IoT under siege: The return of the Mirai-based Gayfemboy Botnet - Agains

Data: 2025-08-24 08:40:36

Autor: Inteligência Against Invaders

IoT under siege: The return of the Mirai-based Gayfemboy Botnet

Mirai-based Gayfemboy botnet resurfaces, evolving to target systems worldwide; Fortinet researchers provided details about the new campaign.

FortiGuard Labs researchers tracked a new Gayfemboy botnet campaign, the malware exploits known flaws in DrayTek, TP-Link, Raisecom, and Cisco, showing evolved tactics and renewed activity.

The Gayfemboy botnet was first identified in February 2024, it borrows the code from the basicMiraivariant and integrates N-day and 0-day exploits.

By November 2024, Gayfemboy exploited 0-day vulnerabilities in Four-Faith industrial routers and Neterbit routers and Vimar smart home devices, with over 15,000 daily active nodes. Operators behind the botnet also launched DDoS attacks against researchers tracking it.

In January 2025, QiAnXin XLab experts observed the Gayfemboy delivering its bot by exploiting more than 20 vulnerabilities, they also attempted to exploit Telnet weak credentials. The researchers discovered that attackers targeted the zero-day vulnerabilityCVE-2024-12856in Four-Faith industrial routers along with several unknown vulnerabilities affecting Neterbit and Vimar devices.

In July 2025, FortiGuard Labs found a Gayfemboy payload exploiting multiple device flaws. Attacks originated from IPs 87[.]121[.]84[.]34 and 220[.]158[.]234[.]135. The experts identified the downloader scripts for multiple devices targeted by the bot, including Asus, Vivo, Zyxel, and Realtek. The malicious code fetched malware and XMRig miners, with product names passed as parameters to Gayfemboy for execution.

“Gayfemboy employs its first layer of obfuscation during the file download stage. Unlike Mirai and Gafgyt variants, which typically use Linux architecture names as file extensions, Gayfemboy assigns distinct names to each architecture, avoiding predictable naming conventions.” reads the report published by Fortinet Labs.

The Gayfemboy botnet targets multiple countries, including Brazil, Mexico, the United States, Germany, France, Switzerland, Israel, and Vietnam. Experts observed victims in multiple sectors, such as Manufacturing, Technology, Construction, and Media or Communications.

Gayfemboy malware employs custom file naming to evade detection and obfuscates binaries with a modified UPX header. The malware kills rival malware processes. It has four core modules: Monitor (anti-analysis, persistence, sandbox evasion, process-killing), Watchdog (ensures single instance, kills unresponsive copies), Attacker (DDoS and backdoor functions), and Killer (removes competing infections).

*“Within the***Monitor***function, Gayfemboy includes two dedicated sub-functions:***Self-Persistence***and***Sandbox Evasion***.* ***Self-Persistence****ensures the malware remains active. If Gayfemboy detects that its process has been terminated, it automatically re-executes itself.” continues the report. “As part of its***Sandbox Evasion***technique, Gayfemboy introduces a deliberate delay of 50 nanoseconds. If executed in a sandbox environment that cannot accurately handle such a fine-grained delay, the timing function fails, causing the malware to misinterpret the result and initiate a fallback sleep of approximately 27 hours.”*

Gayfemboy connects to its C2 by resolving random domains (e.g., *cross-compiling[.]org*, *furry-femboys[.]top*) via public DNS (1.1.1.1, 8.8.8.8) to evade local filtering. It scans 15 ports to establish communication and supports lightweight 4-byte commands (reset, sleep, info) plus extended commands like payload download, reverse shell, firewall rule changes, and launching DDoS. Self-protection includes clock-based sandbox checks and a remote **^kill^** command.

“While Gayfemboy inherits structural elements from Mirai, it introduces notable modifications that enhance both its complexity and ability to evade detection. This evolution reflects the increasing sophistication of modern malware and reinforces the need for proactive, intelligence-driven defense strategies.” concludes the report that includes Indicators of Compromise. “Staying ahead requires not only regular patching but also in-depth analysis and exposure of emerging threats to develop effective countermeasures and mitigate risk.”

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,Gayfemboy botnet)