

Silent Push Identifies More Than 10,000 Infected IPs as Part of SystemBC Botnet Malware Family

 silentpush.com/blog/systembc

Peggy Kelly

February 4, 2026

[threat](#)

February 4, 2026



Key Findings

- Using a custom-built SystemBC tracker, Silent Push Preemptive Cyber Defense Analysts identified more than 10,000 unique infected IP addresses as part of this botnet. While we don't have immediate visibility on any follow-on malware payloads deployed via this current SystemBC botnet, historically, many threat actors have used SystemBC to deploy ransomware on compromised networks, highlighting the importance of remediation.

- Our analysis shows SystemBC infections are globally distributed at scale, with the highest concentration of infected IP addresses observed in the United States, followed by Germany, France, Singapore, and India.
- We identified SystemBC infections within sensitive infrastructure, including compromised IP addresses hosting government websites in Burkina Faso and Vietnam.
- SystemBC command-and-control (C2) infrastructure has been observed leveraging abuse-tolerant bulletproof hosting, including BTHoster (***bthoster[.]com***) and AS213790 (BTCcloud).
- Our research uncovered a previously undocumented SystemBC variant written in Perl, indicating continued development activity and ongoing evolution of the malware family.

Executive Summary

First documented publicly [in 2019](#), SystemBC (also known as “Coroxy” or “DroxiDat”) is a long-running, multi-platform proxy malware that converts compromised systems into SOCKS5 proxies—and, in some cases, deploys additional malware.

Serving two primary functions, SystemBC proxies traffic through compromised systems and acts as a backdoor to maintain external access to infected internal networks. Some variants, including the Windows version, have been observed dropping additional malware, often alongside ransomware payloads, to tunnel malicious traffic back to attacker-controlled C2 infrastructure. The result is a resilient, anonymizing design that expands the potential blast radius of a compromise.

In May 2024, SystemBC [was among](#) the malware families targeted during Europol’s Operation Endgame, a coordinated effort to disrupt large-scale criminal infrastructure. That attention mirrors years of [public reporting](#) linking SystemBC activity to breaches that culminated in ransomware deployment—reinforcing why early detection of this activity matters.

Silent Push began tracking SystemBC in 2025, which led to the development of a SystemBC-specific tracking fingerprint to expand visibility into active infections and supporting infrastructure. Using that fingerprint, our team identified more than 10,000 unique infected IP addresses worldwide. Across the dataset, infections were widespread: the largest concentrations of detected victims appeared in the U.S., followed by Germany, France, Singapore, and India.

The dataset also captured infections in sensitive government environments, such as compromised high-density IP addresses hosting official websites in Burkina Faso and Vietnam. That same analysis revealed a previously undocumented SystemBC variant written in Perl, underscoring that this malware is continuing to evolve.

