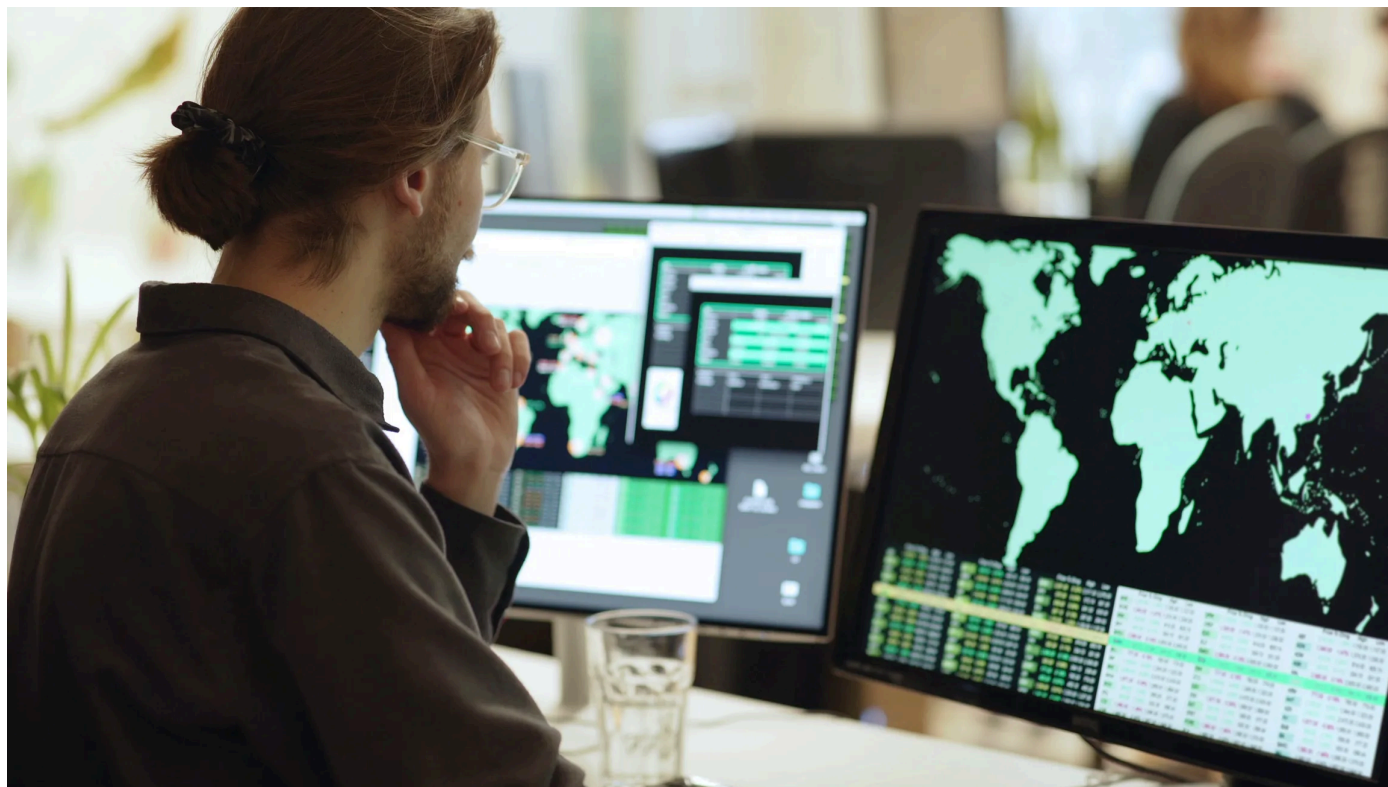


Tracking & Detecting GhostSocks Malware

 darktrace.com/blog/phantom-footprints-tracking-ghostsocks-malware

Gernice Lee

March 26, 2026



Phantom Footprints: Tracking GhostSocks Malware

GhostSocks is an emerging threat turning compromised devices into residential proxy nodes to help attackers evade detection. Darktrace identifies its growing use alongside Lumma Stealer, highlighting the malware's stealth, payload delivery, and persistence. AI-driven detection and Autonomous Response reveal the full attack lifecycle and underscore the need for proactive defense.

Why are attackers using residential proxies?

In today's threat landscape, blending in to normal activity is the key to success for attackers and the growing reliance on residential proxies shows a significant shift in how threat actors are attempting to bypass IP detection tools.

The increasing dependency on residential proxies has exposed how prevalent proxy services are and how reliant a diverse range of threat actors are on them. From cybercriminal groups to state-sponsored actors, the need to bypass IP detection tools is fundamental to the success of these groups. One malware that has quietly become notorious for its ability to avoid [anomaly detection](#) is **GhostSocks**, a [malware](#) that turns compromised devices into residential proxies.

What is GhostSocks?

Originally marketed on the Russian underground forum xss[.]is as a Malware-as-a-Service (MaaS), GhostSocks enables threat actors to turn compromised devices into residential proxies, leveraging the victim's internet bandwidth to route malicious traffic through it.

