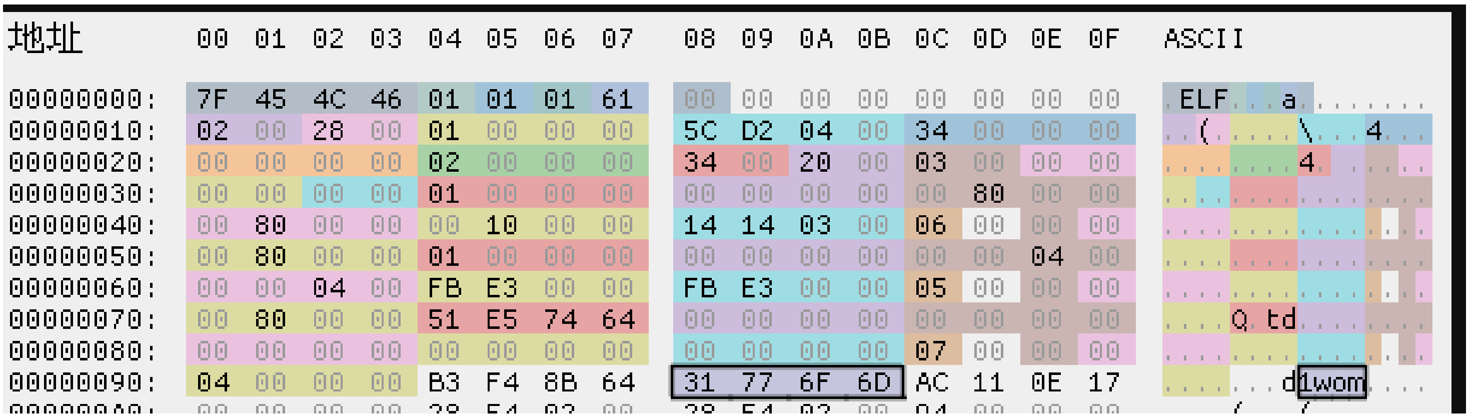
EN

Gayfemboy: A Botnet Deliver Through a Four-Faith Industrial Router 0-day Exploit.

Wang Hao, Alex.Turing, Acey9

2025年1月7日 • 9 min read



```
地址        00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ASCII

00000000:   7F 45 4C 46 01 01 01 61  00 00 00 00 00 00 00 00  .ELF...a........
00000010:   02 00 28 00 01 00 00 00  5C D2 04 00 34 00 00 00  ..(.....\...4...
00000020:   00 00 00 00 02 00 00 00  34 00 20 00 03 00 00 00  ........4. .....
00000030:   00 00 00 00 01 00 00 00  00 00 00 00 00 80 00 00  ................
00000040:   00 80 00 00 00 10 00 00  14 14 03 00 06 00 00 00  ................
00000050:   00 80 00 00 01 00 00 00  00 00 00 00 00 00 04 00  ................
00000060:   00 00 04 00 FB E3 00 00  FB E3 00 00 05 00 00 00  ................
00000070:   00 80 00 00 51 E5 74 64  00 00 00 00 00 00 00 00  ....Q.td........
00000080:   00 00 00 00 00 00 00 00  00 00 00 00 07 00 00 00  ................
00000090:   04 00 00 00 B3 F4 8B 64  31 77 6F 6D AC 11 0E 17  .......d1wom....
000000A0:   00 00 00 00 28 F4 02 00  28 F4 02 00 04 00 00 00  ....(...(.......
```

Overview

Exploitation Details

BOT Scale

BOT IP Count Trend

Main Infected Devices

DDoS Analysis

Attack Targets

Attack Capabilities

Sample Analysis

Conclusion

Contact Us

IoC

loader IP

i. Downloader

i. CC

i. Sample SHA1

Overview

Countless script kiddies, dreaming of getting rich, rush into the DDoS black-market industry armed with `Mirai` source code, imagining they can make a fortune with botnets. Reality, however, is harsh—these individuals arrive full of ambition but leave in dismay, leaving behind a series of Mirai variants that survive no more than `3–4` days. However, today's focus, `Gayfemboy`, is an exception.

The `Gayfemboy` botnet was first discovered by XLab in early February 2024 and has remained active ever since. Its early versions were unremarkable—simply Mirai derivatives packed with UPX, showing no innovation. However, the developers behind it were clearly unwilling to remain mediocre. They launched an aggressive iterative development journey, starting with modifying registration packets, experimenting with UPX polymorphic packing, actively integrating N-day vulnerabilities, and even discovering 0-day exploits to continually expand Gayfemboy's infection scale.

By early November 2024, Gayfemboy evolved further, leveraging a 0-day vulnerability in Four-Faith industrial routers and unknown vulnerabilities in Neterbit routers and Vimar smart home devices to spread its payloads. This discovery prompted us to conduct an in-depth analysis of this botnet. We `registered several C2 domains` to observe infected devices and measure the botnet's scale. Our findings revealed that Gayfemboy operates with over 40 grouping categories and has more than 15,000 daily active nodes. Interestingly, when it detected our registration of its domains, it retaliated immediately with a DDoS attack—an act of notable hostility.

With the capabilities of XLab's `Cyber Threat Insight and Analysis` system, reviewing Gayfemboy's evolution has allowed us to witness its transformation from an ordinary Mirai variant into today's unique large-scale botnet, equipped with 0-day exploitation capabilities and a ferocious attack arsenal.

