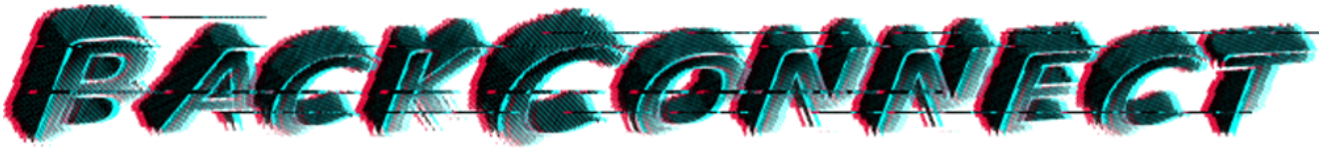
Inside the IcedID BackConnect Protocol

team-cymru.com/post/inside-the-icedid-backconnect-protocol

S2 Research Team December 21, 2022



Deriving Threat Actor TTPs from Management Infrastructure Tracking

You can find our previous work on Stage 1 and Stage 2 of IcedID's initial infection chain in our Dragons News Blog. Data on Stage 1 C2 infrastructure is now also shared as part of our Botnet Analysis and Reporting Service (BARS).

As part of our ongoing tracking of IcedID / BokBot, we wanted to share some insights derived from infrastructure associated with IcedID's BackConnect (BC) protocol. When deployed post "initial" compromise, the BC protocol allows the threat actor(s) additional functionality, using the infected host as a proxy.

Amongst other things, the BC protocol contains a VNC module, providing the malware operator(s) with a remote-access channel which can be brokered for profit.

For a comprehensive description of the BC protocol, we recommend this blog by Netresec. Furthermore, we must credit @malware_traffic having drawn upon his collection of threat actor telemetry data to confirm some of the observations shared in this post.

Key Findings

- Eleven BC C2s identified since 01 July 2022, managed via two VPN nodes.
- Operators likely located in Moldova and Ukraine managing distinct elements of the BC protocol.
- Evidence of malicious use of the SpaceX Starlink network identified.
- Exposure of several tools and processes utilized by the operators, including temporary SMS messaging, file sharing, cryptocurrency wallets, and a favorite local radio station.

Starting Point - 51.89.201.236

The starting point for our analysis is derived from the two sources mentioned above; although not a new phenomenon, reporting on the BC protocol is fairly scarce, with the last major point of reference, prior to the most recent coverage, being made in May 2020.

In early October 2022, an IOC (**51.89.201.236**:8080) derived from an IcedID infection was identified by @malware_traffic. The IOC was later attributed as a C2 server for the BC protocol by Netresec, noting a change in the *auth value* (0x08088b1f) used by the bot and C2 server for verification purposes.

