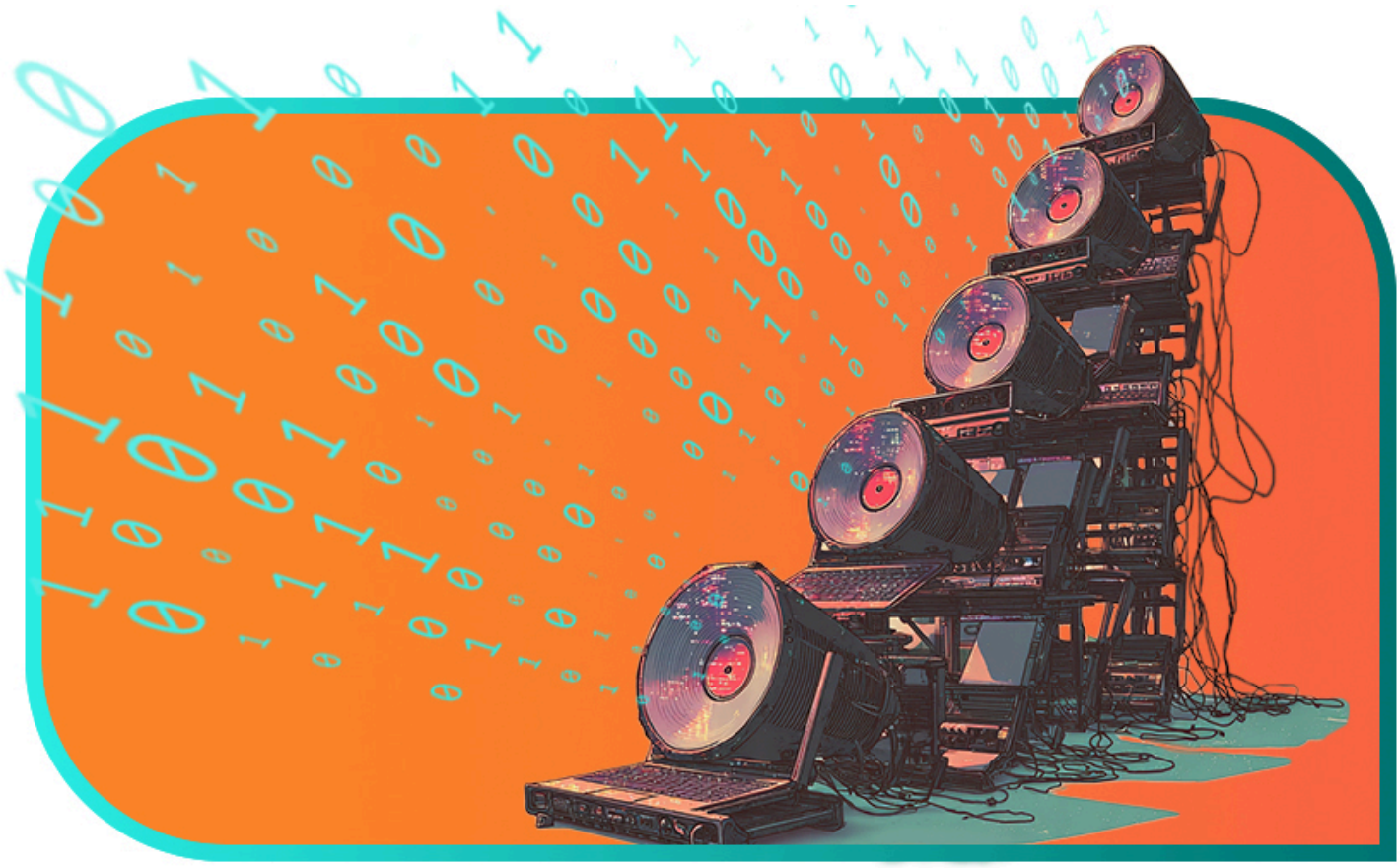
SystemBC – Bringing the Noise

⋮ 9/18/2025

Black Lotus Labs Posted On September 18, 2025



Executive Summary

The Black Lotus Labs team at Lumen Technologies has uncovered new infrastructure behind the "SystemBC" botnet, a network composed of over 80 C2s with a daily average of 1,500 victims, nearly 80% of which are compromised VPS systems from several large commercial providers. The victims are made into proxies that enable high volumes of malicious traffic for use by a host of criminal threat groups. By manipulating VPS systems instead of devices in residential IP space as is typical in malware-based proxy networks, SystemBC can offer proxies with massive amounts of volume for longer periods of time. Similar, high-bandwidth proxies in residential IP space would alert and disrupt users of smaller, lower bandwidth devices.

Black Lotus Labs has observed these proxies in use by multiple networks in the criminal ecosystem; including at least two different Russia-based proxy services, one Vietnamese proxy service, and a Russian parsing service. While selling the same bots on multiple platforms, the service generates very large amounts of traffic without regard to the attention it draws – nearly 100% of the bots are eventually listed on "block list" sites for mass scanning, exploitation, and brute forcing.

One primary user of the SystemBC botnet is an interesting proxy network known as "REM Proxy," which offers roughly 80% of the SystemBC network to their users. REM Proxy is a sizeable network, which also markets a pool of 20,000 Mikrotik routers and a variety of open proxies it finds freely available online. This service has been a favorite for several actors such as those behind TransferLoader, which has ties to the Morpheus ransomware group. REM Proxy is marketed in a dedicated criminal forum created for it and four other services that offer additional supporting capabilities for attackers.

Lumen Technologies has blocked all traffic across our global network, to or from the dedicated infrastructure associated with the SystemBC and REM Proxy 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.

Black Lotus Labs would like to thank our partners at Spur, Infoblox and others throughout the industry for their contribution to our efforts to track and mitigate this threat.

Introduction

A major concern for any threat actor is to hide their online activity long enough to conduct their plans without alerting victims or law enforcement. Services like TOR offer degrees of anonymity; however, there are downsides like low bandwidth speeds and stability issues. Dedicated solutions like VPNs come with a cost and risk that a VPN provider may disript or interfere"with threat actor activity. Threat actors continue to move towards proxy services such as NSOCKS and ProxyAM, offering thousands or even millions of residential devices through which to pass traffic in nearly any physical location on the planet. Some proxy pools, like the pair mentioned above as well as TheMoon, are created entirely from other botnets. Black Lotus Labs tracked the SystemBC network for several months, as it fed directly into multiple other services we have observed over the same time.

