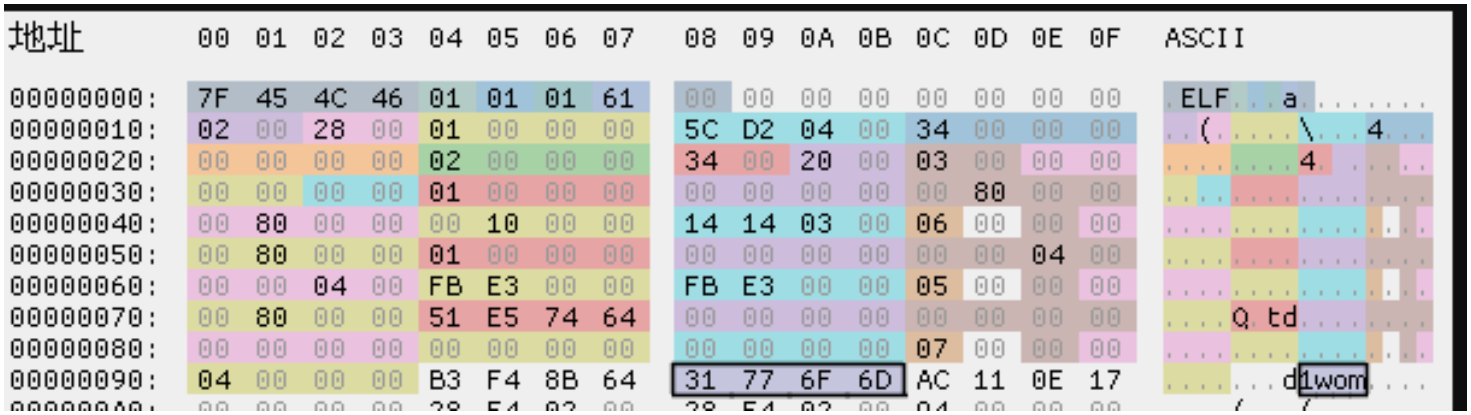
CN

Gayfemboy：一个利用四信工业路由oDAY传播的僵尸网络

Wang Hao, Acey9, Alex.Turing

2025年1月7日 • 12 min read



概述

无数脚本小子怀揣着发财梦，拿着 Mirai 的源码兴高采烈地杀入 DDoS 黑产行业，幻想着靠僵尸网络大赚一笔。现实是残酷的，这些人来时满怀雄心，去时却灰头土脸，只给安全社区留下一个又一个只能活跃 3–4 天的 Mirai 变种。然而，今天的主角**Gayfemboy**是一个例外。

Gayfemboy 僵尸网络首次于 2024 年 2 月初被 XLab 捕获，并持续活跃至今。它的早期版本并不起眼，仅仅是一个使用 UPX 加壳的 Mirai 派生版本，毫无新意。然而，其背后的开发者显然不甘平庸，随后展开了一场激进的迭代进化之旅。他们从修改上线报文入手，开始尝试 UPX 变形壳，积极整合 Nday 漏洞，甚至自行挖掘 0day 漏洞，持续扩大 Gayfemboy 的感染规模。

到了 2024 年 11 月初，Gayfemboy 再次进化，开始利用 四信工业路由器 0day 漏洞 以及 Neterbit 路由器 和 Vimar 智能家居设备 的未知漏洞传播样本。这一发现让我们决定对该僵尸网络进行更深入的分析，于是**注册了部分 C2 域名**用以观察被感染的设备，以及度量僵尸网络的规模。结果显示 Gayfemboy 拥有40多个上线分组，日活跃节点已经超过 1.5 万。有意思的是，当它发现域名被我们注册后，马上对我们抢注的域名展开了DDoS攻击，相当睚眦必报。

依托于XLab大网威胁感知系统的能力，回顾Gayfemboy的演化历程，我们见证了它从一个普通的Mirai变种，一步步进化为今天`拥有0day利用能力，攻击颇为凶猛，具有自身特色的大型僵尸网络`。

