ADVISORY FOR ICM SECTOR

Mirai-based botnet resurges to target Media industry

Original report published on: Aug 2025[1]

Executive Summary

FortiGuard Labs observed a resurgence of a Mirai-derived IoT botnet family dubbed “Gayfemboy” in July 2025, which has been exploiting network routers and devices vulnerabilities from vendors such as DrayTek, TP-Link, Raisecom, and Cisco. The botnet has been observed across multiple countries and sectors including the media and communications sector. The malware employs evasion techniques, including custom file naming to avoid predictable patterns, obfuscation with modified UPX headers, and self-protection mechanisms.

Background

The campaign targets routers and other networked devices from vendors including DrayTek, TP-Link, Raisecom and Cisco that leverages a mix of N-day and 0-day vulnerabilities (Refer to Annex A) to establish persistence, launch DDoS or cryptomining activity and provide backdoor/C2 access to operators.

The malware demonstrates defense evasion and persistence techniques (e.g. automatic file renaming, hibernation, sandbox-evasion), modular botnet with functions such as:

- Monitor (persistence, sandbox evasion, process killing)
- Watchdog (ensure only one instance, restart if killed)
- Attack / backdoor module (carry out DDoS, remote commands)
- Killer (remove competing malware)

Gayfemboy activity has been observed across multiple countries and sectors including the Media and Communications sector. Fortinet classifies the activity as high-severity and has deployed signatures/filters to mitigate it.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the Microsoft Sharepoint attacks identified in this advisory:

- Scan for Indicators of Compromise listed in Annex A to detect potential threat activities.
- Refer to the MITRE ATT&CK techniques in Annex B to create, test, and validate detection rules against the observed threat behaviours.
- Update firmware for exposed vendors (DrayTek, TP-Link, Raisecom, Cisco) and apply vendor-supplied fixes. Regular scanning and patching of internet-facing system vulnerabilities.
- Ensure all IoT and router admin accounts do not use default or weak passwords; enforce MFA for admin interfaces where supported.
- Identify all IoT/network devices, place them in segmented VLANs, with firewall and strict east-west controls and limit internet egress traffic.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

IP	Description
141[.]11[.]62[.]222	C2
149[.]50[.]96[.]114	C2
220[.]158[.]234[.]135	C2
78[.]31[.]250[.]15	C2
5[.]182[.]206[.]7	C2
5[.]182[.]204[.]251	C2

Domain	Description
cross-compiling[.]org	C2
i-kiss-boys[.]com	C2
furry-femboys[.]top	C2
twinkfinder[.]nl	C2
3gipcam[.]com	C2

SHA 256	Description
1940296f59fb5fb29f52e96044eca25946f849183ceda4feb03e816b79fbaa81	Downloader
269259e5c2df6b51719fd227fa90668dd8400d7da6c0e816a8e8e03f88e06026	Downloader
87b6917034daa6f96f1f3813f88f2eb6d5e5c1b8f6b5b9ab337ab7065d4cb4c0	Downloader
ca93203a9b795ffa66e5949e1ef643314bc3f3a3db4bed551ecd1c1e20b06089	Downloader
26375b74e64d786ebc769cfd04e75eebec3b100da3637976e433a67ffa0cac79	Downloader
2bfe2748bc594614dd03577053b58a5fb9fb8a6182fecc2025f1b715554d7fe1	Downloader
39fdef9339c75723d865481283f3d4566f78969743eef38061beddcbf5a2690d	Downloader
7eee9ad9bb0154c8e60201f3dbfe3cff84692f95f0515c6c66fab7240e864b64	Downloader
ed3f85e537ada33c5f3b1f09b5df6e8b4345514e920f7e75fc0a6535b7e4a352	Downloader
728dbb47e10a245b612453b8f9aaf3fb125760691d5f0397b01da2190f2e9709	Downloader
9cc814ac2e15d1405fb4d35cb72d6341c0df8ae26741d1b08a243f236ef4f531	Downloader
e764413c5ed6a9dba0d69b95a15841fb9b867f7aab3be7600381547eb5c2c1ab	Downloader
400cc665fd3f23a6ca7a88c4c0f8cbb4f64b7a950786f202acc64623a8e452d7	Downloader
b83b1484cf9dc6fe34a7d100c0ee582eaa2917f50bca1f7f9da7891698e3bedb	Downloader
57861ee774b1ff56035f62e48590ce16246f484503bd0670c597ea102679d86b	Downloader
737a795bfb19059062ee2f0a7b2ea0e88283413e76d1b796782423006f3b2cdf	Downloader
7fda54c9a489fea2dc8f7248d7bf72e1e356e47366478c0d5f4ba421dddf4ab7	Downloader
01c0a184c145ee382174937bb891bff90b3d574ee0616f40b3eb3ccfb68ba786	Downloader
c3862c9b2d85c74dc5b2e38c600474e8df92677c064973b0a464a1aaa12f607e	Downloader
9f77b86621c7cec885ab89a3dcf0548a7ee17c8c88f66780dfc7dcb2a13da146	Downloader
e85291d70a144ebe2842aeba2c77029762ca8ebfd36008b7bb83cda3e5d5d99d	Gayfemboy Malware Binary
dd0c9a205b0c0f4c801c40e1663ca3989f9136e117d4dcb4f451474ceb67c3da	Gayfemboy Malware Binary
6ca219e62ca53b64e4fdf7bff5c43a53681ed010cbaa688fa12de85a8f3de5e7	Gayfemboy Malware Binary
0672a9aebc7597eef44490f40c42e203d5ddfebc9300b62f38b0d1312a852235	Gayfemboy Malware Binary