Table of contents

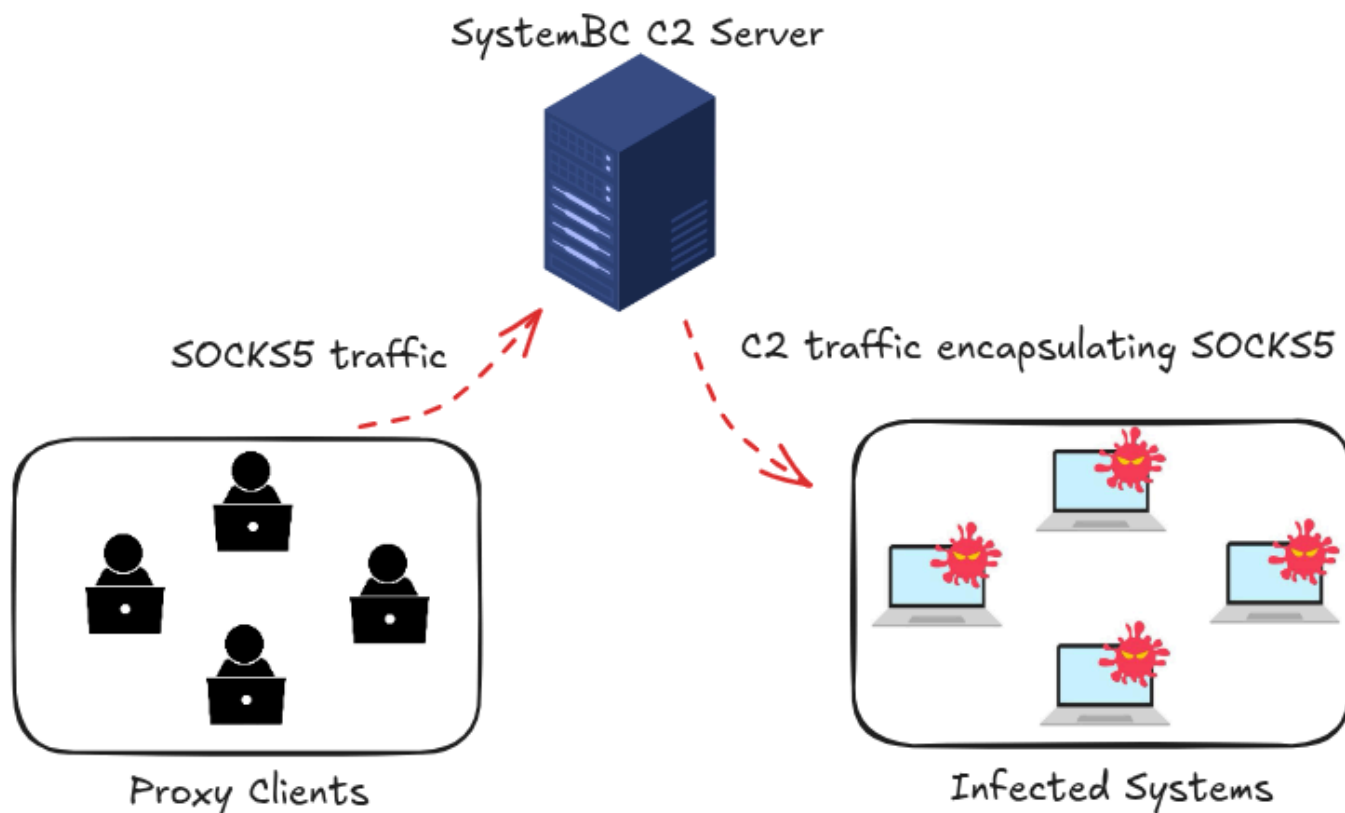
Background

SystemBC is a multi-platform proxy malware that turns infected systems into SOCKS5 proxies, allowing all kinds of malicious traffic to be sent through them. Also known as “Coroxy” or “DroxiDat,” SystemBC was first documented by [Proofpoint](#) in 2019. Upon reviewing several forum posts by the creator, written in Russian, our team believes the creator may be Russian or have ties to the country.

SystemBC is commonly used to proxy traffic through compromised systems or to maintain persistent access to internal networks. In some cases, including observed Windows variants, SystemBC has also been used to deploy additional malware, meaning its presence may indicate broader compromise or follow-on infections on the affected system. When a victim server is compromised, SystemBC uses a custom binary protocol and RC4 encryption to encapsulate SOCKS5 traffic.

Unlike virtual private networks (VPNs), [SOCKS/SOCKS5](#) is a specific internet protocol for proxies. Proxies are versatile network protocols that act as middlemen, or relays, between devices and the internet. They can route internet traffic (TCP, UDP, etc.) for different applications, masking IP addresses to bypass online blocks, access geo-restricted content, and enhance privacy for specific applications. Many threat actors use proxies to hide their real infrastructure from defenders.

Since most infected systems are not directly reachable over the internet, SystemBC employs a “backconnect,” or rotating, architecture: clients connect to the exposed C2 servers, which then relay traffic through the infected systems, acting as proxies. This design enables threat actors to route external traffic through compromised hosts and expose otherwise internal networks to external access, thereby significantly increasing the potential impact of any compromise.



Simple map of SystemBC's network traffic

Initial Intelligence

Investigations have [repeatedly documented](#) SystemBC's role in intrusions that later escalate into ransomware deployment. SystemBC was targeted during Europol's [Operation Endgame](#) in May 2024, but updates from its developer, "[psevdo](#)," continue to appear on the Russian-language forum ***forum[.]exploit[.]in***. This activity prompted deeper analysis—uncovering a highly active SystemBC C2 cluster, a previously undocumented Perl variant, and a trail of global victims.

Psevdo's updates are written in Russian, with selected translations shown below:

psevdo

seller
●●●●●●



Seller

11

405 posts

Joined

07/31/12 (ID: 45104)

Activity

вирусология / malware

Autogarrant

0

Posted July 19, 2018 (edited)

продаю **socks5 backconnect систему**

система разработана на ассемблере. высокая скорость минимальный размер (около 10кб)

состоит из:

клиентская и админская часть

1) socks.exe - windows bot. работает начиная с XP до новых версий windows.

автозапуска нет (не будет возвращаться после перезагрузки ПК)

примерно 10 - 20% постоянного онлайн при норм крипте с автозапуском

криптом не занимаюсь. поискать можно на форуме

2) socks32.dll socks64.dll - клиент в виде dll 32/64 bit для инжекта в ваш бот (стартовая функция rundll)

инжектировать рекомендуется в память без сброса на диск (для обхода антивирусов)

3) также имеется полноценный бот для linux

socks.out - запускается почти на любых linux машинах. работает даже без root привилегий. автозапуска нет (не будет возвращаться после перезагрузки ПК)

админка устанавливается очень просто - достаточно запустить на руте сервере server.out (для linux) или server.exe (для windows server) + залить php файлы в веб папку

для админки рекомендуется выделенный (не shared) канал 1 gbit, 2гб оперативки и 4 ядра для 1 000 соксов

