SystemBC: The Multipurpose Proxy Bot Still Breathes

bitsight.com/blog/systembc-multipurpose-proxy-bot-still-breathes

Written by João Batista September 21, 2022 Share Facebook Twitter LinkedIn

SystemBC is a malware written in C that turns infected computers into SOCKS5 proxies. The bot communicates with the command and control server using a custom binary protocol over TCP and uses RC4 encryption. This malware has evolved its capabilities since it was documented by Proofpoint [1] back in 2019, and now it can also download and run additional files. Moreover, this malware can target both Windows and Linux platforms.

SystemBC is sold on underground marketplaces, and after completing the purchase, the buyer receives an archive containing the bot executable, the command and control (C2) server executable, and a PHP admin panel.

Figure 1. Archive contents

The main capability of SystemBC is to turn the infected computers into SOCKS5 proxies. Since most bots are not reachable from the internet, this malware uses a backconnect architecture that allows clients to use the proxies (infected computers) through the backconnect (C2) server without ever needing to interact directly with them.

In practice, what happens is that for each infected computer that connects to the backconnect (C2) server, the server opens a new TCP port that will accept the SOCKS5 traffic from clients. That traffic is wrapped inside SystemBC's communications protocol and forwarded to the infected computers that will unwrap the traffic, send it to the destination, and send the response back to the backconnect (C2) server that will finally forward that response back to the client that initialized the communication.

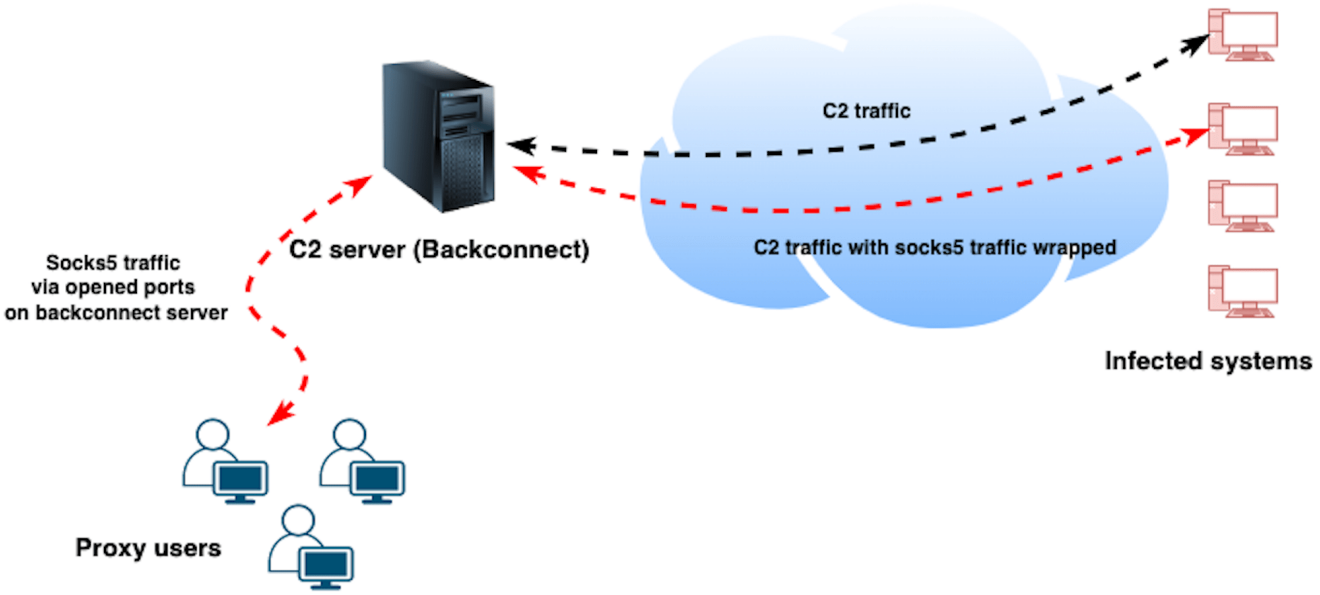

Figure 2. SystemBC backconnect architecture

There are a couple of variants of SystemBC with some differences in the bot capabilities. All variants turn the infected computer into a SOCKS5 proxy and can perform self-updates, but the more complete variant of SystemBC also presents the following capabilities:

- Support for C2 communications over TORCheck for the Emsisoft Anti-Malware process (a2guard.exe)
- Download and execute executable files (.exe and .dll)
- Download and execute shellcode
- Download and execute batch scripts (.cmd and .bat)
- Download and execute PowerShell scripts (.ps1)
- Download and execute Visual Basic scripts (.vbs)

Several threat actors leveraged SystemBC to maintain a foothold within a company's network and launch additional post-exploitation tools. In some panels, we could find tasks showing that SystemBC was used to push CobaltStrike [2] and PoshC2 [3].

