Christmas in July: A Finely Wrapped Malware Proxy Service

spur.us/2023/07/christmas-in-july-a-finely-wrapped-proxy-service/

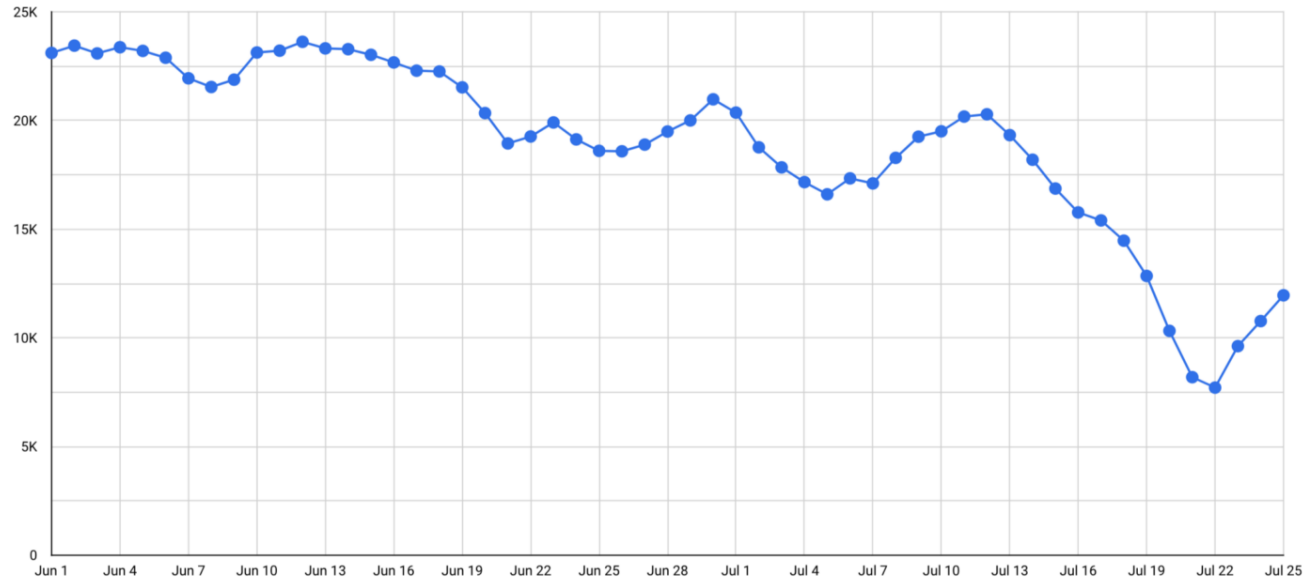
July 26, 2023

It is not often that Spur has the opportunity to glean full insight into a malware proxy service. Because we track hundreds of proxy and VPN services, our focus is generally on the proxies from a network standpoint rather than any related malware or its provenance. Even rarer do we get awareness into the actor(s) operating a malware network facilitating the proxy service.

But thanks to a recent article from Black Lotus Labs, and with the help of Brian Krebs's investigative reporting, Christmas has come early this year at Spur.

The Disappearance

A few weeks ago, we noticed a few key metrics and details associated with SocksEscort — one of the oldest malware proxy services we track — suddenly change. The amount of proxies we had insight into plummeted, and the communicating infrastructure seemingly moved.



Around July 11, we started noticing a significant downward trend in the number of available endpoints. The count of available endpoints for a given service tends to ebb and flow but this halving of the online proxy count merited a closer look.

The proxy control servers appeared to still be online based on the indicators we use to track them. The below is a screenshot from driftnet.io, an excellent infrastructure profiling service showing a seemingly still-active SocksEscort control server after the decrease in proxy

counts.

	Date (UTC)	IP	Port	Hosting Entity
⌄	2023-07-18	155.254.23.254	tcp/3322	H4Y-TECHNOLOGIES
⌄	2023-07-16	155.254.23.254	tcp/3322	H4Y-TECHNOLOGIES
⌄	2023-07-12	155.254.23.254	tcp/3322	H4Y-TECHNOLOGIES
⌄	2023-07-12	155.254.23.254	tcp/9001	H4Y-TECHNOLOGIES
⌄	2023-07-10	155.254.23.254	tcp/8080	H4Y-TECHNOLOGIES
⌄	2023-07-10	155.254.23.254	tcp/3322	H4Y-TECHNOLOGIES

However, around the same time, we also saw the count of victims per server (as shown for June in the figure below) drop to 0.

