Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

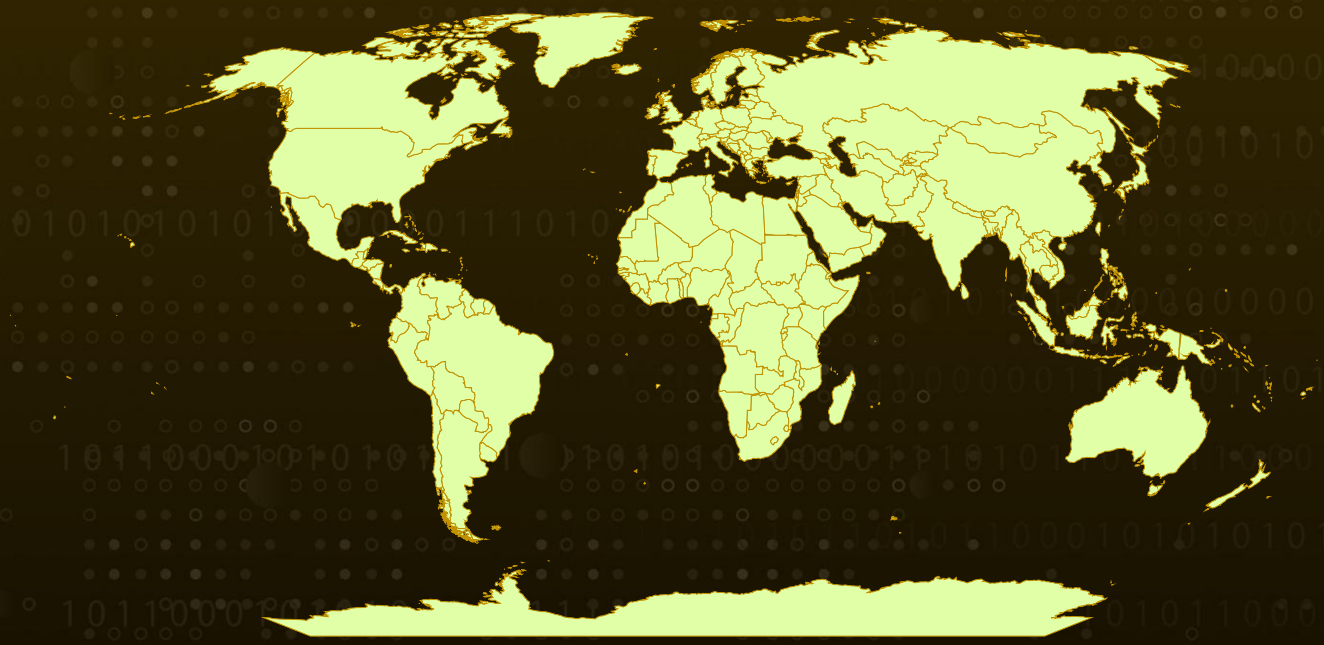
Masjesu: Exploit-Driven Botnet with Stealth, Scale, and Staying Power

Date of Publication	Admiralty Code	TA Number
April 10, 2026	A1	TA2026097

Summary

First Seen: Early 2023
Targeted Regions: Global
Targeted Platforms: Linux-based IoT devices across i386, MIPS, ARM, SPARC, PowerPC, M68K (Motorola 68000), AMD64 architectures
Targeted Products: D-Link routers, GPON routers, Huawei Home Gateway routers, MVPower DVRs, Netgear routers, Eir D1000 routers, TP-Link routers, Vacron NVR, Realtek-based devices, CCTV/DVR systems, UPnP-enabled services
Targeted Industries: Internet Service Providers, Telecommunications, Smart Home/Consumer Electronics, Gaming, Content Delivery Networks, Enterprises
Malware: Masjesu botnet (aka XorBot)
Attack: Masjesu is a commercially operated IoT botnet active since early 2023, marketed as a DDoS-for-hire service via Telegram. It propagates by scanning random IP addresses and exploiting known vulnerabilities in consumer routers and IoT devices from manufacturers including D-Link, GPON, Netgear, and Huawei. The botnet uses XOR-based encryption to obfuscate strings and C2 configurations, employs process name spoofing and cron-based persistence to evade detection, and supports a wide array of DDoS flood methods including TCP, UDP, HTTP, GRE, OSPF, and Valve Source Engine attacks capable of generating approximately 290 Gbps of traffic.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-10561	Dasan GPON Routers Authentication Bypass Vulnerability	Dasan GPON Routers	✗	✓	✗
CVE-2018-10562	Dasan GPON Routers Command Injection Vulnerability	Dasan GPON Routers	✗	✓	✗
CVE-2024-12847	NETGEAR DGN1000 authentication bypass vulnerability	NETGEAR DGN1000	✗	✗	✓

