What to Know: GhostSocks Residential Proxy IoCs

spycloud.com/blog/on-the-hunt-for-ghostsocks/

James

March 25, 2025

Our ongoing research into LummaC2 infostealer malware family led the SpyCloud Labs team to uncover a very interesting connection between GhostSocks, a residential proxy plugin, and the pervasive infostealer. Through our digging, we found that recent versions of LummaC2 give bad actors a backconnect proxy into their infected victim's machines, allowing them to launch attacks as if they were the victim.

The consequences of this, as you can imagine, are substantial. It gives actors a much easier time of bypassing access control methods, such as Google's cookie access control methods, which LummaC2 heavily abuses to refresh expired tokens.

In order to better understand the threat that GhostSocks poses to organizations, our analysts here at SpyCloud Labs decided to do a deeper analysis of GhostSocks, and in doing so, uncovered some key, unique techniques that make GhostSocks a threat that defenders should take quite seriously:

Its persistence mechanisms allow for long lasting proxy servers

- Its ability to dynamically update the C2 list adds a high level of resiliency

- Its inclusion of TLS wrapping on the established backconnect tunnel adds a level of secrecy and security to connections

Here’s our full analysis.

Independent persistence

While most GhostSocks binaries depend on the malware that installed it for persistence, our analysts were able to find EXE binaries that have a persistence mechanism baked into GhostSocks directly. This mechanism, which can be viewed below and leverages registry run keys, allows for GhostSocks infections to survive restarts, allowing for a more long-lasting proxy uptime.

```
if (-Not (Test-Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\App")) {Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" -Name "App" -Value "" }
```

GhostSocks executes this command with PowerShell, which means defenders should be on the lookout for the above command string as it could be indicative of a GhostSocks infection and, possibly, additional malware leveraging the GhostSocks infection.

Static config

Inside of each GhostSocks binary is a static configuration which contains a list of C2 nodes, affiliate information, build version, and the proxy username and password to be used with the SOCKS5 backconnect tunnel.

Some of these values are obfuscated using GhostSock's custom obfuscation algorithm, which splits each string into four (4) byte chunks and then uses arithmetic shifts to reveal the deobfuscated text, as shown below.

Image A: An example of the obfuscated C2 buffer.

When communicating with the C2 during the check-in phase of network communication, GhostSocks assembles the affiliate information, build version, proxy username and password, and hash of the binary into a JSON dictionary, which can be observed in Image B.

Image B: JSON dictionary compiled during the check-in phase.

These C2s are used with GhostSocks' initial check-ins, however, GhostSocks has the ability to change these C2s on the fly following the initial check-in. Presumably, if one or more of the C2s go down, the GhostSocks check-in server would issue new IPs, which an infected bot is prepared to handle (and will be discussed in the next section).

Networking: TLS tunneling

After GhostSocks assembles its JSON configuration dictionary, it encrypts the dictionary with XOR using the key "config" and sends it to one of the C2s contained in its hardcoded C2 list in a basic request, as observed in Image C:

Image C: A check-in and response from a GhostSocks C2.

In order to properly communicate with the C2, GhostSocks must first set an X-API-Key header that is an 8-character randomly generated alphanumeric string. While older samples communicate over HTTP, newer samples have been spotted leveraging HTTPS, making detection of this a bit more challenging than just looking for unexpected “Go-http-client/1.1” user agents.

On successful check-ins, GhostSocks responds with a relay server IP used for establishing a SOCKS5 backconnect tunnel, the port GhostSocks should open, as well as a buffer of obfuscated C2s, which GhostSocks deobfuscates and uses for additional check-ins.

While normally this buffer is the same as the hardcoded one, GhostSocks also has the ability to insert new IPs if a given IP is taken down, or if a bot is using outdated IPs, allowing for more resilience than a single hardcoded config.

For ease of understanding, we refer to the hardcoded C2s/the C2s that are received on check-in as **Tier 1 C2s,** or **T1 C2s**, and then the relay server received during check-in are labeled as **T1 relays**.

Based on error outputs from the T1 C2s, our team at SpyCloud Labs theorizes that GhostSocks proxies back to another server, which would be GhostSocks’ Tier 2, however we have not uncovered this infrastructure yet.

Once GhostSocks receives the relay server IP and port, it opens the same port on its victim machine, establishes connection with the relay server IP for backconnect traffic, and then wraps **TLS 1.3 on top of all traffic that it sends and receives from the relay server.**

TLS wrapping is not something that SOCKS5 does; instead, this is something that the GhostSocks developers likely added themselves in order to properly secure connections. *This functionality gives GhostSocks a much stealthier form of tunneling, as the traffic is not sent in clear text and is fully encrypted on both ends.*

Throughout our analysis, we observed the following T1 C2 IPs:

- 46.8.232.106
- 46.8.232.61
- 91.212.166.91
- 91.212.166.9
- 147.45.196.157

- 38.180.61.247
- 195.2.70.38
- 91.142.74.28
- 188.130.206.243

- 38.180.205.164
- 93.185.159.253

- 195.2.70.38
- 91.142.74.28

And we observed the following T1 relay IPs:

- 185.245.106.67
- 185.121.233.152
- 77.238.237.190
- 185.157.213.253

- 195.200.28.33
- 185.21.13.144
- 212.34.130.72
- 195.200.31.22

Once the stealthy TLS1.3 + SOCKS5 backconnect tunnel is established, actors can then leverage the tunnel to bypass many authentication controls that look at a victim's IP/machine footprint in order to verify that a user is who they say they are. This includes Google's cookie authentication and many financial services.

