# Silence of the hops:The KadNap botnet

By By Black Lotus Labs

Archived: 2026-04-05 14:46:02 UTC

Published on Mar 10, 2026 | 16 minute read

The Black Lotus Labs team at Lumen has discovered a sophisticated new malware named “KadNap.” This threat primarily targets Asus routers, conscripting them into a botnet that proxies malicious traffic. Since August 2025, we have been monitoring the growth of this network, which is now above 14,000 infected devices.

KadNap employs a custom version of the Kademlia Distributed Hash Table (DHT) protocol, which is used to conceal the IP address of their infrastructure within a peer-to-peer system to evade traditional network monitoring. Infected devices use the DHT protocol to locate and connect with a command-and-control (C2) server, while defenders cannot easily find and add those C2s to threat lists. In short, the innovative use of the DHT protocol allows the malware to establish robust communication channels that are difficult to disrupt by hiding in the noise of legitimate peer-to-peer traffic.

Once added to the network, bots are then marketed by a proxy service called “Doppelganger,” which is specifically tailored for criminal activity and appears to be a rebrand of the Faceless service, which was powered by victims of TheMoon malware.

Using the expansive Lumen global backbone to observe KadNap’s infrastructure, we found that more than 60% of KadNap’s victims are based in the United States. While Asus routers are the primary targets, the operators are using the malware effectively against a variety of edge networking devices and set aside a number of C2s used to silo their infrastructure by victim type.

As of this publication, Lumen has proactively blocked all network traffic to or from the control infrastructure. Given the obfuscation of C2 servers inherent to this protocol, Black Lotus Labs will share the indicators of compromise (IoCs) and will begin distributing the indicators of compromise (IoCs) into public feeds to enable others to help disrupt this threat.

Lumen Technologies would like to thank our partners at Spur for their contributions to our efforts to track and mitigate this threat.

## Introduction and understanding Kademlia

As modern society increasingly relies on internet-exposed Internet of Things (IoT) devices, the opportunities for malicious actors to exploit vulnerabilities continue to abound. Threat actors are building large-scale botnets specifically designed to hijack devices in this growing pool of targets, using them to route traffic and evade detection by network security systems.

Large residential proxy services offer millions of infected devices used by both legitimate users and malicious actors. In contrast, smaller botnets such as REMPROXY or Quad7 are exclusively operated by and marketed to criminal actors for more focused attacks, posing a significant threat whenever their IPs are active. To monitor the proliferation of both small and large botnets across the landscape, Lumen has created multiple algorithms to search for new and emerging networks as they appear.

In early August of 2025, our algorithm detected over 10,000 Asus devices that were all communicating with a particular set of servers. Our investigation into these C2s uncovered a malicious file which was used to download a shell script from a server at *212.104.141[.]140*, in a file called *aic.sh.* This file sets the stage for the KadNap malware and initiates the process of incorporating the victim into the P2P network.

The file sets up a cron job to pull the malicious shell script from the server at the 55-minute mark of every hour, rename it to *.asusrouter* and then run it from */jffs/.asusrouter* location. After the persistence was initialized, it would then pull down a malicious ELF file for the Asus routers, rename it to *kad*, and then execute it:

## Kademlia

Kademlia is an implementation of a distributed hash table (DHT) that allows for efficient decentralized lookups of information across peers and has been proven through multiple real-world protocols such as BitTorrent DHT, eMule, I2P and Etherum.

To better understand this system, think of Kademlia like using a chain of friends to find someone's phone number: each friend does not know the whole number but knows someone who can get you closer to the answer. Passing your request along this chain, you quickly put together the whole phone number. Likewise, Kademlia nodes forward queries to others that are "closer" to the target, enabling fast and efficient searches without knowing the whole network.

The KadNap malware is a custom implementation of a Kademlia DHT. Naming the ELF file *kad* was likely in relation to using this protocol to hide the IP address of the C2 server.

## Malware analysis

Once the ELF file from the malware server is loaded, it begins the process of installing KadNap. In addition to creating a "phone tree" for finding the hidden C2 addresses, the malware was designed with some versatility—Black Lotus Labs identified samples of KadNap for both ARM and MIPS processors. Each sample begins initialization by forking, setting STDIN, STDOUT and STDERR to */dev/null*, determining the external IP address, and storing into an initialized struct.

Next it will cycle through a list of NTP servers until it makes a connection, retrieves the current time and stores it along with the host uptime. These values are used later in the network communications to create a hash used to "phone friends" and find other peers in the network.

From here, the malware has enough information to move into the Kademlia DHT implementation.

## Find peers thread

After the time synchronization it will fork, creating a child process that connects to the BitTorrent network using known bootstrap nodes and generates a custom DHT packet to search for other infected nodes from which to receive commands. The child process then creates a custom infohash by filing the “name” field of the bencoded string with an XOR key computed from contacting a NTP server and the computers uptime. It then SHA-1 hashes the 0x40 bytes hardcoded string *6YL5aNSQv9hLJ42aDKqmnArjES4jxRbfPTnZDdBdpRhJkHJdxqMQmeyCrkg2CBQg* with the XOR key, and stores that value in the “pieces” field of the bencoded string.

