Inside the IcedID BackConnect Protocol (Part 2)

team-cymru.com/post/inside-the-icedid-backconnect-protocol-part-2

S2 Research Team July 28, 2023

- S2 Research Team
-
-
  - Jul 28
  -
  - 11 min read

Introduction

In this blog post, we will provide an update on our continued analysis and tracking of infrastructure associated with IcedID's BackConnect (BC) protocol; a continuation of the analysis we shared in late-December 2022, which you can read here, in addition to our campaign metrics and infrastructure tracking blog posts.

Note: whilst the same BC protocol is utilized by several other threat operations, including Bazar and QakBot, this blog post focuses specifically on IcedID infrastructure.

Given that it is deployed post-compromise following initial assessments of the value of a victim host, the use of the BC protocol is of particular interest to us, and remains a priority for our overall tracking of IcedID. Analyzing activity related to BC infrastructure provides a strategic view into threat actor activity and interests, as it is a window into what occurs after a successful infection and the victim was deemed valuable for their use.

Since our last post, updates were made to the version of the BC protocol used by the IcedID threat actors during mid-April 2023. The last time we observed updates to the protocol was 7 months ago in September 2022. One of the more noticeable changes, shared by Palo Alto Networks' Unit 42, was in the port utilized by victim hosts when connecting to the BC command and control (C2) server, which was updated from TCP/8080 to TCP/443.

In our previous blog post, we referenced 11 IcedID BC C2 servers, active from the beginning of July 2022 through the end of 2022. Our analysis highlighted that generally two C2 servers were active at any given time, and the average life cycle for a C2 server was around four weeks. We will revisit this C2 timeline in order to assess how IcedID's use of the BC protocol has evolved over the past six months, and in doing so also review the associated management infrastructure used to access / administer it.

Key Findings

- The overall quantity of BC C2s has increased.
- A total of 34 medium and high confidence IcedID BC C2 servers were identified since 23 January 2023, up from 11 we observed from July 2022 until the end of the year.
- The average life cycle for a BC C2 has decreased.
- The average uptime of a BC C2 decreased from 28 days to eight days, and concurrently active servers increased from two to a maximum of four.
- Additional management infrastructure has been identified.
- Management activity continues to be sourced from two static VPN nodes, with other common management peers observed.
- Management-related activity has evolved from our last blog post.
- Management activity now varies from C2 to C2, we do not always observe connections from the same management IPs.
- Observed management activity is likely a mix of IcedID operator and affiliate access.
- Victims can communicate with multiple BC C2 servers over time.
- A possible connection between BC-infected victims and spamming activity was identified.

C2 Server Timeline

As explained in our previous blog post, a methodology was established for tracking BC C2 servers based on the observance of management traffic from a number of static IP addresses. By regularly monitoring outbound traffic from these IPs, we continue to identify new C2 servers as communications commence.