Build differences

One of the known features of GhostSocks is the collaboration that it has with LummaC2. LummaC2 allows users of LummaC2 and GhostSocks to build and deploy GhostSocks binaries from the LummaC2 panel using GhostSocks' panel API, however LummaC2 may not be the only family/group with access to this API.

Judging by URI paths in the static C2s stored in a GhostSocks binary, it is possible to differentiate between binaries built using GhostSocks' API and binaries built using GhostSocks' panel. Binaries that contain the

/api/helper-first-register

URI path for static C2s were most likely built using GhostSocks' panel API (such as through the LummaC2 panel or through another malware family's panel), while binaries that do not use that URI path were most likely built using the GhostSocks panel. This doesn't necessarily indicate where they are used, however, as binaries that are built using the GhostSocks panel can still be deployed through a family like LummaC2. That being said, it's an interesting attribution point.

YARA rules

SpyCloud Labs analysts have made the following YARA rule to help defenders identify GhostSocks binaries that are found not packed:

```
rule GhostSocks {
meta:
description = “Rule to detect GhostSocks binaries”
author = “SpyCloud Labs”
strings:
$s1 = “POST”
$s2 = {89 EE C1 E5 02 39 EB 77}
$s3 = {0F B6 ?? ?? ?? 0F B6 ?? ?? ?? 31 CA 88 ?? ?? ?? 40}
condition:
```

all of them
}
Additionally, we found the following samples using the above YARA rule:

- 701a35ba073fee56ad2308d91844601e6ef48fb302c574a8cb2f15d7771a7398
- a7c8b47226d0c97bb694ca34d7f02d014b08dbe2b995941e4d525a64276cc4a1
- cbdf4f845fda37f9f6633ea8d1ca502f44ba1e053182f8dfc4c4d4463561df50
- db331fe09bfc7d2e54944c010bfa9bcfe4433830f35cbe74e5319ef7755437b6
- 86a52400ef6f1277e02290368e46dd6bb0217cc8f4b7eab1915e9c8aab35f0d2
- aee5bd8da7bdcce3a8151c564e35cf320960be7d4c20ed43cec7ab545357b11b
- 0ffd8ffbd8c6935ce6cb7df55e8c7f7a5360c172cbf5bf3819270c2021191a1a
- 8cde873e0503d3645ca7cf2ab916e5fc6219f9c49e729997c957ab77806c2935
- a07ab3819ddd1b14d7c80d37452205bc67dbf6ea4661da00ac2049baff020f78
- c1719c1a01a7590c2425ced044115cad898879ed71f5510917eb17f317ab46d6
- 6c165db5f330f0eb7d490634950b634dba82c130c7da20a9a0d385c5ba2d1b45
- 88b666224ab9b2ac937747ffdb1b93a20476e1efa39c45e7c8d716ae1e3f7e21
- 6cc9b9fae906ecba357fd5305a4aeecf6c7bd06398d8e0be1d0f2cb23aea6a77
- 9aae38b23bc89ca6a08a37425e0903a2edfd1e7cda025a430cd72a69e56122fa
- 7f620d10d6836b3e9e5f83f7ed9b971521d7ce2bd3b859749ae8955884f4db1a
- ecea2a947a56b03100ebc3940169ed2785c1c0615dfaea10b2550f26631daf98
- 65ed421d1b6cfe9b5285756a474d255e1fcb0cc7cc4e320269d7790db12dfc23
- cd8ba142563cc184bd42f47ad3f29af756c2f5789dc9bf1af91003c3021f3d79
- 1fdbbd54d17b341ceb3dfbd230693633cbe12b4ced5c5f60562c07629426fa2e
- dbd4584d6665b0ee2b5b012d4633eea58432c68d762bc2ee4af53e61d41c1d7e
- affb740d7b4efd943f29366966ae96c4a9e4ec6b59772fb011de7db632df8428
- 1fa1c5305c68ce4da09f1fda96d786711fe2c96275d8e82c8a68be832e57ba31
- 0407f729b2804c6b640bedb1afb012104d742f2a779e812d1cb2885f7b9a2d5e
- e5fac74de619a3228e35e52be5acdaa709a5ae1da98067792d6ab4b88c169540
- d19e87d90136f506e1eb1ecdc83015811490afc7019214b40cf304657eafeddf
- 839f8c77e1344f5ef5f47a176604caa9d97f04253cdcf96f4322dfecfece3b20
- a4c578abfd4b46c7a5d6c0e8dbfb36baf65cbddfdeeae3090f71109d8056e3d3
- dd8e06b6596893db253ea1d1f1749731a6882ed812898fbb8d04a34112dc7fbf
- 49d54d5c83609ba0f5dd558de757f8704c1e806dfa241aefe07a2be7d3c833cd
- 7003fab73a02bd5545afbf53a0a088dc66bfe3d4ed52a16defc521deecbd24b6
- 72046ea151d669d0b65ae63211e263aaba70cc51c6cd635d83df61a4c0a97770
- ced4ee8a9814c243f0c157cda900def172b95bb4bc8535e480fe432ab84b9175
- 4d12acca2de5b315071a2d6d43950f548740d5c451d3dc203b21220603ab32e3
- fbf51fd5fd3c455ac0234d2926b2602e27eb465ddbf50181dae0137fdc98bd3b
- d235fd0653d7ba640b42b34047eb8a3793b5243ecd62b7878f54fb5e2e6f56c0
- 6cfce42140a3920fea064243cf9b7e8634630edb0766f0aa1e3d8b02b3ae52e1
- bba64b1f6979828ae7dd4e3d7bfb0a6fad963736a3b647551b2d14c716646283
- 4fc2402835af8af7e73ab7e149009146ee3e3157d86940937be49eb3f128a549
- 57eacedd25ddeb4b87aeca0e847e55b7c4f7383657175a578cc863b259861e46
- b34a158b5d70cd54b8228a209a0772a7b91edaad1faf5b8b2779221512f8ff61
- 491770484e1dc9896cd2bb80283ea9b6bbeba3c4b38bdf7e1c4aa6813e8fc8e9
- 14885f61261396bc1af2a3d7bc3e3bfa94a247e532a40fa9985e2726430a84af
- 5fea56db43330f4823f1170fa56f1d7a18a271465f484e532cb4b5f00b3c1339
- 220aa1f46c63d690a90db20485b645d8b3ded71cdf27b635e0812be3f86e574a
- 189c85c5b8e2d29486c6eb9ef391aa0169eae334292961de6ce4c81356fdbba8
- 9f606e37f89aa1c33575739021cab01df44dbc898425ad42a1588f1a8d163e3c
- ef27dc4e15227ddb74043e223995447bc30d2f91fc25167a15cda9753d8e1894
- c00e4faa78ccf7e29b2380dc50251034ad638e81e15c84ee4df5af015b82c223
- c5c9072aa653fbbc82260e6c1acb89c438ac008a8e14ab679370c5fab36ed919
- 3b74367815f5f26ba60f8cb0c3c4926e064beaf1e1744b7841b4faa72bc95cb2
- 2dc72c0044ab8aee07635ae5daffa21569c87170d176d71a31b5a0671325ff20