While we could not determine the initial access vector used by SystemBC operators, our research revealed that, on average, each victim shows 20 unpatched CVEs and at least one critical CVE – with one address shown as having over 160 unpatched vulnerabilities.

The SystemBC malware was originally documented in 2019 by Proofpoint. It is commoditized in underground forums and frequently used by a variety of criminal threat groups. Its core design is to open proxy functionality on victims and can be configured to enable the retrieval and execution of additional malware. SystemBC has been extremely effective over its lifetime, gaining the attention of law enforcement during Operation Endgame given its ability to facilitate the deployment of ransomware. This well-rounded network has been used in conjunction with notorious entities such as IcedID and Trickbot.

Malware Analysis

The samples we examined, along with those mentioned by Polyswarm, do not appear to have any additional functionality aside from proxying traffic. The first sample, *1c74b1195250632f2f1d1a9066f07f6e0a8c12dff40aeb3c1fe22440c97bc8ee,* is a Linux variant of the SystemBC malware. The malware first decrypts and connects to the C2 contained in the embedded config. The config is XOR encoded using a hardcoded 40-byte key.

```
void __convention("regparm") xorData(char arg1, char* data, int32_t keyLen,
  int32_t dataLen @ esi, int32_t key @ ebx)

    int32_t dataLen_1 = dataLen
    int32_t edi
    int32_t var_18 = edi
    char* data_1 = data
    int32_t ecx = 0

    while (dataLen_1 != 0)
        *data_1 ^= *(ecx + key)
        data_1 = &data_1[1]
        dataLen_1 -= 1
        ecx += 1

        if (ecx == keyLen)
            ecx = 0
```

Figure 1: Decoding configuration

It then creates a payload composed of the composed of the 40-byte key, 10-bytes of padding, and then an encrypted beacon consisting of *0xffff* followed by forty-eight 0x00 bytes.

```
__builtin_memset(dest: data_1, ch: 0, count: 0x10000)
__builtin_memcpy(dest: data_1, src: &key, count: 0x32)
data_1->startOfData.w = 0xffff
encrypt(eax.b, data: &data_1->startOfData, keyLen: 0x32, dataLen: 0x32, &key)
sendToSockfd(eventfd: 0, size: 0x64, data: data_1, sockfd: sockets.c2Socket)
```

Figure 2: Encryption process

The beacon is encrypted by first XORing the beacon with the key (as above), RC4 encrypting with said key, and then XORing once again with the same key.

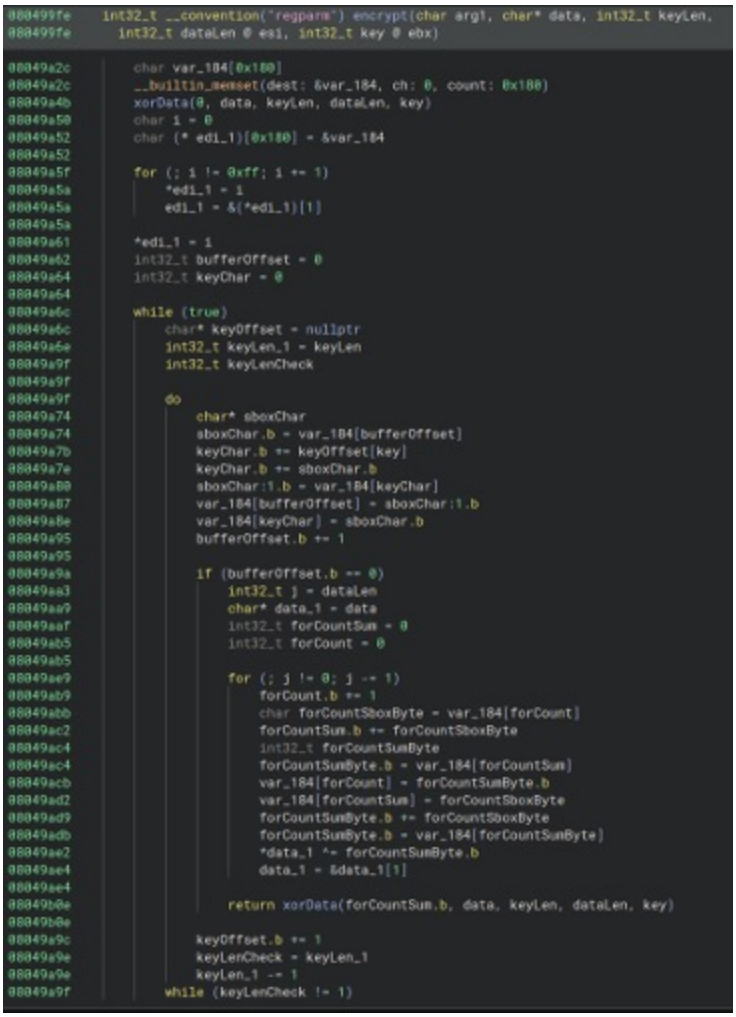


Figure 3: C2 response and instructions

The response from the C2 will include a 4-byte header which is decrypted in the same manner that the initial payload was encrypted: XOR, RC4, XOR. The header contains the type (new proxy (0), additional data for an already open proxy (1), or exit execution (0xff).