если они просто висят и не используются - интернет не расходует. для стабильной работы каждый сокс потребляет от 1 мегабита

НЕ РЕКОМЕНДУЕТСЯ ДЕРЖАТЬ В ПАНЕЛИ БОЛЕЕ 1000 СОКСОВ

фастфлюкс поддерживается но необходимы предварительные настройки
желательно не использовать фастфлюкс т.к. требуется домен который часто блокируют. лучше цеплять на IP

также разместить можно на белом хосте за 10 \$ если грузите не более 100 соксов

Фичи

- firewall (доступ к соксам только от доверенных IP)
- авторизация на соксах по логину и паролю
- GeoIP
- отображение имени компьютера/пользователя
- удаление бота
- добавление комментариев
- удаление офлайн ботов

лоадера нет. только socks5 софт

Screenshot of psevdo's announcements (in Russian), posted on July 19, 2018

Post-Endgame forum activity shows the codebase continuing to evolve:

psevdo

seller

●●●●●●



Seller

11

405 posts

Joined

07/31/12 (ID: 45104)

Activity

virology/malware

Autogarrant

0

Posted August 4, 2024

in touch. corrected errors and shortcomings in the Linux bot, as well as a non-working dns. update required server.exe or server.out and socks.out. updates are available in tox

+ Quote

*Announcement of "Linux bot and C2 server updates"
(Russian text translated to English)*

U R

psevdo
seller
●●●●●●



Seller
+ 11
405 posts
Joined
07/31/12 (ID: 45104)
Activity
virology/malware
Autogarrant
0

Posted August 15

a global test of the entire code was carried out. flaws and minor bugs were removed

+ Quote

« PREV 1 **2** Page 2 of 2 ▾

*Announcement of “global tests and bug fixes”
(Russian text translated to English)*

The continued forum activity suggests that Operation Endgame did not, in fact, mark the end of SystemBC development.

Same Threat, New Platform

Files we saw communicating with a known C2 in this cluster included an unusual Perl script, which had zero detections across the 62 antivirus engines on VirusTotal.

185.93.89.145

8/95 security vendors flagged this IP address as malicious

Community Score: 8/95

185.93.89.145 (185.93.89.0/24)
AS 213790 (Limited Network LTD)

IR Last Analysis Date: 15 hours ago

DETECTION DETAILS RELATIONS **COMMUNITY 6**

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Communicating Files (8)

Scanned	Detections	Type	Name
2025-08-19	22 / 65	ELF	common.lib
2025-09-22	23 / 65	ELF	5v48mv.exe
2025-09-05	33 / 63	ELF	termspage
2025-09-10	1 / 62	Shell script	fdgd
2025-07-16	32 / 65	ELF	phone_categories
2025-08-17	0 / 62	Perl	updateAction
2025-08-19	24 / 65	ELF	26d923888022307baf5255cae3acc53e
2025-08-24	31 / 65	ELF	uploadbusplan

[VirusTotal results for 185.93.89.\[145 – Relations](#)

Further analysis revealed the Perl script was a previously undocumented SystemBC variant designed specifically to infect Linux systems.

```

46 #!/usr/bin/perl
45
44 use strict;
43 use warnings;
42 use Socket;
41 use Socket qw(IPPROTO_TCP TCP_NODELAY);
40 use Fcntl;
39 use Fcntl qw(:flock);
38 use threads;
37 use threads::shared;
36
35 my $host = '185.93.89.145';
34 my $port = 443;
33
32 my $xordata = "\x00" x 50;
31
30 for (my $i = 0; $i < 50; $i++) { substr($xordata, $i, 1) = pack('C', rand(255)); }
29
28 sub Rc4_crypt {
27
26     my $passw = shift(@_);
25
24     my $length = shift(@_);
23
22     my $buff0 = shift(@_);
21
20     my $start = shift(@_);
19
18     my $sz = shift(@_);
17
16     my $rc4 = "\x00" x 256;
15
14     my $pockemon0 = 0;
13
12     my $pockemon1 = 0;
11
10     my $pockemon2 = 0;
9
8     my $pockemon3 = 0;
7
6     my $pockemon4 = 0;
5
4     my $pockemon5 = 0;
3
2     my $pockemon6 = 0;
1
47     my $pockemon7 = 0;
1

```

Example of the SystemBC Perl variant

Examining the files that dropped the Perl script revealed two additional ELF binaries: [SafeObject](#) and [StringHash](#).

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Domain	Detections	Created	Registrar
api.apple-cloudkit.com	0 / 95	2015-01-29	NOM-IQ Ltd dba Com Laude
api.snapcraft.io	0 / 95	2016-05-16	MarkMonitor Inc.
c.apple.news	0 / 95	2015-07-06	NOM-IQ Ltd dba Com Laude
h3.apis.apple.map.fastly.net	0 / 95	2011-04-18	MarkMonitor Inc.