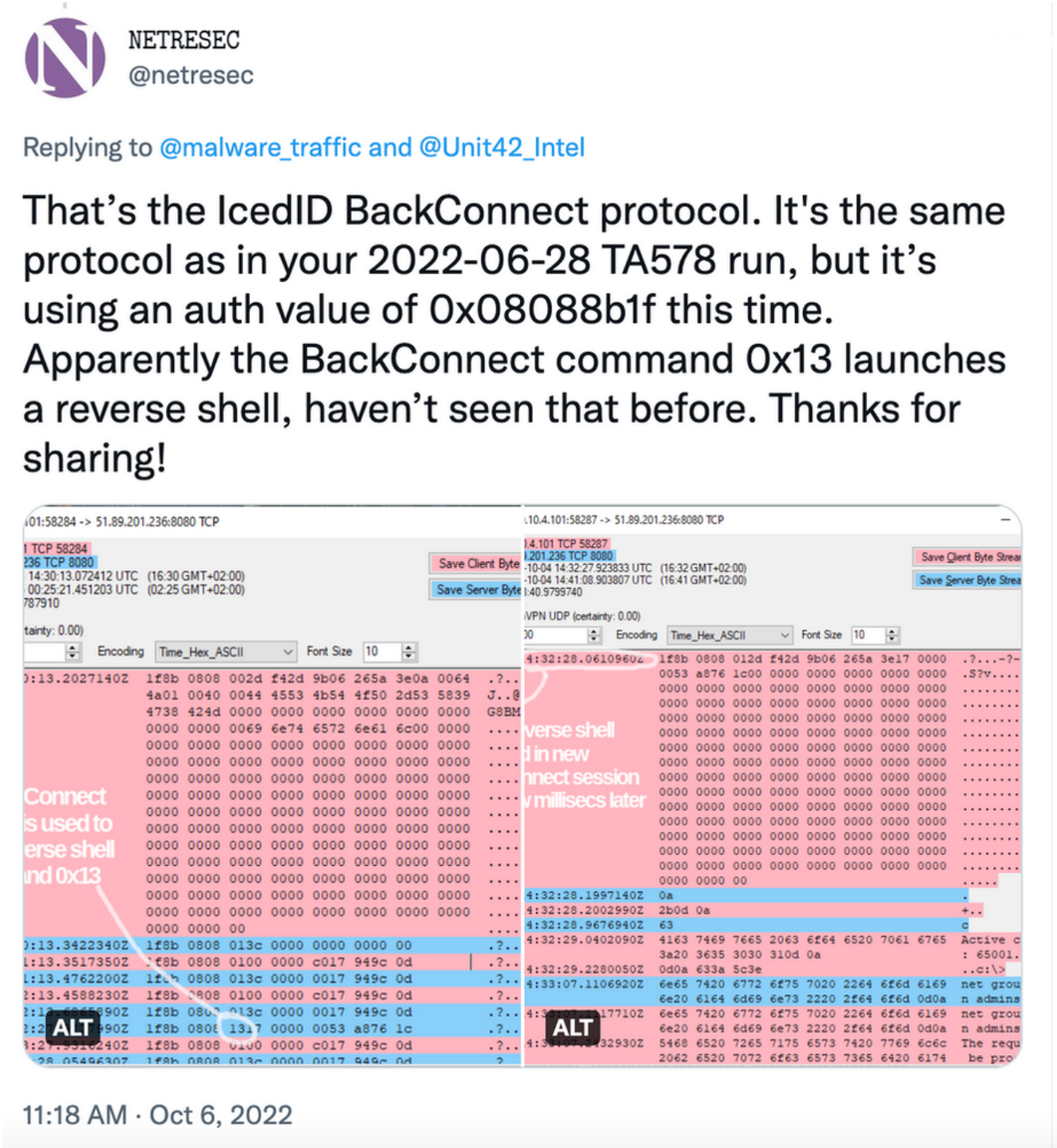


Figure 1: https://twitter.com/netresec/status/1577966512459087874

With an active C2 server for the BC protocol identified, our first step was to examine our network telemetry data surrounding this IP address, looking for indications of management access, common peers, and subsequent similar patterns of activity, e.g., evidence of victim communications over TCP/8080.

