Classic Rock: Hunting a Botnet that preys on the Old

blog.lumen.com/black-lotus-labs-criminal-proxy-network/

May 9, 2025

Black Lotus Labs Posted On May 9, 2025

2.3K Views

Executive Summary

Along with the Department of Justice and the Dutch National Police, Lumen's Black Lotus Labs team has tracked a criminal proxy network for over a year as it infected thousands of IOT and end-of-life (EoL) devices, powering a botnet designed to offer anonymity for malicious actors online. Through Lumen's global backbone, we discovered a weekly average of 1,000 unique bots in contact with the command-and-control (C2) infrastructure, located in Turkey (Türkiye). Over half of these victims are in the United States, with Canada and Ecuador showing the next two highest totals. Their website claims to have been in operation since 2004, and while they may not maintain the size of some well documented proxies like CloudRouter or Proxy.AM, their target selection and longevity show they are equally as dangerous.

The botnet controllers require cryptocurrency for payment. Users are allowed to connect directly with proxies using no authentication, which as documented in previous cases, can lead to a broad spectrum of malicious actors gaining free access. By targeting IOT and SOHO devices in the residential IP space, cybercriminals create a veil of legitimacy for their traffic that complicates tracking and mitigation efforts. Given the source range, only around 10% are detected as malicious in popular tools such as VirusTotal, meaning they consistently avoid network monitoring tools with a high degree of success. Proxies such as this are designed to help conceal a range of illicit pursuits including ad fraud, DDoS attacks, brute forcing, or exploiting victim's data.

Lumen has partnered with the Department of Justice, the Federal Bureau of Investigation, and the Dutch National Police in their efforts to take down the criminal proxy network. As this botnet was being used to facilitate an array of illicit activity against U.S. based organizations and around the world, we have disrupted the known architecture by null routing all traffic to and from their known control points, across the Lumen global backbone.

Lumen would also like to thank Spur for their contributions to our research. For defenders, we include a list of known IOCs and C2s to our GitHub page.

Introduction

Anonymity is the key to success for criminals of all stripes. This group has maintained a low profile over an extended time, ostensibly to avoid the attention of authorities and watch lists. A report from CERT Orange Polska published in 2023 brought their activities to light. Lumen prioritized their tracking a year ago and, through our global backbone telemetry, mapped their architecture over time. Our research reveals the activities of a network designed to enable widespread malicious activity by targeting devices with malware in the residential IP space. In predatory fashion, they abuse equipment that has aged out of the vendor support lifecycle and cannot be patched or protected.