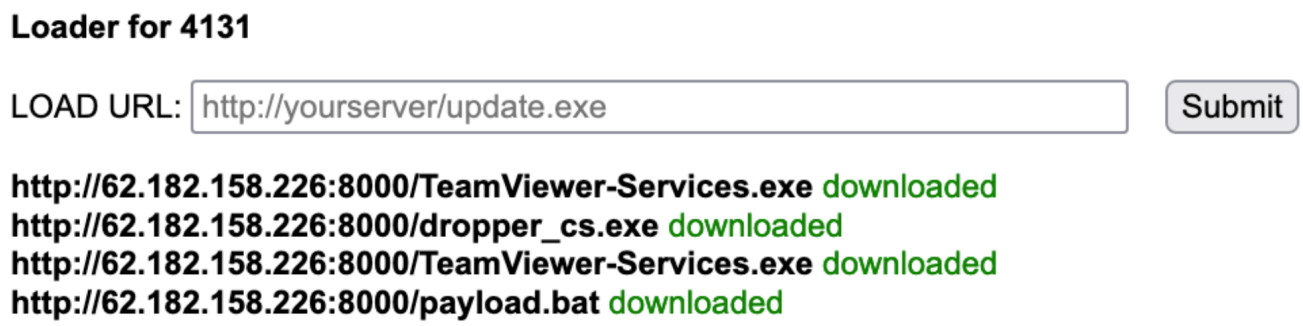

Figure 3. Tasks issued to an infected machine

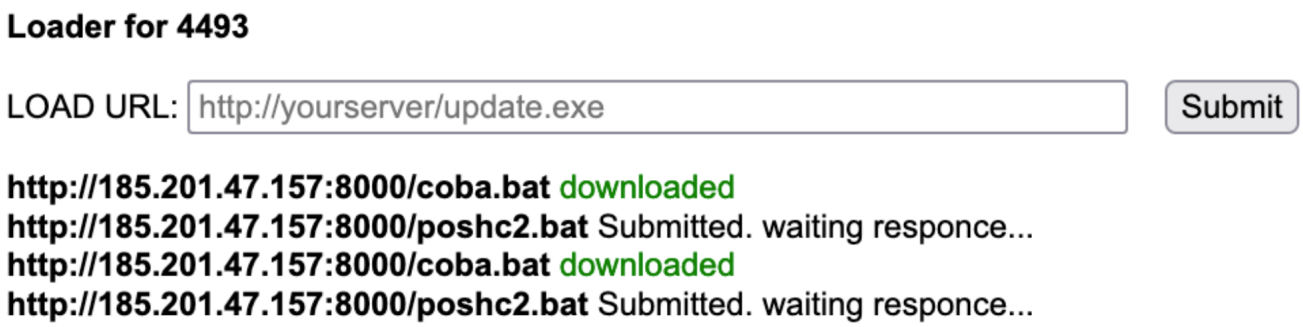

Figure 4. Tasks issued to an infected machine

When the downloaded file is a DLL, SystemBC maps it into its own memory space and creates a new thread to execute the entry point meaning that the DLL file does not touch the disk. Similarly, to download and run files containing shellcode, SystemBC allocates memory inside its process memory and creates a new thread to start the execution.

All other types of files are downloaded and saved to disk under the C:\Windows\Temp directory with a random name and executed using scheduled tasks. The tasks registered to run the PowerShell files will launch powershell.exe with the following command line: -WindowStyle Hidden -ep bypass -file “<DOWNLOADED POWERSHELL FILE>”.

Infections telemetry

While the usage of this malware has declined among threat actors, our telemetry via sinkholes and active command and control (C2) servers still reveals a significant number of infected systems. Since early August, BitSight has observed over 56,000 unique IP addresses infected with SystemBC.