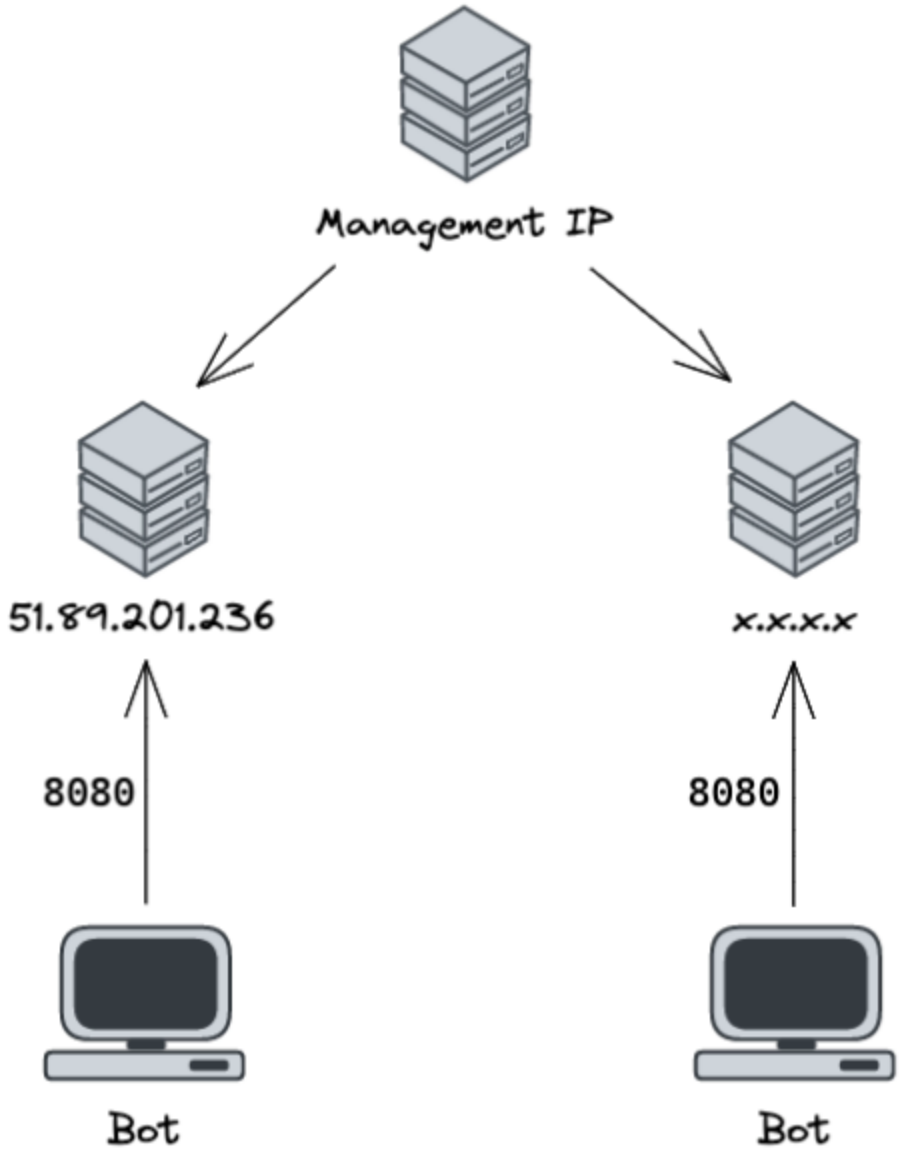


Figure 2: Initial Data Pivots

Over time, by repeating this process it was possible to identify two long standing management IP addresses, which were observed in communication with **11** distinct BC C2 servers (including **51.89.201.236**) since 01 July 2022.

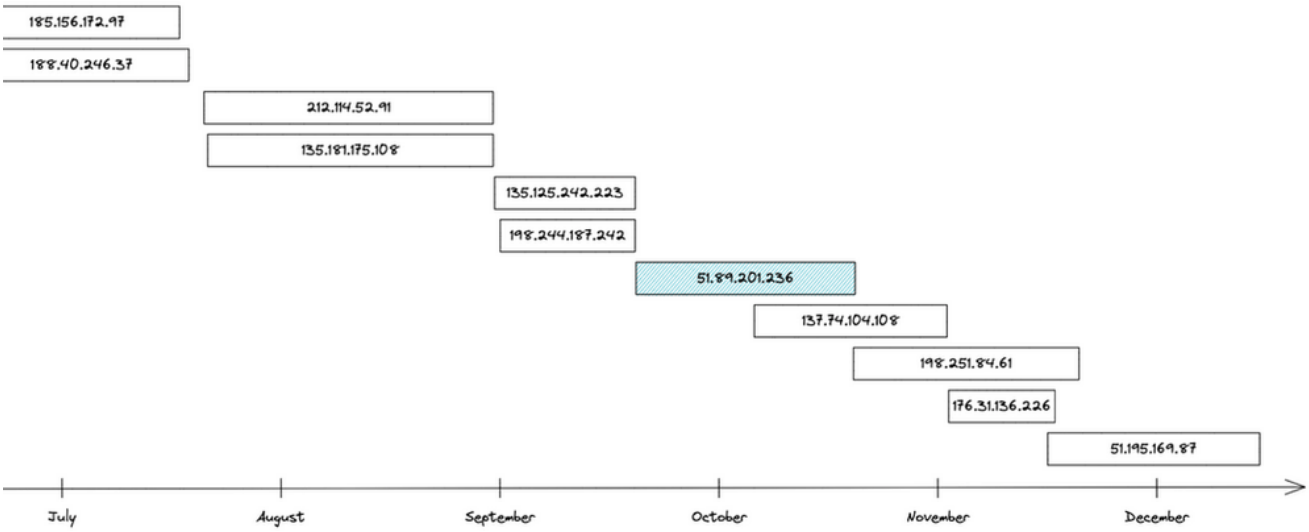


Figure 3: C2 Server Timeline (Based on Management Traffic)

Based on the data behind Figure 3, we can state that the average life cycle for a BC C2 server, based on first and last observations of management traffic, is approximately four weeks and that there are generally one or two servers active at any given time.

Additionally, in all cases communications between the C2 and management servers commenced and ceased on a Monday to Friday schedule - indicating a degree of “professionalism” to the operation and a point which became a trend during this analysis.

Auth Value Changes

Returning to the aforementioned *auth value* (0x08088b1f), based on our investigations, the campaigns involving **51.89.201.236** are the first time the “new” auth value was observed. However, this finding is caveated with the fact that relevant PCAP data was not available for the two preceding C2 IPs - **135.125.242.223** and **198.244.187.242**.

All prior C2s used the “previous” *auth value* (0x974f014a), which was associated with IcedID dating back a number of years. The change in *auth value* therefore likely happened at some point between 30 August and 22 September 2022.

```
Internet Protocol Version 4, Src: 135.181.175.108, Dst
Transmission Control Protocol, Src Port: 8080, Dst Por
```

```
000  00 08 02 1c 47 ae 20 e5  2a b6 93 f1 08 00 45 00
010  00 35 ef f2 40 00 31 06  fe 42 87 b5 af 6c 0a 07
020  1a 65 1f 90 eb 9a 00 f7  0d 2f bf 8b 1d 77 50 18
030  00 e5 36 ea 00 00 4a 01  4f 97 01 3c 00 00 00 74
040  2d c6 5d
```

Figure 4: Auth Value for **135.181.175.108** (Last Active 30 August 2022)

Management Insights

The remainder of this blog will focus on the two management IP addresses which have been associated with the operation of the BC protocol for at least half a year.