- 2024年02月12日，XLAB首次发现Gayfemboy样本，使用普通upx壳
- 2024年4月15日，upx幻数修改为`YTS\x99`，开始使用`gayfemboy`上线报文，
- 2024年6月初，upx幻数修改为`1wom`，bot代码基本固定，偶尔新增几个C2域名
- 2024年8月底，样本硬编码6个C2，后3个C2是未注册的状态

- 2024年11月09日，观察到Gayfemboy开始使用四信工业路由0day漏洞传播样本，样本运行参数为`faith2`
- 2024年11月17日，我们注册了Gayfemboy样本中部分未注册的域名，用来观察Gayfemboy感染的设备和僵尸网络规模。
- 2024年11月23日，Gayfemboy的所有者发现我们注册了他的CC域名，开始定期对我们注册的域名发起DDoS攻击。
- 2024年12月27日，VulnCheck公开了四信工业路由器 0day的漏洞信息。

漏洞利用

Gayfemboy使用20多个漏洞和Telnet弱口令传播样本，其中包括四信工业路由0day漏洞(当前漏洞已经公布，CVE编号为：CVE-2024-12856)，部分未知漏洞涉及Neterbit和vimar设备（这部分因为漏洞未公开，为防止漏洞被滥用，本文暂且按下不表）。Gayfemboy利用的主要漏洞如下：

VULNERABILITY
cve_2013_3307
cve_2014_8361
cve_2016_20016
cve_2017_17215
cve_2017_5259
cve_2020_25499
cve_2020_9054
cve_2021_35394
cve_2023_26801
CVE-2013-7471
CNVD-2022-77903
CVE-2024-8957,CVE-2024-8956
CVE-2024-12856

VULNERABILITY
KGUARD DVR RCE
Lilin DVR RCE
OptiLink ONT1GEW GPON 2.1.11_X101 Build 1127.190306 - Remote Code
TVT editBlackAndWhiteList RCE
ZTE ZXV10 H108L Router RCE
Anheng DAS TGFW sslvpn RCE

感染规模

BOT数量趋势

根据我们收集到的数据看，Gayfemboy僵尸网络的日活Bot IP数量在1.5万左右。

主要感染分布在中国、美国、伊朗、俄罗斯、土耳其

主要感染的设备

Gayfemboy Bot连接CC时携带一个分组信息，这些分组信息是为了标识并组织被感染的设备，以便攻击者更有效地管理和控制庞大的僵尸网络。这个分组信息通常包含一些关键的标识符，例如设备的操作系统类型、或者其他识别信息。很多攻击者也喜欢用感染设备的方式来作为标识。Gayfemboy的上线分组信息是设备信息。感染的主要设备如下：

GROUP	COUNT OF BOT IP	METHOD OF INFECTION	AFFECTED DEVICE
adtran	2707	Unknown	Unknown
asus	2080	NDAY	ASUS Router
bdvr7	1461	NDAY	Kguard DVR
peeplink	1422	Unknown	Neterbit、LTE、CPE、NR5G Router
faith2	590	0DAY(CVE-2024-12856)	Four-Faith Industrial Router

GROUP	COUNT OF BOT IP	METHOD OF INFECTION	AFFECTED DEVICE
vimar7	442	Unknown	Vimar Smart Home Device

DDoS 分析

攻击目标

Gayfemboy僵尸网络的发起攻击从2024年02月至今断断续续的一直有，其中去年10月和11月份攻击目标最多。每天攻击上百个目标。攻击目标遍布全球，分布在各个行业，主要攻击目标分布在中国、美国、德国、英国、新加坡等地区。

攻击目标趋势如下：

攻击目标地理位置分布：

攻击能力

我们将抢注的Gayfemboy域名解析到了云厂商的VPS。Gayfemboy的所有者发现后开始定期对我们注册的域名发起DDoS攻击，每次攻击时长10到30秒。云厂商发现我们的VPS被攻击后会立即将我们的VPS流量黑洞路由24小时以上，这将导致我们的VPS无法提供服务，也无法访问(我们的VPS还没有被Gayfemboy打死，就被云厂商先干死了，云厂商服务策略如此)。一旦VPS服务恢复，Gayfemboy又攻过来了。因为我们没有购买抗DDoS服务，最终选择停止解析Gayfemboy的域名。部分攻击指令记录如下图所示：