IP	Detections	Autonomous System	Country
142.251.184.94	0 / 95	15109	US
151.101.131.6	0 / 95	54113	US
151.101.195.6	0 / 95	54113	US
151.101.3.6	0 / 95	54113	US
151.101.67.6	0 / 95	54113	US
169.254.169.254	0 / 95	-	-
17.138.175.254	0 / 95	714	US
17.157.64.66	0 / 95	714	US
185.125.188.54	0 / 95	41231	GB
185.125.188.57	1 / 95	41231	GB

Scanned	Detections	Type	Name
2025-08-22	2 / 65	ELF	SafeObject
2025-09-09	20 / 65	ELF	StringHash

Graph Summary

3 dropped files 2 execution parents

SystemBC Perl – Execution Parents

The SafeObject file is a UPX-packed variant of StringHash. Once unpacked, it recursively hunts for writable directories before dropping and executing 264 embedded SystemBC payloads, including both ELF and Perl variants.

Behavior aside, the dropper is unusually noisy and littered with Russian-language strings—an unscientific but familiar clue about the threat actor’s origins.

```

Не удалось создать директорию %s: %s\n
Не удалось создать файл %s: %s\n
Ошибка записи файла %s: %s\n
Не удалось сменить директорию на %s\n
Запущен %s в %s (PID: %d)\n
Не удалось создать процесс: %s\n
Запуск деплойера. Всего бинарников: %d\n
Развертывание бинарника %d/%d...\n
Не удалось развернуть бинарник %d\n
\nРазвертывание завершено.
Успешно запущено: %d\n
Ошибок: %d\n

```

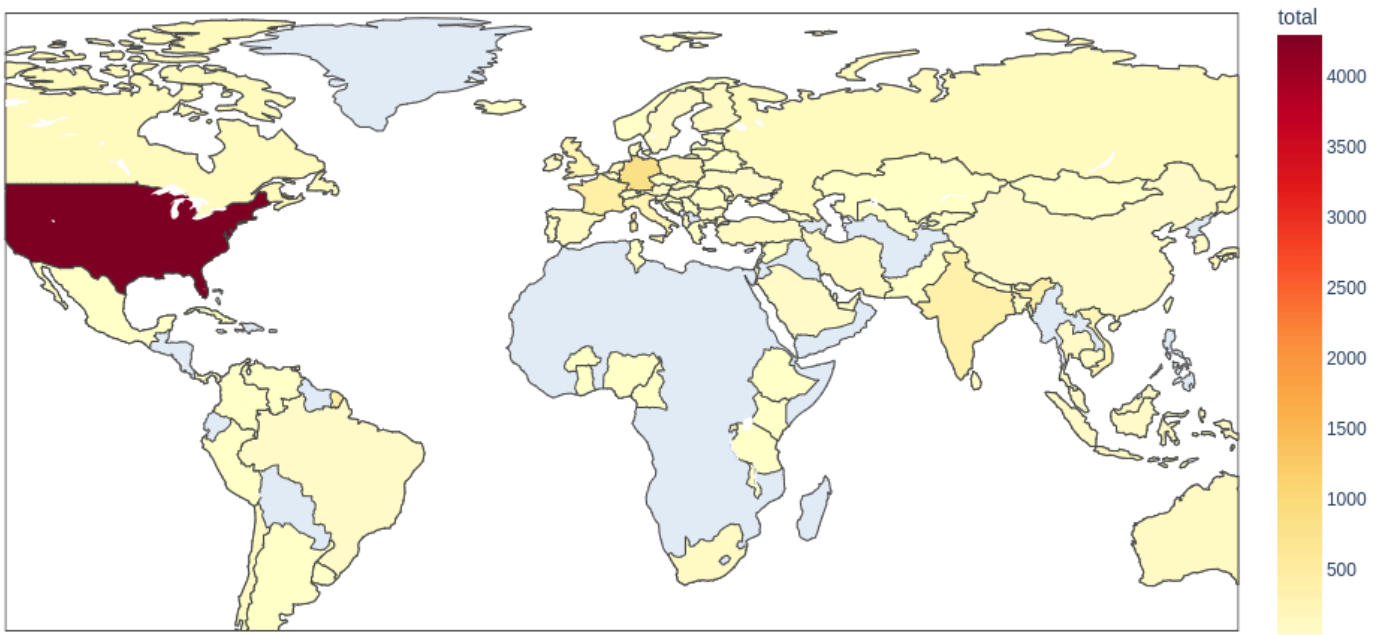
Screenshot of Russian strings observed

Where Infections Hit Hardest

Much of the SystemBC C2 infrastructure observed here appears to rely on hosting tied to abuse-tolerant providers, including BTHoster-linked environments and AS213790 (BTCLOUD). Zeroing in on the AS213790-hosted cluster alone, we identified more than 10,340 distinct victim IP addresses. Activity was steady—averaging roughly 2,888 victim IPs per day—with infections persisting far longer than typical. On average, systems remained infected for 38 days, with some lasting more than 100 days.