These IPs consistently connect to the BC C2 servers on the same two (separate) static ports, one which hosts a VNC service and the second which we hypothesize is associated with the SOCKS proxy module.

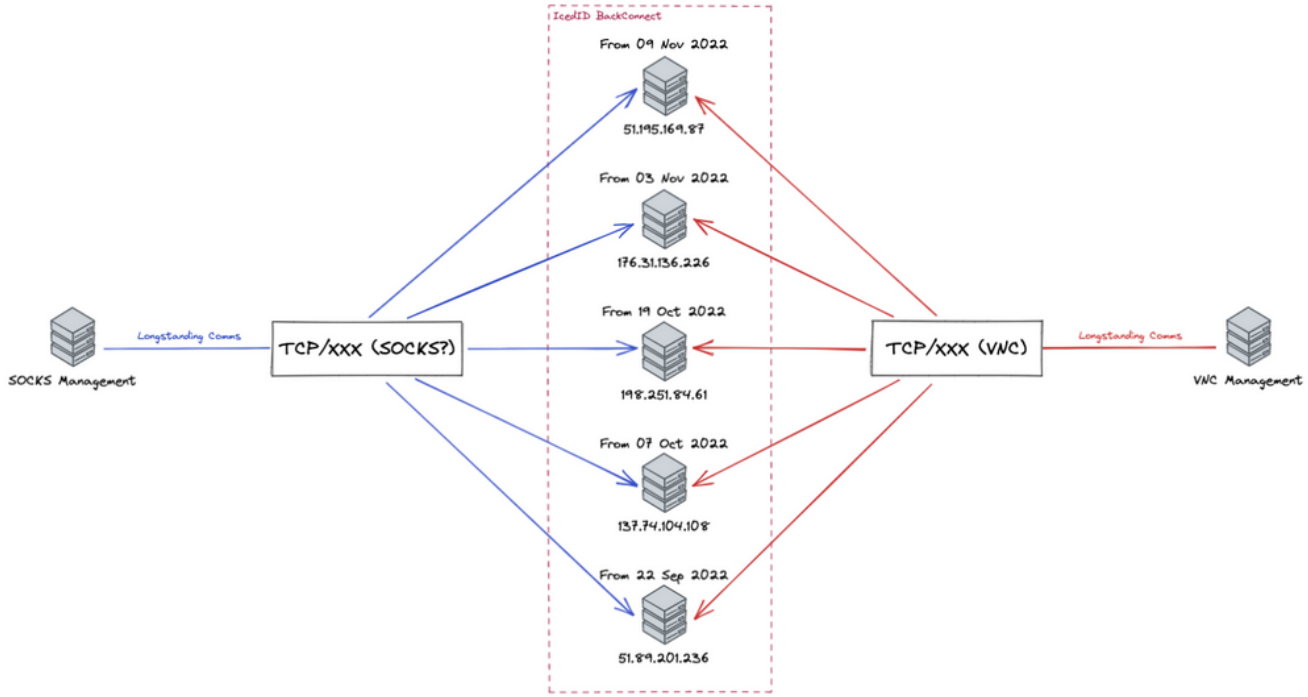


Figure 5: BackConnect Management

Setting the BC protocol management communications to one side, examining the rest of the data available for these two IP addresses provides an insight into the threat actor(s) operation, with some hints at attribution.

VNC Management

The first observation with the VNC Management is that it appears to be a VPN node. When examining inbound connections, a large proportion take place on UDP/1194, a port commonly associated with OpenVPN as the service's default port.

The VNC Management IP is therefore most likely used for routing traffic / providing anonymisation to the operator(s) and may not host any digital artifacts.

On the other side of the OpenVPN connections are numerous Moldovan IPs, the vast majority of which are assigned to a large residential broadband provider. In the 30-day period prior to the time of writing this report, 31 distinct Moldovan IPs were observed connecting to

the VNC Management IP. Interestingly, the communications do not overlap, pointing towards a single user / access point.

Our hypothesis in this case is that the operator(s) of VNC Management IP are employing some operational security measures whilst operating from / via a residential access point. The data available points to an end user frequently rebooting their router in order to refresh their public IP address.

Turning to outbound connections, a number of observations can be made, indicating potential operator TTPs.

Firstly, regular traffic to TeamViewer infrastructure was observed, indicating that the software may be installed on the operator's machine, with usage routed through TeamViewer's servers. Like VNC, TeamViewer has been used previously by threat actors for remote access management purposes, for example, it is leveraged to gain access to networks and establish persistence in ransomware operations.

