KadNap Botnet: Kademlia DHT C2 Evasion on ASUS Edge Devices

Analysis of a P2P Router Botnet Powering the Doppelgänger Criminal Proxy Service

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-11

Analysis of a P2P Router Botnet Powering the Doppelgänger Criminal Proxy Service

Cloud Security Alliance AI Safety Initiative | March 11, 2026

Key Takeaways

- KadNap is a botnet that had compromised more than 14,000 edge devices as of its March 10, 2026 public disclosure by Lumen Technologies' Black Lotus Labs, with ASUS routers running ARM and MIPS firmware as the primary targets. The botnet was first detected in August 2025 [1].
- The botnet employs a custom Kademlia Distributed Hash Table (DHT) implementation for command-and-control communications, blending malicious peer discovery traffic with legitimate BitTorrent ecosystem traffic to evade detection and resist takedown [1].
- Despite its decentralized design, KadNap's architecture relies on two persistent intermediary nodes that all command traffic transits, creating an investigative chokepoint that researchers exploited to map the underlying infrastructure [1].
- Infected devices are enrolled as residential proxy exit nodes for Doppelgänger, a criminal proxy service launched in May–June 2025 that researchers assess to be a rebrand of the defunct Faceless proxy network that previously leveraged TheMoon malware [1][2][12].
- No specific CVEs have been attributed to KadNap's initial infection vector; available evidence points to credential-based entry against devices with default or weak passwords, compounded by delayed or absent firmware patching practices [1].

Background

Edge devices—consumer and small-business routers, VPN concentrators, and broadband CPE—have become a sustained focus of criminal and state-affiliated threat actors because they sit at the perimeter of both home and enterprise networks, operate with minimal visibility, and are frequently left unpatched for extended periods. The scale of the threat has grown substantially: according to sensor network data

aggregated by Help Net Security, 2.97 billion malicious sessions targeted edge infrastructure in the second half of 2025 alone, averaging approximately 212 sessions per second across the observation period [3]. The volume of opportunistic scanning and exploitation activity directed at this class of device reflects both its prevalence and the historically limited monitoring coverage applied to it.

ASUS routers have emerged as a particularly targeted class within this broader trend. In 2025, Black Lotus Labs tracked AyySSHush, a separate botnet campaign that exploited CVE-2023-39780—an authenticated command injection flaw in ASUS AiProtection—to maintain SSH backdoors on thousands of ASUS ZenWiFi, Lyra, and RT-series devices [4]. The WrtHug campaign, identified in November 2025, leveraged legacy ASUS WRT-series hardware that had passed end-of-life and would never receive patches [5]. Against this backdrop, ASUS published a batch of ten or more firmware security advisories in November 2025, including two rated CVSS 9.8: CVE-2025-59366, an authentication bypass combined with a Samba command injection enabling unauthenticated remote code execution on AiCloud-enabled routers, and CVE-2025-59367, an unauthenticated remote access flaw affecting DSL-AC51, DSL-N16, and DSL-AC750 devices [6]. The accumulation of unpatched ASUS devices across consumer and small business deployments may have contributed to KadNap's ability to scale rapidly after its launch in August 2025.

The specific technique KadNap employs for command-and-control—Kademlia Distributed Hash Table routing—has a documented lineage in malware research extending back nearly two decades. The Overbot proof-of-concept, presented at SecureCom 2008, first demonstrated how a structured P2P protocol could provide botnet operators a resilient, decentralized C2 channel without a central server to sinkhole [7]. Subsequent botnets including Hajime and Mozi applied similar P2P architectures to the IoT context, with Mozi operating at scale before its takedown in 2023 [8]. KadNap represents the current state of this technique's evolution, adapting the Kademlia model with custom obfuscation layers designed to frustrate both network defenders and law enforcement.

Security Analysis

Infection Chain and Persistence

KadNap's deployment process follows a staged, scripted model with multiple sequential components: initial access, payload staging, ELF binary delivery, and cron-based persistence. After gaining initial access—assessed to occur through credential stuffing against SSH or administrative web interfaces—the operator downloads and executes a shell script named `aic.sh` from the staging host `212.104.141[.]140` [1]. This script initiates the full installation sequence. ELF binaries compiled

for both ARM and MIPS processor architectures are retrieved and renamed `kad`, reflecting the Kademlia protocol the botnet employs. Persistence is established through hourly cron job entries, ensuring the malware restarts after process termination or device reboots [1].