根据云厂商提供的流量监控服务可以看到Gayfemboy攻击流量可能在`百G`左右。

样本分析

该家族使用魔改UPX壳，早期使用的幻数为"YTS\x99"，自2024年6月之后开始使用独特幻数"1wom"

在代码方面基于Mirai进行修改：

1. 删除Mirai字符串表，使用明文字符串
2. 添加隐藏pid函数
3. 修改上线包为"gayfemboy"
4. 添加新的指令功能

为增加分析难度、保护程序，botnet开发者往往会对字符串进行加密，但该开发者似乎不重视字符串的保护，字符串全部使用明文，样本在运行后会输出"we gone now\n"，该特征从发现样本开始一直没有改变

为隐藏恶意进程，样本启动后会尝试从根目录开始查找可写入的目录，并尝试写入随机的2032字节文件`test_write`作为测试，成功后会删除该文件，在遇到以下目录时会跳过

```
/proc
/sys
/dev/fd
/boot
```

当找到可写入目录时，尝试通过挂载该目录到`/proc/<pid>`上使该进程在/proc文件系统中不可见，以此隐藏指定的PID。

在网络协议方面，保留了Mirai的指令格式，修改上线包并添加新的指令功能：

CMD_ID	DESC
14	update self
18	start scan
19	stop scan

CMD_ID	DESC
23	attack kill all
24	kill attack ip

常规的DDoS相关指令：

当收到自更新指令时，会从指令中获取下载服务器和botid，默认使用`meowware.ddns.net`作为下载服务器，样本中硬编码了多个下载相关的指令格式字符串

作用是使用wget从固定目录`chefrvmanabat`下载文件，以botid为参数执行。

当收到扫描指令时，从指令中解析多个自定义参数，如扫描端口、上报服务器、上报端口、验证返回包等

总结

DDoS（分布式拒绝服务）作为一种高度可重复使用且成本相对较低的网络攻击武器，因其能够通过分布式僵尸网络、恶意工具或放大技术，瞬间发起大规模流量攻击，对目标网络资源进行耗尽、瘫痪或服务中断，已成为网络攻击中最常见和最具有破坏力的手段之一。其攻击模式多样化、攻击路径隐蔽性强，并能通过不断变化的策略与技术手段，针对不同的行业和系统实施精准打击，从而对企业、政府机构和个人用户造成严重威胁。企事业和个人应从不同层面制定完善的防御策略降低DDoS攻击的风险，提升系统的整体抗压能力。

Contact Us

Readers are always welcomed to reach us on twitter.

