Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Gayfemboy Botnet: Evolution of a Potent Threat

Date of Publication	Admiralty Code	TA Number
January 9, 2025	A1	TA2025007

Summary

Attack Discovered: November 2024
Targeted Countries: China, United States, Russia, Turkey, Iran, Germany, United Kingdom, and Singapore
Malware: Gayfemboy Botnet
Attack: The Gayfemboy botnet is a sophisticated Mirai variant that exploits a 0-day vulnerability in Four-Faith industrial routers. Its advanced development includes modifications to registration packets, UPX packing, and exploitation of multiple vulnerabilities. With over 15,000 active nodes, it has launched significant DDoS attacks, peaking at 100GB of traffic. The botnet's ability to leverage both known and zero-day vulnerabilities highlights critical cybersecurity concerns and the pressing need for robust security measures.

Attack Regions

Attack Details

#1 Gayfemboy botnet discovered in February 2024, has evolved into a formidable cyber threat with advanced exploitation capabilities. Originally identified as a derivative of the Mirai botnet, it began as a series of malware samples packed with UPX. Over time, its developers continuously refined its architecture, experimenting with techniques like UPX polymorphic packing, modifying registration packets, and incorporating 0-day exploits.

#2 By November 2024, Gayfemboy had expanded its operations, targeting vulnerabilities in Four-Faith industrial routers (CVE-2024-12856) and unknown flaws in Neterbit routers and Vimar smart home devices. This evolution enabled the botnet to maintain over 15,000 daily active infections distributed across more than 40 grouping categories. Its reach spans regions such as China, the United States, Iran, Russia, and Turkey, making it a global menace.

#3 The botnet's operators have equipped Gayfemboy with a robust arsenal of over 20 known vulnerabilities, coupled with weak Telnet credentials for initial access. It employs sophisticated evasion techniques, such as concealing its process ID (PID) and mounting writable directories to hide malicious activities. Additionally, its developers have customized the Mirai-based code, adding functionalities like self-updating mechanisms and enhanced scanning capabilities to increase its attack efficiency.

#4 Since its inception, Gayfemboy has been launching intermittent DDoS attacks, with a marked increase in activity in October and November 2024. The attacks have targeted hundreds of organizations worldwide, with significant concentrations in China, the United States, Germany, the UK, and Singapore. Using its extensive botnet, Gayfemboy has generated traffic volumes estimated at 100 GB per attack, lasting between 10 and 30 seconds.

Recommendations

Apply Patch: Ensure all systems are updated with the latest patches to address vulnerabilities exploited by the botnet. Ensure timely updates for vulnerabilities to close exploitable gaps.

Strong Authentication Practices: Replace weak Telnet credentials with robust password policies and disable Telnet where possible.

DDoS Mitigation Strategies: Implement anti-DDoS solutions, including rate limiting and traffic filtering, to withstand high-volume attacks.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Strengthen Endpoint Defense: Implement advanced Endpoint Detection and Response (EDR) solutions to effectively detect, analyze, and mitigate in-memory malware activity, ensuring comprehensive protection against sophisticated threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0011 Command and Control	**TA0040** Impact	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1498 Network Denial of Service	**T1082** System Information Discovery	**T1059** Command and Scripting Interpreter	**T1027** Obfuscated Files or Information
T1057 Process Discovery	**T1562** Impair Defenses	**T1568** Dynamic Resolution	**T1583** Acquire Infrastructure
T1583.003 Virtual Private Server	**T1134** Access Token Manipulation	**T1134.004** Parent PID Spoofing	**T1584** Compromise Infrastructure
T1584.005 Botnet			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	123[.]249[.]103[.]79, 123[.]249[.]109[.]227, 123[.]249[.]111[.]22, 123[.]249[.]116[.]30, 123[.]249[.]116[.]81, 123[.]249[.]126[.]147, 123[.]249[.]64[.]207, 123[.]249[.]68[.]177, 123[.]249[.]82[.]162, 123[.]249[.]82[.]229, 123[.]249[.]87[.]110, 123[.]249[.]90[.]104, 123[.]249[.]90[.]23, 123[.]249[.]91[.]159, 123[.]249[.]94[.]157, 123[.]249[.]99[.]231, 124[.]71[.]235[.]245, 176[.]97[.]210[.]250, 178[.]211[.]139[.]105, 178[.]211[.]139[.]196, 178[.]211[.]139[.]241, 185[.]16[.]39[.]37, 193[.]32[.]162[.]34, 193[.]34[.]214[.]123, 193[.]42[.]12[.]166, 194[.]50[.]16[.]198, 198[.]98[.]51[.]91, 198[.]98[.]54[.]234, 209[.]141[.]32[.]195, 209[.]141[.]51[.]21, 37[.]114[.]63[.]100, 45[.]128[.]232[.]200, 45[.]142[.]122[.]187, 45[.]142[.]182[.]126, 45[.]145[.]41[.]175, 45[.]148[.]10[.]230, 45[.]95[.]147[.]211, 5[.]181[.]188[.]158, 70[.]36[.]99[.]15, 77[.]90[.]22[.]10, 77[.]90[.]22[.]35, 94[.]156[.]10[.]163, 94[.]156[.]10[.]164,