A particularly aggressive persistence measure distinguishes KadNap from less staged campaigns: immediately after installation, the malware deploys firewall rules blocking inbound SSH traffic on port 22 [1]. This move appears to serve a dual purpose. It denies remote remediation access to device owners or network administrators attempting to connect via SSH, and it prevents competing threat actors from using the same credential-based entry path to displace KadNap's implant. The combined effect is a device that is silently compromised, nearly opaque to external diagnosis, and defended against basic cleanup attempts.

Kademlia DHT Command-and-Control Architecture

The defining technical characteristic of KadNap is its use of a custom, modified Kademlia DHT implementation for command-and-control communications. Standard Kademlia is the peer discovery protocol underlying the BitTorrent DHT network and numerous other distributed systems; it routes lookup queries through a network of peers using XOR-based distance metrics to locate data stored at specific infohashes. KadNap adapts this protocol as an adversarial communication channel, exploiting its architectural properties to resist traditional C2 disruption techniques [1].

In KadNap's implementation, infected devices generate custom infohashes using XOR keys derived from NTP server timestamps and device uptime values [1]. These time-seeded hashes serve as dynamic lookup keys that allow infected peers to locate one another and receive commands or updated payloads. The initial peer discovery bootstrap uses legitimate BitTorrent DHT bootstrap nodes, meaning the first network connections made by an infected device are indistinguishable in type—though not necessarily in content—from ordinary BitTorrent client behavior [1]. C2 configuration data, including IP addresses and port assignments for command servers, is stored in encrypted `.sose` files delivered as payloads to infected nodes; traffic between peers is encrypted using AES, and peer identity verification employs SHA-1 hashing [1].

The defensive value of this architecture for operators is significant. Because there is no central C2 server, there is no single IP address or domain that defenders can block to neutralize the botnet's command channel. Takedown approaches that work against traditional centralized C2—blocking the C2 domain, sinkholing DNS, seizing a server—do not apply cleanly to a DHT-based system. The botnet's command traffic also benefits from protocol-level camouflage: deep packet inspection must distinguish malicious DHT activity from the vast volume of legitimate BitTorrent DHT traffic traversing the same networks.

The Intermediary Node Vulnerability

Despite the architectural elegance of its DHT design, KadNap's implementation contains a structural weakness that researchers at Black Lotus Labs exploited to map the botnet's true command infrastructure. All C2 traffic—regardless of which infected peer it originates from or which distributed hash lookup it follows—passes through one of two persistent intermediary nodes: `45.135.180[.]38` and `45.135.180[.]177` [1]. These two hosts function as a mandatory relay layer between the DHT peer network and the actual command infrastructure, a design choice that centralized an otherwise decentralized architecture.

This "phone tree" model may reflect an operator decision to maintain reliable control over the peer network without exposing the real command servers directly to all 14,000 infected devices. However, it paradoxically created exactly the kind of chokepoint that network defenders and intelligence researchers can monitor. By identifying and analyzing traffic through these two intermediary nodes, Black Lotus Labs was able to characterize the botnet's command and payload delivery patterns and publish the associated infrastructure as indicators of compromise [1]. Organizations with network visibility into egress traffic to these hosts can use that signal retroactively to identify historical KadNap activity.

Proxy Monetization and Criminal Infrastructure Linkage

Infected ASUS devices are not simply held in reserve for future use; they are actively monetized as residential proxy exit nodes for the Doppelgänger proxy service [1][2]. Doppelgänger launched in May–June 2025 and is assessed by researchers to be a functional rebrand of the Faceless anonymous proxy service that had previously relied on TheMoon malware to build its device pool [2][12]. Criminal proxy networks of this type provide customers—who may include fraud operators, credential stuffers, nation-state actors seeking traffic obfuscation, or a range of other threat actors—with outbound internet connections that appear to originate from residential broadband addresses rather than data center IP ranges.

The proxy monetization model transforms each compromised router into a recurring revenue source. ASUS routers deployed in residential and small business contexts typically carry IP addresses that fraud detection services classify as residential—a characteristic that operators of criminal proxy networks seek in order to evade IP reputation filters that would flag data center addresses. This creates a direct economic incentive for operators to accumulate and maintain large pools of high-quality residential device compromises, rather than simply using compromised routers as transient stepping stones for direct attacks.

The connection to Doppelgänger also suggests KadNap is not a standalone operation but part of a broader criminal ecosystem with defined service tiers, customer acquisition, and infrastructure investment. This pattern echoes what CSA documented in the BADBOX 2.0 and Kimwolf research note published the previous day, in which compromised Android IoT devices were similarly enrolled in residential proxy services and rented to third-party threat actors [9].

