Targeting Innovation: Sliver C2 and Ligolo-ng Used in Operation Aimed at Y Combinator

Published: 2024-11-12 · Archived: 2026-04-06 01:10:31 UTC

TABLE OF CONTENTS

Inside the Sliver Framework

Sliver, a cross-platform command-and-control (C2) framework developed by Bishop Fox, was originally created to support adversary emulation and red teaming. However, its robust functionality has led to cybercriminals and nation-state groups adopting it as a stealthy alternative to more recognizable tools like Cobalt Strike.

Core Capabilities:

- **Cross-Platform Operation**: Works on Windows, macOS, and Linux.
- **Encrypted Communications**: Supports secure channels via mTLS, WireGuard, HTTP(S), and DNS protocols.
- **Advanced Payload Options**: Provides features like process injection and in-memory execution of .NET assemblies.
- **Modular Design**: Allows users to expand capabilities through custom payloads and third-party integrations.

Adoption by Threat Actors:

- **Supply Chain Attack via Korean Software Vendor**: A compromised Korean software installer delivered Sliver, enabling attackers to mask their presence within seemingly legitimate applications-an evolving tactic in supply chain threats.
- **North Korean Group Using Play Ransomware**: North Korean actors deployed Sliver's stealth capabilities to facilitate the execution of Play ransomware, underscoring its utility in advanced evasion techniques.
- **Nitrogen Campaign Leading to BlackCat Ransomware**: In a recent Nitrogen operation, Sliver provided initial access and reconnaissance capabilities, eventually leading to the deployment of BlackCat ransomware.

Detection Challenges: Sliver's flexibility in payload customization, protocol use, and rapid development updates make it difficult to detect using traditional methods. Its ability to mimic legitimate traffic and quickly adapt to

detection efforts poses significant challenges for defenders relying on signature-based tools.

Ligolo-ng Overview

Ligolo-ng is a tunneling and pivoting tool that allows security professionals to securely access internal networks via a reverse TCP/TLS connection. Unlike traditional SOCKS proxies, it leverages a TUN interface, enabling seamless traffic routing through compromised machines.

Ligolo-ng is a favored tool among penetration testers because of its ease of use and cross-platform compatibility. It supports lateral movement within complex network environments, making it ideal for stealthy internal network exploration and effective pivoting during security assessments.

