TheMoon Malware Resurfaces

By By Black Lotus Labs

Archived: 2026-04-05 19:05:01 UTC

The darkside of themoon

Published on Mar 26, 2024 | 6 minute read

Executive summary

The Black Lotus Labs team at Lumen has identified a multi-year campaign targeting end-of-life (EoL) small home/small office (SOHO) routers and IoT devices, associated with an updated version of "TheMoon" malware. TheMoon, which emerged in 2014, has been operating quietly while growing to over 40,000 bots from 88 countries in January and February of 2024. As our team has discovered, the majority of these bots are used as the foundation of a notorious, cybercriminal-focused proxy service, known as Faceless. While Lumen has previously documented this malware family, our latest tracking has shown TheMoon appears to enable Faceless' growth at of a rate of nearly 7,000 new users per week.

Through Lumen's global network visibility, Black Lotus Labs has identified the logical map of the Faceless proxy service, including a campaign that began in the first week of March 2024 that targeted over 6,000 ASUS routers in less than 72 hours. Faceless is an ideal choice for cyber-criminals seeking anonymity, our telemetry indicates this network has been used by operators of botnets such as SolarMarker and IcedID. Lumen Technologies has blocked all traffic across our global network, to or from the dedicated infrastructure associated with both Faceless and TheMoon. We are releasing indicators of compromise (IoCs) to help others identify and take action, to disrupt this operation and impact the larger cybercrime ecosystem.

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

Introduction

The majority of anonymizing services are used for benign purposes, from bypassing censorship, or anonymizing a user's identity. However, there are services that exist to proxy internet traffic for those with ill intent. Black Lotus Labs has continued to refine our internal network-focused analytics to identify botnets and harmful proxies, and in late 2023 we uncovered a SOHO/IoT-based activity cluster communicating with tens of thousands of distinct IP addresses per week. As we began research into this cluster's command and control (C2) infrastructure, we found a file hosted at that address carrying a new variant of TheMoon, a botnet that was previously thought to have been rendered inert. While its influence may have waned since Lumen described it in 2019, we found that TheMoon has entered a new phase. Our analysis indicates that the operators behind this botnet were enrolling the compromised end of life (EoL) devices into an established residential proxy service called Faceless. Faceless has become a formidable proxy service that rose from the ashes of the "iSocks" anonymity service and has become an

integral tool for cybercriminals in obfuscating their activity. We noted such a strong statistical correlation of TheMoon bots gravitating toward Faceless that we believe TheMoon is the primary, if not the only, supplier of bots to the Faceless proxy service.

Malware analysis

The infection process for victim proxy devices began with a lightweight loader file, which first checked for the presence of "/bin/bash," "/bin/ash," or "/bin/sh." If none of these shells are found, the file ceases execution. If one of those three shells is available, it will decrypt, drop, and execute the next stage payload ".nttpd." This file once again begins by checking for the presence of shell. Next it looks for the file ".nttpd.pid," if not found it creates the file and writes the processes pid along with the hardcoded version 26. If .nttpd.pid exists, it will open the file and if the version is newer than 26, it will kill all of the processes named .nttpd.pid.

The binary will then set up these iptable rules:

- INPUT -p tcp –dport 8080 -j DROP
- INPUT -p tcp –dport 80 -j DROP
- INPUT -s 91.215.158.0/24 -j ACCEPT
- INPUT -s 195.3.144.0/24 -j ACCEPT
- INPUT -s 185.246.128.0/24 -j ACCEPT

Following the creation of rules, it sets up a thread to contact an NTP server from a list of legitimate NTP servers; we suspect they are likely using NTP as a mechanism to ensure the infected device has internet connectivity, and determine it is not being run in a sandbox. Following this, it attempts to cycle through a set of hard-coded IP addresses, establish a connection on port 15194, and send a hardcoded packet on port 16194. We suspect the hardcoded packet is likely a check-in packet, signaling a successful connection.

The C2 may respond with a packet that gives a specific filename and a location from which it can be retrieved. The infected device then requests and downloads the corresponding ELF executable. Thus far we have identified two subsequent modules, one appears to be a worm while the other file is named ".sox," which is used to proxy traffic from the bot to the internet on behalf of a user.

Worm module

To obtain the worm module it will send another file, ".scz," that will decrypt, drop, and execute an additional file, ".scn." The .scn executable will attempt to spread itself by scanning an IP block supplied by the C2, in search of vulnerable web servers on ports 80 and 8080. If it finds one, it will attempt to write and execute the file as .nttpd using a series of echo calls to the vulnerable web server.