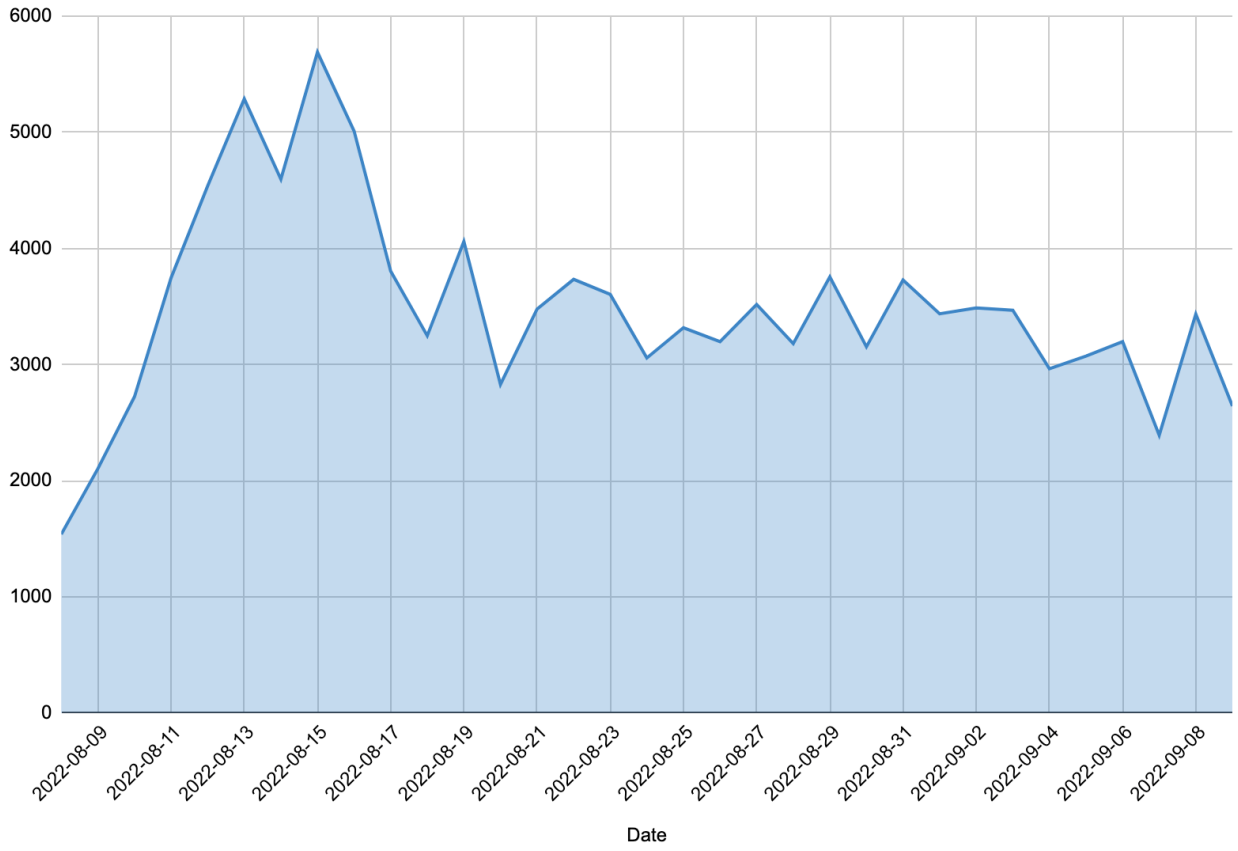

Figure 5. Daily infections observed by BitSight

The geographic distribution reveals the wide impact of SystemBC around the world. Countries like India, Indonesia, Pakistan, Thailand, Brazil, United States, Egypt, Philippines, Algeria and Turkey are in the top 10 of the most affected countries, representing around 58% of the total number of infections observed.

