Desde Chile con Malware (From Chile with Malware)

team-cymru.com/post/from-chile-with-malware

S2 Research Team February 24, 2023

- S2 Research Team
-
-
    - 5 days ago
    -
    - 5 min read

Spoiler Alert: They weren't actually from Chile.

Introduction

This blog post provides a short update on our ongoing tracking of infrastructure associated with IcedID. We have posted publicly on IcedID on several occasions over the past year, and as far back as May 2021; they remain a persistent threat.

To recap...

IcedID (also known as BokBot) started life in early 2017 as a banking trojan that later evolved to include dropper malware capabilities. These capabilities enable IcedID to download and deploy additional malware such as Cobalt Strike, with infections sometimes leading to ransomware.

Late last week we identified a 'new' IP address connecting to **5.196.196.252**; one of the currently active IcedID BackConnect C2 servers. These connections were made to the same remote port, associated with the SOCKS proxy module, which we wrote about in December 2022.

Key Findings

- Identification of an IP address geolocated to Chile, used to access various elements of the IcedID infrastructure.
- The Chilean IP resides in a /24 netblock which is also utilized for hosting IcedID Bot C2 infrastructure (on separate IPs).
- Threat telemetry data shows consistent connections sourced from the Chilean IP, to an IP geolocated to the Netherlands which is used to host two IcedID-connected domains.
- Web browsing activity originating from the Chilean IP provides a snapshot into suspected threat actor TTPs. With an apparent interest in DNS and visits to services noted for association with Conti and LockBit ransomware.

From Chile... Kind Of

The ‘new’ IP address is assigned to Zappie Host, a New Zealand-based VPS provider, although geolocation data places it in Chile. Zappie Host, and the specific /24 netblock in which this IP resides (**216.73.159.0/24**), is regularly used to host IcedID Bot C2 infrastructure.

In our initial assessment of this ‘Chilean’ IP, we noted a gap in activity between 12 December 2022 and 26 January 2023; interestingly, this matched timelines we had observed in the case of IcedID Bot, Loader, and BackConnect infrastructure.

We have generally attributed these drops in activity to the festive and new year celebration period, infrastructure updates, and on occasion an indication of internal issues impacting the threat operators.

Further, we noted the use of WireGuard VPN to access the Chilean IP; up to 12 December 2022. When activity returned in January 2023 this changed to OpenVPN. Both WireGuard VPN and OpenVPN were noted in our aforementioned investigation into BackConnect, hinting at the potential of a common playbook being used across various elements of infrastructure management associated with IcedID.

Further Ties to IcedID

Examining threat telemetry data for the Chilean IP, we observed connections to the panel port of the IcedID Loader Tier 2 server. This server is used to manage the Tier 1 Loader C2s, which serve the purpose of receiving initial victim communications and delivering the IcedID DLL. We have previously blogged about these first stage Loader C2s.

Further connections were also observed to **168.100.8.93**:443 (assigned to BLNWX - BitLaunch), commencing 27 January 2023 and continuing daily until the time of writing. During this period of activity, we identified two domains resolving to **168.100.8.93**, based on pDNS and certificate data:

- **neonmilkustaers[.]com** - registered 9 November 2022
- **svoykbragudern[.]com** - registered 18 November 2022

Both domains are typical of current IcedID domain nomenclature. Looking at domain registration data for the above dates, filtered by registrant organization (Tucows) and name server usage (Njalla), we found other domains registered within close temporal proximity:

- **trbiriumpa[.]com** - registered 9 November 2022
- **whothitheka[.]com** - registered 9 November 2022
- **ebothlips[.]com** - registered 9 November 2022
- **olifamagaznov[.]com** - registered 18 November 2022

If these domains look familiar, that's because they are - and we applaud your attention to detail. All four domains have been utilized for IcedID Loader C2 infrastructure over the past three months, and as recently as last week.

However, the standout observation for **168.100.8.93** and therefore the domains hosted on it, are the differences in behavior when compared to other IcedID C2 infrastructure. According to our threat telemetry data, we do not see the expected victim communications we would usually expect for C2 infrastructure, which therefore makes us question the purpose of these domains.

Victim communications with the Loader C2s tend to occur over TCP/80, so the connections from the Chilean IP appear to be related to another service. One hypothesis we have is that the Chilean IP and by extension **168.100.8.93** may be used for some form of development or testing purpose.