The highest concentration of infected systems seen in our analysis was in the U.S., with more than 4,300 affected IPs. Germany (829), France (448), Singapore (419), and India (294) followed.

Global Distribution of Victim IPs



Global distribution of IP addresses map

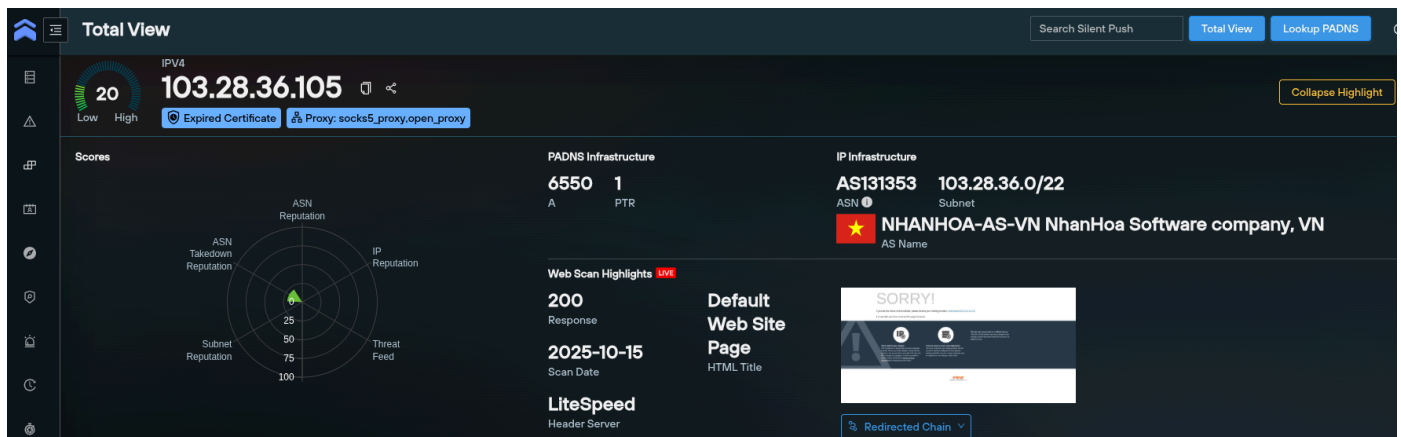
ASNs Tied to Victim IP Addresses

Looking at the ASNs tied to victim IPs, this cluster overwhelmingly targets hosting providers rather than residential networks, which helps explain why infections tend to linger—residential IPs typically change far more frequently.

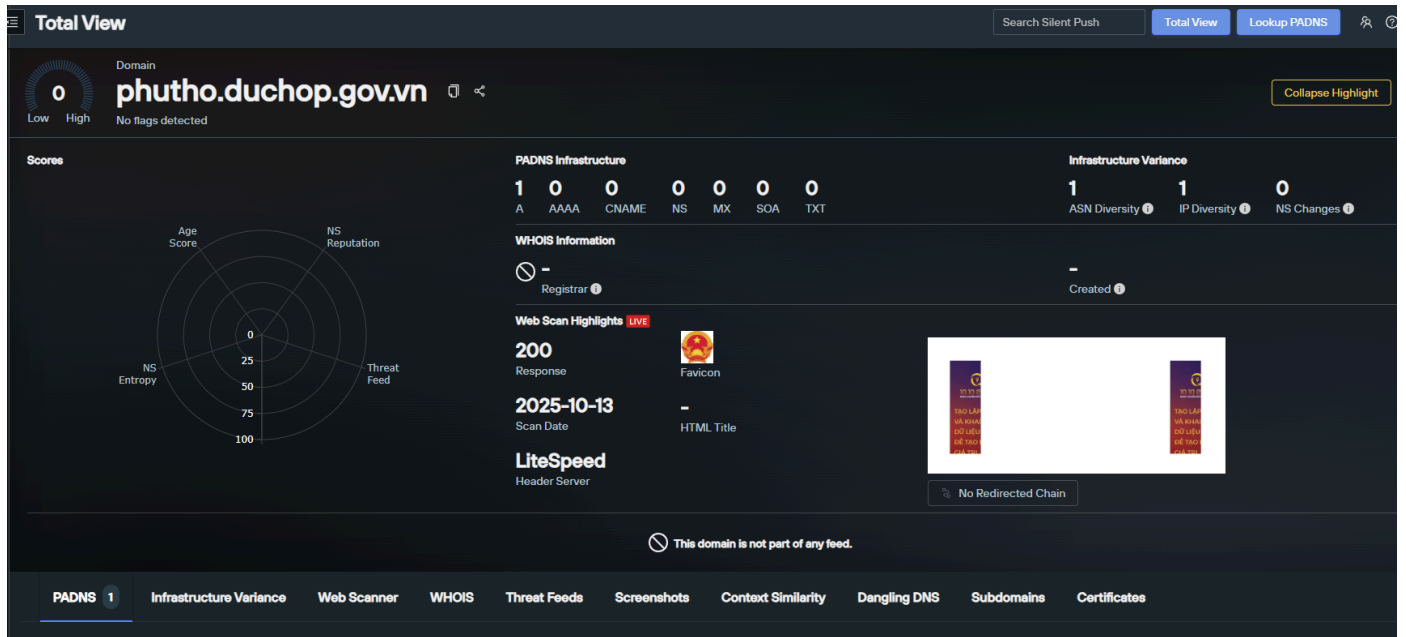
ASN	AS Name	AS Type
19871	NETWORK-SOLUTIONS-HOSTING	Hosting
46606	UNIFIEDLAYER-AS-1	Hosting
22612	NAMECHEAP-NET	Hosting
398101	GO-DADDY-COM-LLC	Hosting
8560	IONOS-AS	Hosting
16509	AMAZON-02	Hosting
16276	OVH	Hosting
24940	HETZNER-AS	Hosting
26496	AS-26496-GO-DADDY-COM-LLC	Hosting
14061	DIGITALOCEAN-ASN	Hosting