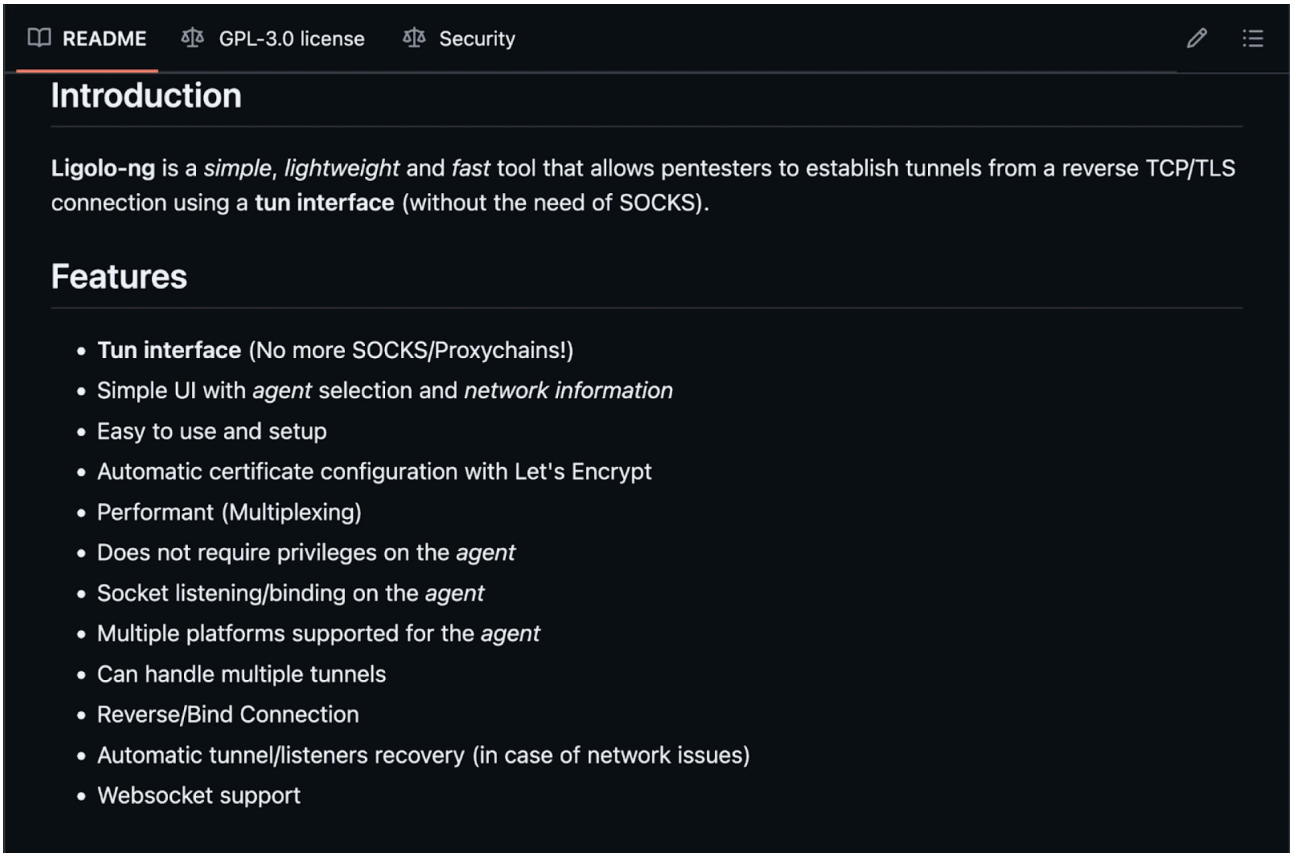


Figure 1: Ligolo-ng GitHub README.

Initial Findings - IP Address and Domain Linkage

During our analysis of recent entries in Hunt's C2 Infrastructure feature, we identified an IP address flagged as a Sliver controller: `179.60.149[.]75`, hosted on the HOSTKEY ASN in the United States. The IP exhibited active Sliver C2 ports on **3333**, **22813**, and **43215**, alongside Ligolo-ng on port **22913**. This discovery led us to investigate the infrastructure surrounding this server further.