Global Telemetry

Users of the proxy network reach out to SystemBC C2s on high numbered ports, which then sends the user through to one of the victims. This pattern is shown in the image below:

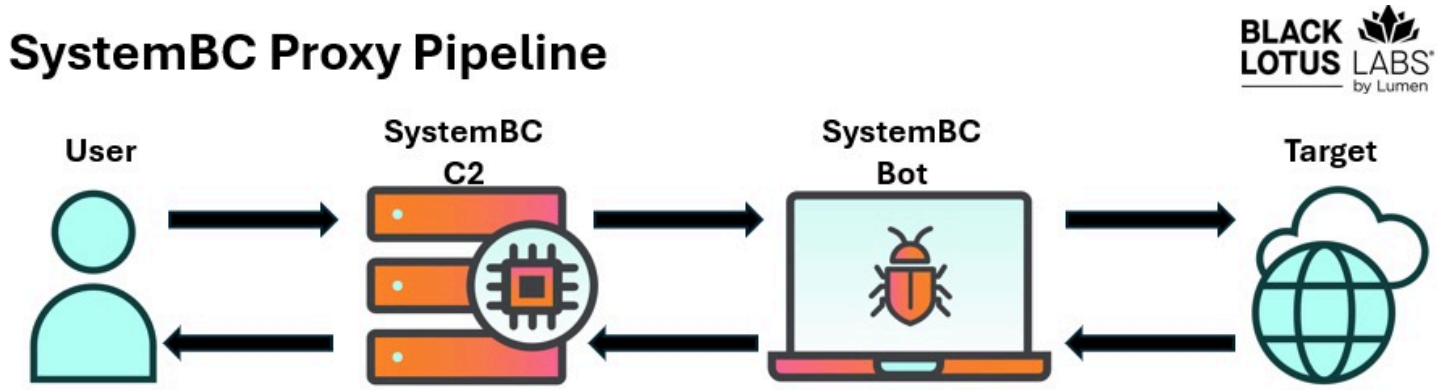


Figure 4: SystemBC proxy pipeline

Victim Analysis

The pool of victims revealed that unlike most botnets and proxy related services, the primary targets were VPS servers instead of residential users. Over a period of study lasting several months, SystemBC maintained a daily average of 1,500 bots, including 300 that are a part of the GoBrut botnet.

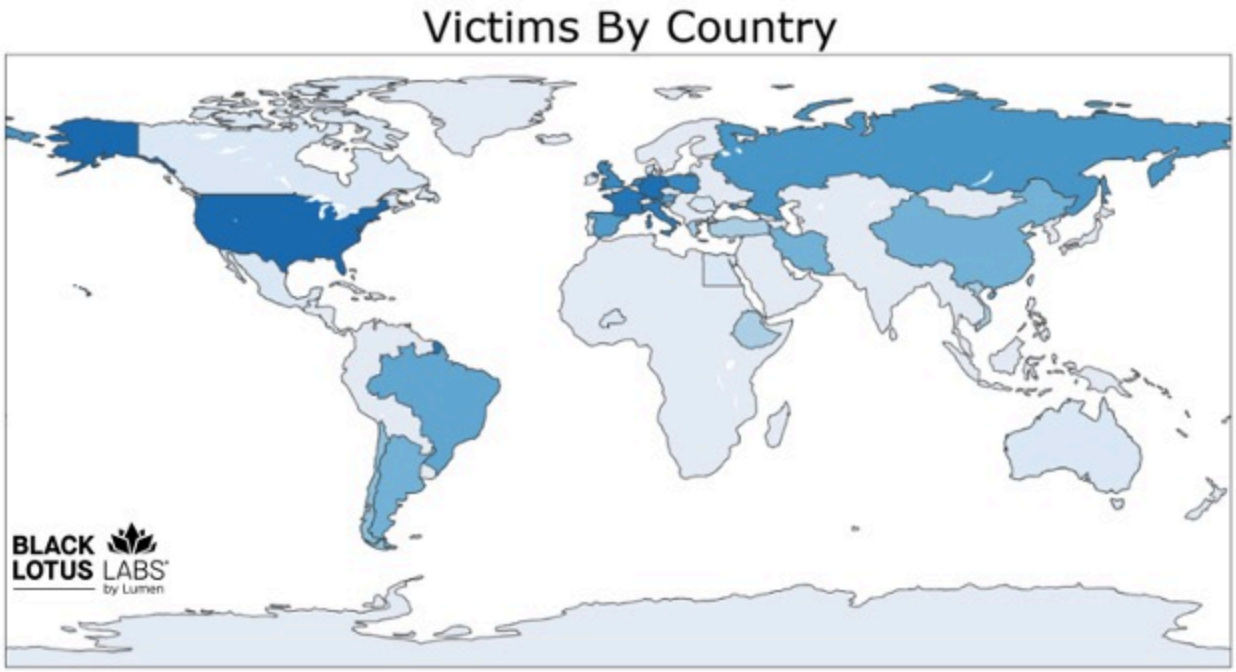


Figure 5: Victim locations of the infected SystemBC bots

Of those 1,500 daily bots, close to 80% came from just five large commercial VPS providers. Given that the victims are primarily VPSs, we also see extremely long average infection lifetimes, where close to 40% stay infected for well over a month.

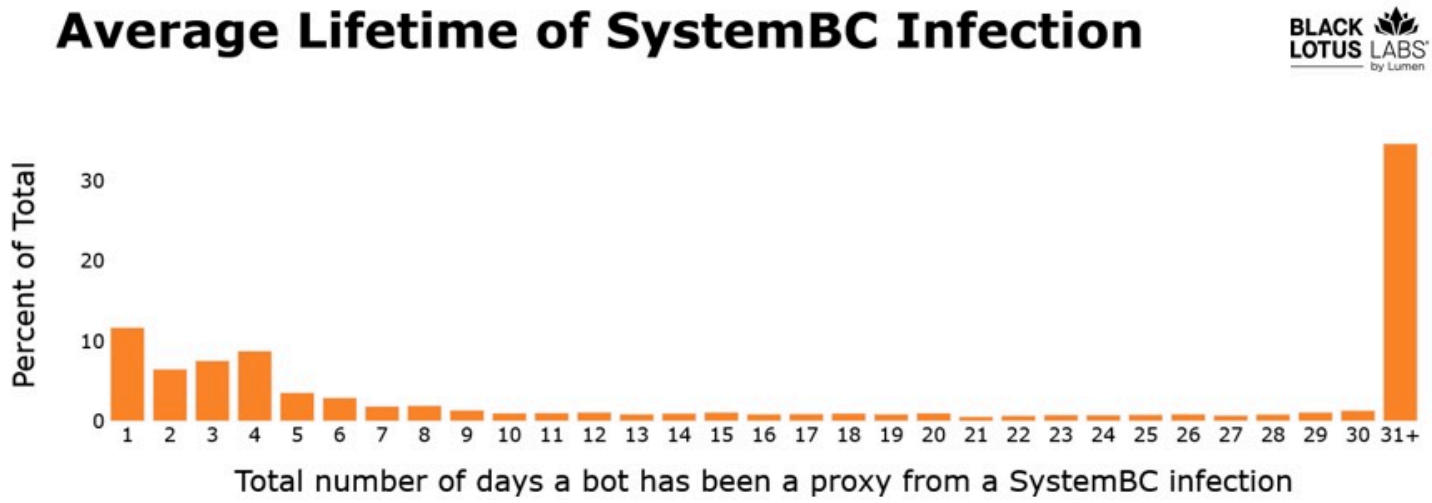


Figure 6: Shows the infection lifespan for this SystemBC botnet. Close to 40% of these infections last over a month