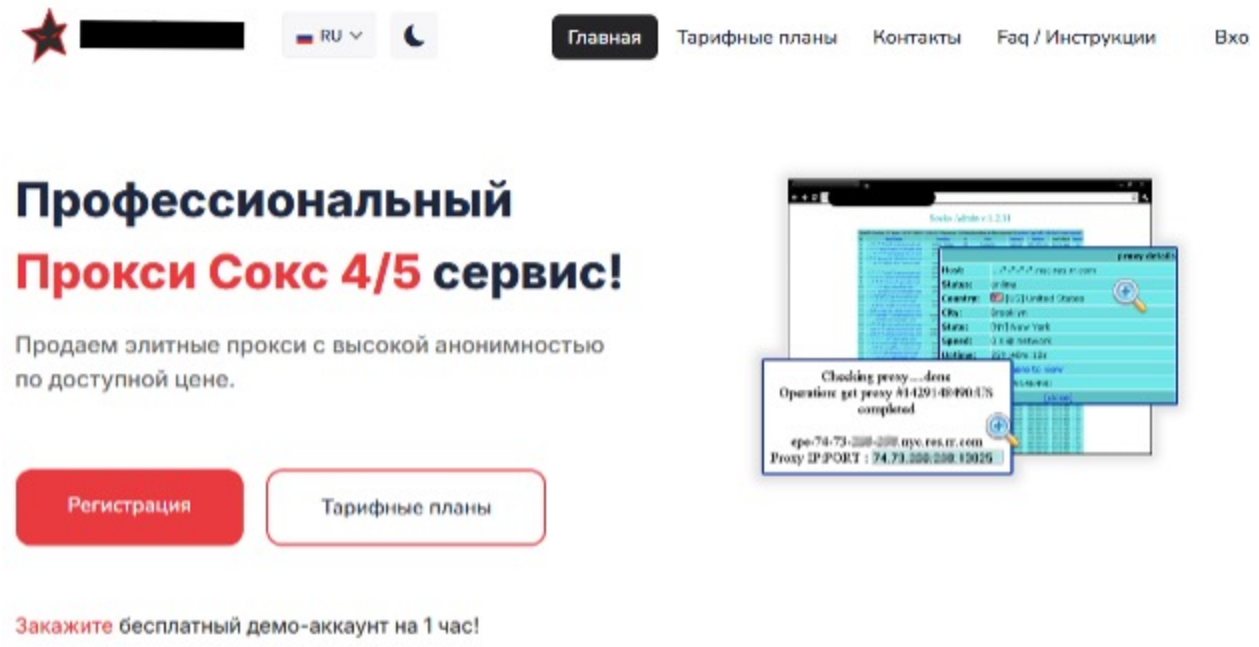

Figure 1: Proxy network homepage,

According to their own website, the service has been around since 2004, which is a testament to how well it has served its users. The quality of their proxies' connections allows malicious actors to obfuscate their activity by blending into residential traffic, which presents a challenge for network defenders. Our research into the Faceless and NSOCKS proxy services are examples of similar networks that favored the same target base and use of

malware to infect their victims. In this report, Black Lotus Labs made the decision not to publicly release details on the malware, as the devices abused by the proxy service are easy to exploit and can be targeted again by others. Instead of risking that exposure, we will focus on this service and the harm it is responsible for.

Global Telemetry

The botnet operators claim that they maintain a daily population of over 7,000 proxies. Based on Black Lotus Labs' telemetry, we can see an average of about 1,000 weekly active proxies in over 80 countries, however we believe their true bot population is less than advertised to potential users. When it comes to proxy services for malicious criminals, the most important attributes are location, stability, and anonymity. As shown in the map below, over half the victims are in the United States, followed by Ecuador and Canada with the next highest infection rates.

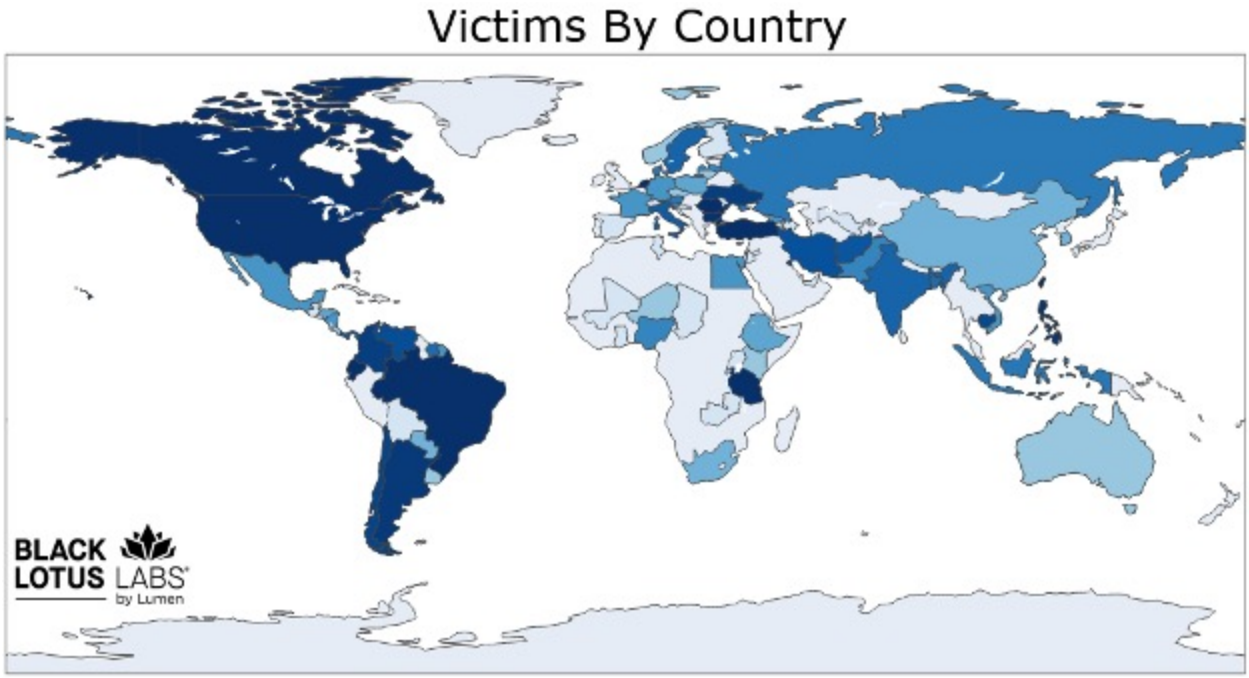

Figure 2: Victims by country, where darker shades of blue represent higher victim counts

Black Lotus Labs can see a wide variety of infected IoT device types, indicating this botnet is likely using several exploits to obtain new victims, though we do not assess the operators are using zero or one-day vulnerabilities at this time. Instead, we believe they rely on exploits that have been around for years, corresponding with their focus on unpatched or EoL devices. Choosing to avoid more up-to-date devices, they can maintain an average lifecycle of a given bot for over a week and, as stated previously, only 10% of their proxies appear in VirusTotal. Their foothold in locations around the world permits effective targeting by criminals for many different use cases.