- February 12, 2024: XLab first discovered Gayfemboy samples, packed with a standard UPX shell.
- April 15, 2024: The UPX magic number was modified to `YTS\x99`, and the bot began using the `gayfemboy` registration packet.
- Early June 2024: The UPX magic number was changed to `1wom`. The bot code became relatively stable, with only occasional additions of new C2 domains.
- Late August 2024: Samples hardcoded six C2 domains, with the last three remaining unregistered.
- November 9, 2024: Gayfemboy was observed exploiting a 0-day vulnerability in Four-Faith industrial routers to deliver its samples. The samples were executed with the parameter `faith2`.
- November 17, 2024: We registered several unregistered domains found in Gayfemboy samples to observe infected devices and measure the botnet's scale.
- November 23, 2024: Gayfemboy's operators detected our registration of their C2 domains and began periodically launching DDoS attacks against the domains we registered.
- December 27, 2024: VulnCheck publicly disclosed the 0-day vulnerability information for Four-Faith industrial routers.

Exploitation Details

Gayfemboy deliver its samples using more than 20 vulnerabilities and Telnet weak credentials. These include the Four-Faith industrial router 0-day vulnerability (now disclosed as CVE-2024-12856) and several unknown vulnerabilities affecting Neterbit and Vimar devices. (For ethical reasons and to prevent misuse, we will not discuss the undisclosed vulnerabilities in this article.) The primary vulnerabilities exploited by Gayfemboy are as follows:

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
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

BOT Scale

BOT IP Count Trend

Based on the data we collected, the Gayfemboy botnet maintains approximately 15,000 daily active Bot IPs.

The primary infections are distributed across regions including China, the United States, Iran, Russia, and Turkey.

Main Infected Devices

When Gayfemboy bots connect to the C2, they carry grouping information used to identify and organize infected devices, enabling attackers to efficiently manage and control the large botnet. This grouping information typically includes key identifiers, such as the device's operating system type or other identifying details. Many attackers also prefer to use the infection method as an identifier. Gayfemboy’s grouping information is based on device details. The main infected devices are as follows:

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
vimar7	442	Unknown	Vimar Smart Home Device

DDoS Analysis

Attack Targets

The Gayfemboy botnet has launched intermittent attacks from February 2024 to the present, with the highest frequency of attacks occurring in October and November of the previous year. The botnet targets hundreds of different entities each day. The attack targets are spread across the globe, covering various industries. The main attack targets are concentrated in regions such as China, the United States, Germany, the United Kingdom, and Singapore.

The attack target trend is as follows:

Geographical distribution of attack targets:

Attack Capabilities

We resolved the registered Gayfemboy domains to a VPS from a cloud provider. After Gayfemboy's operators discovered this, they began regularly launching DDoS attacks against our registered domains, with each attack lasting between 10 to 30 seconds. When the cloud provider detected that our VPS was being attacked, they would immediately blackhole route the VPS traffic for over 24 hours, making our VPS unavailable and inaccessible. Once the VPS service was restored, Gayfemboy would attack again. Since we had not purchased DDoS protection, we ultimately decided to stop resolving Gayfemboy's domains. Some attack command records are shown in the figure below:

According to the traffic monitoring service provided by the cloud provider, the DDoS attack traffic from Gayfemboy is estimated to be around `100GB`.

Sample Analysis

This family uses a modified UPX shell. The early versions employed the magic number `YTS\x99`, while since June 2024, it has started using the unique magic number `1wom`.

The code is based on Mirai with the following modifications:

- Removed the Mirai string table and used plaintext strings.
- Added a function to hide the process ID (pid).
- Modified the registration packet to "gayfemboy."
- Added new command functionalities.

To increase analysis difficulty and protect the program, botnet developers often encrypt strings. However, the developer behind this botnet seems to neglect string protection, as all strings are in plaintext. After the sample runs, it outputs `we gone now\n`, a feature that has remained unchanged since the discovery of the sample.

To hide the malicious process, the sample attempts to find writable directories starting from the root directory upon startup. It then tries to write a random 2032-byte file named `test_write` as a test. If successful, the file is deleted. The sample will skip the following directories:

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

When a writable directory is found, the sample attempts to mount the directory to `/proc/<pid>`, making the process invisible in the `/proc` filesystem and thereby hiding the specified PID.

In terms of the network protocol, the botnet retains the Mirai command format but modifies the registration packet and adds new command functionalities:

CMD_ID	DESC
14	update self
18	start scan
19	stop scan
23	attack kill all

CMD_ID	DESC
24	kill attack ip

The standard DDoS-related commands include:

Upon receiving a self-update command, the sample retrieves the download server and bot ID from the command. By default, it uses `meowware.ddns.net` as the download server. The sample also hardcodes multiple command format strings related to downloading.

The purpose is to use `wget` to download files from a fixed directory `chefrvmanabat`, with the bot ID passed as a parameter for execution.

Upon receiving a scanning command, the sample parses multiple custom parameters from the command, such as the scanning port, reporting server, reporting port, and validation of the response packet.

Conclusion

DDoS (Distributed Denial of Service) is a highly reusable and relatively low-cost cyberattack weapon. It can launch large-scale traffic attacks instantly using distributed botnets, malicious tools, or amplification techniques, depleting, disabling, or interrupting the target network's resources. As a result, DDoS has become one of the most common and destructive forms of cyberattacks. Its attack modes are diverse, attack paths are highly concealed, and it can employ continuously evolving strategies and techniques to conduct precise strikes against various industries and systems, posing a significant threat to enterprises, government organizations, and individual users. Organizations and individuals should develop comprehensive defense strategies at various levels to mitigate the risks of DDoS attacks and enhance the overall resilience of their systems.

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?

30 Responses

👍 Upvote　😝 Funny　😍 Love　😲 Surprised　😤 Angry　😥 Sad

0 Comments　　1 Login ▾

G　Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share　　Best Newest Oldest