founder88	telecomadmin	admintelecom	root	xc3511
adm	\	admin	BrAhMoS@15	admin	12345	root	root621	adm	telnetadm
admin	2601hx	admin	1q2w3e	telnet	telnet	root	Fireitup	root	icatch99
root	123456	telnetadmin	\	root	Zte521	CMCCAdmin	aDmSH%MdA	root	tsgoingon
root	/*6.=_ja	telecomadmin	admintelecom	admin	Admin@123	CMCCAdmin	Cmcc10086	CMCCAdmin	aDmSH%MdA
root	root	root	root621	suma123	panger123	root	Zte521	yhtcAdmin	Cuc@YHfw
root	hkipc2016	root	Fireitup	debug	debug	guest	12345	root	e2008jl
service	service	CMCCAdmin	aDmSH%MdA	root	pass123	guest	\	root	solokey
root	zlxx	CMCCAdmin	Cmcc10086	admin	admin	default	default	root	1234horses
root	founder88	root	Zte521	guest	12345	default	12345	root	Zte521
root	ivideo	guest	12345	guest	\	root	root	superadmin	Is$uper@dmin
root	pass	guest	\	root	solokey	root	\	root	admin
root	zsun1188	default	\	root	colorkey	root	admin	root	070admin
admin	eSehome	default	12345	root	sixaola	root	123456	admin	v2mprt
admin	eSetelnet	root	\	root	vizxv	root	12345	root	[GEPON]
admin	digitel	root	admin	root	/*6.=_ja	root	icatch99	root	/*6.=_ja
root	taZz@02	root	123456	root	hkipc2016	root	solokey	adm	adm
ubnt	ubnt	root	12345	default	default	root	tsgoingon	root	12345
root	icatch99	root	icatch99	adm	telnetadm	root	/*6.=_ja	admin	1234
root	admin	root	solokey	eSehomeasb	eSehomeasb	root	xc3511	eSehomeasb	\
admin	7ujMko0admin	root	tsgoingon	support	support	root	vizxv	admin	adminpass
root	xmhdipc	root	/*6.=_ja	daemon	daemon	root	zlxx.	root	system
root	cxlinux	root	xc3511	root	root621	root	hkipc2016	superadmin	zteadmin123
tech	tech	root	vizxv	root	root	root	cat1029	root	tslinux
1234	1234	root	zlxx.	root	\	root	tl789	keomo	\
Administrator	\	root	hkipc2016	root	tsgoingon	adm	telnetadm	CUAdmin	\
admin	\	root	cat1029	admin	1234	support	\	admin	conexant
sysadm	sysadm	root	tl789	admin	chzhdpl	ftp	\	admin	263297
admin	password	adm	telnetadm	root	pon521	ftp	ftp	admin	362729
telecomadmin	admintelecom	support	\	root	Zxic521	eSehomeasb	\	root	huigu309
		ftp	\	CMCCAdmin	aDmSH%MdA	Is$uper@dmin	superadmin	admin	epicrouter
		eSehomeasb	\	CMCCAdmin	Cmcc10086	user	\	admin	12345
		superadmin	Is$uper@dmin	CMCCAdmin	\	CMCCAdmin	aDmSH-cmcadmin	useradmin	admin!@#$%^
		user	\	CMCCAdmin	25802580	fiberhomehg2x0	hg2x0	root	2010vesta
		CMCCAdmin	\	root	gwladmin	useradmin	admin!@#$%^	admin	GeNeXiS@19
		fiberhomehg2x0	hg2x0	root	e2008jl	telecomadmin	nE7jA%5m	ONTUSER	SUGAR2A041
		useradmin	\	rapport	r@p8p0r+	admin	888888	root	davox
		root	[GEPON]	super	xJ4pCYeW	root	[GEPON]	root	realtek
		root	e2008jl	admin	h@32LuyD	user	user1234	CMCCAdmin	Cmcc10086
		ONTUSER	SUGAR2A041	supervisor	zyad1234	root	2010vesta	CMCCAdmin	aDmSH-cmcadmin
		root	huigu309	admin	1q2w3e	root	2011vesta	ftpuser	asteriskftp
		admin	362729	root	plumeria0077				
		admin	263297	root	Fireitup				
				admin	BrAhMoS@15				
				keomeo	keomeo				
				eStelnet	eStelnet				
				eSehome	eSehome				

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 1 日至 5 月 23 日该 Mirai 变种僵尸网络日上线境内肉鸡数最高达到 2.1 万台，累计感染肉鸡数达到 11.2 万。每日境内上线肉鸡数情况如下。