TYPE	VALUE
IPv4	95[.]214[.]53[.]211, 95[.]214[.]54[.]53, 101[.]42[.]158[.]190, 101[.]43[.]141[.]112, 107[.]189[.]28[.]60, 108[.]233[.]83[.]51, 1[.]13[.]102[.]222, 152[.]32[.]237[.]129, 193[.]32[.]162[.]34, 198[.]98[.]54[.]234, 203[.]23[.]159[.]152, 209[.]141[.]32[.]148, 209[.]141[.]35[.]56, 209[.]141[.]51[.]21, 209[.]141[.]55[.]38, 209[.]141[.]57[.]222, 37[.]114[.]63[.]100, 45[.]142[.]122[.]187, 65[.]175[.]140[.]164, 77[.]90[.]22[.]35, 95[.]214[.]53[.]211
Domain	meowware[.]ddns[.]net
SHA1	3287158c35c93a23b79b1fbb7c0e886725df5faa, Ba9224828252e0197ea5395dad9bb39072933910, Fe72a403f2620161491760423d21e6a0176852c3

CVEs

Gayfemboy primarily exploits the following vulnerabilities. To streamline remediation, each CVE includes a hyperlinked checkmark under 'Patch Link' for quick access to the relevant patches.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2024-12856	Four-Faith OS Command Injection Vulnerability	Four-Faith F3x24 and F3x36	✓	✗	✗
CVE-2013-3307	Cisco Linksys x3000 firmware Command Injection Vulnerability	Cisco Linksys x3000_firmware	✗	✗	✗

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2014-8361	Realtek SDK Improper Input Validation Vulnerability	Realtek SDK	✗	✓	✓
CVE-2016-20016	MVPower Remote Command Execution Vulnerability	MVPower tv-7104he_firmware	✗	✗	✗
CVE-2017-17215	Huawei hg532_firmware Improper Input Validation Vulnerability	Huawei hg532_firmware	✓	✗	✓
CVE-2017-5259	Cambium Networks cnpilot_r190v_firmware Active Debug Code Vulnerability	Cambium Networks cnpilot_r190v_firmware	✗	✗	✗
CVE-2020-25499	Totolink a3002r_firmware Command Injection Vulnerability	Totolink a3002r_firmware	✗	✗	✗
CVE-2020-9054	Zyxel Multiple NAS Devices OS Command Injection Vulnerability	Zyxel Multiple Network-Attached Storage (NAS) Devices	✗	✓	✓
CVE-2021-35394	Realtek Jungle SDK Remote Code Execution Vulnerability	Realtek Jungle Software Development Kit (SDK)	✗	✓	✓
CVE-2023-26801	lb-link bl-lte300_firmware Command Injection Vulnerability	lb-link bl-lte300_firmware	✗	✗	✗
CVE-2013-7471	D-Link DIR-300 Router Command Injection Vulnerability	D-Link DIR-300 Router	✗	✗	✗
CVE-2024-8957	PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability	PTZOptics PT30X-SDI/NDI Cameras	✓	✓	✓
CVE-2024-8956	PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability	PTZOptics PT30X-SDI/NDI Cameras	✓	✓	✓

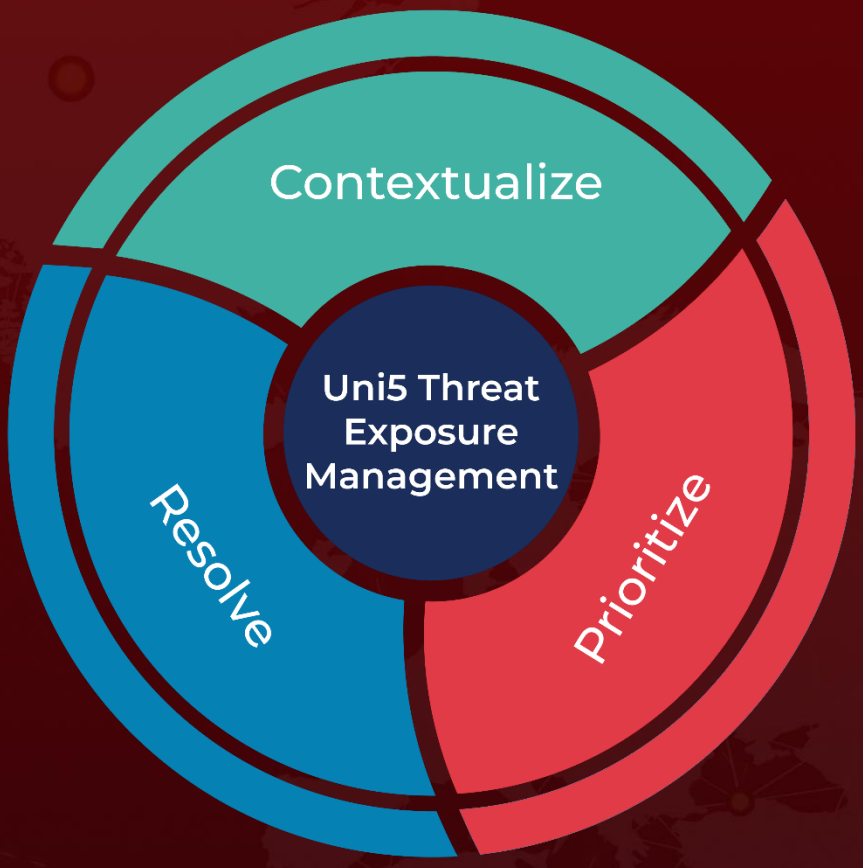
References

https://blog.xlab.qianxin.com/gayfemboy-en/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 9, 2025 • 11:30 PM

More at www.hivepro.com