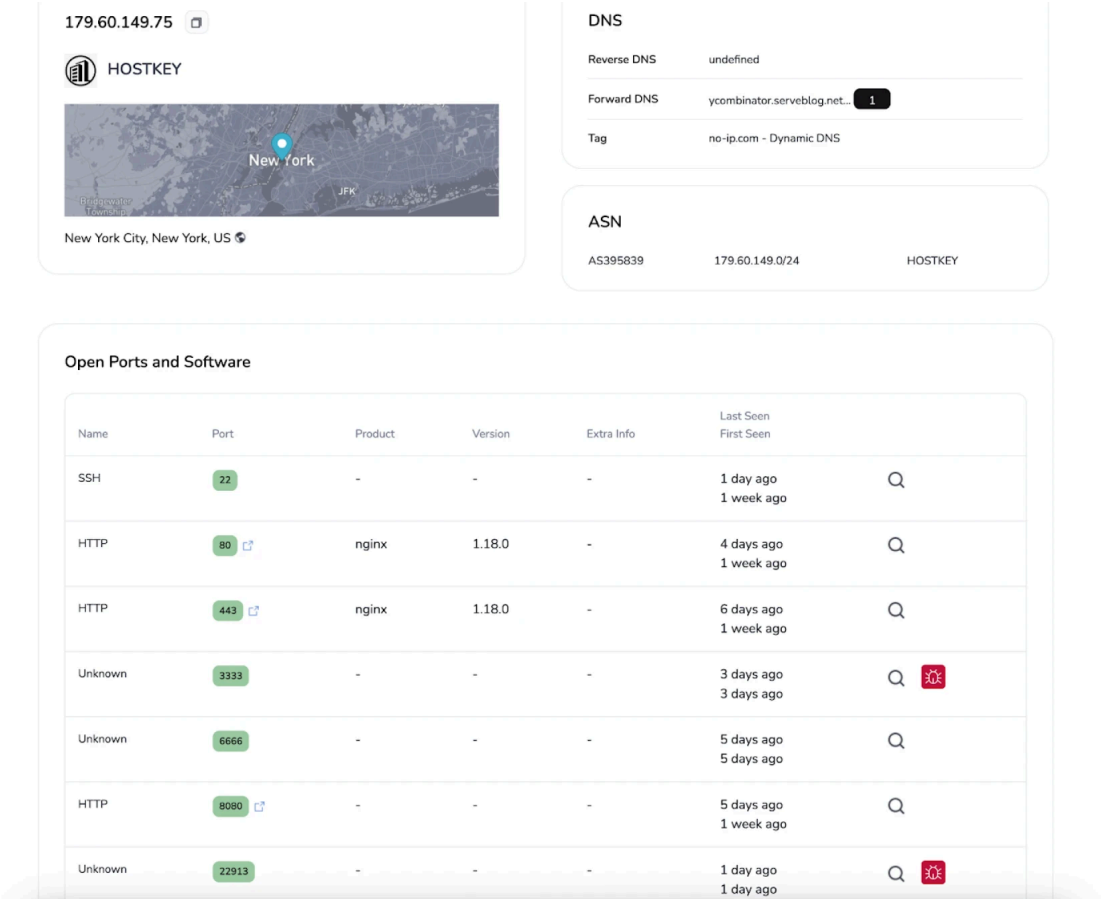


Figure 2: Overview of the Sliver C2 in Hunt.

Additional analysis uncovered an associated domain, `ycombinator.serveblog[.]net`, crafted to resemble Y Combinator, a well-known venture capital firm. The similarity to the legitimate brand name suggests a potential attempt to establish trust or credibility, possibly to deceive users or networks that recognize the firm's status within the tech community.

Upon navigating to this spoofed domain, we observed an immediate HTTP redirect to Y Combinator's legitimate website-a tactic likely intended to deflect suspicion while maintaining a functional appearance.