Secondly, communications with a single Tor relay were observed over an extended period. This particular finding may be indicative of a single operator accessing the Tor network via the VNC Management IP.

By default, the Tor browser utilizes a small pool of Guard relays, which is refreshed approximately every 60 days. Ongoing communications with a single Tor relay is therefore indicative of an end user accessing Tor via the Tor browser.

As each instance of the Tor browser has its own set of Guard relays, multiple users accessing the Tor network via the same VPN access point would result in the observation of connections to multiple Tor relays.

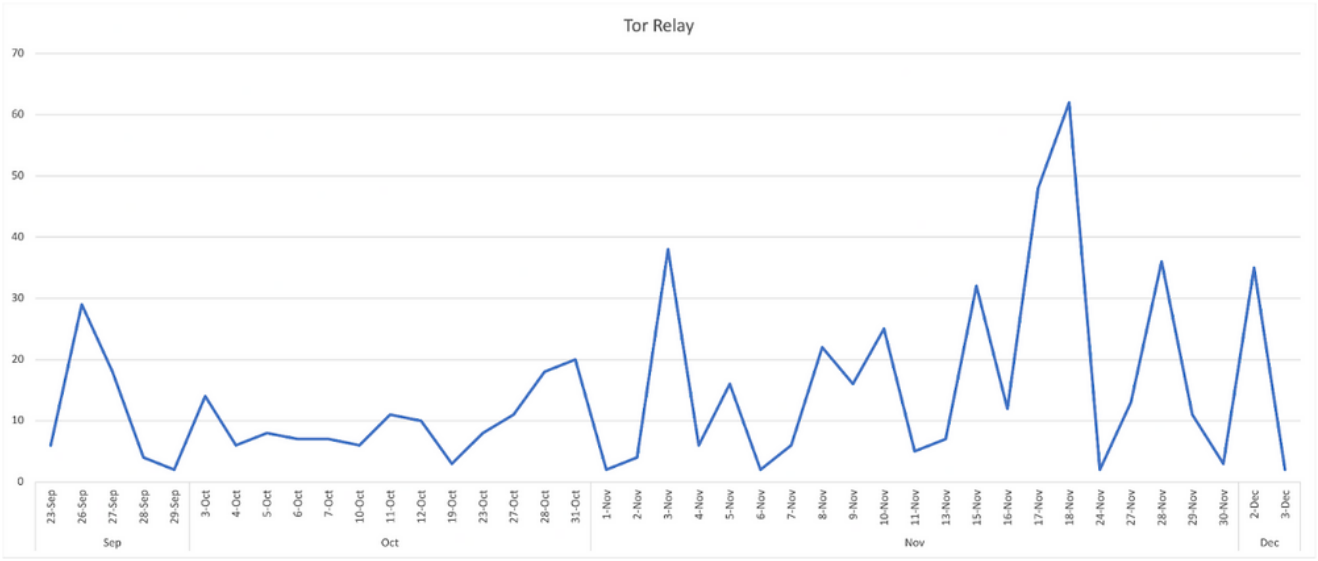


Figure 6: Communications with Tor Relay

By examining the timeline of activity involving communications with this particular Tor relay, we can see that it was likely associated with the operator until 3 December 2022, when the Guard pool likely reset. Since this date we have not observed any further connections to Tor relays; likely as a result of a coverage gap.

The majority of the Tor activity fits to a Monday to Friday schedule, although there were some days where access took place over the weekend. Most notably on 5 and 6 November 2022, following a spike in activity on 3 November 2022.

This activity coincided with a resurgence of Emotet activity, which included a new version of IcedID being dropped alongside it. The spike is therefore a possible indicator of collusion between the operators of Emotet and IcedID.

Aside from Tor, connections were also observed to IPs assigned to Telegram, indicating likely use of Telegram messenger. This finding is not particularly exciting (Telegram is used widely), but serves to highlight the overall TTPs of the VNC Management IP operators.

More interestingly, traffic to **onlinesim[.]ru** caught our attention. This website appears to provide temporary ‘virtual’ numbers to be used for sending / receiving SMS messages.

By virtue of the fact that this domain was accessed via the same infrastructure as is used to manage the BC C2s, it can be inferred that these temporary numbers serve a purpose in the overall process; although the exact use-case is currently unknown.

Another indicator for operator attribution came in the form of connections to an API for a local radio station based in Chelyabinsk, Central Russia.

We have two hypotheses for this activity, a) the API is embedded in another website and is pulling data from the radio station in Chelyabinsk, or b) the operator has some ties to that particular region of Russia; an expat living in Moldova?