47785b773808d7e1d2f1064b054e7e13b8b2ce9a35c68b926cd32c006c78f655	Gayfemboy Malware Binary
48d2c2c68fa0bd44eb70c1a6cf572406442b289fb6030e946f0530ce6f9fad98	Gayfemboy Malware Binary
5a2d60ab5d281e0118603cc793f49f7e95a87de959a25bb3275c09ec8e8762e5	Gayfemboy Malware Binary
92f9bcf6c55008c60013b75b49e143a1c9673e838efe0971490d19a241146fe5	Gayfemboy Malware Binary
915ee7620406946b859dd4a00f9862d77fba8b452aebee5d94587e66c1085c88	Gayfemboy Malware Binary
e597b492a88f0524ea38121e6b8230d9515a82ea8ca28cdcc64413c33ed846c9	Gayfemboy Malware Binary
fed7a3cec01cad14d9a46804b43e64a8021e89d8d38a49a700cf8c2e0c2578f6	Gayfemboy Malware Binary
bcdbeb7eeb64d6daf5aa6e13f1f70acfe057df50ec4773f434ffab684b78aead	Gayfemboy Malware Binary
282ada9a29a5f3144114373ef3c5826bcc8fb5018cd0f2ecb97d2a7bee1df296	Gayfemboy Malware Binary
bba29011e0b51eb0907735933641c226f3441f79a8e49ab6047c1625dd0b5176	Gayfemboy Malware Binary
08a4bd4758e4cbf39fff22a0cc5fb28d9bdd9944a0cd2120fdbe9222aaecbcf4	Gayfemboy Malware Binary
f99b33bd086f9b331a0df40525a45326bb977fee5272111edaffbe4be56e78fa	Gayfemboy Malware Binary
49b1a220b9a7450e151f19eec3da496b26799612811e512d138da88e0ee596bc	Gayfemboy Malware Binary
493e33d9ade8781e93fe9cd982de42a8032d2fc6b07baf5b202e0761a0fbe89d	Gayfemboy Malware Binary
ac14a60064081215f5a308ebeb6de69d67e6cb52ebb38d60fef99137fc1ea93a	Gayfemboy Malware Binary
7863ba5267cb187ba3892060f3868dca8b0dfae712649a650847e22d47ccb60a	Gayfemboy Malware Binary
58af5c340d271ac41f4a6009281466c7ad996b1a029a27b88f03e5ec6d95c54b	Gayfemboy Malware Binary
b03cf96cf2583ea45e4c13833e7201c2c55b96a4931a909925624913e9ad8d33	Gayfemboy Malware Binary
b979fb79cf120f5d8789adb25fc016816c68e6d52bdc5749c817f4386e0c32da	Gayfemboy Malware Binary
77df7c3d6d364474d411845fa185b196dcda437134f7093126a3f3bd145bdeee	Gayfemboy Malware Binary
228b3f006d63b8d75dcb8f66951cbf75e2a4ebdf13af9e2f47ad1c1a9b2e5753	Gayfemboy Malware Binary
2c758b1eac4fda920f90c459b773e7c3017e90f9049502b41d8b5391a8b61621	Gayfemboy Malware Binary
834d7c6bb4fd6b5da03e36fed96d7a828342d7e8bf27222b17f9f39bc6aaed80	Gayfemboy Malware Binary
05cfcef1273063c0c8b0eadf429e850471223bc2403a7cc943c252306d72e561	Gayfemboy Malware Binary
fbc42240f07235d3a0290f3e82a06ef4376e845973c146e423f8de4913a1cce4	Gayfemboy Malware Binary

82b221177f2e31052245d761e9aca47a511ae3ee9d6602ddb1f9b5be25745638	Gayfemboy Malware Binary
1b6deb5f47ebfe3a0cbb35751f3df6a893c6570cb7863c74e4262397edd6552e	Gayfemboy Malware Binary

CVEs affected
CVE-2020-8515: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2020-14993: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2023-1389: TP-Link.Archer.AX21.luci.stok.Command.Injection
CVE-2024-7120: Raisecom.Gateway.Devices.Base.Config.Command.Injection
CVE-2024-45884: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-45885: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-45887: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-45888: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-45890: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-45891: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2024-48074: DrayTek.Devices.mainfunction.cgi.Command.Injection
CVE-2025-20281: Cisco.ISE.InternalUser.Remote.Code.Execution

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1547	Boot or Logon Autostart Execution
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1497.003	Virtualization/Sandbox Evasion: Time Based Evasion
Defense Evasion / Impact	T1562.001	Impair Defenses: Disable or Modify Tools
Discovery	T1057	Process Discovery
Discovery	T1046	Network Service Scanning
Command and Control	T1071	Application Layer Protocol
Command and Control	T1043	Commonly Used Port
Collection / Ingress	T1105	Ingress Tool Transfer
Impact	T1498	Network Denial of Service
Impact / Persistence	T1219	Remote Access Tools / Backdoor

References

1. The Resurgence of IoT Malware: Inside the Mirai-Based Botnet Campaign