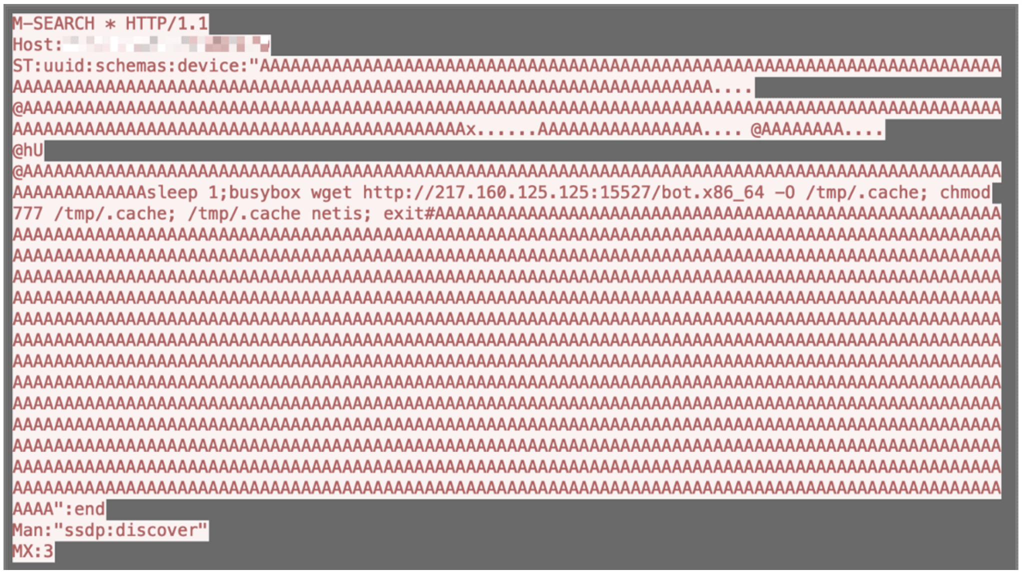
IOT BOTNET C0XMO ADDS COMPETITOR-KILLING CAPABILITY

Pierluigi Paganini June 08, 2026



C0XMO is a new Gafgyt botnet variant exploiting old router flaws, spreading across IoT devices, killing rivals, and enabling large-scale DDoS attacks.

In March 2026, FortiGuard Labs discovered a new variant of the Gafgyt botnet, dubbed C0XMO, which is noticeably more capable than its predecessors. The malware spreads through CVE-2021-27137, a stack buffer overflow in the UPnP service of DD-WRT router firmware that's been sitting unpatched on countless devices since 2021. The entry point is a crafted UDP packet sent to port 1900, exploiting how the SSDP parser handles oversized values in M-SEARCH requests. The attack doesn't require authentication.

for ARM, MIPS, PowerPC, SuperH, x86, and x86_64, covering essentially every Linux architecture you'd find in a router, DVR, or network-attached device. The attacker's distribution server at 217.160.125.125:15527 serves both the main bot binary and the Python scanner script that drives lateral movement.

The persistence mechanism runs in four stages. C0XMO copies itself to hidden paths at /tmp/.sys, /var/tmp/.sys, and /dev/shm/.sys, sets permissions to 755, creates cron jobs that relaunch it every 15 minutes, and appends execution commands to shell profile files like .bashrc and .bash_profile. If the process gets killed for any reason, it relaunches itself automatically. The operators clearly wanted this to survive basic cleanup attempts.

After locking itself in, C0XMO goes after the neighborhood. It scans every active process in /proc against an internal blacklist and terminates anything that matches: competing botnets, red team tools, network services, programming utilities. Then it goes further.

"C0XMO attempts to eliminate competing botnets run by other threat actors." states the report. "It not only deletes rival malware binaries but also tries to remove associated persistence mechanisms such as cron jobs, rc.local, init.d services, system services, and shell profile scripts."

The malware uses a custom command-and-control (C2) system with a three-step handshake to connect to its server. First, the bot sends a secret string and waits for a reply. Then it identifies itself as a bot, receives confirmation, and sends a final code before entering standby mode. Once connected, it waits for instructions such as checking status, starting or stopping scans, or launching attacks. The attack options are extensive, with 19 different methods.

It can launch many types of DDoS attacks, including UDP, TCP, SYN and ICMP floods, as well as amplification attacks like NTP and Memcached. It also targets gaming services, voice platforms, and tries to bypass protections like OVH and Cloudflare. This shows the operators are not only targeting easy victims but also more protected and hardened systems.

What separates C0XMO technically from older Gafgyt variants is the decision to split scanning into a standalone Python script rather than embedding it in

“Unlike traditional botnets, C0XMO isolates its scanning function into an independent Python script.” continues the report. “The malware fetches this script from the same IP address and port—217[.]160[.]125[.]125:15527—that it uses to distribute the main C0XMO binary.”

Keeping the scanner as a separate module lets attackers easily update, replace, or adapt it for new device types without changing the main malware. This makes the botnet more flexible and easier to maintain.

The malware also includes a large set of HTTP exploits. The scanner targets CVE-2021-27137 (the same DD-WRT flaw used for initial access), CVE-2015-2051 in D-Link devices, CVE-2022-35914 in GLPI, AVTECH DVR vulnerabilities including CVE-2025-34054 and CVE-2016-15047, NVMS-9000 flaws, Zyxel SysTools remote code execution, and several others. The ADB module goes after Android devices with exposed debug interfaces, which is a category of vulnerable hardware most enterprise security teams don’t monitor at all.

C0XMO is more advanced than older IoT botnets. It uses modular components, multi-step spreading methods, and a more structured design that makes it flexible and scalable. Separating scanning and infection functions shows a shift toward more efficient and adaptable botnet operations compared to typical Gafgyt malware.

“C0XMO exhibits a considerably more advanced architecture and feature set compared to earlier IoT botnets. Its modular exploitation features, multi-phase propagation methods, and overall design suggest a greater degree of operational sophistication and complexity than typical Gafgyt malware.” concludes the report. “The distinction between its scanning and propagation parts underscores an evolution towards more adaptable and scalable botnet deployment strategies.”

Follow me on Twitter: @securityaffairs and Facebook and Mastodon

Pierluigi Paganini

(SecurityAffairs – hacking, botnet)

C0XMO botnet | Cybercrime | DDoS | Gafgyt botnet | Hacking | hacking news | information security news | IT Information Security | malware | Pierluigi Paganini | Security Affairs | Security News

NEWSLETTER

Subscribe to my email list and stay up-to-date!

Your email address

SIGN UP

RECENT ARTICLES

SECURITY AFFAIRS MALWARE NEWSLETTER ROUND 106

MALWARE / July 19, 2026

Security Affairs newsletter Round 586 by Pierluigi Paganini – INTERNATIONAL EDITION

BREAKING NEWS / July 19, 2026

Attackers Can Take Over WordPress Sites Using Newly Released wp2shell Exploits

OpenSSL Fixes HollowByte Memory Exhaustion Bug

HACKING / July 18, 2026

Daxin: 13-Year-Old China-Linked Malware Found Still Active on Manufacturer's Network

MALWARE / July 18, 2026

securityaffairs

To contact me write an email to:

Pierluigi Paganini :
pierluigi.paganini@securityaffairs.co

LEARN MORE

QUICK LINKS