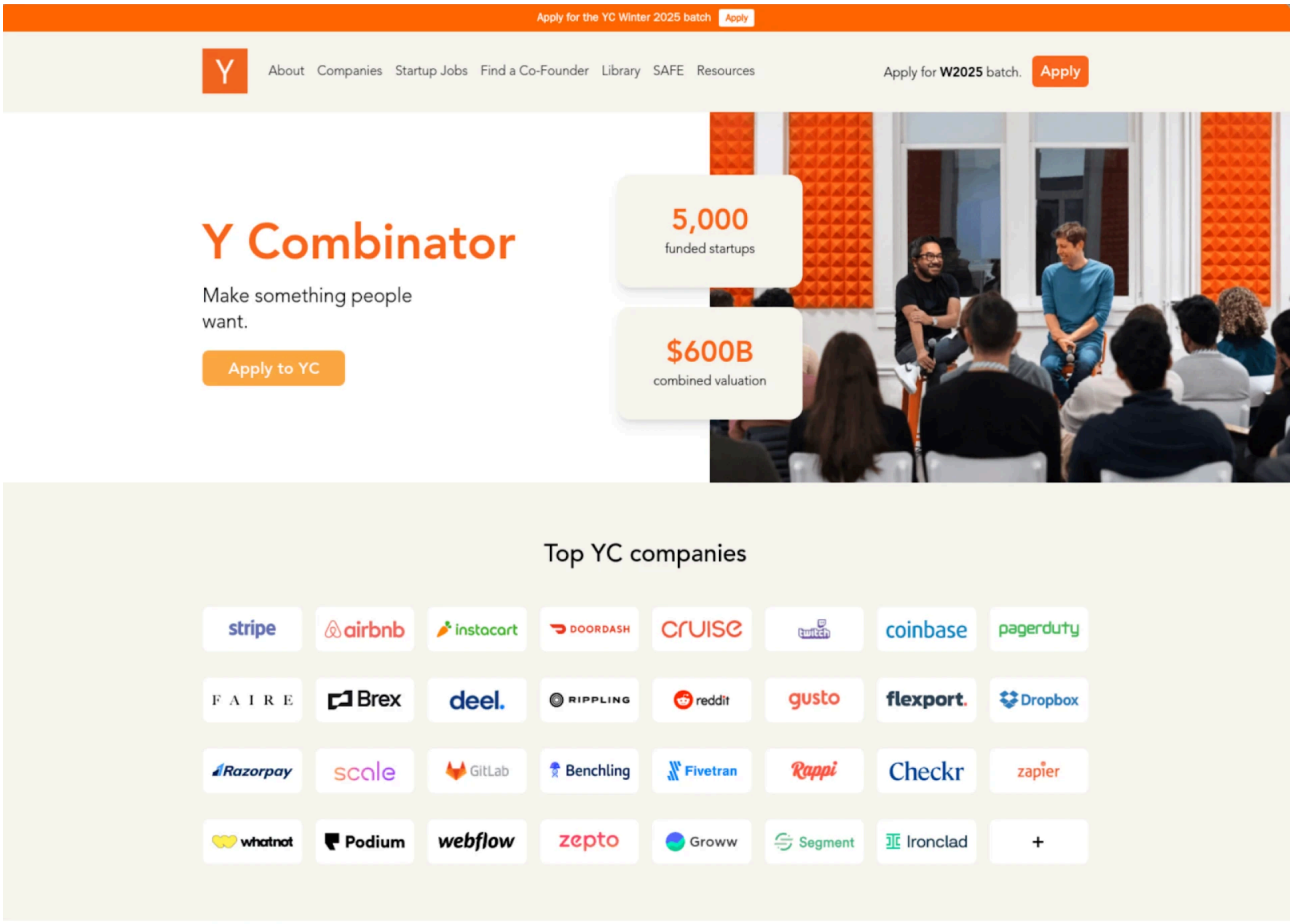


Figure 3: Screenshot of the legitimate Y Combinator website after navigating to ycombinator.serveblog[.]net (Source: URLScan).

We combed through multiple malware repositories and encountered a malicious ELF file communicating with the subject IP over port 443. Named " `cloud` " (SHA-256: **c8b524ca90adea19d920beb5cc6bd86dd03b23b0b2c61675cef9d6c0446aea84**), this file was flagged by 31 vendors on VirusTotal as a Sliver implant.

Although executing the file in a local sandbox environment did not yield active network communications, HTTP requests associated with this implant were visible on VirusTotal, revealing specific URL paths on the target server.

The most commonly accessed paths included:

- `/data/bundles`
- `/data/javascripts`
- `/data/authenticate`

Attempts to open these URLs in a browser resulted in 404 responses, indicating the paths are inactive or accessible only under certain conditions.

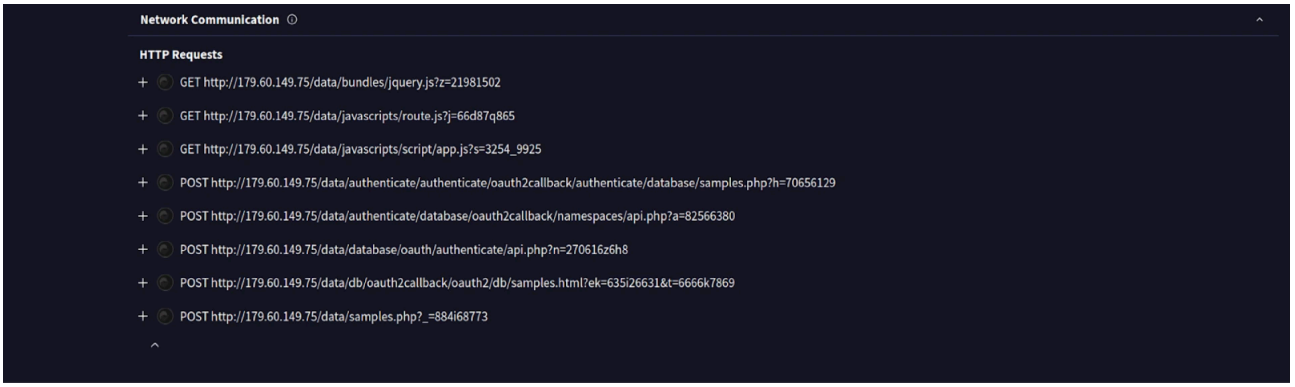


Figure 4: Screenshot of HTTP requests from the Sliver implant (Source: VirusTotal).