We could not find evidence of specific targeting of VPS providers, however, we discovered that nearly all victimized servers appeared to be riddled with easy to exploit vulnerabilities such as the one below which, according to Censys, has over 160 unpatched CVEs.

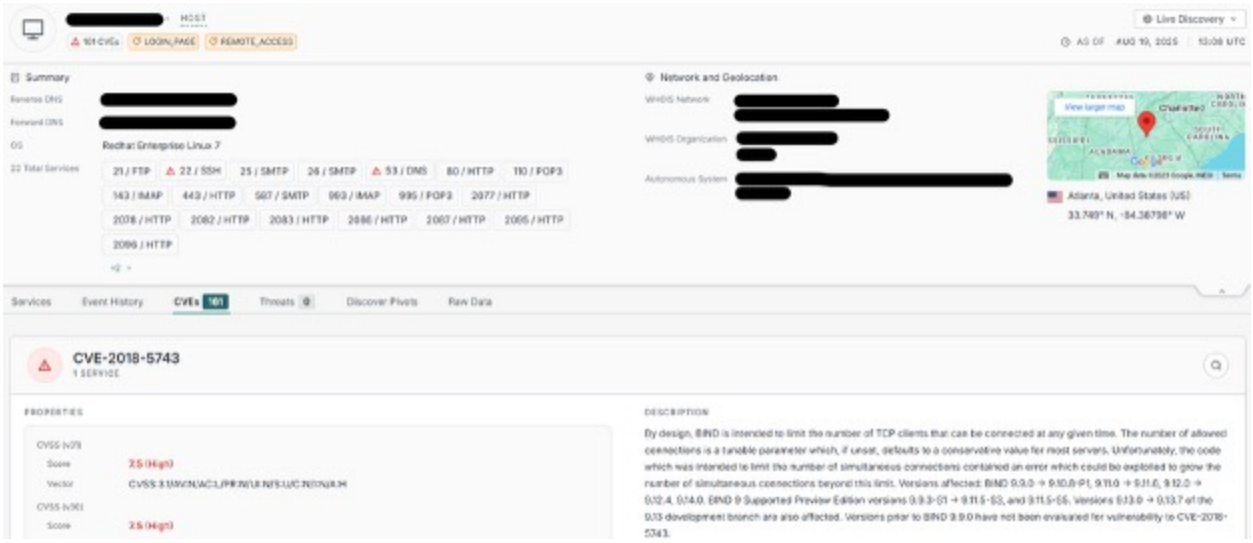


Figure 7: Example of VPS victim in the SystemBC botnet with over 160 vulnerabilities

Analysis of our global IP telemetry revealed that *104.250.164[.]214* appears to be the source of attacks to recruit potential victims, as well as the sole host of the SystemBC malware samples. Initial access attempts are sent on port 443, and, if successful, the new bot will call back on port 80 to download a shell script (with Russian comments) that forces the download over 180 samples of the SystemBC malware. The script will also direct the victim to run every sample simultaneously, with each sample under a separate file name. An image showing the process is below:

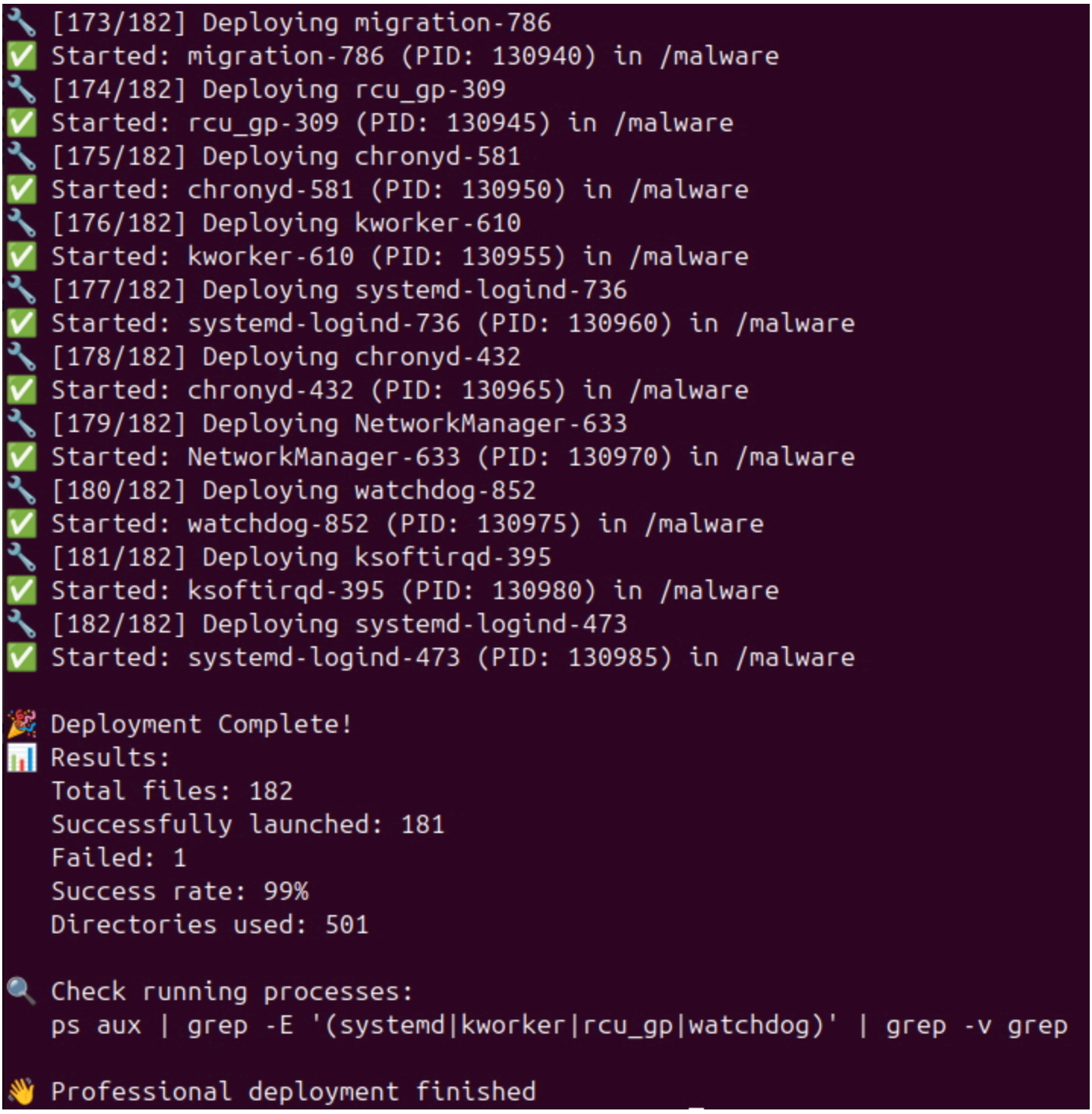


Figure 8: Example of malware download from SystemBC host

When dissecting the C2 infrastructure we found that all the SystemBC C2s were operated under a single Autonomous System (AS). This AS is small enough that the 80 C2s make up approximately 10% of their network.

Proxy Analysis

Most proxy services offer modest traffic volumes per proxy, seldom reaching gigabyte-scale data transfers on a regular basis. This restraint is typically attributed to the residential devices that constitute these networks, such as Internet of Things (IoT) endpoints or legacy routers. Excessive traffic routed through such devices not only risks network instability leading to possible discovery but also increases the probability of the host's IP address being blacklisted. Our analysis suggests that the operators and customers of this botnet have little concern for evasion or stealth. As an example, the bots' IP addresses are neither obfuscated nor systematically rotated to avoid detection. Volume seems to be the only concern; for one 24-hour window we observed a particular IP address generate an excess of 16 gigabytes of proxy data, which we confirmed by observing the malware in a simulated environment. This amount of data is an order of magnitude greater than what is commonly observed in typical proxy networks.

Our analysis of netflow revealed several prominent crime groups using SystemBC victims as proxies and likely more we did not find. When grouping the user groups together it becomes clear how the victimized proxies can generate so much malicious traffic:

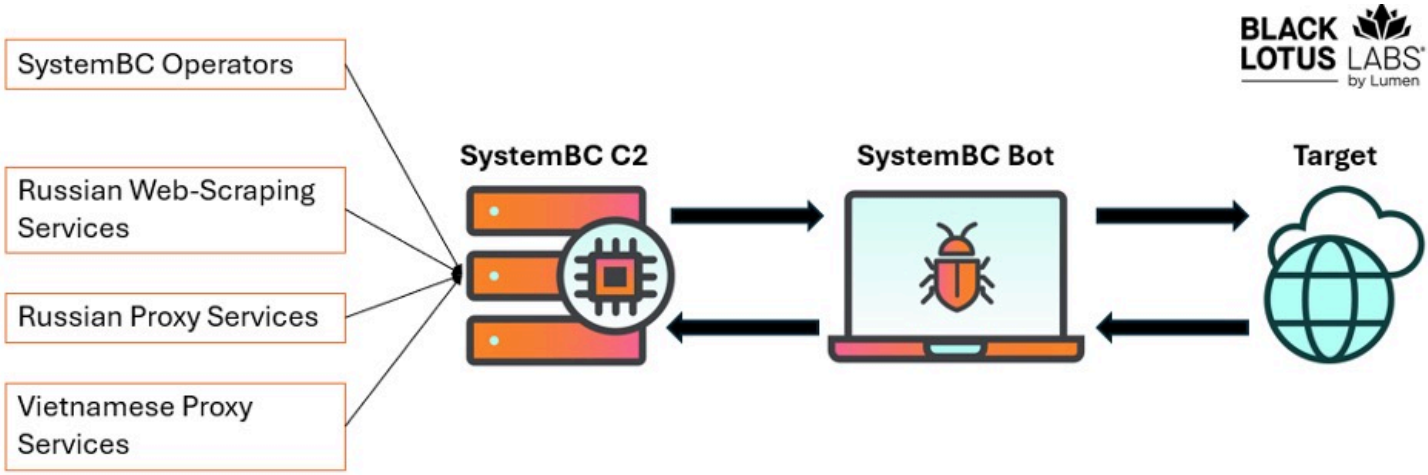


Figure 9: Known users of the SystemBC botnet

The largest use of the botnet is by the SystemBC operators themselves, using their own network to brute force WordPress credentials, then likely selling the harvested credentials to brokers who inject the sites with malicious code.

The next largest user by volume was a very large Russian web-scraping service. Based on traffic analysis, we saw a direct connection between this services' architecture and the SystemBC C2s on the user entry ports. This parsing service offers the option of choosing between regular and premium proxies. The SystemBC proxies are likely sold alongside their regular proxies, as they market to users who do not care about IP quality, or IPs that are blacklisted or might get blocked easily.

We also observed the Vietnamese-based VN5Socks (a.k.a. Shopsocks5) proxy service offering these IPs in their service, similar to their use of Ngioweb bots acquired through NSOCKS. It appears that after the Ngioweb takedown, VN5Socks diversified their sources and started buying from the actor behind this SystemBC botnet.