.sox files

Once the .sox file is executed on the infected system it begins by checking the shell. Next it confirms it is running the most current version of the software, if not it will cease execution and run the latest version. Finally, it has the ability to embed functionality to modify iptables, this enables the malware to open up additional ports to download the next modules.

The file then checks for the presence of a file called ".sox.twn." If .sox.twn is not found, the .sox file attempts to contact a hard-coded IP address embedded in the .sox file. Research indicated these embedded IP addresses did not seem to respond and are possibly decoys or old C2s. The Sox file will continue to attempt to connect to the hard-coded IP on a port between 4210 and 4217, until the Moon C2, aware the infection is active, finally sends the .sox.twn file.

Once the .sox.twn file is received, the .sox file reads four bytes from a hard-coded offset in the .sox.twn file and uses this value to replace the hard-coded IP address. The four bytes read from the .sox.twn file represent a known Faceless C2, 195.3.147[.]73. The Sox file will then attempt to contact the new C2 on a random port between 4210-4217 every 5 seconds. If it receives a response, it will then contact the C2 on port 501#.

This process is illustrated below, showing the port 4215 activity followed by the port 5015 activity. The C2 on port 5015 then forwards requests to the infected host on behalf of the Faceless user.

Update C2 & clean-up scripts

The Moon C2 can occasionally respond with a handful of other files. The first file named ".soxT," is a bash script that writes the binary file "/tmp/.sox.twn." This file is used to update the C2 server for the Faceless proxy.

Another shell script, ".soxP," appears to do some cleanup and host-based evasion by removing the threat actor-dropped files from disk. An excerpt of the cleanup script is below:

#!/bin/sh

dd /tmp

rm –r .sox1 .sox2* …*

cp .sox.pid sox10.pid

cp sox.pid .sox20.pid …

Overlap between TheMoon and Faceless

After successfully discovering a co-habitation where a single device contained both a copy of TheMoon and Faceless executables; we observed a highly significant statistical overlap between the two family's activity clusters. In a ten-day period, approximately 80% of bots that talk to Faceless C2s were also seen talking to the Moon C2. In fact, multiple Faceless C2s that Lumen has monitored, have a 90% overlap with the bots that are also talking to the TheMoon C2.

In the graph above, the X-axis indicates the number of days it took for a newly infected bot communicating with TheMoon C2, to then communicate with a Faceless C2. Only 5% of the total bots had a scenario in which we first saw the bot reach out to a Faceless C2 prior to a TheMoon C2. We observe 40% of new Moon bots go on to talk to a Faceless C2 on the same day. In the event a bot does not talk to both on the same day, the trend shows 80% of new TheMoon bots will talk to a Faceless C2 within 3 days, again pointing to the Moon being the initial infection point for Faceless. Faceless C2s communicate with bots on ports with the scheme 421x, 481x and 501x, where the

final number is randomly selected between 0 to 7. This is the same scheme we detailed above, used by TheMoon. We have observed TheMoon payload hosted on multiple different servers, and in one instance, we observed the payload simultaneously hosted on a Faceless C2.

Further analogous activity showed one of the Faceless C2s contacting the Moon C2 on port 80, from the start of 2024 through the middle of February. Based upon the totality of evidence we assess with high confidence that TheMoon is the singular botnet that powers Faceless.

Global telemetry analysis – faceless

Faceless proxy server infrastructure

The Faceless proxy service offers their users the ability to mimic a connection, as if they were a legitimate ISP end-user in a country of their choice. The user maintains anonymity all the way throughout this process, because Faceless doesn't have a "know your customer" (KYC) verification process and only accepts money through cryptocurrencies. These are ideal conditions for those who wish to perform criminal activity without being traced.

They fabricate this network by compromising IoT Devices located around the globe, many of which appear to be end-of-life. We suspect these devices are preferred as they are no longer supported by the manufacturer, and as time goes by, they become more vulnerable to exploitation as patches and updates are no longer forthcoming. There is also the potential that devices such as these may sometimes be forgotten or abandoned.