Infrastructure Expansion - Identifying Linked Server via Certificate Analysis

Over the past two weeks, `179.60.149[.]75` frequently cycled through TLS certificates, including those commonly associated with Sliver C2 infrastructure. Among these, one certificate issued by Let's Encrypt uses the previously identified spoofed domain, while others bear the "multiplayer" subject common name, the default certificate widely used to track framework infrastructure.

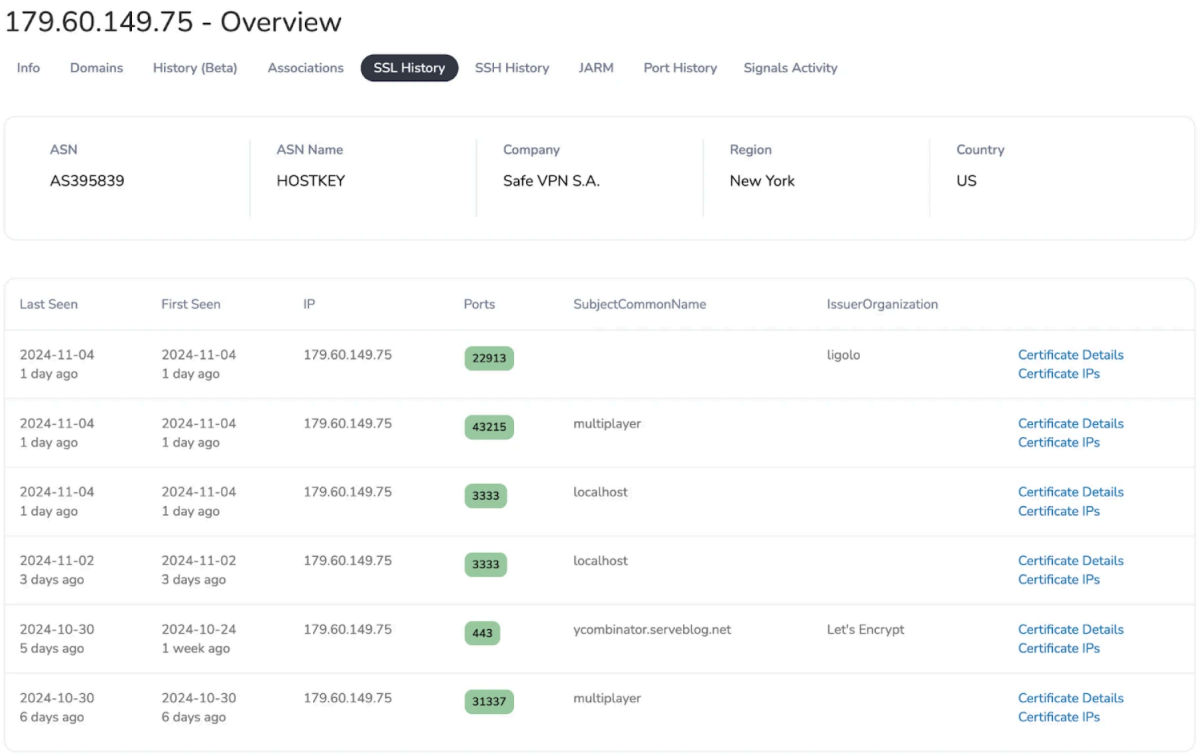
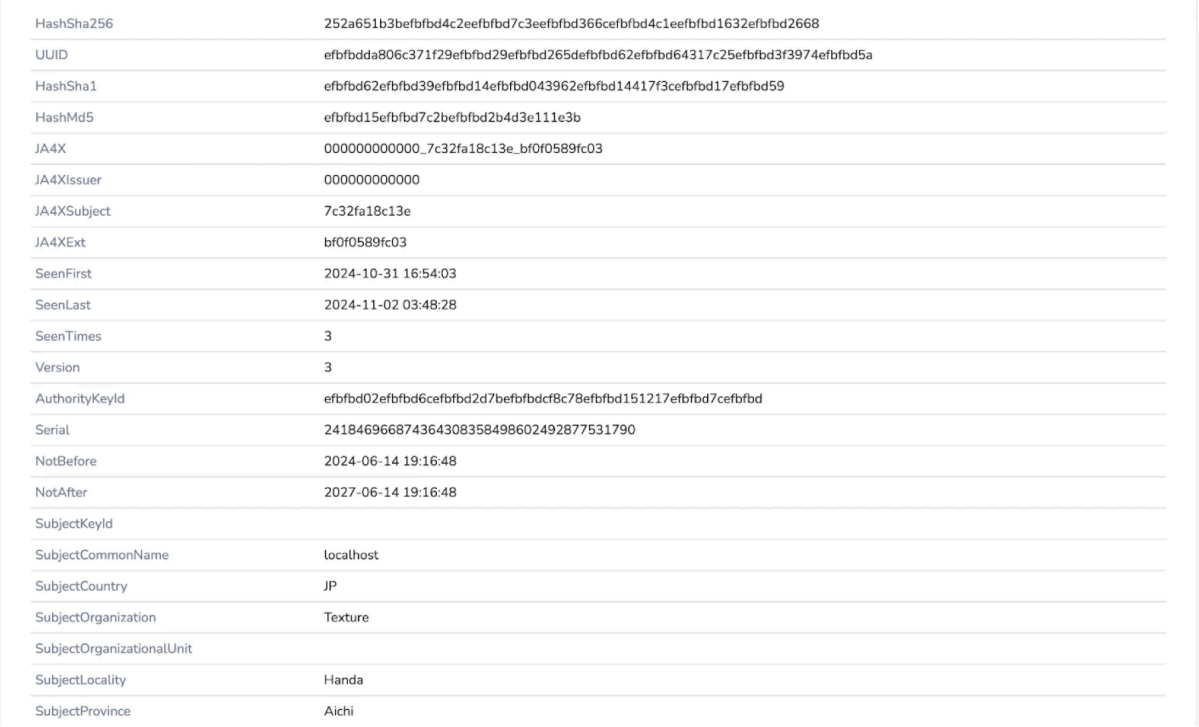