Key takeaways

Our findings mark a bit of a turning point in the evolution of infostealer malware. The collaboration between GhostSocks and LummaC2 (and other stealer families) already stretched the more “traditional” rules of how threat actors are using malware, but our latest analysis of GhostSocks shows how truly robust and striking this pivot is:

- The GhostSocks residential proxy plugin can maintain its own persistence on a device, even surviving restarts

- It’s also quite resilient to C2 takedowns, due to dynamic configuration acquisition

- Because it leverages TLS for tunneling, it’s extra hard to spot

- Since it’s often bundled with LummaC2, it massively lowers the skill requirement to perform successful MFA bypass

The potential dangers are real to consumers and defenders alike. Defenders should:

- Keep an eye out for the PowerShell command string specified above that could indicate GhostSocks’ presence on a device

- Defenders can use YARA rules to hunt across organization environments or on malware datasets that allow for rule upload

- Monitor for evidence of LummaC2 and other infostealer infections that can open the door to GhostSocks’ functionality (not to mention other unfortunate consequences like account takeover, session hijacking, ransomware, or fraud)

Learn more about other recent malware trends in our latest Malware & Ransomware Defense Report.
Read now

Keep reading

Cybercrime Wins in 2024: Major Takedowns & Arrests

- March 14, 2025
- SpyCloud Labs Research Team

Discover the biggest wins from 2024 against cybercrime—from major infostealer takedowns to global ransomware crackdowns—and what they mean for the future of cybersecurity.

Security Research, SpyCloud Labs

The Most Notable Data Breaches of 2024

- March 13, 2025
- SpyCloud Labs Research Team

Headline-making breaches in 2024 exposed millions of records, compromising sensitive data. This blog explores what was stolen and the impact that has on security strategies to stay ahead.

Cyberattack Trends, SpyCloud Labs

Black Basta Leaks, B1ack's Stash, & Billions of Stealer Log Records

- March 10, 2025
- Aurora Johnson | Keegan Keplinger

A deep dive into February's cybercrime trends, including Black Basta ransomware insights, stolen credit card databases, and the latest threat actor activities.

SpyCloud Labs