Botnet Infrastructure

Newly conscripted victims will reach out to the Turkish-based C2 infrastructure, which is made up of 5 servers, with 4 of the 5 servers communicating with infected victims on port 80. One of these 5 servers uses UDP on port 1443 to receive victim traffic, while not sending any in return. We suspect this server is used to store information from their victims.

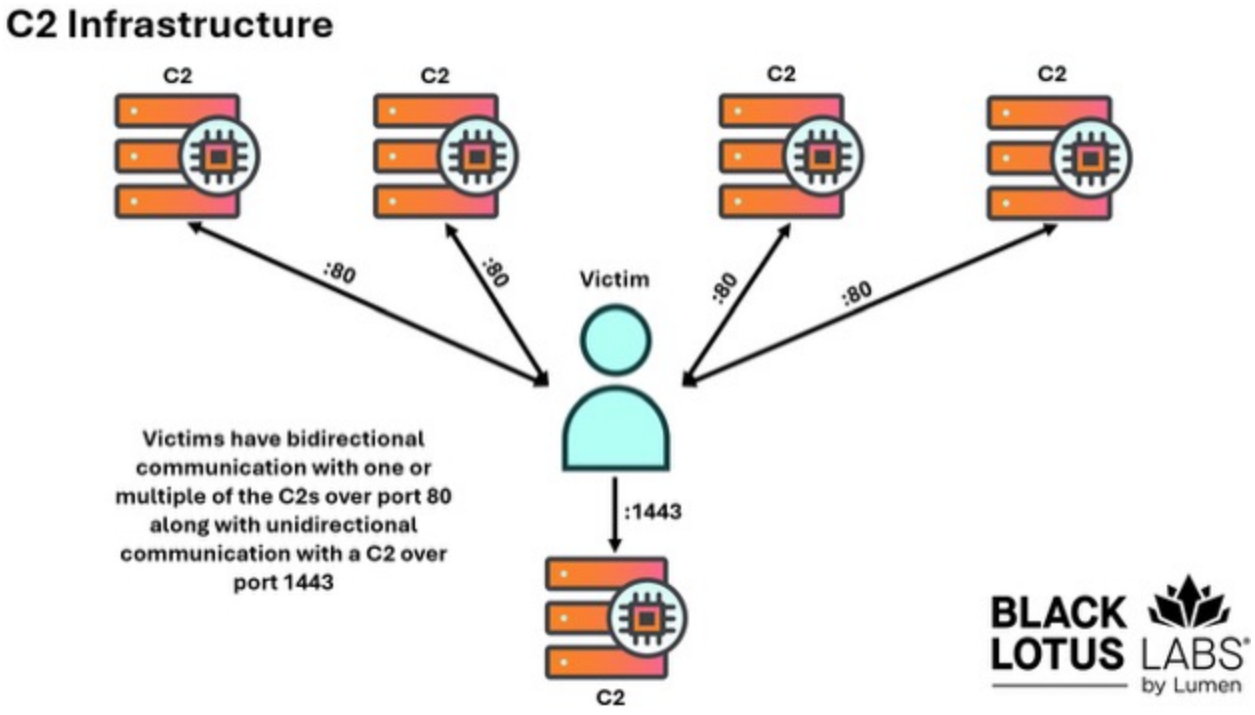

Figure 3: Command and control infrastructure

Rent-a-Proxy as a Service

When making a purchase, users are presented with the following screen:

Socks Admin v.1.2.11

	proxy details
Host:	...-*-*.dnvr.dynamic.dslblast.com
Status:	online
Country:	[US] United States
City:	Torrington
State:	[WY] Wyoming
Speed:	1 s @ network
Uptime:	3h:42m:39s
IP:PORT	click here to view
Proxy ID:	#2929318908

Figure 4: User view of proxy location and details

Once the transaction is made, users are presented with the true IP address and port, which is available for the next 24 hours. According to Spur: “once the 24-hour time window for a proxy ends that port will be closed. When that proxy is purchased again, a different port will likely open for proxying.”

