


Sliver Case Study: Assessing Common Offensive Security Tools

 team-cymru.com/post/sliver-case-study-assessing-common-offensive-security-tools

S2 Research Team

May 3, 2022



- [S2 Research Team](#)

-

-

- May 3

-

- 6 min read

The Use of the Sliver C2 Framework for Malicious Purposes

The proliferation of Cobalt Strike during the early 2020s has been undeniable, and its impact unquestionable. In response to this challenge, the detection strategies of defenders have steadily matured. Consequently, threat actor decision making with regards to tooling is likely evolving too. We therefore decided to identify and track Cobalt Strike “alternatives”, specifically *off-the-shelf* Offensive Security Tools (OST).

In this post we will discuss the Sliver C2 framework and its usage for potentially malicious purposes since the start of 2022.

Sliver is a Golang based implant and thus is compatible with the major operating systems. Our focus centered on the detection of new Sliver samples associated with Linux, MacOS, and Windows operating systems, and the extracted network infrastructure contained within those samples. To understand threat actor TTPs, we subsequently tracked network telemetry for the wider C2 infrastructure in cases where Sliver was deployed.

Key Findings

- Sliver utilized as a beachhead for the initial infection tool-chain
- Sliver utilized in the ransomware delivery framework for attacks observed in the wild
- Sliver deployed via active opportunistic scanning and possible exploitation of Log4j / VMware Horizon vulnerabilities
- Sliver utilized in the targeting of organizations within Government, Research, Telecom, and University sectors, in addition to sporadic victims of opportunity

Identification of Sliver Samples

Sliver’s current advantage lies in its obscurity alongside other less commonly utilized OSTs, with most organizations still focused on Cobalt Strike detection. This opens a possible gap in coverage – no one can be expected to detect all the things. This gap exposes organizations to the risk of these lesser known, yet still highly capable, OST C2 frameworks.

During Q1 of 2022, we observed 143 Sliver samples, detected with the potential for usage as a first stage tool in malicious activity. For comparison, 4,455 samples of Cobalt Strike were observed within the same time-period. Based on the continued prevalence of Cobalt Strike, organizations focusing on detection of that toolset are certainly justified. However, if organizations have the resources to do so, we strongly recommend some study of Sliver to identify possible detection opportunities.

This should be considered an anecdotal analysis of samples, as no detection rule is infallible, and no malware corpus complete. It is also not feasible to distinguish between legitimate versus malicious use for the totality of samples identified.

What follows is our analysis of two distinct malicious campaigns which leveraged Sliver for C2 purposes.

Sliver Campaign 1 – “Scan & Exploit”

193.27.228.127 (SELECTEL, RU)

C2 PORTS: 8888, 13338, 23338, 33338

Between 03 February – 04 March 2022 Sliver samples were discovered, utilizing Russian-hosted infrastructure, in the targeting of organizations in various sectors distributed globally. These samples and associated C2 IP (**193.27.228.127**) were deemed malicious, based on observations of **193.27.228.127** sweeping ranges in an indiscriminate manner, likely seeking exploitation opportunities.

Data from [GreyNoise](#) further highlighted the use of **193.27.228.127** for malicious purposes, targeting Log4j and Exchange (ProxyShell) vulnerabilities.

Based on the identification of Virlock samples (as discussed later in this blog) it is assessed that in some cases the actors sought to monetize the accesses they had gained.

In one instance, a victim was observed connecting to TCP/80 on **193.27.228.127**, potentially indicative of an exploitation of Log4j, with subsequent connections to **193.27.228.127:8888**. This victim was identified running VMware Horizon and was therefore likely vulnerable to [CVE-2021-44228](#) and [CVE-2021-45046](#).

The use of TCP/8888 aligns with several identified Sliver samples configured to communicate with **193.27.228.127**. After a period of approximately 14 days, we observed the C2 communications 'migrate' to TCP/13338, TCP/23338, and TCP/33338.

NOTE: TCP/8888 is associated with Sliver's default mTLS configuration, the use of the additional TCP ports ending in *3338 appeared more unique to this threat actor and were utilized in circumstances where victim communications persisted over extended time-periods.