Figure 5: TLS Historical records for the first Sliver C2 in Hunt.

Several certificates use the generic common name "localhost." In our analysis of recent C2 deployments, this detail has emerged as a solid secondary indicator of command-and-control infrastructure linked to this framework. Using "localhost" likely reflects an attempt to mislead researchers by mimicking certificates typically used for testing.

In addition to the common name, many certificates include random words or fictitious company names in the organization field, often paired with geographic data, such as city names from Canada or Japan. This mix of natural and fake details adds obfuscation, complicating attribution. Despite these challenges, this pattern remains a consistent marker of the infrastructure associated with this framework.



HashSha256	252a651b3befbfbd4c2eefbfbd7c3eefbfbd366cefbfbd4c1eefbfbd1632efbfbd2668
UUID	efbfbdda806c371f29efbfbd29efbfbd265defbfbd62efbfbd64317c25efbfbd3f3974efbfbd5a
HashSha1	efbfbd62efbfbd39efbfbd14efbfbd043962efbfbd14417f3cefbfbd17efbfbd59
HashMd5	efbfbd15efbfbd7c2befbfbd2b4d3e111e3b
JA4X	000000000000_7c32fa18c13e_bf0f0589fc03
JA4XIssuer	000000000000
JA4XSubject	7c32fa18c13e
JA4XExt	bf0f0589fc03
SeenFirst	2024-10-31 16:54:03
SeenLast	2024-11-02 03:48:28
SeenTimes	3
Version	3
AuthorityKeyId	efbfbd02efbfbd6cefbfbd2d7befbfbdcf8c78efbfbd151217efbfbd7cefbfbd
Serial	241846966874364308358498602492877531790
NotBefore	2024-06-14 19:16:48
NotAfter	2027-06-14 19:16:48
SubjectKeyId	
SubjectCommonName	localhost
SubjectCountry	JP
SubjectOrganization	Texture
SubjectOrganizationalUnit	
SubjectLocality	Handa
SubjectProvince	Aichi

Figure 6: Screenshot of one of the localhost certificates showing the random organization name and location in Japan (Hunt).