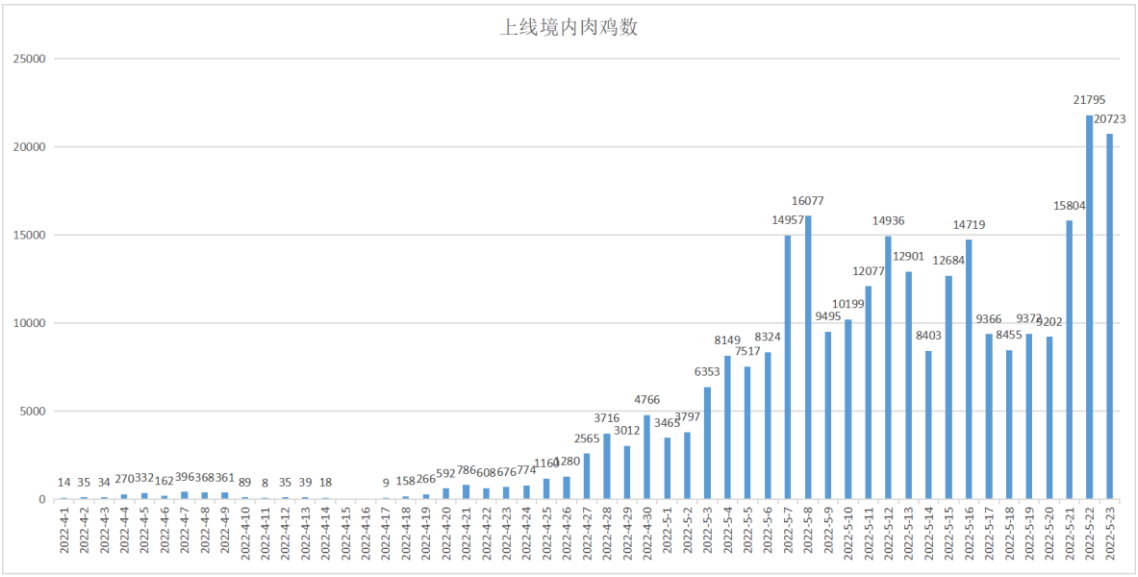

图 6 每日上线境内肉鸡数

该 Mirai 变种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（45.1%）、云南省（16.1%）和广东省（10.7%）；按运营商统计，电信占 93.2%，联通占 6.1%，移动占 0.4%。

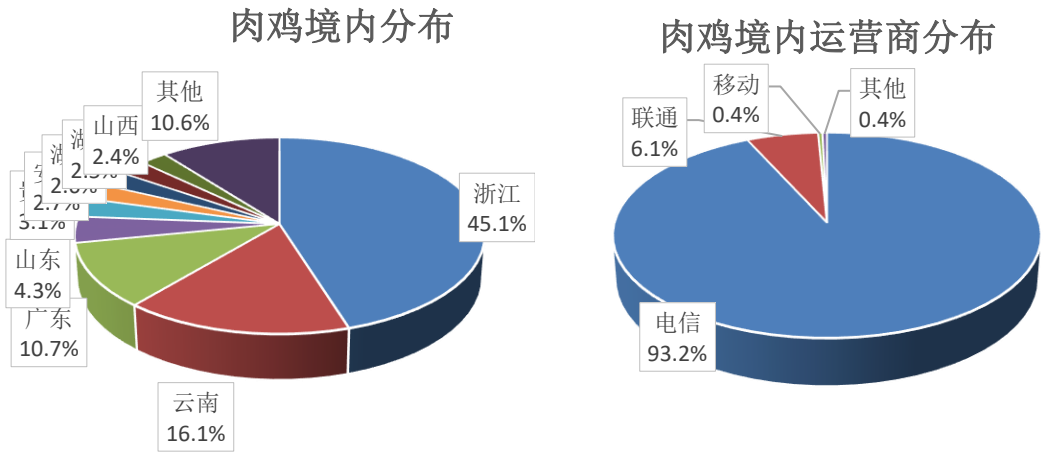

图 7 境内肉鸡按省份和运营商分布

四、 僵尸网络攻击动态

通过跟踪监测发现，该 Mirai 变种僵尸网络自 2022 年 4

月 1 日起一直对外发起 DDoS 攻击，且攻击行为非常活跃。攻击最猛烈的时候是 2022 年 5 月 16 日共发起 47 次 DDoS 攻击，2022 年 5 月 8 日曾先后调动 1.6 万台主机攻击某攻击目标。其攻击事件趋势如下：