The following samples (Table 1) were observed communicating with C2 IP **193.27.228.127**.

SHA-256 Hash	First Detected	Sample Name
1f95397c4634f3348f3001a02eab269148f4c08271c2e2461905a4359f7c4761	2022-02-04	ugly.exe
d8241e046cb9efcfa7ce733249d580eacff996d8669adbe71019eedafb696a55	2022-02-09	SENIOR_REALITY.exe
08137096b85a3a2611249bb57ba9ace4e8efc9ba28cfddd8557edc3e11e9690c	2022-02-13	PRIMARY_FLUTE.exe
2190a7d8d7eafd4af56b01d9a828ab2dc553a804ccda4c291dce51ce01da81f8	2022-02-16	install.exe

When generating payloads, the Sliver configurator outputs a binary based on a naming convention of RANDOMWORD1_RANDOMWORD2.exe by default.

In this case, Sliver was utilized for C2 communications in the first stage of the breach activity. A subsequent sample, identified as Atera Remote Management software, also communicated with **193.27.228.127**. This sample was first uploaded to VirusTotal on February 11, 2022. It appeared the actor used these two tools in concert, potentially switching to the use of Atera after initial compromise was achieved.

Atera Sample

SHA-256: 0ef7eebec233eb5e4156a8a4715c8d21d8930ea97c19780fc274a62260499412

176.113.115.107 (Red Bytes LLC, RU)

C2 PORTS: 8888, 13338, 23338, 33338

Approximately 30 days after first observing victim communications with **193.27.228.127**, the actor was observed switching victims to a new C2 IP (**176.113.115.107**), again assigned to a provider in Russia. As previously, victim communications continued over TCP/13338, TCP/23338, and TCP/33338.

'In-the-wild' file names for samples communicating with **176.113.115.107** continued to point towards exploitation of Log4j and VMware Horizon vulnerabilities (Table 2).

SHA-256 Hash	Name	Tool
fc2b02476805361fc5042adfb40b529431151a9c7da2b21fa3fa73e98fba9f64	vmware_kb.exe	Sliver
d2958f7b646c092fe645cbdc4c7805490ff9d134c12fa8d945132e71880dd6fd	vmware_kb.exe	Sliver
7f0deab21a3773295319e7a0afca1bea792943de0041e22523eb0d61a1c155e2	vmware_kb.exe	Sliver
c139a777b9b1bca0d7e43335d23c123171dbaceccf45a9eeaf359051e0d0be8e	N/A	PowerShell

In addition to the above referenced samples, a sample with possible Virlock ransomware capabilities was also observed communicating with **176.113.115.107**. This sample was first uploaded to VirusTotal on March 11, 2022. This finding is indicative of the actor attempting to monetize the access gained by deploying ransomware on a compromised host. It is unclear whether ransomware deployment was the intended final goal in every case.

Virlock Sample

SHA-256: 2d6785797cd3f2bfb377b985efe55db0220e12e3c7b1e12ee83888b61a5ad8da

45.9.148.243 (NICEIT, DM)