Table of the top 10 ASNs tied to victim IP addresses

Reviewing PADNS data led to an unexpected finding: infections tied to multiple government domains. One example surfaced at IP address **103.28.36[.]105**, a sizable cloud host that was also found hosting **phutho.duchop[.]gov[.]vn**, a Vietnamese provincial government website.



Silent Push Total View of IP address 103.28.36[.]105



Silent Push Total View of domain **phutho.duchop[.]gov[.]vn**



Screenshot of **phutho.duchop[.]gov[.]vn** website

IP address **196.13.207[.]92**, meanwhile, was linked to domains associated with the Government of Burkina Faso in West Africa.

< Back

Explore Basic Raw Data < Previous Next >

196.13.207.92
ANYIPV4 Monitor Save to

Clear Filters Total Results: 146 Results on current page: 100

☐	Query	Query ASN	☐	Answer	Answer ASN	First Seen	Last Seen	Type
☐	dgcoop.gov.bf	-	☐	196.13.207.92	327871	2023-04-27 11:13:21	2025-10-21 19:47:26	A
☐	cnle.gov.bf	-	☐	196.13.207.92	327871	2023-04-21 04:40:36	2025-10-21 19:20:13	A
☐	spgire.gov.bf	-	☐	196.13.207.92	327871	2023-04-27 11:12:53	2025-10-21 19:19:26	A
☐	onlyoffice.gov.bf	-	☐	196.13.207.92	327871	2025-09-18 22:29:40	2025-10-21 19:13:59	A
☐	www.gendarmierienation ale.bf	-	☐	196.13.207.92	327871	2024-05-24 00:05:37	2025-10-21 19:11:53	A
☐	stage.wuri.gov.bf	-	☐	196.13.207.92	327871	2025-09-02 12:16:45	2025-10-21 18:58:40	A
☐	uohg.gov.bf	-	☐	196.13.207.92	327871	2024-11-12 15:28:18	2025-10-21 18:37:53	A
☐	enpe.gov.bf	-	☐	196.13.207.92	327871	2024-09-10 18:55:14	2025-10-21 18:25:56	A
☐	cnamu.bf	-	☐	196.13.207.92	327871	2023-04-26 18:49:51	2025-10-21 18:20:11	A
☐	diospb.formationpro.gov bf	-	☐	196.13.207.92	327871	2025-04-17 12:37:18	2025-10-21 18:14:38	A
☐	formationpro.gov.bf	-	☐	196.13.207.92	327871	2024-08-27 11:40:13	2025-10-21 17:59:14	A
☐	www.spgire.gov.bf	-	☐	196.13.207.92	327871	2023-04-27 11:12:43	2025-10-21 17:50:20	A
☐	enptic.gov.bf	-	☐	196.13.207.92	327871	2024-05-18 11:16:30	2025-10-21 17:27:45	A
☐	eggem.gov.bf	-	☐	196.13.207.92	327871	2023-12-26 13:16:49	2025-10-21 17:27:44	A
☐	cour-comptes.gov.bf	-	☐	196.13.207.92	327871	2024-07-25 20:07:48	2025-10-21 17:27:44	A
☐	www.uohg.gov.bf	-	☐	196.13.207.92	327871	2024-11-13 23:06:32	2025-10-21 17:21:00	A
☐	cil.bf	-	☐	196.13.207.92	327871	2024-02-02 16:35:25	2025-10-21 16:32:38	A
☐	www.csm.bf	-	☐	196.13.207.92	327871	2023-05-12 02:23:15	2025-10-21 16:24:43	A

Screenshot of IP address 196.13.207.[.]92 revealing ties to the Burkina Faso government