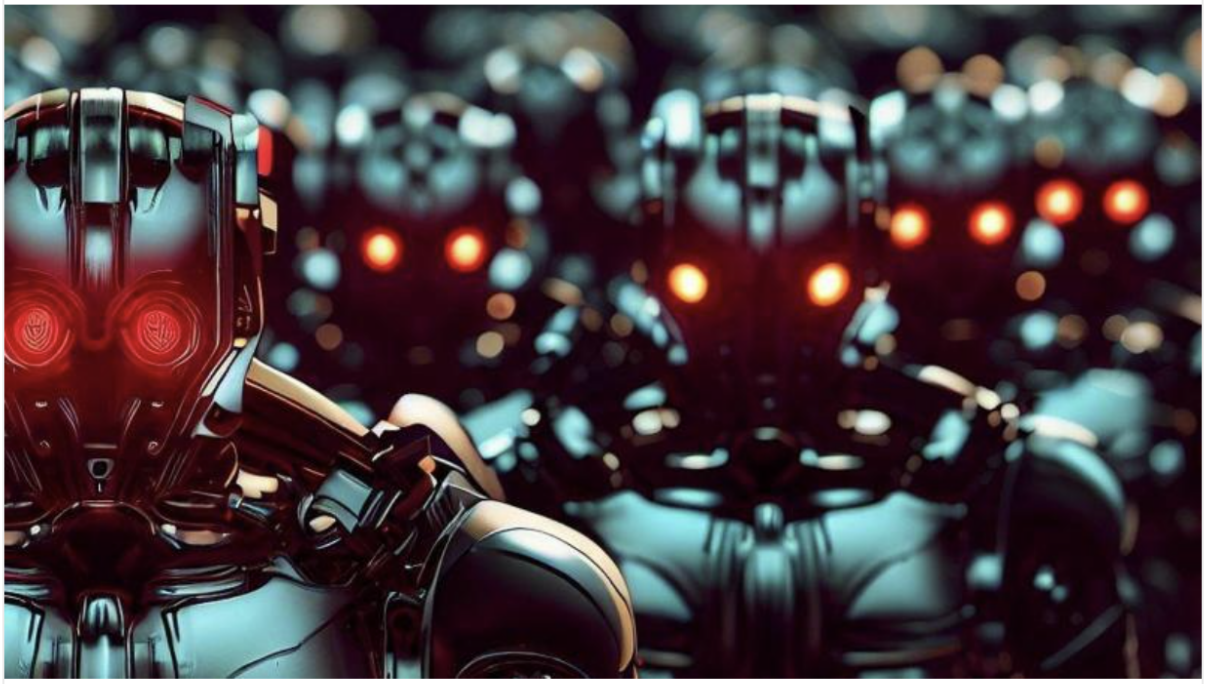
```
Server          Victim Count
155.254.23.254  7506
139.59.231.113  6792
188.138.41.157  167
85.25.214.74    129
85.25.217.95    129
148.72.155.187  107
148.72.155.189  107
148.72.155.112  96
50.30.36.132    96
148.72.155.174  95
50.30.36.27     93
69.64.55.106    69
```

It is not uncommon for the actors operating a malware proxy service to push a code update or rotate their infrastructure, but up until this point, SocksEscort had always been stable. We were mostly blind; nothing about the service itself appeared to have changed. A frustrating result of focusing our efforts on tracking the *proxy service* at the network level rather than the *malware itself* at a broader threat intelligence level is that we're frequently left to only guess at the explanations for these kinds of events.

The Takedown

Purely coincidentally while perusing LinkedIn, I came across interesting research done by Danny Adamitis and Steve Rudd of **Black Lotus Labs**, the threat intelligence arm of Lumen (formerly known as CenturyLink). The specific article, posted just a few weeks ago on July 12, dives deep into a piece of SOHO-based malware they are calling AVrecon. Instead of rehashing the article, I highly recommend reading it. It would do it an injustice to try to summarize it.

> Since at least May 2021, stealthy Linux malware called AVrecon was used to infect over 70,000 Linux-based small office/home office (SOHO) routers to a botnet designed to steal bandwidth and provide a hidden residential proxy service.
> This allows its operators to hide a wide spectrum of malicious activities, from digital advertising fraud to password spraying.
>
> According to Lumen's Black Lotus Labs threat research team, while the AVrecon remote access trojan (RAT) compromised over 70,000 devices, only 40,000 were added to the botnet after gaining persistence.



> **AVrecon malware infects 70,000 Linux routers to build botnet**
> bleepingcomputer.com

Whenever I read similar research posts by other organizations, I'm curious to figure out what (if any) call-back proxy service is tied to the malware as residential proxies tend to be a popular monetization vector for malware operators. It only took a brief overview of the full IoCs published by Black Lotus Labs to identify SocksEscort as the malware proxy service tied to this particular botnet based on the C2 infrastructure.

The smoking gun was in Lumen's remediation as mentioned in the conclusion of the above article: black hole-ing the IP addresses belonging to the stage 2 C2 infrastructure for AVrecon. Assuming Lumen null-routed the control servers sometime shortly before their research team published their article on July 12, we finally had a clear picture as to the reason behind the plummeting proxy numbers for SocksEscort.

The Other Side

As previously mentioned, Spur focuses on tracking a massive breadth of proxies and tunnel services at a network level. We tend to stop short of identifying any potential related malware and its particularities, as it falls outside our bailiwick. Likewise, we also tend not to track the actors operating these botnets and associated services, deferring this tall order to the likes of Brian Krebs and other investigative journalists and threat intelligence specialists in the security space.

Indeed, Krebs wrote about SocksEscort shortly after the 911.re takedown took place (SocksEscort was a front-runner for a 911 replacement). He's recently published another article examining the potential actors ultimately behind the malware proxy service, linking it to an individual as well as a commercial VPN service. Again, instead of attempting to summarize the findings, the article merits its own read.

The Village

Black Lotus Labs and Krebs have been simultaneously investigating the same malware, just from different angles. Our unique insight into malware proxy networks was the missing link connecting their separate research.

And so now a full picture is painted of SocksEscort, tying together the malware itself, with the service profiting from the infections (perhaps one of many), to the proxy operators.

The security community is filled with experts like Krebs and the smart people at Lumen's research wing. Sometimes it takes a few organizations to piece together the puzzle. Spur greatly appreciates the work done by groups like Black Lotus Labs that can better identify and track the malware associated with these services. Additionally, their remediation efforts have put a serious strain on SocksEscort and vastly dropped their available proxy inventory.

If you or your organization have interesting research to share that may concern malware proxies, we'd love to hear from you!