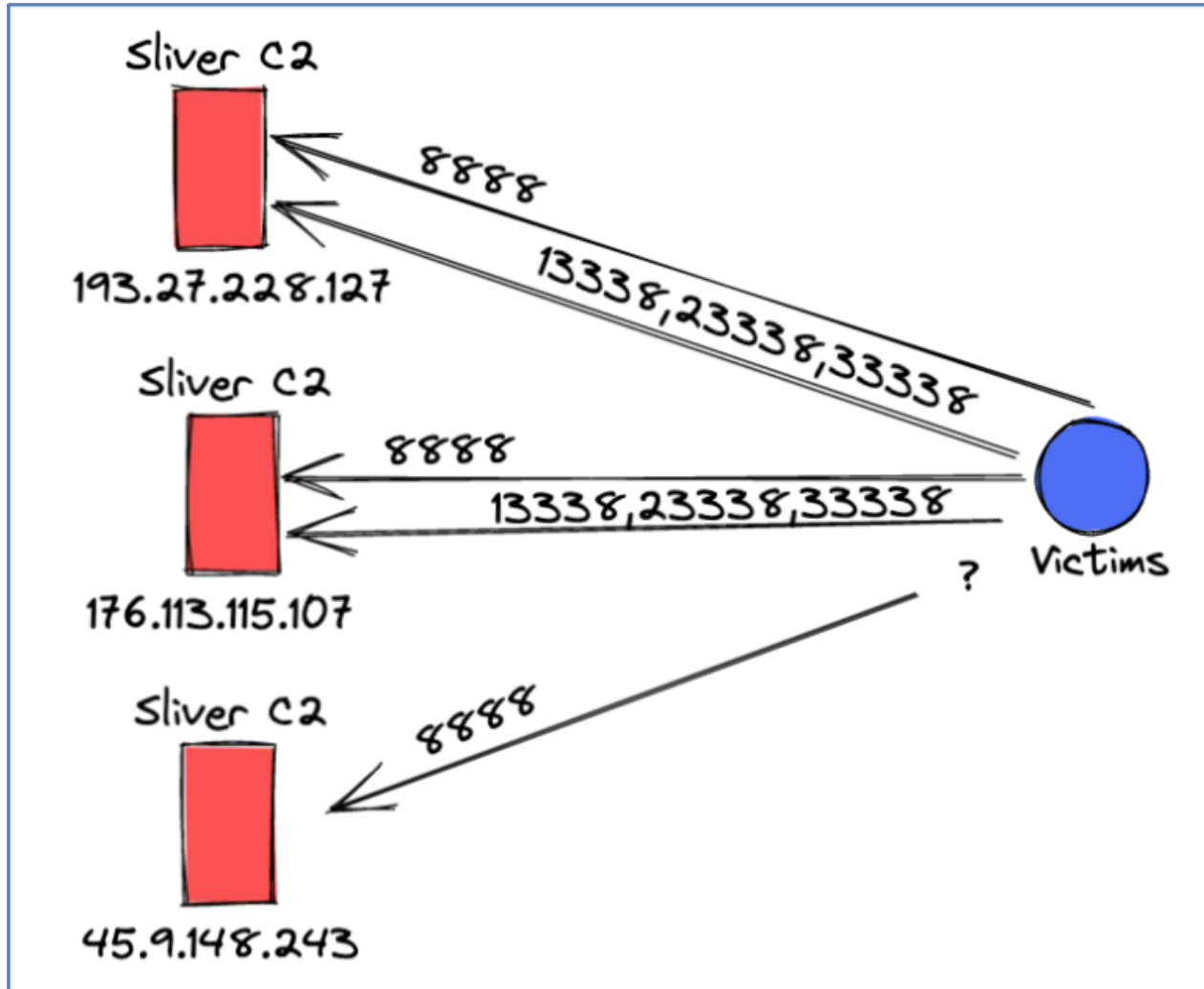
C2 PORT: 8888

Finally, in recent days an additional Sliver sample was detected, communicating with a 'new' C2 IP (**45.9.148.243**) assigned to a provider in Dominica. Network telemetry data does not indicate any current victim communications and it is unclear how this sample / C2 IP is connected to this activity. Updates on this activity will be posted on

Twitter via [@teamcymru_S2](#).

Sliver Sample

SHA-256: b9e95117e23e6a69e71441aef07f9683cf0682f34f8f84f876822d8143a05776



One of the challenges faced when tracking this activity was the volume of noise generated by the ongoing exploitation of hosts via vulnerabilities in utilities such as Log4j and Exchange. In several cases, we observed the same victim likely compromised by multiple threat actors. However, what can be concluded is the apparent utilization of Sliver in malicious activity, coupled with the continuous scanning, exploitation, and triage of victim infrastructure.

The activity associated with this cluster was previously commented on in other public reporting:

Sophos: [Horde of miner bots and backdoors leveraged Log4J to attack VMware Horizon servers](#)

Sliver Campaign #2 – Pakistan & Turkey

The second campaign identified leveraging Sliver was deemed malicious based on the domain name utilized by the actors, which appeared to target government entities in Pakistan and Turkey.

The detected Sliver samples communicated with **ping.turkey.g0v.cq.cn**, which resolved to IP **16.162.223.161** (AMAZON-02, US).

