One sock fits all: The use and abuse of the NSOCKS botnet

By By Black Lotus Labs

Archived: 2026-04-05 16:41:19 UTC

Published on Nov 19, 2024 | 7 minute read

Executive summary

The Black Lotus Labs team at Lumen has expanded the known architecture of the “ngioweb” botnet, its use as a cornerstone of the notorious criminal proxy service known as NSOCKS, and appropriation by others such as VN5Socks and Shopsocks5. One of the most widely used criminal proxies, NSOCKS maintains a daily average of over 35,000 bots in 180 countries, and has been tied to notorious groups such as Muddled Libra. At least 80% of NSOCKS bots in our telemetry originate from the ngioweb botnet, mainly utilizing small office/home office (SOHO) routers and IoT devices. Two-thirds of these proxies are based in the U.S.

Through Lumen’s global internet visibility, we have traced the active and historical command–and–control (C2) nodes used by these networks, some of which were previously undiscovered and have been in use since mid-2022. NSOCKS users route their traffic through over 180 “backconnect” C2 nodes that serve as entry/exit points used to obscure, or proxy, their true identity. The actors behind this service have not only provided a means for their customers to proxy malicious traffic, but the infrastructure has also been engineered to enable various threat actors to create their own services. Among the disruptive activities these networks are used for, NSOCKS has also provided an avenue for various actors to launch powerful DDoS attacks.

Lumen has blocked all traffic across our global network, to or from the dedicated infrastructure associated with the ngioweb botnet. We are releasing indicators of compromise (IoCs) to help others identify and take defensive measures, disrupt this operation, and impact the larger cybercrime ecosystem.

Lumen Technologies would like to thank our partners at Shadowserver, Spur, and throughout the industry for their contribution to our efforts to track and mitigate this threat.

Introduction

Maintaining anonymity and disguising online activity is a critical part of the criminal business model. Although the concept of proxy botnets is not new, we have observed an increase in their prevalence and reach such as with Socks5Sytemz and Cloudrouter.

The tracking and inventory of this global network is the culmination of over a year’s research, though the ngioweb botnet has been well-documented in the past, dating back to 2018 and 2019 as well as more recent publications by LevelBlue Labs. Black Lotus Labs has connected the critical elements of this intricate web with previous research to illustrate its use as the engine driving the NSOCKS service and a random assortment of villainous interests. Though this enterprise was built to offer criminals an avenue to proxy their traffic, users have abused and altered

the network into its present state – one which directly supports many other forms of malicious activity such as obfuscating malware traffic, credential stuffing, and phishing. Botnets such as these present a concerning and persistent threat to legitimate organizations across the internet.

ngioweb infrastructure

The ngioweb botnet is composed of two distinct elements. The first is the "loader" network, which directs the bot to a loader-C2 node for retrieval and execution of the ngioweb malware. Black Lotus Labs was not able to see the initial access vector, however, it likely stems from a variety of exploits the operators have access to (as noted by Netlab360). These exploits will download a shell script that directs an infected user to an IP address holding the latest version:

The hosted files have four letter names that seem to change over time, in this case the "AIDY" name was used. Renaming provides some obfuscation in the event that a researcher tries to gather a file from an older sample, as it may no longer exist. This shell script provides a second defensive measure by quickly removing the file after it begins running on the victim machine.

Black Lotus Labs generally tracks between 15-20 loader nodes at any given time, several of which do not appear in public databases or reporting. Given the recent research by LevelBlue Labs showing that each of these loader C2s is likely searching for at least one specific exploit, we suspect that the ngioweb actor likely has access to at least 10-15 exploits at present. These loader C2s are primarily characterized by their traffic with bots, over port 80 and port 21 (FTP). This entire arm of the botnet is likely monitored and controlled by a node at 103.172.92[.]148, which on average communicates solely with about half of the loaders we track.

Once infected, a victim will reach out to a second stage of C2 domains for management, addresses for these are created by a domain generation algorithm (DGA). This group of C2s appear to determine if a bot is worth adding to the proxy network. We generally see close to 15 domains active at any one time; these gatekeepers form a nexus of control by not only monitoring and checking in on the bots' capacity for traffic, but they also connect useful bots with a "backconnect" C2 which will make them available in the NSOCKS proxy service for anyone to use. Below is an overview of a victim's interaction with this botnet:

Malware analysis

We analyzed a recent sample of ngioweb's malware and there did not appear to be much change in the malware since Net360 analyzed it in 2019. The new sample did not contain any hardcoded C2 URLs in the configuration, we surmise the malware will only use the DGA-created domains.