The Faceless operators display a high level of operational security by siloing their infrastructure. In practice, this means anyone given access to Faceless will only communicate with one Faceless server throughout the time in which it is infected. These Faceless servers were likely all stood up and connected with a singular campaign. Examples of those campaign breakdowns are as follows:

- 85% of one Faceless server's activity primarily interacted with infected devices stemming from a single ASN.
- Two Faceless servers interacted with Network Attached Storage (NAS) devices running HipServ Operating systems and old D-link cameras running "alphapd" web server software, such as DCS-930L. Of note, these align with a worm file that was highlighted in the malware analysis section.
- Another server was stood up to furnish their own scanning infrastructure. In February, 45.143.201[.]87 was seen talking to approximately 3,500 devices on its port 32123, which is an FTP server. Close to 80% of the IPs talking to 45.143.201[.]87:32123 were also seen talking to Moon and/or Faceless C2s during this time. What is also interesting is that on ports 3443 and 7880 of this IP it has an Acunetix Web Vulnerability Scanner service running.
- We were not able to determine how bots were redirected to yet another C2, as the bots for this C2 were all observed communicating with different Faceless infrastructure hosting TheMoon malware. This likely denotes an isolated set of siloed infrastructure, which may have been stood up to provide continuity in case other elements of the campaign were uncovered.
- The latest emerging C2 was primarily focused on Asus devices, and grew to over 6,000 bots in a period of 72 hours.

Faceless bot analysis

Once a bot communicates with a Faceless server, it is enrolled in the Faceless proxy network. We noticed an interesting trend in terms of longevity: 30% of the infections lasted for over 50 days, while around 15% of the devices were part of the network for 48 hours or less. Our analysis revealed an anomalous, large assembly of bots that were only infected for 23 days. This group was a product of Faceless gathering several thousand devices from a specific ASN and subsequently losing control of them 23 days later.

From September 2023 through February 2024, we observed a rolling weekly average of approximately 30,000 distinct bots talking to the Moon C2 and of those, about 23,000 individual bots communicated with Faceless C2s. This shows us that not every bot infected with TheMoon malware became a Faceless bot. We are still seeking to understand the role of the 7,000 bots remaining with TheMoon, and how they interact within these two larger ecosystems.

Logical structure of the Faceless service

An end-user is seamlessly routed through the Faceless network before they egress at their purchased exit point. In some cases, we see certain Faceless C2s playing a dual role of the intermediary IP. This intermediary IP will then forward the request to the Faceless C2 (if that IP isn't itself a C2 already), which will instruct the bot to go to the requested resource and return the value through the same pipeline. In this manner, the true IP of the user is meant to be protected. The entire pipeline can be summarized below.

Black Lotus Labs sees a daily average of 3-5 IPs in contact with the Moon C2 on its port 80, these addresses are observed talking with the Faceless C2s. We suspect these serve as the core intermediary proxies between the end users and Faceless.

User activity

This global network of compromised SOHO routers gives actors the ability to bypass some standard network-based detection tools – especially those based on geolocation, autonomous system-based blocking, or those that focus on TOR blocking. 80% of Faceless bots are located in the United States, implying that accounts and organizations within the U.S. are primary targets. We suspect the bulk of the criminal activity is likely password spraying and/or data exfiltration, especially toward the financial sector. In some cases, we have seen long-duration user connections stemming from SolarMaker and IcedID actor-controlled infrastructure. We assess that these connections are associated with administrative activity, stemming from threat actors connecting to their C2 servers via this obfuscation network, adding another layer of anonymity to their operational security.

Conclusion

This is not the first instance of infected devices being enrolled into a proxy service, and it is a growing trend. We suspect that with the increased attention paid to the cybercrime ecosystem by both Law Enforcement and Intelligence Organizations, criminals are looking for new methods to obfuscate their activity. While some groups rely on tools like commercially available VPN services, there has been at least one case of VPN logs leading to the identification of a criminal. There are some signs that the TOR network itself, could lead to de-anonymization if a given entity controlled enough nodes and received sufficient data from them. Events like these may not eclipse the

use of VPN services, but the tides are shifting toward residential proxy servers as criminal organizations' first choice.

Black Lotus Labs continues to monitor and track large scale botnets to help protect and help better secure the internet as a whole. To that end, we have blocked traffic across the Lumen global backbone to all of the architecture related to TheMoon and Faceless. This includes the Faceless and Moon C2s, intermediary IPs, and IPs used to scan and infect new bots. We have added the indicators of compromise (IoCs) from this campaign into the threat intelligence feed that fuels the Lumen Connected Security portfolio. We will continue to monitor new infrastructure, targeting activity, and expanding TTPs, and we will continue to collaborate with the security research community to share findings related to this activity.

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.

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 TheMoon and Faceless was performed by Chris Formosa and Steve Rudd. Technical editing by Ryan English and Danny Adamitis.

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.