Geographic Distribution and Scale

As of the March 10, 2026 disclosure, KadNap had infected more than 14,000 devices, with over 60 percent of victims located in the United States [1]. Additional concentrations of infected devices were observed in Taiwan, Hong Kong, Russia, the United Kingdom, Australia, Brazil, France, Italy, and Spain [1]. The U.S.-heavy distribution likely reflects both the density of ASUS router deployments in North American residential and small business markets and the documented premium that criminal proxy services place on U.S.-origin residential IP addresses. The geographic spread across multiple continents is consistent with indiscriminate, opportunistic scanning activity rather than a campaign targeting specific geographies or organizations.

Recommendations

Immediate Actions

Network and security teams should immediately check ASUS router firmware versions against the advisories published in November 2025 and apply any outstanding updates, prioritizing the two CVSS 9.8 vulnerabilities CVE-2025-59366 and CVE-2025-59367 for AiCloud-enabled and DSL-series devices [6]. Devices that cannot be updated to a patched firmware version—including end-of-life hardware—should be evaluated for replacement or network isolation. Any ASUS router still using factory-default credentials must have those credentials changed before returning to service; password-based initial access remains the assessed primary infection vector for KadNap.

Security teams should query historical network logs for outbound connections to the two known KadNap intermediary nodes (`45.135.180[.]38` and `45.135.180[.]177`) and review the full indicator of compromise list published by Black Lotus Labs [1]. Connections to the initial staging host (`212.104.141[.]140`) in firewall or proxy logs would indicate that a device on the network

attempted to download the `aic.sh` installer, which may or may not have succeeded. Organizations managing large router fleets should audit for the presence of unexpected cron entries and processes named `kad` on edge devices.

Short-Term Mitigations

AiCloud remote access features should be disabled on ASUS routers where that capability is not operationally required; the November 2025 CVSS 9.8 vulnerabilities both involve AiCloud or related remote access services, and disabling the feature eliminates a significant attack surface even on fully patched hardware [6]. SSH access to routers should be restricted to specific management IP addresses via access control lists, and SSH should be disabled entirely on consumer-facing deployments where it is not needed for administration. Network segmentation that prevents router management interfaces from being accessible from general network segments reduces the exposure of management credentials to lateral movement.

Outbound traffic monitoring should include a watch for connections to BitTorrent DHT bootstrap nodes and unusual UDP traffic patterns that may indicate DHT peer discovery activity originating from network infrastructure devices. Because KadNap's DHT traffic mimics legitimate BitTorrent protocol behavior, behavioral baselines for each device type are more useful than signature-based detection alone. Edge devices that have no legitimate reason to participate in P2P networks should be blocked from initiating or receiving DHT traffic through egress filtering.

Strategic Considerations

The KadNap campaign illustrates a structural security problem in the edge device ecosystem: many routers in the wild are known to operate with default credentials, delayed firmware updates, and limited monitoring coverage—a pattern that this campaign and others like it consistently exploit. Organizations with distributed branch offices, remote workers, or supplier networks that include consumer-grade ASUS routers in scope should establish minimum firmware currency requirements and include router credential practices in their supply chain security assessments. The residential proxy monetization model means that a compromised branch office router could be silently used to route malicious traffic attributed to the organization's IP space, creating legal, reputational, and operational risk beyond the immediate security compromise.

At the strategic level, the DHT C2 evasion technique employed by KadNap represents a durable capability that the threat actor community continues to refine. Network defenders should not assume that the absence of known malicious C2 domains or IP addresses in threat feeds means that P2P-capable malware is not present. Investment in network behavior analytics capable of flagging anomalous

P2P activity from infrastructure devices—as distinct from end-user workstations where such traffic may be expected—represents a high-value defensive capability for detecting future DHT-based C2 techniques. Organizations relying solely on signature-based C2 detection will miss this class of threat until indicators are publicly available.

CSA Resource Alignment

The KadNap botnet and its exploitation of ASUS edge devices connect directly to several foundational CSA frameworks and guidance documents that organizations should consult when developing their response and longer-term security posture.

The **CSA IoT Security Controls Framework v3** provides controls applicable to edge device procurement, deployment, and lifecycle management [10]. The firmware update management, credential hygiene, and network segmentation controls in that framework address the specific weaknesses KadNap exploits. Organizations that have implemented the IoT SCF's device onboarding controls—including mandatory credential rotation at provisioning and automated firmware update checks—would have reduced their exposure to the credential-based initial access assessed for KadNap.