The C2 communications between the ngioweb sample and the DGA-generated C2 did not seem to be any different from initial reporting, however we did see some additional traffic between the bot and the backconnect C2s

As a defensive measure, the malware uses DNS TXT records as a method to prevent the sinkholing or takeover of the DGA domains. The malware expects two TXT records with keys "p" and "v," these values are concatenated and Base64 decoded. The result is an Md5WithRSA encrypted blob that is decrypted using the 0x100 byte array stored in the encrypted config (colored blue in the configuration image). Once the blob is decrypted it contains the MD5 hash for the string "DOMAINNAME\xAA\xBB\xCC\xDD," where "\xAA\xBB\xCC\xDD" is the IP

address that the domain resolves to. So “remalaxation[.]name\x2e\xf6\x60\x28” is hashed with MD5, resulting in 9998be16901e7f80aad8d931305e057e.

After receiving the CONNECT command, the bot will reach out to the backconnect C2 supplied in the command (66.29.128[.]243:443 in this case). The bot will then check-in with the C2 which will direct it to “start proxy” (0x1011). The bot will act on the instruction and send command 0x14 (TCP server started), to which the C2 will respond with a GET request to proxy through the bot to a random looking URL – in this case, the same C2. The bot then requests the URL, and the response contains “It works!” along with the infected machine’s external IP.

After proxying the “random” URL, the C2 will then send a request for the bot to proxy a connection to another arbitrary-looking subdomain of nslookups[.].com. Below is a decrypted payload and the request from bot to resolve the nslookups domain:

After the initial proxy request, the bot will stay connected to the C2 while waiting for additional commands and may receive additional proxy commands during this time. Below is a decrypted request to a proxy checking service:

Occasionally, after a command 0x14 is sent to a C2, it will respond with a request to download a “test.zip” file. This is likely to evaluate the speed of the proxied connection for suitability and later, to possibly factor into the cost per daily use.

Global telemetry analysis

The ngioweb botnet employs a variety of exploits, with 15% of observed devices running vulnerable or discontinued web application libraries such as YUI. Zyxel devices, Alpha Technology devices, and Reolink security cameras each contribute to another 5% of the botnet.

Based on available telemetry, it appears that the ngioweb botnet is not leveraging zero-day exploits. Instead, it is exploiting a significant number of n-day vulnerabilities across various router models. Though many of the victim devices are older, they prove to be valuable for malicious activities as they often evade detection by common network security solutions.

80% of the bots communicating with ngioweb are also NSOCKS bots, indicating ngioweb is the only provider of proxies to NSOCKS. The network maintains a daily average of roughly 35,000 working bots, with 40% remaining active for a month or longer.

One concerning aspect is that serious criminal groups, such as the APT group Pawn Storm, have been found co-habiting the same devices as ngioweb. This means that many devices infected with ngioweb malware are likely being abused by multiple groups simultaneously.

The ngioweb botnet reaches beyond just NSOCKS, however. There are indicators that multiple other services are dependent on the NSOCKS ecosystem, which also implies they are dependent on the ngioweb botnet. About 45% of bots that are part of the ngioweb botnet are also a part of Shopsocks5, with some C2s having as much as a 65% overlap.

All bots that Black Lotus Labs could discover in the Shopsocks5 network are also in use by NSOCKS. We will discuss this connection further below.