Pivoting on one of the localhost certificates (SHA-256: **252A651B3BBAB4F3B84C2E8EE9A37C3E899094CFD7366C814C1EAE1632DA2668**) identified one additional IP, `179.60.149[.]4`, hosted on the same ASN and sharing this certificate.

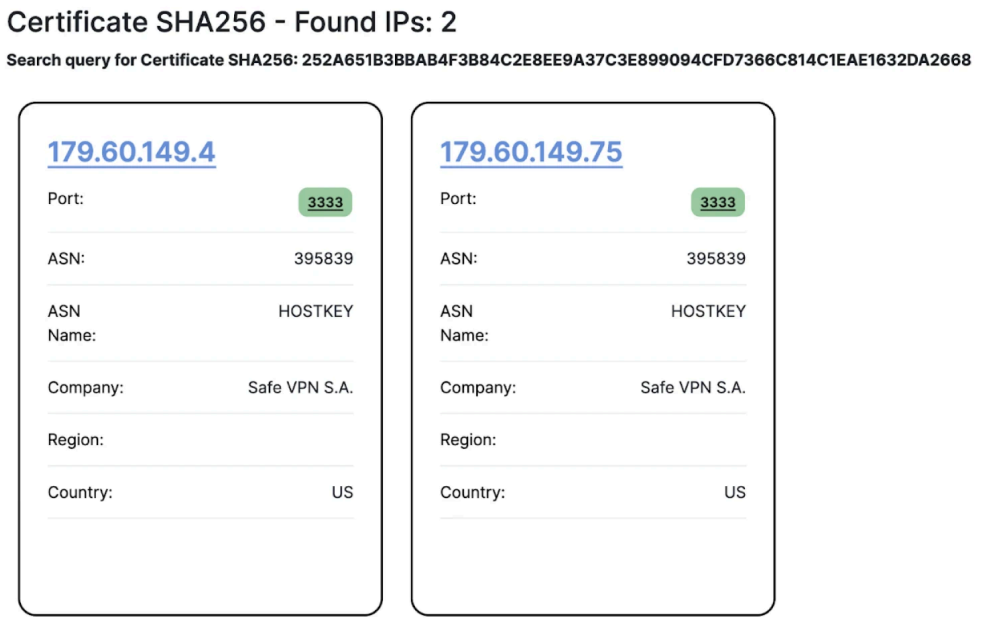


Figure 7: Shared TLS certificates between two Sliver C2s (Hunt).

This IP closely matches the original in port configuration, hosting active Sliver C2 ports alongside Ligolo-ng. Using similar tools and settings suggests the potential for additional infrastructure linked to this campaign.

At the time of writing, no domains were associated with 179.60.149[.]4.