Type Sock	Risk Level	Socks5	Proxy Type	ISP Name	Zip Code	City	State	Country	Speed	Blacklist	Risk Score	Time Online
Hosting	Low	45.146.130.15:20636	SOCKS5 Proxy	DigitalOcean, LLC	627753	Singapore	South West	SG	3.42	No	20/100	0h:0m:23s
Hosting	Low	185.93.89.175:4144	SOCKS5 Proxy	GD MASS Network	67000	Strasbourg	Grand Est	FR	4.35	No	10/100	0h:0m:52s
Hosting	Low	45.146.130.16:14900	SOCKS5 Proxy	Shinjiru Technology Sdn Bhd	58100	Kuala Lumpur	Kuala Lumpur	MY	2.606	No	10/100	0h:1m:2s
Hosting	Low	185.93.89.158:9433	SOCKS5 Proxy	Contabo Asia Private Limited		Singapore	Central Singapore	SG	2.758	No	20/100	0h:1m:2s
Hosting	Low	185.93.89.158:4659	SOCKS5 Proxy	DigitalOcean, LLC	627753	Singapore	South West	SG	2.657	No	10/100	0h:1m:2s
Hosting	Low	Socks offline.	SOCKS5 Proxy	DigitalOcean, LLC	627753	Singapore	South West	SG	3.384	No	10/100	0h:1m:2s
Hosting	Low	45.146.130.47:5820	SOCKS5 Proxy	Host Europe GmbH	67000	Strasbourg	Grand Est	FR	4.358	No	10/100	0h:1m:2s
Hosting	Low	45.146.130.24:5349	SOCKS5 Proxy	OVH SAS	59100	Roubaix	Hauts-de-France	FR	4.723	No	10/100	0h:1m:2s
Hosting	Low	185.93.89.166:16196	SOCKS5 Proxy	GoDaddy.com, LLC	85284	Tempe	Arizona	US	4.146	No	10/100	0h:1m:2s
Hosting	Low	185.93.89.191:39067	SOCKS5 Proxy	Contabo GmbH	67630	Lauterbourg	Grand Est	FR	4.04	No	10/100	0h:1m:2s
Hosting	Low	45.146.130.30:4919	SOCKS5 Proxy	WHG Hosting Services Ltd	400703	Mumbai	Maharashtra	IN	3.472	No	10/100	0h:1m:2s

Figure 10: VN5Socks list of proxies that are using ports on our known SystemBC C2s

Cue the Remix

This brings us to REM (Remix) Proxy, the most interesting service using the SystemBC network. REM Proxy is a proxy service that has been leveraged by ransomware threat actors for multiple facets of their operations, including the initial distribution of phishing emails, interaction with exfiltration servers, and access to victim data.

Figure 11: REM Proxy homepage

Analysis has revealed connections between REM Proxy architecture and ransomware actors dating back to at least 2022, specifically involving the AvosLocker ransomware-as-a-service group, and more recently the Morpheus ransomware group. Over time, we have observed several distinct ransomware actors and threat groups incorporate REM Proxy into their data transfer pipelines. Back in January 2025, Infoblox wrote about an unknown Russian botnet powered by Mikrotik devices. Black Lotus Labs worked with Infoblox and was able to assess with high confidence the botnet they came across was in fact REM Proxy. With their help we were able to find a 50% overlap between the IPs they observed in previous campaigns and ones we found as part of the current makeup of REM Proxy.

According to research from Proofpoint, REM Proxy uses a base of compromised Mikrotik devices, however, these devices represent only part of REM Proxy's operational structure, which offers three distinct tiers of packages, each providing varying capabilities and resources to its users.

Their high-end tier is called "Mix-Speed," and offers proxies with very low detection rates, largely drawn from the pool of Mikrotik devices and includes some of the open proxies. These bots are almost entirely in residential IP space and appear to be overlooked by most security solutions. They also specify that port 25 is left open, which is rare for proxy services. This is useful for threat actors focused on phishing and spamming e-mails; however, most major US residential ISPs block outbound traffic on port 25 for this reason.

On their low-end tier ("Mix-Economy"), they market proxies in the same vein as the aforementioned parsing service, described as useful for those who "aren't demanding on the proxy quality." Almost all proxies in this "Economy" package appear to be those with high detection scores.

The high detection rates of the “Mix-Economy” proxies might not pose a concern for a well-monitored network; however, they are useful in other stages of a malicious actor’s pipeline. For example, actors may use “Mix-Economy” IPs for brute force and credential harvesting, then move to the higher end “Mix-Speed” IPs to execute targeted attacks with lower visibility, using information they acquired from the initial phase of the operation.

Rounding out the REM proxy offerings is a middle tier called “Mix-Mix,” which appears made of random bots taken from both the high- and low-end tiers. This tier seems to mix economy and speed for general purpose use.

REM Proxy Global Telemetry

Analysis of Lumen’s global netflow allows us to observe elements of this network from the portal that users interact with, through to the end use of a given proxy. No matter what tier a user buys, they appear to get bots from all three sources, based on detection rates and quality. In other words, the rare SystemBC victim with a low detection rate, could be part of the higher “Mix-Speed” tier.