How does Ghostsocks malware work?

The malware offers the threat actor a “clean” IP address, making it look like it is coming from a household user. This enables the bypassing of geographic restrictions and IP detection tools, a perfect tool for avoiding anomaly detection. It wasn't until 2024, when a partnership was announced with the infamous information stealer [Lumma Stealer](#), that GhostSocks surged into widespread adoption and alluded to who may be the author of the proxy malware.

Written in GoLang, GhostSocks utilizes the SOCKS5 proxy protocol, creating a SOCKS5 connection on infected devices. It uses a relay-based C2 implementation, where an intermediary server sits in between the real command-and-control (C2) server and the infected device.

How does Ghostsocks malware evade detection?

To further increase evasion, the Ghostsocks malware wraps its SOCKS5 tunnels in TLS encryption, allowing its malicious traffic to blend into normal network traffic.

Early variants of GhostSocks do not implement a persistence mechanism; however, later versions achieve persistence via registry run keys, ensuring sustained proxy operational time [1].

While proxying is its primary purpose, GhostSocks also incorporates backdoor functionality, enabling malicious actors to run arbitrary commands and download and deploy additional malicious payloads. This was evident with the well-known ransomware group [Black Basta](#), which reportedly used GhostSocks as a way of maintaining long-term access to victims' networks [1].

Darktrace's detection of GhostSocks Malware

Darktrace observed a steady increase in GhostSocks activity across its customer base from late 2025, with its Threat Research team identifying multiple incidents involving the malware. In one notable case from December 2025, Darktrace detected GhostSocks operating alongside Lumma Stealer, reinforcing that the partnership between Lumma and GhostSocks remains active despite recent attempts to disrupt Lumma's infrastructure.

Darktrace's first detection of GhostSocks-related activity came when a device on the network of a customer in the education sector began making connections to an endpoint with a suspicious self-signed certificate that had never been seen on the network before.

The endpoint in question, 159.89.46[.]92 with the hostname `retreaw[.]click`, has been flagged by multiple open-source intelligence (OSINT) sources as being associated with Lumma Stealer's C2 infrastructure [2], indicating its likely role in the delivery of malicious payloads.

Figure 1: Darktrace's detection of suspicious SSL connections to `retreaw[.]click`, indicating an attempted link to Lumma C2 infrastructure.

Less than two minutes later, Darktrace observed the same device downloading the executable (.exe) file "Renewable.exe" from the IP 86.54.24[.]29, which Darktrace recognized as 100% rare for this network.

Figure 2: Darktrace's detection of a device downloading the unusual executable file "Renewable.exe".

Both the file MD5 hash and the executable itself have been identified by multiple OSINT vendors as being associated with the GhostSocks malware [3], with the executable likely the backdoor component of the GhostSocks malware, facilitating the distribution of additional malicious payloads [4].

Following this detection, Darktrace's Autonomous Response capability recommended a blocking action for the device in an early attempt to stop the malicious file download. In this instance, Darktrace was configured in Human Confirmation Mode, meaning the customer's security team was required to manually apply any mitigative response actions. Had Autonomous Response been fully enabled at the time of the attack, the connections to 86.54.24[.]29 would have been blocked, rendering the malware ineffective at reaching its C2 infrastructure and halting any further malicious communication.

Figure 3: Darktrace's Autonomous Response capability suggesting blocking the suspicious connections to the unusual endpoint from which the malicious executable was downloaded.

As the attack was able to progress, two days later the device was detected downloading additional payloads from the endpoint `www.lbfs[.]site` (23.106.58[.]48), including "Setup.exe", ".exe", and "/vp6c63yoz.exe".

Figure 4: Darktrace's detection of a malicious payload being downloaded from the endpoint [www.lbfs\[.\]site](http://www.lbfs[.]site).

Once again, Darktrace recognized the anomalous nature of these downloads and suggested that a "group pattern of life" be enforced on the offending device in an attempt to contain the activity. By enforcing a pattern of life on a device, Darktrace restricts its activity to connections and behaviors similar to those performed by peer devices within the same group, while still allowing it to carry out its expected activity, effectively preventing deviations indicative of compromise while minimizing disruption. As mentioned earlier, these mitigative actions required manual implementation, so the activity was able to continue. Darktrace proceeded to suggest further actions to contain subsequent malicious downloads, including an attempt to block all outbound traffic to stop the attack from progressing.

Figure 5: An overview of download activity and the Autonomous Response actions recommended by Darktrace to block the downloads.

Around the same time, a third executable download was detected, this time from the hostname `hxxp[://]d2ihv8ymzp14lr.cloudfront.net/2021-08-19/udppump[.]exe`, along with the file “udppump.exe”. While GhostSocks may have been present only to facilitate the delivery of additional payloads, there is no indication that these CloudFront endpoints or files are functionally linked to GhostSocks. Rather, the evidence points to broader malicious file-download activity.