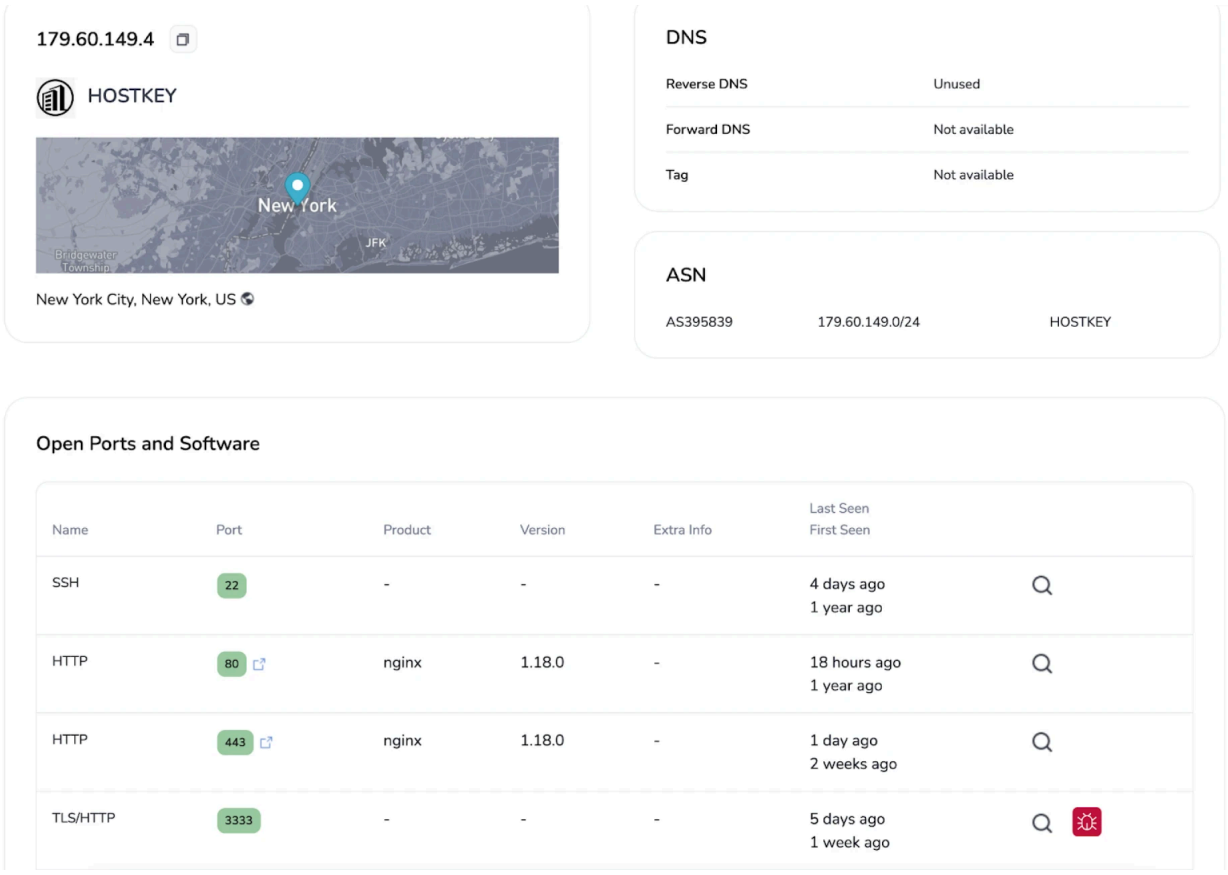


Figure 8: Snippet of IP overview in Hunt for the additional server acting as a Sliver C2 (Hunt).

The above highlights the operators' reliance on the Sliver framework and Ligolo-ng to achieve their objective, whatever that may be. With a clearer understanding of the tactics and tools involved, and no further leads, we can move to the conclusion.

Conclusion

Our research traced a small set of infrastructure leveraging the Sliver C2 framework and Ligolo-ng, connected through distinct indicators such as TLS certificates and port configurations. Alongside this IP, we identified an additional server.

We also observed a domain crafted to mimic a company known for supporting startups, likely aiming to establish credibility with potential targets.

These findings emphasize the importance of monitoring subtle changes in known malicious infrastructure indicators, which can reveal additional IPs that may otherwise go undetected. Proactive analysis remains essential in tracking and disrupting these similar campaigns.

Network Observables

IP Address	Hosting Country	ASN	Domain(s)	Notes
179.60.149[.]75	US	HOSTKEY	ycombinator.serveblog[.]net	Sliver C2 and Ligolo-ng used likely to target Y Combinator.
179.60.149[.]4	US	HOSTKEY	N/A	Sliver C2 & Ligolo-ng Server. *Shares TLS certificate w/ 179.60.149[.]75.

Sliver Implant

File Name	File Type	SHA-256
cloud	ELF 64-bit	c8b524ca90adea19d920beb5cc6bd86dd03b23b0b2c61675cef9d6c0446aea84

Source: https://hunt.io/blog/sliver-c2-ligolo-ng-targeting-yc