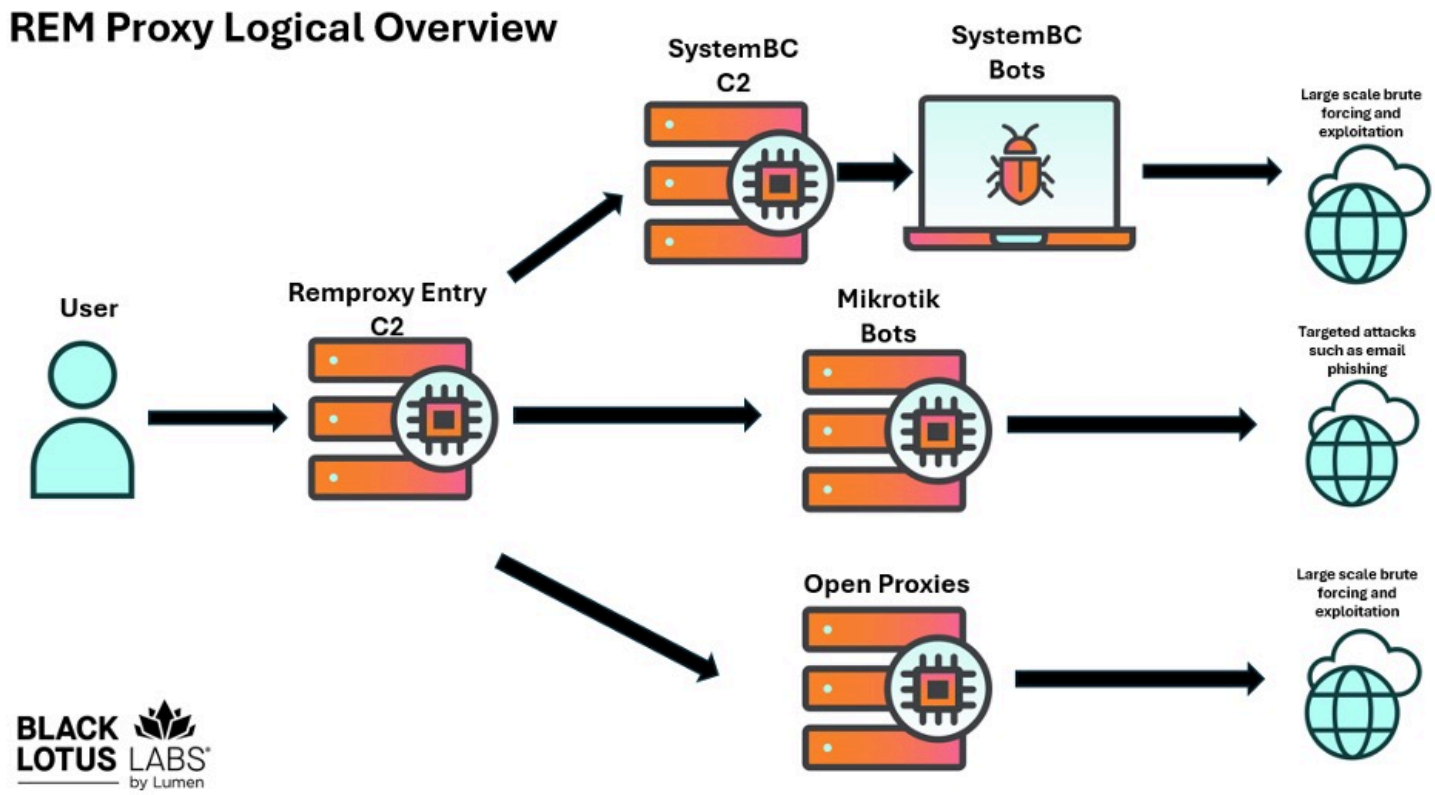


Figure 12: REM Proxy system overview.

When a user buys a REM Proxy subscription, they move to a screen with a link to a “Proxy list URL” which gives the user a menu for different proxies (or “threads”) to which they can connect. An example is shown below:

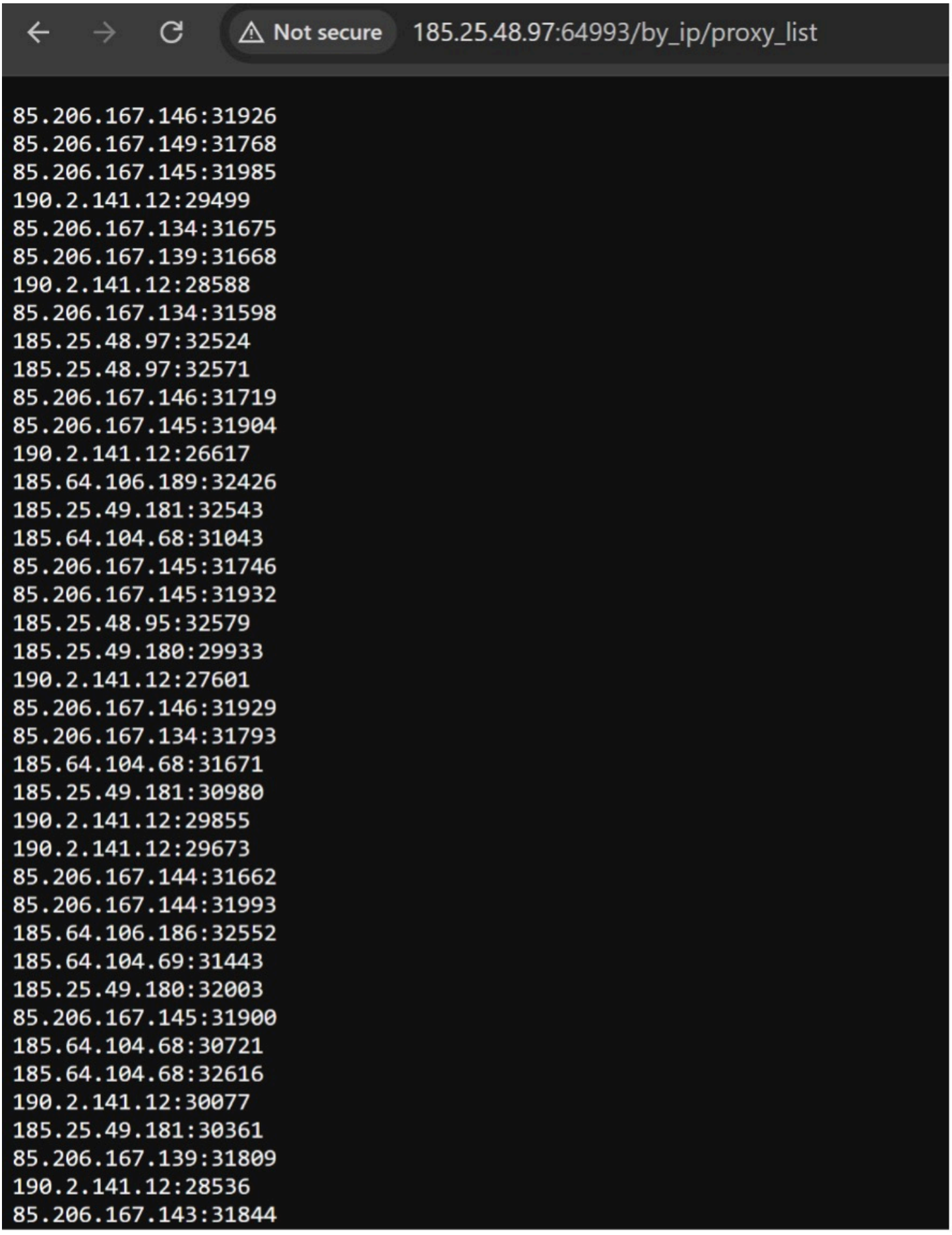

Not secure
185.25.48.97:64993/by_ip/proxy_list
85.206.167.146:31926
85.206.167.149:31768
85.206.167.145:31985
190.2.141.12:29499
85.206.167.134:31675
85.206.167.139:31668
190.2.141.12:28588
85.206.167.134:31598
185.25.48.97:32524
185.25.48.97:32571
85.206.167.146:31719
85.206.167.145:31904
190.2.141.12:26617
185.64.106.189:32426
185.25.49.181:32543
185.64.104.68:31043
85.206.167.145:31746
85.206.167.145:31932
185.25.48.95:32579
185.25.49.180:29933
190.2.141.12:27601
85.206.167.146:31929
85.206.167.134:31793
185.64.104.68:31671
185.25.49.181:30980
190.2.141.12:29855
190.2.141.12:29673
85.206.167.144:31662
85.206.167.144:31993
185.64.106.186:32552
185.64.104.69:31443
185.25.49.180:32003
85.206.167.145:31900
185.64.104.68:30721
185.64.104.68:32616
190.2.141.12:30077
185.25.49.181:30361
85.206.167.139:31809
190.2.141.12:28536
85.206.167.143:31844

Figure 13: List of IP and port combinations available to proxy traffic

REM Proxy has close to one hundred C2s available for user connections. In our study, the C2 connection was to *185.25.48[.]97*, and our netflow revealed users contacting REM Proxy C2s on random ports. Traffic from those same C2s then connects to: Mikrotik devices on SSH port 51922, along with SystemBC C2s on the user entry ports, and many open proxies on ports such as 1080, 8989 and similar.

REM Proxy presents a unique case study, both in its operational mechanics and in user interaction patterns within the network. Victimized devices are brought into the system through an alternative domain, *honipsiops[.]in*, which appears to function as a screening mechanism—allowing REM Proxy to identify new, accessible IP addresses and verify their status. Daily, approximately 3,000 IP addresses contact this site, with an estimated 2,500 attributed to REM Proxy-related infections.

Finally, when users authenticate into the proxy service, they are redirected to a cybercrime forum offering five distinct complimentary services. REM Proxy is featured alongside solutions that include email validation tools and mechanisms for circumventing blacklists, among others:

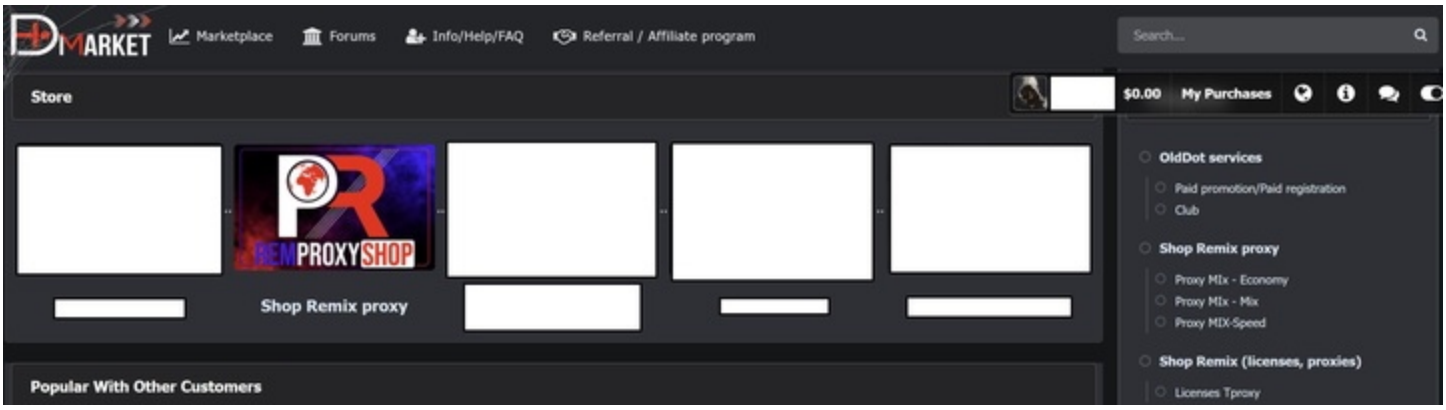


Figure 14: forum featuring REM Proxy alongside ancillary services

Conclusion

SystemBC has exhibited sustained activity and operational resilience across multiple years, establishing itself as a persistent vector within the cyber threat landscape. Originally used by threat actors to enable ransomware campaigns, the platform has evolved to offer the assembly and sale of bespoke botnets. Unlike traditional SOHO-based botnets that offer great size or stealth, SystemBC's use of VPSs is geared toward volume and brute force.

Their model offers considerable advantages: it enables the execution of widespread reconnaissance, spam dissemination, and related activities, allowing an attacker to reserve more selective proxy resources for targeted attacks informed by prior intelligence gathering. Commercial proxy providers such as REM Proxy have adapted to this model by introducing tiered service packages, supporting the full spectrum of malicious operations, from initial reconnaissance to active exploitation.

Alone or together, these two entities demonstrate some of the adaptive strategies of both threat actors and supporting service providers within the cybercriminal ecosystem. Black Lotus Labs continues to monitor and track large scale botnets such as these, to help protect and better secure the internet as a whole. To that end, we have blocked traffic across the Lumen global backbone to all the architecture related to the SystemBC and REM Proxy botnets. 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 collaborate with the security research community to share findings related to this activity.

We have a list of IoCs available on our GitHub, and encourage the community to monitor for and alert on these and any similar IoCs

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.
- Compare the IP address of any purchased VPS against services like Censys, or public block lists.

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 SystemBC and REM Proxy was performed by Chris Formosa and Steve Rudd. Technical editing by Ryan English.

Post Views: 1,432

BLACK LOTUS LABS

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