← → ↻ 📄 concours.gov.bf 🔍 ☆



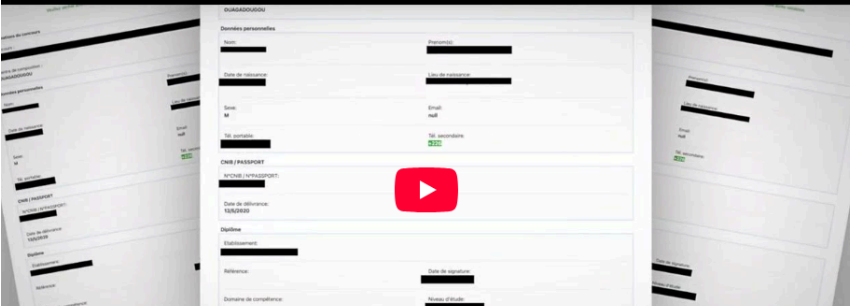
Agence Générale de
Recrutement de l'Etat (AGRE)



Accueil AGRE Textes Communiqués Arrêtés Listes de candidatures Programmation Vacances de postes Forum Médiathèque Actualités Statistiques

ANNONCES Bienvenue sur le site web de l'AGRE / Retrouvez toutes les informations sur l'AGRE

A Comment s'inscrire ? Econcours 2025 Copy link



À la une

rects Inter-Etats de recrutement
leront du 07 au 10 avril 2025)

Communiqué de répartition par sous
SANTÉ par centre , ses

Screenshot of concours[.]gov[.]bf website

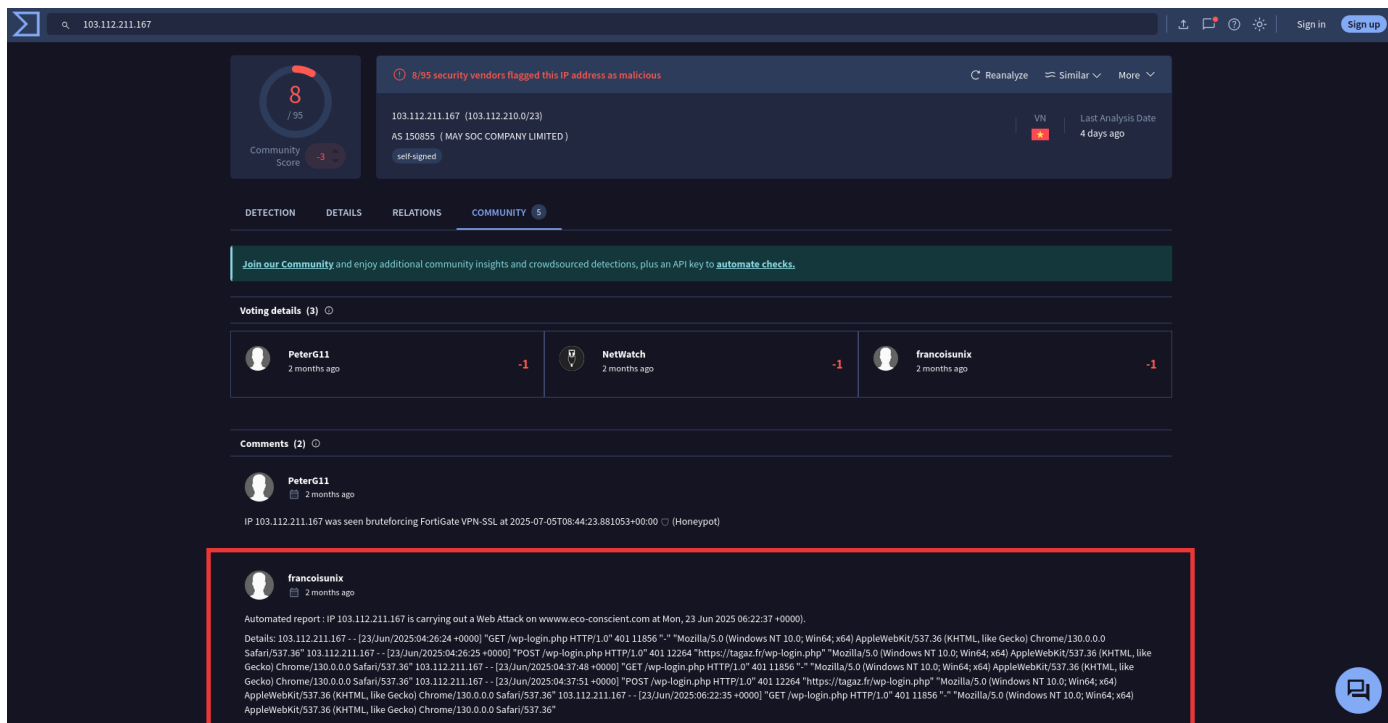
Many infected IP addresses have been reported in VirusTotal comments for engaging in WordPress exploitation activity. Taken together, these observations indicate that threat actors are using SystemBC-associated proxies to target WordPress websites.