Attack Details

#1

Masjesu wastes no time casting a wide net, relentlessly sweeping the internet for exposed devices and weak entry points. By probing random IP addresses across commonly abused ports like 80, 8080, 8443, 37215, and 5555, the botnet identifies systems running vulnerable services and quickly moves to exploit them. Its arsenal includes targeted exploits for GPON routers leveraging CVE-2018-10561 and CVE-2018-10562, alongside newer flaws such as CVE-2024-12847 in Netgear devices. It also targets Huawei Home Gateways, D-Link routers, Eir D1000 devices, and various CCTV/DVR and HNAP/JAWS endpoints. Once access is secured, a malicious shell script is fetched from the C2 server, deploying payloads tailored for multiple architectures, including i386, MIPS, ARM, SPARC, PowerPC, M68K, and AMD64.

#2

After gaining a foothold, Masjesu rapidly establishes control while reinforcing its persistence. It binds a socket on TCP port 55988 to maintain direct communication with operators and suppresses termination signals to resist shutdown attempts. Critical configuration data, such as C2 domains, IPs, and process names, is stored in encrypted form and decrypted at runtime using a layered XOR routine with keys 0x16, 0x9F, and 0x8. To ensure long-term access, the malware renames itself to mimic a legitimate Linux binary and installs a cron job that re-executes it every 15 minutes, effectively surviving reboots and cleanup attempts.

#3 Masjesu is equally aggressive in eliminating competition and restricting administrative control. It actively terminates processes like wget, curl, and sshd, preventing both rival botnets from deploying payloads and administrators from accessing the system via SSH. The malware further tightens its grip by modifying permissions in the /tmp directory to read-only, blocking other malware that relies on shared storage. It also hunts down and kills processes associated with competing botnets such as Mirai and Gafgyt, often identified through "i386" naming conventions, ensuring exclusive control over the compromised device.

#4 Its command-and-control infrastructure reflects a shift toward resilience and redundancy. The latest variant rotates across four domains with a fallback IP, maintaining connectivity even if parts of the infrastructure are disrupted. Communications are encrypted using the same multi-stage XOR technique, and infected hosts beacon back system details, including architecture and botnet version (1.04). When triggered, Masjesu can launch a wide range of DDoS attacks, dynamically selecting from 13 attack vectors, including UDP, TCP SYN, TCP ACK, HTTP, GRE, ICMP, IGMP, OSPF, RDP, and Valve Source Engine floods based on encoded instructions.

#5 Perhaps most notably, Masjesu demonstrates calculated restraint to avoid unnecessary exposure. It deliberately excludes IP ranges associated with the US Department of Defense, federal agencies, and critical government infrastructure from its scanning activity. This selective targeting reduces the likelihood of attracting high-profile law enforcement attention, allowing the botnet to operate longer and more quietly. Combined with its multi-architecture reach, exploitation of known CVEs, and aggressive control mechanisms, Masjesu stands out as a well-engineered and persistent threat built for both scale and survivability.

Recommendations

- **Patch IoT Firmware Immediately:** Apply the latest firmware updates for all D-Link, GPON, Netgear, Huawei, TP-Link, Eir, Realtek, and Vacron devices. Masjesu exploits known vulnerabilities including CVE-2018-10561, CVE-2018-10562, and CVE-2024-12847 to gain initial access, and patching eliminates these entry points.
- **Replace Default and Weak Credentials on IoT Devices:** Change all default usernames and passwords on routers, gateways, DVRs, and NVRs immediately after deployment. Botnet operators routinely brute-force factory-default credentials to gain device access.

Monitor for Suspicious Cron Job Creation: Audit cron schedules on Linux-based IoT and embedded devices for unexpected entries executing binaries every 15 minutes, particularly those referencing paths resembling legitimate system linkers like "usr/lib/ld-unix.so.2."

Detect Process Name Spoofing: Implement file integrity monitoring and process auditing to detect when process names are altered to impersonate legitimate system components such as "/usr/lib/systemd/systemd-journald." Cross-reference running process names against their actual binary paths.

Alert on the "masjesu" User-Agent String: Configure web proxies, IDS/IPS, and network monitoring tools to flag HTTP traffic containing the user-agent string "masjesu," which is a distinctive fingerprint of Masjesu botnet exploit payloads.

Monitor for Anomalous Outbound DDoS Traffic: Deploy traffic analysis to detect high-volume outbound UDP, TCP SYN, GRE, ICMP, and HTTP flood patterns originating from internal IoT device segments. Masjesu has demonstrated DDoS throughput exceeding 290 Gbps from its distributed infrastructure.