The **CSA Zero Trust Guidance for IoT** [11] addresses the architectural principle most directly relevant to KadNap's persistence mechanism: the botnet's firewall manipulation to block SSH remediation access is effective precisely because edge devices are typically not subject to the same continuous verification and least-privilege access controls applied to cloud workloads. Treating router management access as a Zero Trust resource—requiring explicit authorization, device health attestation, and least-privilege SSH access scoped to administrative IPs—limits the window in which an attacker can entrench after initial compromise.

The **MAESTRO framework** for agentic AI threat modeling, while developed in an AI context, includes threat layers relevant to the infrastructure that AI systems depend upon. KadNap's ability to silently route traffic through compromised routers means that AI-enabled enterprise systems communicating over networks that include infected edge devices may have their traffic observable or manipulable by the Doppelgänger operator. Organizations deploying AI agents that communicate with cloud APIs should ensure that traffic egresses through managed, monitored network infrastructure—not unmanaged consumer-grade routers that may be outside the organization's security perimeter—and should monitor for unexpected routing changes or proxy insertion.

The **CCM (Cloud Controls Matrix)** infrastructure security domains—particularly IVS (Infrastructure & Virtualization Security) and SEF (Security Incident Management, E-Discovery, & Cloud Forensics)—apply to the detection and response activities needed to identify KadNap compromise. The SEF controls' requirements for log retention and network monitoring capability are prerequisites for the retrospective analysis of KadNap intermediary node connections that would allow organizations to determine whether they were affected before the public disclosure.

The CSA research note on BADBOX 2.0 and Kimwolf IoT supply chain systemic risk, published the day before this disclosure, provides relevant context on the broader residential proxy ecosystem that KadNap feeds [9]. The two campaigns share the same criminal infrastructure monetization model and the same structural reliance on devices that operate outside enterprise monitoring coverage. Organizations responding to one campaign should review the other for complementary indicators and overlapping defensive guidance.

References

[1] Lumen Technologies / Black Lotus Labs, "Silence of the Hops: The KadNap Botnet," blog.lumen.com, March 10, 2026. https://blog.lumen.com/silence-of-the-hops-the-kadnap-botnet/

[2] BleepingComputer, "New KadNap Botnet Hijacks ASUS Routers to Fuel Cybercrime Proxy Network," bleepingcomputer.com, March 2026. https://www.bleepingcomputer.com/news/security/new-kadnap-botnet-hijacks-asus-routers-to-fuel-cybercrime-proxy-network/

[3] Help Net Security, "2.97 Billion Malicious Sessions Targeted Edge Infrastructure in H2 2025," helpnetsecurity.com, February 25, 2026. https://www.helpnetsecurity.com/2026/02/25/edge-infrastructure-attacks-internet-wide-exploitation/

[4] Censys, "Tracking AyySSHush: A Newly Discovered ASUS Router Botnet Campaign," censys.com, 2025. https://censys.com/blog/tracking-ayysshush-a-newly-discovered-asus-router-botnet-campaign/

[5] The Hacker News, "WrtHug Exploits Six ASUS WRT Flaws to Build Persistent Router Botnet," thehackernews.com, November 2025. https://thehackernews.com/2025/11/wrthug-exploits-six-asus-wrt-flaws-to.html

[6] Field Effect, "ASUS November 2025 Security Advisories," fieldeffect.com, November 2025. https://fieldeffect.com/blog/asus-november-2025-security-advisories

[7] Wang, P. et al., "Overbot: A Botnet Protocol Based on Kademlia," SecureCom 2008, September 2008. https://seclab.nu/static/publications/securecomm2008overbot.pdf

[8] Unprotect Project, "Peer-to-Peer C2," unprotect.it, accessed March 2026. https://unprotect.it/technique/peer-to-peer-c2/

[9] Cloud Security Alliance AI Safety Initiative, "BADBOX2 and Kimwolf: IoT Supply Chain Systemic Risk," CSA Research Note, March 10, 2026. output/white-papers/CSA_research_note_badbox2_kimwolf_iot_supply_chain_systemic_risk_20260310.md

[10] Cloud Security Alliance, "Guide to the IoT Security Controls Framework v3," cloudsecurityalliance.org. https://cloudsecurityalliance.org/research/guidance/guide-to-the-iot-security-controls-framework-v3

[11] Cloud Security Alliance, "Zero Trust Guidance for IoT," cloudsecurityalliance.org. https://cloudsecurityalliance.org/research/guidance/zero-trust-guidance-for-iot

[12] The Hacker News, "KadNap Malware Infects 14,000+ Edge Devices, Powering Stealth Proxy Botnet," thehackernews.com, March 2026. https://thehackernews.com/2026/03/kadnap-malware-infects-14000-edge.html