It then SHA-1 hashes the full bencoded string and uses that as the info hash to find other peers, then sends this through a pipe to be read by another thread.

Another thread is created immediately to read six bytes from the pipe that are the IP and port of a peer on the network. It will connect to the peer and receive a buffer 0x1000 bytes in size and uses a hardcoded key to decrypt it. It then SHA-1 hashes the decrypted payload and uses the hash as the key to encrypt/decrypt follow on traffic.

It then parses the payload, which is SHA-1 hashed again. This hash is used as the key to AES encrypt/decrypt follow on traffic.

Upon reaching the final peer, if the initial handshake succeeds, the malware will receive an additional payload that is decrypted and saved as a file. The path and filename are sent to a second pipe, to be read from another thread. Two files were received after contact with the final peer the malware was searching for. One was named *fwr.sh* (likely a firewall rule) which also closed port 22 on the infected device.

The other was named *.sose* and placed in the */tmp* directory.

## Malicious thread

The parent thread continues after starting the previous two threads and goes into a loop that calls two main functions. The first function *readCommandFromPipe2AndExecute* reads a filename sent on the pipe and executes it.

The above function, labeled *tmpSose*, will check for the presence of the file */tmp/.sose* and if it exists, it will read ten bytes from the file. */tmp/.sose* contains a list of C2 IP:port as well as some other config information. The sample will then fork and attempt to reach out to the C2s.

## Kademlia Weak Custom Implementation

In a true Kademlia peer-to-peer network, the final peer changes over time, reflecting its decentralized nature. However, in analyzing our KadNap samples dating back to August 2025, we consistently found the same two final hop nodes before reaching the C2 servers. This indicates the attackers maintain persistent nodes to retain control over the network. Those two longstanding nodes were *45.135.180[.]38* and *45.135.180[.]177*

## Global telemetry analysis

Black Lotus Labs has monitored this network since August of 2025, as it had grown to maintain a daily average of 14,000 distinct victims, while using three to four active C2s on average. The botnet struggled to maintain a

consistent victim pool in the initial stages; however, as shown in the chart below, its operators have maintained a consistent size in the last few months.

The victims are distributed across several countries, with 60% located in the United States and 5% each in Taiwan, Hong Kong and Russia.

Our analysis and telemetry indicate that not all infected devices communicate with every C2 server. This suggests the threat actor is segmenting their infrastructure based on device types and models. More than half of the botnet (all the Asus victims) connects to two Asus C2 servers, while the rest communicate with one of two other active C2s.

KadNap's purpose was unclear when first discovered. However, through our partnership with Spur, they were able to tie the C2 servers we discovered as entry points for a known malicious proxy service. Based on the botnet's structure, Black Lotus Labs confidently agrees with Spur that this is likely a new botnet linked to the now defunct Faceless proxy service, which previously used TheMoon malware.

## Conclusion

The KadNap botnet stands out among others that support anonymous proxies in its use of a peer-to-peer network for decentralized control. Their intention is clear: avoid detection and make it difficult for defenders to protect against. KadNap's bots are sold through Doppelganger, a service whose users leverage these hijacked devices for a range of malicious purposes, including brute-force attacks and highly targeted exploitation campaigns. As a result, every IP address associated with this botnet represents a significant, persistent risk to organizations and individuals alike.

Black Lotus Labs will continue to find, monitor and track malicious botnets to help secure the internet. With KadNap, Lumen Defender℠ customers have been protected from this network since August 2025. We will share indicators of compromise (IoCs) in public feeds to support global defenders and disrupt this threat.

We encourage the community to monitor and alert on these and any similar IoCs. We also advise the following actions.

## Corporate network defenders

- Continue to look for attacks on weak credentials and suspicious login attempts, even when they originate from residential IP addresses which bypass geofencing and ASN-based blocking
- Protect cloud assets from communicating with bots that attempt to perform password spraying attacks and begin blocking IoCs with Web Application Firewalls
- Check for devices reaching out to public BitTorrent trackers and exhibiting connectivity to any known peers within the KadNap network

## Consumers with SOHO routers

- Users should follow best practices for regularly rebooting routers and installing security updates and patches. For guidance on how to perform these actions, please see the best practices document prepared by

Canadian Centre for Cybersecurity.

- Organizations that manage SOHO routers: make sure devices do not rely upon common default passwords. They should also ensure that the management interfaces are properly secured and not accessible via the internet. For more information on securing management interfaces, please see DHS' CISA BoD 23-02 on securing networking equipment.
- Check for devices reaching out to public BitTorrent trackers or exhibiting connectivity to any known peers within the KadNap network.
- We also recommend replacing devices once they reach their manufacturer end of life and are no longer supported.

Analysis of KadNap was performed by Chris Formosa and Steve Rudd with technical editing by Ryan English.

Current IOCs will be found on our GitHub page and continuously updated there. We encourage the community to monitor and alert on these and any similar IoCs.

If you would like to collaborate on similar research, please contact us on LinkedIn or X @BlackLotusLabs.



**Author**

**Black Lotus Labs**

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.

---