Finally, we observed RDP connections to a set of IPs that share a distinct machine name, however it is unclear what the purpose of these connections are beyond the obvious use of the RDP protocol.

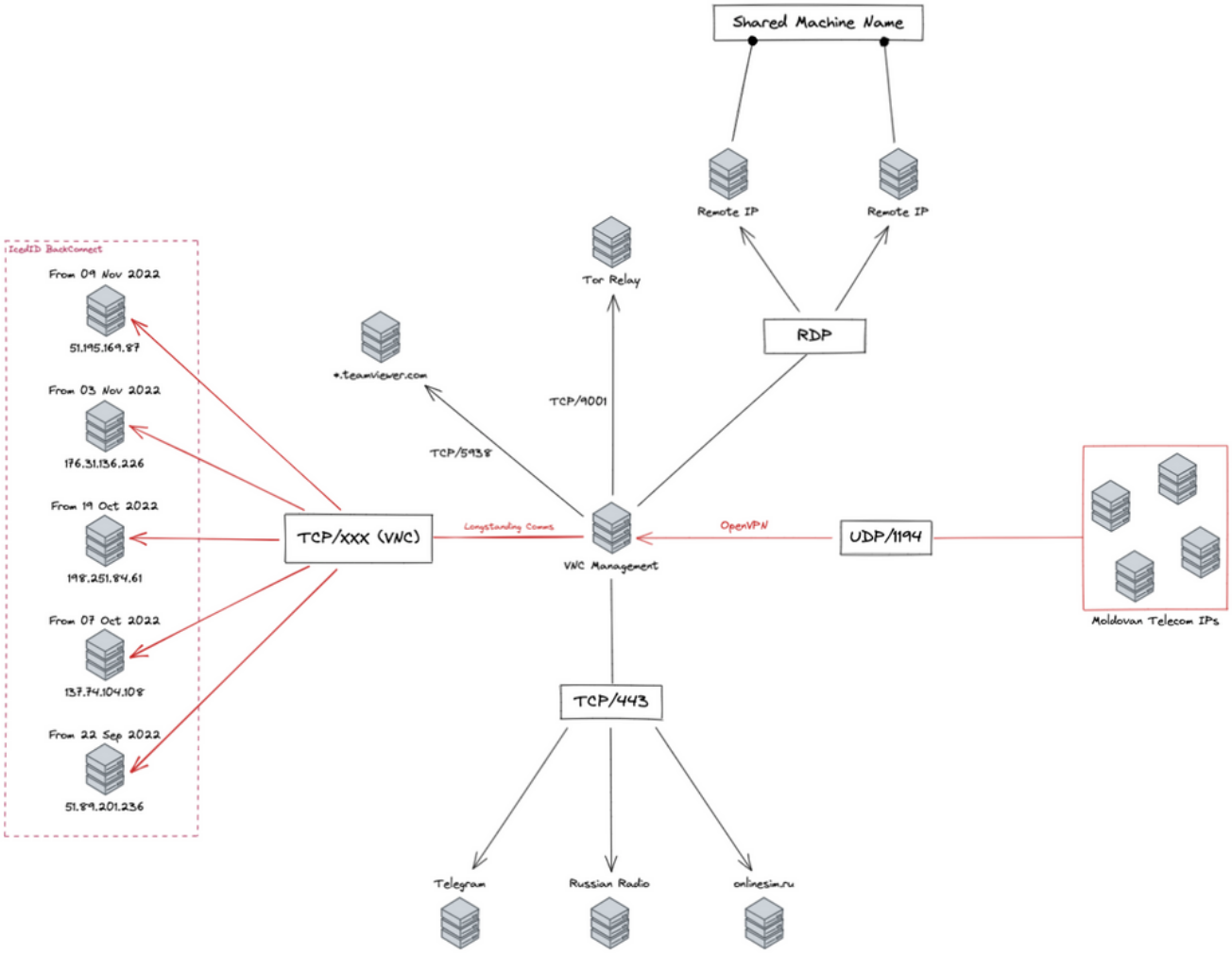


Figure 7: Summary of Activity - VNC Management IP

SOCKS Management

Intriguingly, although the SOCKS Management IP serves a similar purpose to the VNC Management IP, there are variations in both how this is accomplished and by whom.

Like the VNC Management IP, the SOCKS Management IP appears to be a VPN node, masking the true location of the operator(s), used to funnel not only BC protocol-related communications, but also other (mostly) connected activities.

Inbound traffic to the SOCKS Management IP is observed over UDP/51820, the default port for the open-source WireGuard VPN service.

Noting the similar use of an (albeit different) open-source, and likely private, VPN service.

On the other end of these communications are a handful of IPs assigned to providers in Ukraine. Most significantly, several of these IPs are attributable to ‘SpaceX Starlink’ infrastructure provided to Ukraine to help maintain Internet connectivity since the commencement of Russia’s “special operation” / illegal invasion in February 2022.