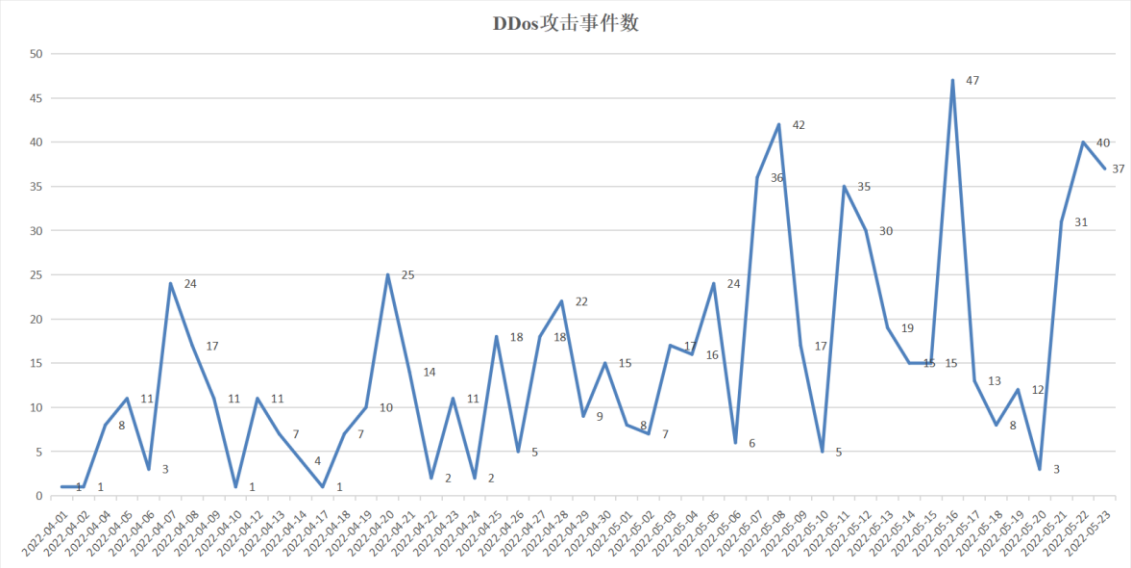

图 8 Mirai 变种僵尸网络攻击趋势

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、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：

79b5152e07ac9f67f337553afd8fdf49

73963353779b44bce2891d11e66d0e91

4cb48ee8d5e948cfe90eb1a9a3b5111f

17659ffa9ba80830b2ec6a7e1601fd38

0c05bcb28832937369e39ee113a6be81

c6ad4c67d5b8c4b2730a187161008da3

70efbb538061fbc2c399f2437a6e0e06

ba8ccfb46737d33e3eceec65d5ea17dd

5704172e740810bd7a808d17a62a2b63

1b469287783dc5f83222c515576653f5

4c160ae988d2489b9f1c27914c1657bf

9ee59e00d14bf71c0e2f1e09c9469dd6

d9e9923f705b6a3bce4bf4ddbb9ab2ec

a9f1e01e6793af26162bfe13f134a285

41dc20f7d94d11d8fceb524ff6b2391f

下载链接：

http[:]//5.255.101.44/garm

http[:]//5.255.101.44/garm5

http[:]//5.255.101.44/garm6

http[:]//5.255.101.44/garm7

http[:]//5.255.101.44/gmpsl

http[:]//5.255.101.44/gm68k

http[:]//5.255.101.44/gsh4

http[:]//5.255.101.44/gppc

http[:]//5.255.101.44/gx86

http[:]//5.255.101.44/gmips

http[:]//103.136.41.159/garm

http[:]//103.136.41.159/garm5

http[:]//103.136.41.159/garm6

http[:]//103.136.41.159/garm7

http[:]//103.136.41.159/gmpsl

http[:]//103.136.41.159/gm68k

http[:]//103.136.41.159/gsh4

http[:]//103.136.41.159/gppc

http[:]//103.136.41.159/gx86

http[:]//103.136.41.159/gmips

http[:]//194.31.98.230/garm

http[:]//194.31.98.230/garm5

http[:]//194.31.98.230/garm6

http[:]//194.31.98.230/garm7

http[:]//194.31.98.230/gmpsl

http[:]//194.31.98.230/gm68k

http[:]//194.31.98.230/gsh4

http[:]//194.31.98.230/gppc

http[:]//194.31.98.230/gx86

http[:]//194.31.98.230/gmips

http[:]//194.31.98.186/garm

http[:]//194.31.98.186/garm5

http[:]//194.31.98.186/garm6

http[:]//194.31.98.186/garm7

http[:]//194.31.98.186/gmpsl

http[:]//194.31.98.186/gm68k

http[:]//194.31.98.186/gsh4

http[:]//194.31.98.186/gppc

http[:]//194.31.98.186/gx86

http[:]//194.31.98.186/gmips

http[:]//107.174.137.24/garm

http[:]//107.174.137.24/garm5

http[:]//107.174.137.24/garm6

http[:]//107.174.137.24/garm7

http[:]//107.174.137.24/gmpsl

http[:]//107.174.137.24/gm68k

http[:]//107.174.137.24/gsh4

http[:]//107.174.137.24/gppc

http[:]//107.174.137.24/gx86

http[:]//107.174.137.24/gmips

控制 IP：

46.175.146.159

103.136.42.158