This screenshot shows the VirusTotal report for IP address 202.142.184.234. The interface includes a top navigation bar with a search icon, the IP address, and user options (Sign in, Sign up). Below the navigation bar, a summary section displays a Community Score of 4/95, a status of '4/95 security vendors flagged this IP address as malicious', and the IP's details (202.142.184.234, AS 9260, Multinet Pakistan Pvt. Ltd.). A 'Join our Community' banner is present. The 'Voting details' section shows two votes: NetWatch (5 months ago) and francoisunix (9 months ago), both with a score of -1. The 'Comments' section, highlighted with a red border, contains a comment from francoisunix (2 months ago) reporting a Web Attack on www.eco-conscient.com at Fri, 11 Jul 2025 15:24:36 +0000. The comment includes a detailed automated report listing various user agents and their associated IP addresses.

Screenshot of 202.142.184[.]234 on [VirusTotal](#)

This screenshot shows the VirusTotal report for IP address 148.113.208.227. The interface includes a top navigation bar with a search icon, the IP address, and user options (Sign in, Sign up). Below the navigation bar, a summary section displays a Community Score of 7/95, a status of '7/95 security vendors flagged this IP address as malicious', and the IP's details (148.113.208.227, AS 16276, OVH SAS). A 'Join our Community' banner is present. The 'Voting details' section shows two votes: NetWatch (2 months ago) and francoisunix (4 months ago), both with a score of -1. The 'Comments' section, highlighted with a red border, contains a comment from francoisunix (3 months ago) reporting a Web Attack on www.eco-conscient.com at Fri, 30 May 2025 06:12:03 +0000. The comment includes a detailed automated report listing various user agents and their associated IP addresses.

Screenshot of 148.113.208[.]227 on [VirusTotal](#)



Screenshot of 103.112.211[.]167 on [VirusTotal](#)

Interested in Learning More About Preemptive Cyber Defense?

Our enterprise customers have access to the exclusive report we created for the SystemBC botnet family. If you would like to learn more about our capabilities for tracking adversarial frameworks—or how you can hunt for them on our platform—we encourage you/your organization to [reach out](#) to our team for a demonstration of Silent Push cyber defense technology.

[Book a Demo](#)

Connect with our platform experts for an overview of the Silent Push Enterprise Edition platform. We are happy to provide you with a tailored walkthrough for your specific use case, along with insights into integrations and API capabilities.

Mitigation

SystemBC-associated infrastructure presents a sustained risk due to its role early in intrusion chains and its use across multiple threat actors. Proactive monitoring is critical, as activity tied to SystemBC is often a precursor to ransomware deployment and other follow-on abuse.

Our analysts have developed SystemBC-specific Indicators of Future Attack™ (IOFA™) feeds to help identify related infrastructure and emerging variants before they cause downstream impact. These feeds include:

- SystemBC C2 Domains
- SystemBC C2 IPs
- SystemBC Infected IPs

The IOFA™ feeds are available as part of a Silent Push Enterprise subscription. Enterprise users can ingest this data into their security stack to inform their detection protocols or use it to pivot across attacker infrastructure using the Silent Push Console and Feed Analytics screen.

SystemBC IPs

- 36.255.98[.]159
- 62.60.131[.]191
- 36.255.98[.]179
- 62.60.131[.]184
- 36.255.98[.]152
- 36.255.98[.]160
- 62.60.131[.]187
- 62.60.131[.]204
- 62.60.131[.]180
- 36.255.98[.]165

Malicious SystemBC SHA256 Hashes

SystemBC Perl

c729bf6ea292116b3477da4843aaeec73370e2bd46e7a27674671e9a65fb473a

SystemBC Perl Droppers

- 0f5c81eaf35755a52e670c89b9546e7047828d83f346e3c29be1f6958e14a384
- da95384032f84228ef62f982f3c0f9e574dc6b06b606db33889ea6a5f93d6ae2

Ready to dive deeper into the world of preemptive cyber defense? Take our technology for a test drive with the free Silent Push Community Edition today.

[Register for Community Edition](#)

Continuing to Track SystemBC

Our threat intelligence and research teams will continue to track the SystemBC malware while expanding our understanding of the code variants, victims, and methods for monitoring the associated infrastructure. We believe SystemBC remains an active threat to major enterprises and expect the Tactics, Techniques, and Procedures (TTPs) of the multiple threat actors leveraging this malware to continue evolving indefinitely.

If you or your organization has any information to share regarding the findings of this report, we would love to hear from you.

[Blog](#)

Pushing Forward with Silent Push

February 6, 2026

[News Source](#)

[Blog](#)

Special Alert: SLSH Malicious "Supergroup" Targeting 100+ Organizations via Live Phishing Panels

January 26, 2026

[News Source](#)

[Blog](#)

The Invisible Insider: Why AML and KYC Compliance Fail Against Digital Deception

January 21, 2026

[News Source](#)