It is possible that this is the first example of the Starlink infrastructure being used by cyber criminals.

Beyond the Ukrainian IPs, in this case it is difficult to attribute the management activity more specifically; as the infrastructure is likely utilized by tens, or even hundreds of users at any given time.

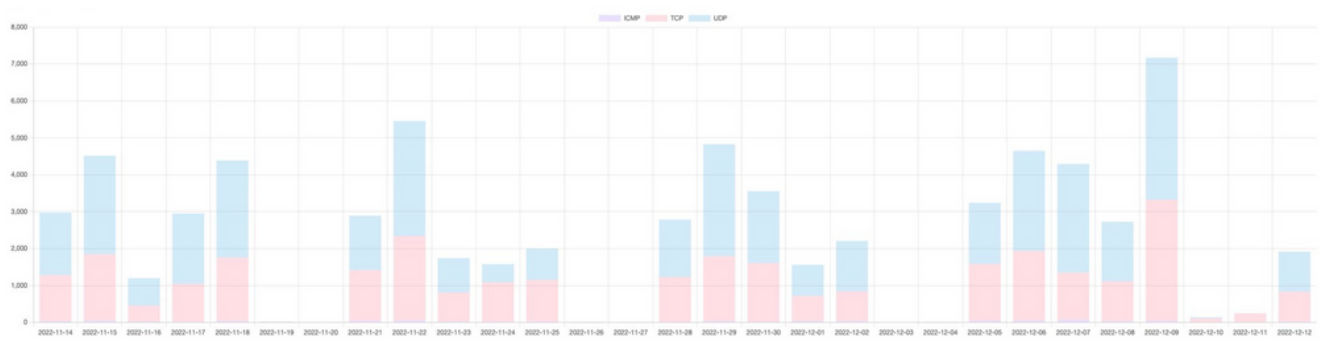


Figure 8: Inbound and Outbound Activity - SOCKS Management IP

Looking at outbound connections from the SOCKS Management IP, there is similar use of Tor and Telegram. Although, in the case of Tor, this may be more indicative of some form of automated or hidden service-related activity as communications with numerous Tor relays were observed.

This is in comparison with the VNC Management IP which appeared to only communicate with the one Tor relay; matching more closely the 'expected' behavior of an individual using the Tor browser.

Additionally, a large volume of connections, both inbound and outbound, over TCP and UDP/33445 were observed, generally associated with Tox messenger.

Tox has been utilized by cyber criminals in the past, including for C2 purposes. The default port for Tox is UDP/33445, however mobile connections default to TCP - it is therefore possible that the operator(s) of the SOCKS Management IP are using it to access Tox on both desktop and mobile.

In much the same way as the BC C2s have a life cycle of around four weeks, the SOCKS Management IP also communicates with cloud infrastructure (accessed via SSH) with the cloud peer IP changing over time. However, it was noted that all of the cloud IPs displayed the same unique SSH Server Host Key, indicating a likely consistent setup.

Finally, looking at outbound web-browsing activity (TCP/80 and TCP/443), the SOCKS Management IP is used to access IP addresses associated with Gofile (file sharing), ProtonMail, Trezor (cryptocurrency wallet), and a not insignificant number of pornographic sites (someone in IcedID senior management needs to crack down on adherence to the Acceptable Use Policy!).