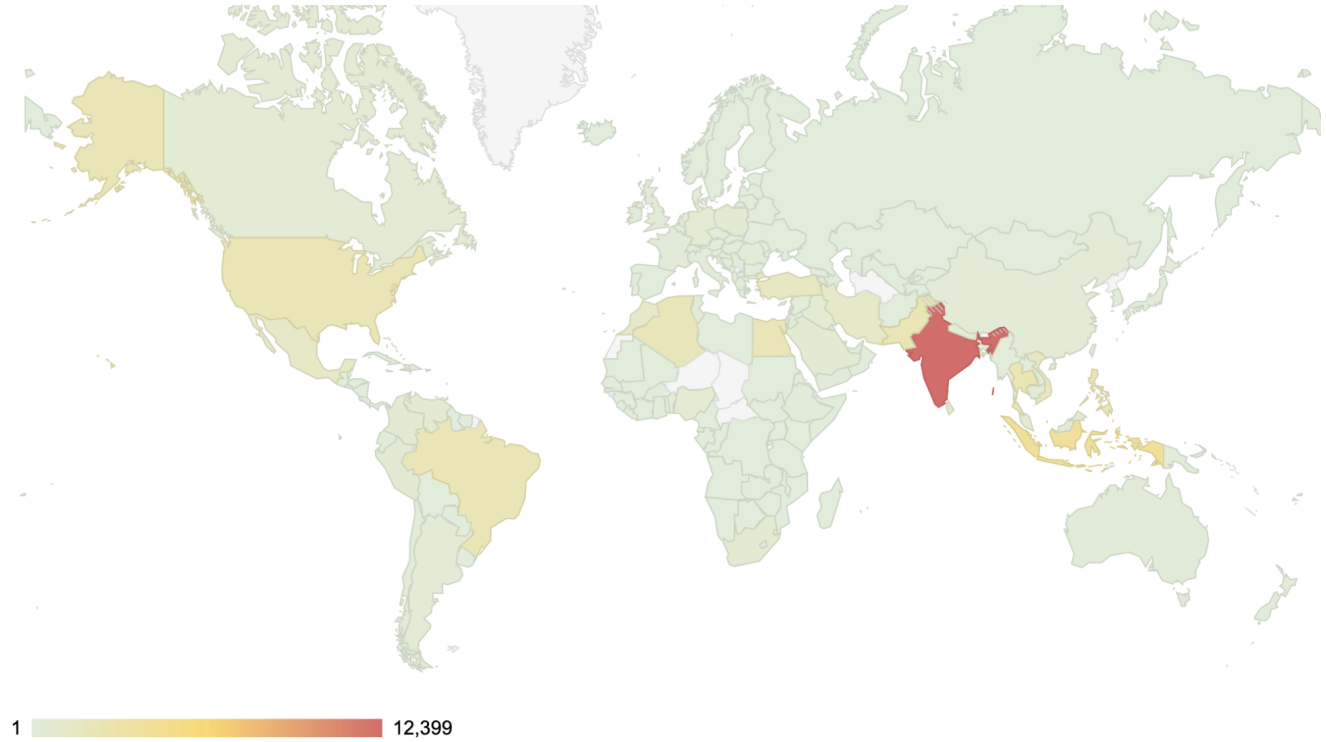

Figure 6. Geographic distribution of infected systems

Conclusion

SystemBC is an interesting piece of malware that can be leveraged differently depending on the threat actor's goals. Sometimes infected computers are only used to send traffic, but they can also be instructed to download and run post-exploitation tools such as CobaltStrike. While the usage of this malware has decreased compared to the previous years, we continue to see significant numbers of victims all over the world.

References

[1] https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits
[2] https://www.cobaltstrike.com/
[3] https://github.com/nettitude/PoshC2/

Indicators of Compromise (IOCs)

Backconnect (C2) servers observed since early August:

193.106.191[.]168
188.127.224[.]46
45.10.42[.]221
193.106.191[.]184
193.106.191[.]185

185.215.113[.]105
188.214.129[.]3
139.144.79[.]152
45.66.248[.]209
89.22.225[.]242
195.62.53[.]253
20.115.47[.]118
92.53.90[.]84
152.89.198[.]73
194.36.177[.]46
162.33.179[.]100

Updated list available in the following url:
https://raw.githubusercontent.com/bitsight-research/threat_research/main/systembc/c2.txt

Get the Weekly Cybersecurity Newsletter

Subscribe to get security news and industry ratings updates in your inbox.

-
- *
  Read more
  By checking this box, I consent to sharing this information with BitSight Technologies, Inc. to receive email and phone communications for sales and marketing purposes as described in our privacy policy. I understand I may unsubscribe at any time.