IoC

loader IP

```
123.249.103.79  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.109.227 China|Beijing|Beijing City      AS55990|HUAWEI
123.249.111.22  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.116.30  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.116.81  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.126.147 China|Beijing|Beijing City      AS55990|HUAWEI
123.249.64.207  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.68.177  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.82.162  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.82.229  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.87.110  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.90.104  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.90.23   China|Beijing|Beijing City      AS55990|HUAWEI
123.249.91.159  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.94.157  China|Beijing|Beijing City      AS55990|HUAWEI
123.249.99.231  China|Beijing|Beijing City      AS55990|HUAWEI
124.71.235.245  China|Beijing|Beijing City      AS55990|HUAWEI
176.97.210.250  Germany|Hessen|Frankfurt am Main        AS49581|Ferdinand Zink trad
178.211.139.105 Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
178.211.139.196 Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
178.211.139.241 Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
185.16.39.37    Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
193.32.162.34   The Netherlands|None|None       AS47890|UNMANAGED LTD
193.34.214.123  Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
193.42.12.166   Germany|Hessen|Frankfurt am Main        AS58212|dataforest GmbH
194.50.16.198   The Netherlands|Noord-Holland|Amsterdam AS49870|Alsycon B.V.
198.98.51.91    United States|New York|Staten Island    AS53667|FranTech Solutions
198.98.54.234   United States|New York|Staten Island    AS53667|FranTech Solutions
209.141.32.195  United States|Nevada|Las Vegas  AS53667|FranTech Solutions
209.141.51.21   United States|Nevada|Las Vegas  AS53667|FranTech Solutions
37.114.63.100   Germany|Hessen|Frankfurt am Main        AS60461|intercolo GmbH
45.128.232.200  Bulgaria|Sofia|Sofia    AS202685|Aggros Operations Ltd.
45.142.122.187  Russia|Moscow|Moscow    AS210644|AEZA GROUP Ltd
45.142.182.126  Germany|None|None       AS44592|SkyLink Data Center BV
45.145.41.175   United States|Washington|Seattle        AS205770|SC ITNS.NET SRL
45.148.10.230   The Netherlands|Noord-Holland|Amsterdam AS48090|PPTECHNOLOGY LIMITE
45.95.147.211   The Netherlands|Noord-Holland|Amsterdam AS49870|Alsycon B.V.
5.181.188.158   Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
70.36.99.15     United States|California|Los Angeles    AS22439|Perfect Internation
77.90.22.10     Germany|Hessen|Frankfurt am Main        AS12586|GHOSTnet GmbH
77.90.22.35     Germany|Hessen|Frankfurt am Main        AS12586|GHOSTnet GmbH
94.156.10.163   Bulgaria|None|None      AS0|
```

```
94.156.10.164   Bulgaria|None|None      AS0|
95.214.53.211   Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
95.214.54.53    Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
```

Downloader

```
101.42.158.190  China|Beijing|Beijing City      AS45090|Tencent
101.43.141.112  China|Beijing|Beijing City      AS45090|Tencent
107.189.28.60   Luxembourg|Luxembourg|Luxembourg        AS53667|FranTech Solutions
108.233.83.51   United States|California|Santa Clara    AS7018|AT&T
1.13.102.222    China|Jiangsu|Nanjing City      AS45090|Tencent
152.32.237.129  United States|Virginia|Reston   AS135377|UCLOUD INFORMATION TECHNOL
193.32.162.34   The Netherlands|None|None       AS47890|UNMANAGED LTD
198.98.54.234   United States|New York|Staten Island    AS53667|FranTech Solutions
203.23.159.152  Australia|Victoria|Southbank    AS9648|Australia On Line Pty Ltd
209.141.32.148  United States|Nevada|Las Vegas  AS53667|FranTech Solutions
209.141.35.56   United States|Nevada|Las Vegas  AS53667|FranTech Solutions
209.141.51.21   United States|Nevada|Las Vegas  AS53667|FranTech Solutions
209.141.55.38   United States|Nevada|Las Vegas  AS53667|FranTech Solutions
209.141.57.222  United States|Nevada|Las Vegas  AS53667|FranTech Solutions
37.114.63.100   Germany|Hessen|Frankfurt am Main        AS60461|intercolo GmbH
45.142.122.187  Russia|Moscow|Moscow    AS210644|AEZA GROUP Ltd
65.175.140.164  United States|Massachusetts|Boston      AS11776|Breezeline
77.90.22.35     Germany|Hessen|Frankfurt am Main        AS12586|GHOSTnet GmbH
95.214.53.211   Poland|Mazowieckie|Warsaw       AS201814|MEVSPACE sp. z o.o.
meowware.ddns.net
```

CC

```
meowware.ddns.net
```

Sample SHA1

```
3287158c35c93a23b79b1fbb7c0e886725df5faa
ba9224828252e0197ea5395dad9bb39072933910
fe72a403f2620161491760423d21e6a0176852c3
```

What do you think?

3 Responses

 Upvote

 Funny

 Love

 Surprised

 Angry

 Sad

0 Comments Login ▾

G Start the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS

Name

♡ Share Best Newest Oldest