Restrict TCP Port 55988: Block or monitor traffic on TCP port 55988, which Masjesu uses as a hardcoded listener port for direct attacker connectivity to compromised devices.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
	T1543: Create or Modify System Process	
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Discovery	T1018: Remote System Discovery	
	T1046: Network Service Discovery	
Lateral Movement	T1210: Exploitation of Remote Services	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1008: Fallback Channels	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
Impact	T1498: Network Denial of Service	T1498.001: Direct Network Flood

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f39b67fff1f106fb1b4fa9beb386427c8e7eb010f306ad0445da70bffc855f2e, dfd830368724f6abcc542bc8b85e3d5fa2aedf8282d3805d0d6d53f45c7e0937, de5fb68023465cb5d8ace412e11032d98a41bd6af2a83245c046020530130496, d8018e31b77b135ed300a988757f409347d013b76f9c9a4972e48cb715f45967, cb4a3665ebd12bdb094b9fc188793c67ec3008363a49b1dde00d488b54df984b, b53d4781bbadb17014da280e274e11f2de9063a35f2eabd32d4596707b147306, 4190491b9006404cab256d66125bd77b1c3a0e63451fbb3d829617d7e87acc9b, 85758df12964024af3ae829e3630f9ad5de7c55dae00181198033da8816e3293, 8340ff8920412a70f0c29cdf72f6f218e61142b3f210e70e24811c413971a8ed, 620f6949b82f9ef987b7511fbbb09c2da57d8be47b019fa6a9686ce08b4c3e70, 87f11a3ee2486bc4845a28465c2e70d2d9f98725edf4a73c3359c23a43ed74b7, 9c683b0be86d4cd274a7a16073bdf092218f259b055a72f848d589574e9b8084, 8ce9145fee0d3d2444554d901b334c36e71bb1346280ada7ff366cf9d25c5938
Domains	conn[.]masjesu[.]zip, Gpbtpz[.]rodeo, conn[.]elbbird[.]zip, starlight[.]fans, satanshop[.]net, conn[.]f12screenshot[.]xyz
IPv4:Port	158[.]94[.]208[.]122[:]443, 178[.]16[.]54[.]252[:]443, 192[.]168[.]5[.]220[:]443

Patch Link

https://www.netgear.com/support/product/dgn1000

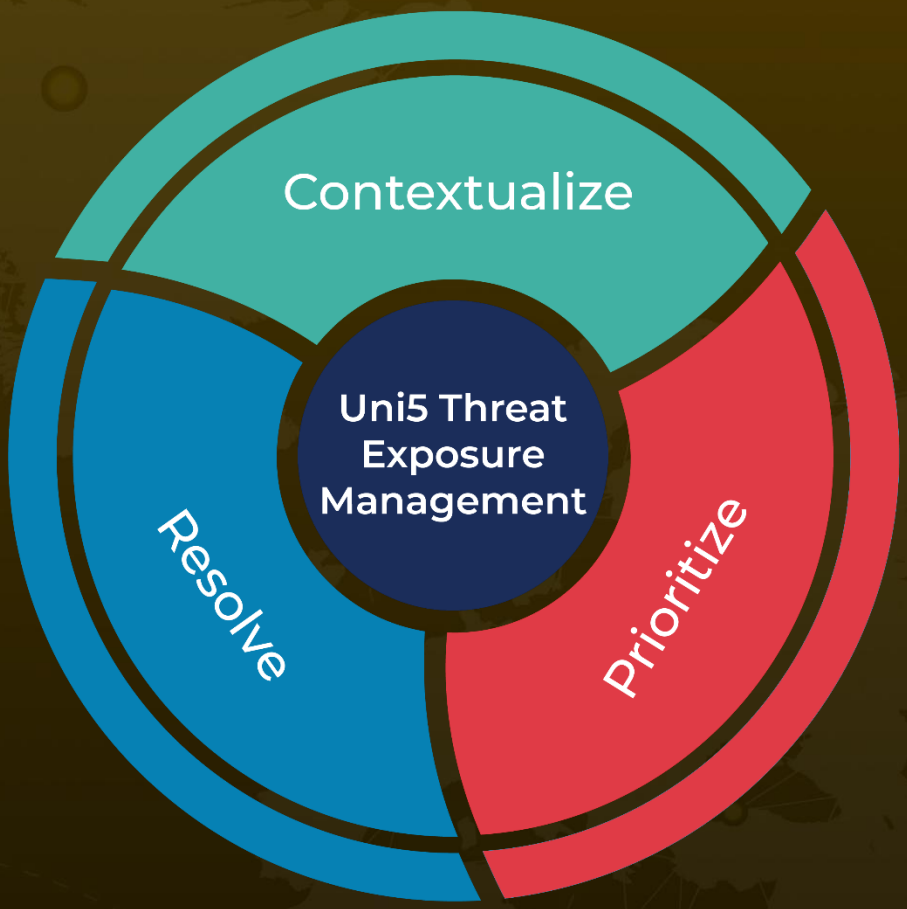
References

https://www.trellix.com/blogs/research/masjesu-rising-stealth-iot-botnet-ddos-evasion/

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

April 10, 2026 • 9:00 AM

More at www.hivepro.com