Sliver Samples

SHA-256: f301e581bb62b251abc7009a709fb163ceeb63de42625d6bfc2ac9a07d9d3adb

SHA-256: a862e2d3aa3a74e23665010ded23510210927d3c056d645f32479be0974e057a

Network telemetry data for **16.162.223.161** did not identify current victim communications, however this does not rule out ongoing or future malicious activity.

Passive DNS data for **16.162.223.161** identified three further domains resolving to this IP address:

- nationalhelpdesk.pk
- pkgov.org
- sngpl.org.pk

Given the similarity in the apparent spoofing of government entities, it was inferred that these domains related to the domain (**ping.turkey.g0v.cq.cn**) identified in the Sliver samples.

A further pivot on **pkgov.org** identified an email address (**abdulrehm8282@gmail.com**) used in the domain registration. This email address was used in the registration of two further domains, which resolved to IP **15.152.186.38** (AMAZON-02, US):

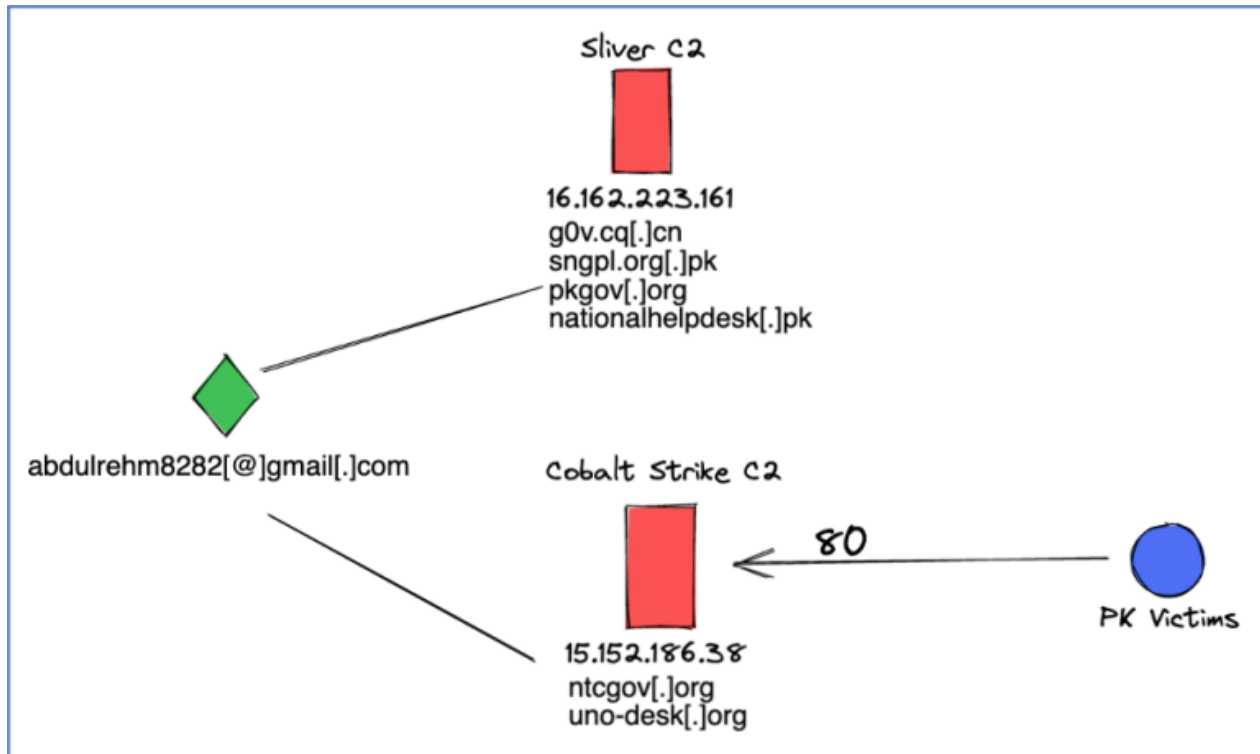
- ntcgov.org
- uno-desk.org

In this case, network telemetry for **15.152.186.38:80** provided evidence of inbound connections from potential victims located in Pakistan.

NTC is likely a reference to one of two Pakistani organizations; the National Telecom Corporation, or the National Technology Council.