The NSOCKS proxy network first appeared in the fall of 2022, although according to Spur, likely operated under the name of LuxSocks prior to that. Based on old ngioweb domains and files dating back several years, we suspect that LuxSocks was mostly powered by the ngioweb botnet as well. NSOCKS is notoriously advertised and highly recommended by users on criminal forums such as Blackhatworld. It has seen extensive use by Muddled Libra along with the now recently defunct Truesocks proxy service. Entities based in the US are especially targeted as 60% of NSOCKS available proxies are based in this country. End users can purchase available IPs with cryptocurrency for 24 hours to use however they would like which based on our analysis is generally for fraud, reconnaissance, spam and phishing related activity. NSOCKS has two interesting features in the UI that they allow users to see how many others are currently using a proxy, and lets users filter by domain such as .gov and .edu, which can allow for very targeted use cases, as shown in the image below:

NSOCKS infrastructure

Our analysis reveals that NSOCKS employs a large layer of backconnect C2s, which serve a dual purpose. Not only do these C2s signal to the bots that they are available within the NSOCKS proxy service, but they also act as the point of connection for users who have purchased a proxy. Essentially, whenever a user buys a proxy in this service, they connect to these backconnect C2s.

We assess with high confidence that there exists a group of over 180 backconnect C2s dedicated to the NSOCKS proxy service. These C2s are specifically used to route and proxy traffic, playing a critical role in the operational infrastructure of NSOCKS.

Black Lotus Labs assesses the user interactions with the NSOCKS proxy service is as follows:

There are 3 IPs that share an SSH key with this backconnect C2 layer, but do not share the same characteristics. They resolve to the respective names dnslookips[.]com, ipscoredns[.]com and nslookups[.]com. We believe based on our malware analysis and understanding of how the UI works, they are gathering all relevant information on the bot's DNS server so prospective buyers can see what an infected victim is using

NSOCKS – The multi-armed bandit

When Black Lotus Labs began to focus on the backconnect C2s, we discovered that they were more than just alternate communication routes. According to public reporting, most of these IPs appear on free proxy lists. These lists are routinely abused by threat actors, and the proxies therein are often used in various malware samples, such as Agent Tesla, to proxy traffic.

When users purchase a proxy, they receive an IP and port combination for connection. Unfortunately, beyond this address and port, these proxies often lack any additional authentication once activated. This inadequate security measure allows not only "normal" NSOCKS users access to the network, but also permits any other malicious actors who discover the same IP and port combinations to exploit them for nefarious purposes.

Our telemetry has revealed that DDoS actors have been leveraging these open proxies to amplify their attack capabilities. Specifically, we have observed backconnect C2s, as well as numerous NSOCKS proxies, being used

in several large-scale DDoS attacks recently. The proxies are notably robust, with around 40% remaining active for over 30 days on average. This prolonged availability provides a significant window for malicious actors to continually exploit the proxies and discover additional ones within the service. Our data indicates there are nearly 15,000 IPs contacting these backconnect C2s each week.

Furthermore, our study of the backconnect layer unveiled a multi-layer architecture that led us directly to a backend database connected to the Shopsocks5 and VN5Socks proxy services. Due to the open access policies of the NSOCKS botnet operators, it appears this architecture is used either to siphon proxies from the NSOCKS proxy service, or as part of a partnership where NSOCKS willingly permits other proxy services to utilize some of its proxies.

Conclusion

Proxy botnets are becoming increasingly popular and, consequently, more dangerous. These networks are often leveraged by criminals who find exploits or steal credentials, providing them with a seamless method to deploy malicious tools without revealing their location or identities. What is particularly alarming is the way a service like NSOCKS can be used. With NSOCKS, users have the option to choose from 180 different countries for their endpoint. This capability not only allows malicious actors to spread their activities across the globe but also enables them to target specific entities by domain, such as .gov or .edu, which could lead to more focused and potentially more damaging attacks.

Moreover, the architecture setup of NSOCKS is facilitating further malicious activities, such as distributed denial of service (DDoS) attacks. This setup makes it easier for attackers to coordinate and execute these attacks, increasing the threat level significantly.

As part of a coordinated effort to limit the danger of NSOCKS and increase awareness, the Shadowserver Foundation are sinkholing some of the known Ngioweb botnet DGA domains. Statistics about the daily distribution of those victims are available on their public Dashboard. Detailed remediation data about compromised devices infected with ngioweb are available via Shadowserver's Sinkhole HTTP Reports.

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

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 are attempting to perform password spraying attacks and begin blocking IoCs with web application firewalls.
- Updating and blocking IP addresses belonging to known open proxies.

Consumers with SOHO routers:

- Users should follow best practices of 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.

- 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 NSOCKS and the ngioweb malware was performed by Chris Formosa and Steve Rudd. 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 Twitter @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.

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.