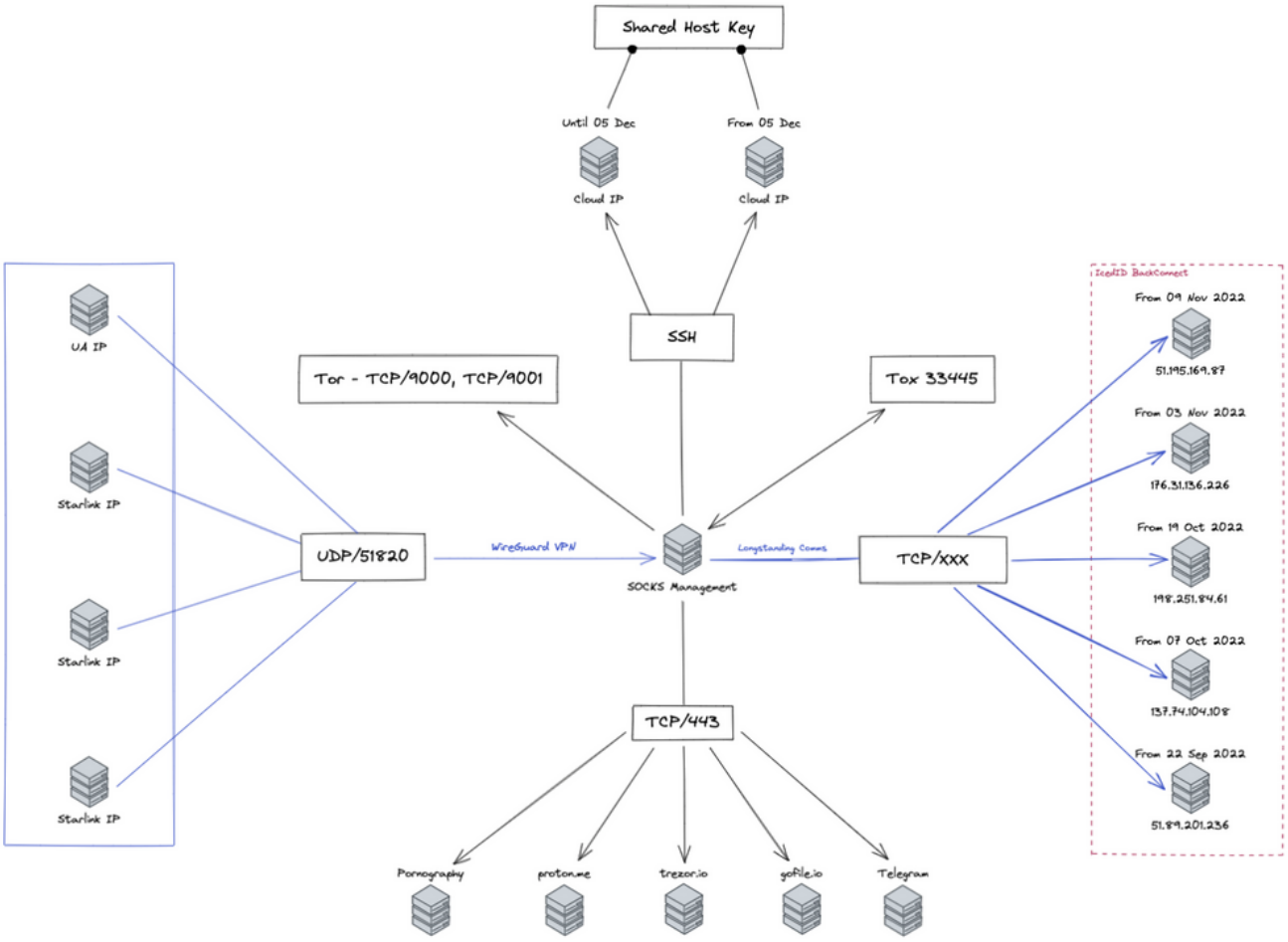


Figure 9: Summary of Activity - SOCKS Management IP

Conclusion

This blog serves two purposes, the first is to highlight our tracking of BC C2 infrastructure, sharing details of C2 servers and the process we undertake behind the scenes in order to identify them.

We will continue to share details of new / emerging BC C2 servers via our Twitter account @teamcymru_S2.

The second is to provide a snapshot into a ‘day in the life of’ the BC operators, and in doing so, providing wider context on threat actor TTPs.

In the case of BC, there appears to be two operators managing the overall process within distinct roles. Much of the activity we observe and have described in this blog occurs during the typical working week (Monday to Friday).

Both of these points indicate a degree of 'professionalism' in the operation of the BC protocol, and by extension IcedID itself.

Evidence of a 'dispersed' workforce undertaking specific tasks may also help to explain some of the variations in the TTPs observed. Whilst seemingly using two distinct VPN services, we can see an overall 'playbook' in use, i.e., its best practice to use a VPN for purposes of anonymization. The fact that both services are configured with default settings indicate either laziness, attempts to 'hide within the noise', or a lack of understanding / appreciation of the tooling in use.

We were surprised that beyond the use of a VPN node, very few steps appear to have been taken to cover the operators' tracks; we think this speaks to a confidence in 'invincibility', by operating from regions where law enforcement action is difficult to effect / prioritize.

The use of services like ProtonMail, TeamViewer and Telegram is commonly observed within threat actor operator playbooks, and these mainstream tools continue to be used by maliciously motivated individuals. Services like Gofile and **onlinesim[.]ru** may point to more 'operator-specific' TTPs, whilst also highlighting a general use of file sharing and temporary SMS platforms.

Finally, by highlighting a number of areas where we still have question marks in our understanding, we hope that we can encourage future collaboration on the BC protocol.

We hope that this blog post has been informative and has served to provide confidence in the IOCs which we have previously shared on this subject matter.

IOCs

BackConnect C2 Servers

```
135.125.242.223
135.181.175.108
137.74.104.108
176.31.136.226
185.156.172.97
188.40.246.37
198.244.187.242
198.251.84.61
212.114.52.91
51.195.169.87
51.89.201.236
```