Shortly after the multiple executable files had been downloaded, Darktrace observed the device initiating a series of repeated successful connections to several rare external endpoints, behavior consistent with early-stage C2 beaconing activity.

Cyber AI Analyst’s investigation

Figure 7: Darktrace’s detection of additional malicious file downloads from malicious CloudFront endpoints.

Throughout the course of this attack, Darktrace’s Cyber AI Analyst carried out its own autonomous investigation, piecing together seemingly separate events into one wider incident encompassing the first suspicious downloads beginning on December 4, the unusual connectivity to many suspicious IPs that followed, and the successful beaconing activity observed two days later. By analyzing these events in real-time and viewing them as part of the bigger picture, Cyber AI Analyst was able to construct an in-depth breakdown of the attack to aid the customer’s investigation and remediation efforts.

Figure 8: Cyber AI Analyst investigation detailing the sequence of events on the compromised device, highlighting its extensive connectivity to rare endpoints, the related malicious file-download activity, and finally the emergence of C2 beaconing behavior.

Conclusion

The versatility offered by GhostSocks is far from new, but its ability to convert compromised devices into residential proxy nodes, while enabling long-term, covert network access—illustrates how threat actors continue to maximise the value of their victims’ infrastructure. Its growing popularity, coupled with its ongoing partnership with Lumma, demonstrates that infrastructure takedowns alone are insufficient; as long as threat actors remain committed to maintaining anonymity and can rapidly rebuild their ecosystems, related malware activity is likely to persist in some form.

Credit to Isabel Evans (Cyber Analyst), Gernice Lee (Associate Principal Analyst & Regional Consultancy Lead – APJ)

Edited by Ryan Traill (Content Manager)

Appendices

References

1. <https://bloo.io/research/malware/ghostsocks>
2. <https://www.virustotal.com/gui/domain/retreaw.click/community>
3. <https://synthient.com/blog/ghostsocks-from-initial-access-to-residential-proxy>
4. <https://www.joesandbox.com/analysis/1810568/0/html>
5. <https://www.virustotal.com/gui/url/fab6525bf6e77249b74736cb74501a9491109dc7950688b3ae898354eb920413>

Darktrace Model Detections

Real-time Detection Models

Anomalous Connection / Suspicious Self-Signed SSL

Anomalous Connection / Rare External SSL Self-Signed

Anomalous File / EXE from Rare External Location

Anomalous File / Multiple EXE from Rare External Locations

Compromise / Possible Fast Flux C2 Activity

Compromise / Large Number of Suspicious Successful Connections

Compromise / Large Number of Suspicious Failed Connections

Compromise / Sustained SSL or HTTP Increase

Autonomous Response Models

Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block

Antigena / Network / External Threat / Antigena Suspicious File Block

Antigena / Network / Significant Anomaly / Antigena Controlled and Model Alert

Antigena / Network / External Threat / Antigena File then New Outbound Block

Antigena / Network / Significant Anomaly / Antigena Alerts Over Time Block

MITRE ATT&CK Mapping

Tactic – Technique – Sub-Technique

Resource Development – T1588 - Malware

Initial Access - T1189 - Drive-by Compromise

Persistence – T1112 – Modify Registry

Command and Control – T1071 – Application Layer Protocol

Command and Control – T1095 – Non-application Layer Protocol

Command and Control – T1071 – Web Protocols

Command and Control – T1571 – Non-Standard Port

Command and Control – T1102 – One-Way Communication

List of Indicators of Compromise (IoCs)

86.54.24[.]29 - IP - Likely GhostSocks C2

http[:]//[86.54.24[.]29/Renewable[.]exe - Hostname - GhostSocks Distribution Endpoint

http[:]//[d2ihv8ymzp14lr.cloudfront[.]net/2021-08-19/udppump[.]exe - CDN - Payload Distribution Endpoint

www.lbfs[.]site - Hostname - Likely C2 Endpoint

retreaw[.]click - Hostname - Lumma C2 Endpoint

alltipi[.]com - Hostname - Possible C2 Endpoint

w2.bruggebogeyed[.]site - Hostname - Possible C2 Endpoint

9b90c62299d4bed2e0752e2e1fc777ac50308534 - SHA1 file hash – Likely GhostSocks payload

3d9d7a7905e46a3e39a45405cb010c1baa735f9e - SHA1 file hash - Likely follow-up payload

10f928e00a1ed0181992a1e4771673566a02f4e3 - SHA1 file hash - Likely follow-up payload

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Written by

Gernice Lee

Associate Principal Analyst & Regional Consultancy Lead

[Share this post](#)

[Latest blogs](#)



[When Reality Diverges from the Playbook: Darktrace Identifies Encryption in a World Leaks Ransomware Attack](#)

[Network](#)

•

[March 17, 2026](#)

[Tiana Kelly](#)

[Senior Cyber Analyst & Team Lead](#)



[State of AI Cybersecurity 2026: 92% of security professionals concerned about the impact of AI agents](#)

[AI](#)

[:](#)

[March 26, 2026](#)

[The Darktrace Community](#)