Figure 5: User’s view showing the IP:port combination purchased

A key piece of information is presented to the buyer, and worth pointing out. The botnet operators perform a check to see if the IP is on any deny-list, letting the user know their selection is more likely to get around most monitoring tools. But another element is much more critical. These IPs, similar to the TTP used by NSOCKS, ask for no authentication from users. The user pipeline is shown in Figure 6; however, it is important to note that the “User” of this botnet can be anyone who manages to discover the open proxy and port.

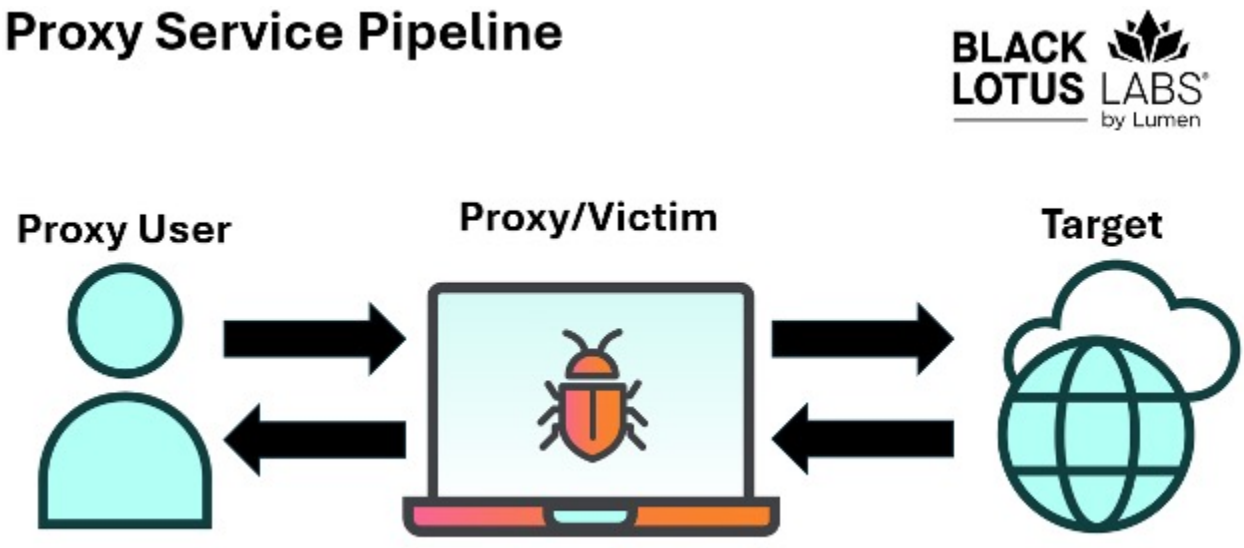

Figure 6: Direct pipeline for user’s proxy traffic

It is not clear how the botnet operators profit from an “open access” policy, but it suggests they allow much more harmful activity than what is restricted to users who rent these IPs outright. We have seen malicious actors use these services for everything from Ad fraud, in DDoS and brute force attacks, to exploiting victims’ data.

Conclusion

Proxy services have and will continue to present a direct threat to internet security as they allow malicious actors to hide behind unsuspecting residential IPs, complicating detection by network monitoring tools. As a vast number of end-of-life devices remain in circulation, and the world continues to adopt devices in the “Internet of Things,” there will continue to be a massive pool of targets for malicious actors. In our research on similar botnets like NSOCKS and Faceless, we noted how several well-known criminal groups manipulate open access policies as they are often marketed on criminal forums. Black Lotus Labs will continue to search for networks like these and share information with domestic and international law enforcement whenever the opportunity for legal action presents itself. Lumen would like to commend the FBI and the Dutch National Police for their efforts to disrupt this network.

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

Corporate Network Defenders:

> Continue to look for attacks against 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 are attempting brute force or password spraying attacks and begin blocking IoCs with web application firewalls.
>
> Updating and blocking IP addresses belonging to known open proxies, or leveraging sophisticated network perimeter countermeasures like Lumen Defender, which proactively stop proxy services from interacting with corporate networks.

Consumers with SOHO routers:

> Users should follow best practices of regularly rebooting routers, ensuring your router is not end-of-life 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.

For 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.

We also recommend replacing devices once they reach their manufacturer end of life and are no longer supported.

Analysis of the proxy service was performed by Chris Formosa. Technical editing by Ryan English.

For additional IoCs associated with this campaign, please visit our GitHub page.

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

This information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk.

Post Views: 2,319

CyberthreatsEnterprise Collaboration PlatformNetwork Security

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.

Trending Now

You may also like

Services not available everywhere. ©2025 Lumen Technologies. All Rights Reserved.