Data from our Botnet Analysis and Reporting Service (BARS) indicated that a Cobalt Strike Beacon server was listening on TCP/80 of **15.152.186.38**, associated with the following shellcode sample:

SHA-256: bc94d6ed7abfea4239e941817cdad65a0a243e2e4a718ef401db4cbbef0bf478



Passive DNS data for **ntcgov.org** identified several subdomains, providing an insight into the intended targets of this campaign:

- dxb.ntcgov.org
- geo-raabta.ntcgov.org
- geo-tv.ntcgov.org

The string dxb possibly relates to DXB, the airport code for Dubai International, and the string raabta possibly relates to a project undertaken by the Centre for Pakistan and Gulf Studies.

It could be inferred that this campaign was undertaken to gain insight into collaborative projects conducted between Pakistan and the Gulf States (which includes Dubai, UAE).

CONCLUSION

We have observed a steady increase in detected Sliver samples over Q1 of 2022, providing insight into actor deployment methods and objectives. Of note we identified two separate campaigns which leveraged Sliver for likely malicious purposes. The latter campaign highlighted the potential use of both Sliver and Cobalt Strike in conjunction with each other. As previously stated, the threat posed by malicious utilization of Cobalt Strike has not diminished, however we would recommend that organizations also remain mindful of other OSTs, by applying resources to develop detection mechanisms for frameworks like Sliver.

RECOMMENDATIONS

Improve visibility

Consider an attack surface management solution to track remediation of vulnerable assets.

Be proactive

- Monitor (and hunt externally, beyond your network perimeter) for Sliver with community Snort / YARA rules, for example:

- UK NCSC ([link](#))
- Travis Green ([link](#))

Monitor and hunt internally within your infrastructures, look specifically for Sliver as an initial payload, or in concert with other OSTs (like Cobalt Strike).

Research

- Review threat actor TTPs where Sliver was leveraged in previous malicious campaigns, for example:
- SANS ([link](#))
- @pathtofile ([link](#))
- Alexis Rodriguez ([link](#))

FURTHER READING

If you are concerned about the risks and vulnerabilities of external assets, you can access our eBook on Attack Surface Management here: <https://team-cymru.com/ebook-the-future-of-attack-surface-management-brad-laporte/>

INDICATORS OF COMPROMISE

IP Addresses

193.27.228.127

176.113.115.107

45.9.148.243

16.162.223.161

15.152.186.38

Domains

ping.turkey.g0v.cq.cn

nationalhelpdesk.pk

pkgov.org

sngpl.org.pk

uno-desk.org

dxn.ntcgov.org

geo-raabta.ntcgov.org

geo-tv.ntcgov.org

SHA-256 Hashes

1f95397c4634f3348f3001a02eab269148f4c08271c2e2461905a4359f7c4761
d8241e046cb9efcfa7ce733249d580eacff996d8669adbe71019eedafb696a55
08137096b85a3a2611249bb57ba9ace4e8efc9ba28cfddd8557edc3e11e9690c
2190a7d8d7eafd4af56b01d9a828ab2dc553a804ccda4c291dce51ce01da81f8
0ef7eebec233eb5e4156a8a4715c8d21d8930ea97c19780fc274a62260499412
fc2b02476805361fc5042adfb40b529431151a9c7da2b21fa3fa73e98fba9f64
d2958f7b646c092fe645cbdc4c7805490ff9d134c12fa8d945132e71880dd6fd
7f0deab21a3773295319e7a0afca1bea792943de0041e22523eb0d61a1c155e2
c139a777b9b1bca0d7e43335d23c123171dbaceccf45a9eeaf359051e0d0be8e
2d6785797cd3f2bfb377b985efe55db0220e12e3c7b1e12ee83888b61a5ad8da
b9e95117e23e6a69e71441aef07f9683cf0682f34f8f84f876822d8143a05776
f301e581bb62b251abc7009a709fb163ceeb63de42625d6bfc2ac9a07d9d3adb
a862e2d3aa3a74e23665010ded23510210927d3c056d645f32479be0974e057a
bc94d6ed7abfea4239e941817cdad65a0a243e2e4a718ef401db4cbbef0bf478