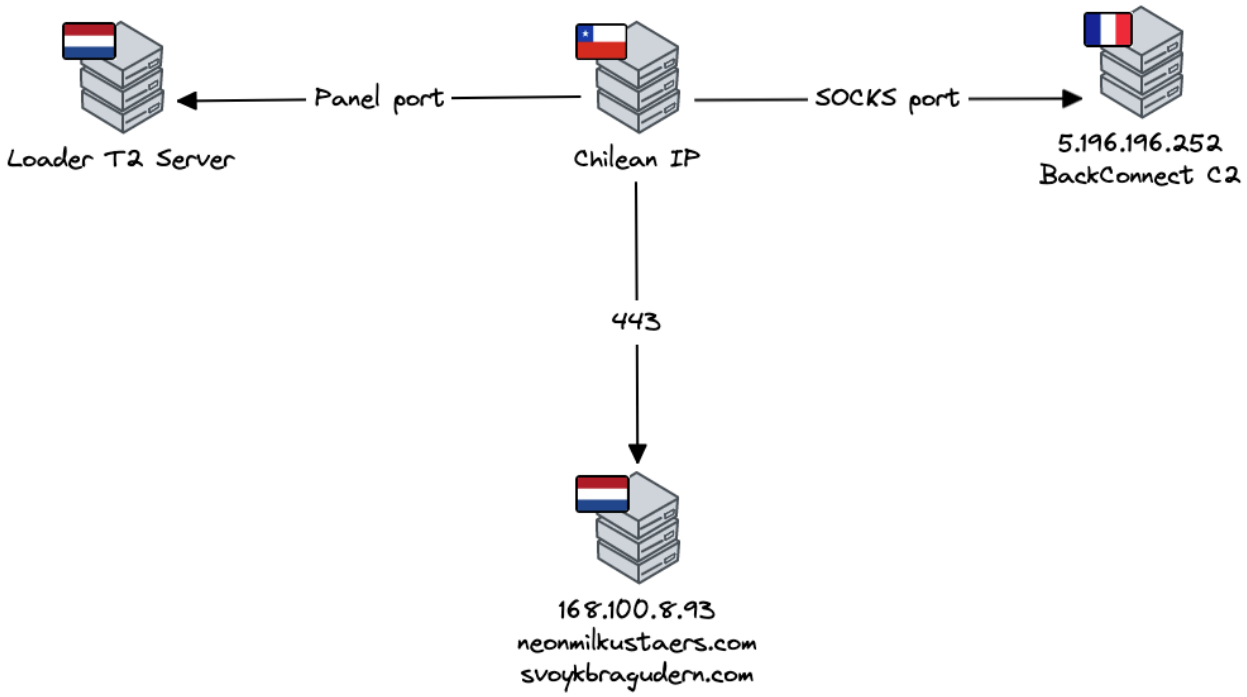

Figure 1: Summary of Chilean IP Threat Telemetry

Threat Operator TTPs

In addition to the connections to IcedID-linked infrastructure, since 26 January 2023 the Chilean IP has communicated with dozens of other IP addresses over TCP/443 (HTTPS).

Based on our internal pDNS data, combined with OSINT investigations, we were able to identify domains (or define the general purpose) associated with the majority of these destination IP addresses - i.e., the targets of the connections.

Most consisted of websites related to DNS, privacy, and expected threat actor activity such as Tox and Tor usage. There were also visits to Yandex IP space, the Russian search engine popular in CIS countries.

Below we have listed some of the sites visited, which by extension provides an insight into the services and tools the suspected threat actor behind the Chilean IP is interested in:

Sape Russian-language SEO service	**Qaz[.]im** Disposable email / file sharing service
MegaNerd encrypted DNS Encrypted DNS server and anonymized DNS relay	**Libsodium** Library for encryption/decryption, signatures, password hashing
Njalla Anonymous domain name registrar, hosting and VPN provider	**NextDNS** DNS resolution service with a core focus on encryption and privacy
Ibksturm Open-source DNS and Tor relay operators	**Digitalsize** Public, non-tracking, non-filtering DNS resolver
Libredns[.]gr Public encrypted DNS for maintaining secrecy of DNS traffic	**DoH & DNSCrypt Server by alekberg** Open-source encrypted DNS
Drink Open-source dynamic authoritative DNS server	**Send.vis[.]ee** Securely share files via command line
WalletConnect Open-source protocol for connecting decentralized applications to mobile wallets with QR code scanning or deep linking	**Control D** Customizable DNS service that can redirect traffic through a series of transparent proxies

A few of these sites are particularly pertinent:

- **Libsodium**, the library which includes features such as encryption, password hashing, etc., is also utilized in the LockBit ransomware.
- **Njalla** is currently IcedID's domain registrar of choice, so it is somewhat unsurprising that it appears here.

- **Qaz.im** appears in the Conti Leaks, and Conti ransomware was often dropped by IcedID. Based on our observations, it appears this service continues to be used; likely a result of it being hosted in Russian IP space and therefore deemed (rightly or wrongly) to be outside the reach of LEA action.
- **Sape**, the SEO service, is notable given the recent use of malvertising campaigns as an initial delivery mechanism for IcedID.

Conclusion

Tracking the background infrastructure associated with the day-to-day operation of threats like IcedID allows us to not only identify new victim-facing C2 infrastructure, but also to illuminate other elements of interest.

In this blog we identify a Chilean IP, which based on its activities is likely not operated by a Chilean actor, utilized for the purposes of access / management of IcedID-linked infrastructure. The surrounding activities provide us with an insight into the motivations of this actor and highlight some of the services and tools they may be using or investigating.

We also allude to some techniques which can be used to identify or confirm IcedID domains, a topic which we are planning further expansion on in the future.

In the case of IcedID, whilst we find that the operators can change their spots (making all leopards jealous), this is often a gradual process which provides us with opportunities for pattern-of-life, and as a result infrastructure, identification.

Recommendations

- Although not used exclusively by IcedID operators to host their C2 infrastructure, we would recommend that defenders take interest in any activity within their networks inbound to / outbound from **216.73.159.0/24**.

- BackConnect C2 infrastructure is fairly static, with a life-cycle of approximately 30 days, it is therefore viable to block connections to current C2s. We will continue to post updates to this infrastructure on our Twitter feed - @teamcymru_S2.
- Users of Pure Signal Recon will be able to track this activity by querying for inbound connections to **168.100.8.93**:443 and pivoting from there.

IOCs

IcedID Bot C2s from 216.73.159.0/24 (Nov 2022 - Feb 2023):

216.73.159.132

216.73.159.134

216.73.159.29

216.73.159.44

216.73.159.60

216.73.159.80

Recently active BackConnect C2s:

135.148.217.85

5.196.196.252

80.66.88.71

IcedID domains (mentioned):

neonmilkustaers[.]com

svoykbragudern[.]com

olifamagaznov[.]com

trbiriumpa[.]com

whothitheka[.]com

ebothlips[.]com