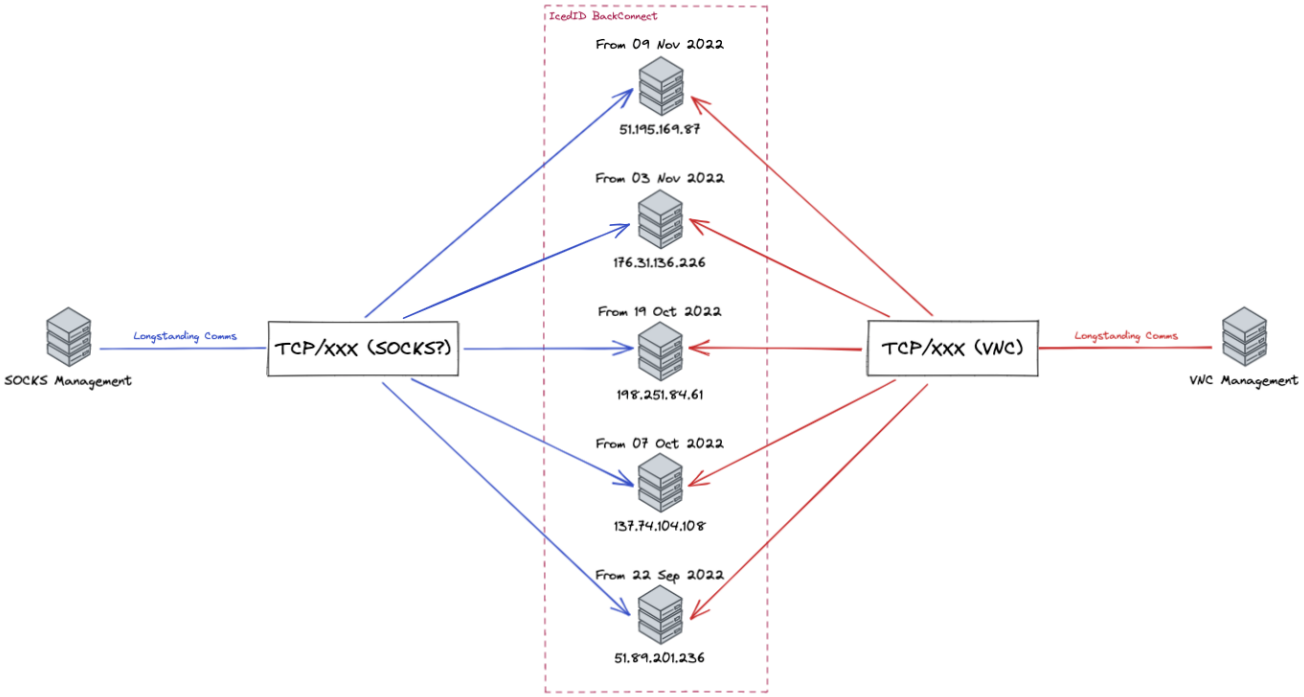

Figure 2: IcedID BC Protocol Management - c. November 2022

In this instance, *management traffic* is defined as IP addresses observed in communications with multiple C2 servers, connecting to specific ports of interest, in repeated established sessions. The *established sessions* element is inferred based upon observed ephemeral ports and TCP flags, in simple terms; scenarios involving a consistent ephemeral port with evidence of a successful TCP three-way handshake and subsequent activity / data transfer.

Record #	Ephemeral Port	TCP Flags
1	55001	2 (SYN)
2	56002	2 (SYN)
3	57003	2 (SYN)

Record #	Ephemeral Port	TCP Flags
1	60000	2 (SYN)
2	60000	18 (SYN-ACK)
3	60000	16 (ACK)

Figure 3: A Simple Visualization of the Previous Waffle 🙂

Getting back to the C2 servers, the following timeline illustrates the periods when we observed management traffic, and by extension an indication of when the C2 servers were in active use.

Whilst this section is based on the enumeration of BC C2 servers *since* the aforementioned updates in April 2023, for completeness we include all identified C2 servers (since the beginning of 2023) in the *Indicators of Compromise* section at the end of this post.

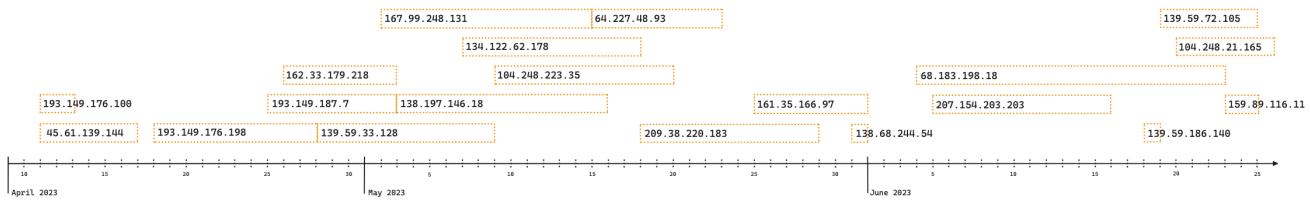

Figure 4: Timeline of BC C2 Servers from mid-April 2023 Onwards

Since 11 April 2023, a total of 20 high confidence BC C2 servers were identified, based on pivots from management infrastructure.

The first observation is that the number of concurrent C2 servers in operation has increased since our previous blog post, with as many as four C2 servers receiving management communications on a particular day. We also note that the life cycle of the C2 servers has decreased significantly, from around 28 days to just over eight.

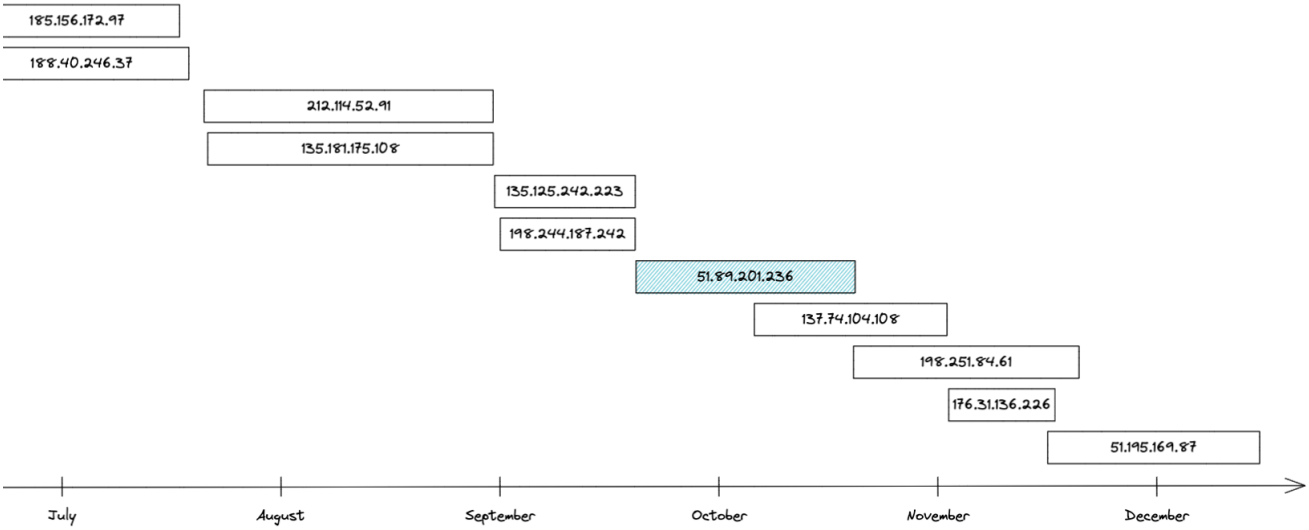

Figure 5: Previous Timeline - July to December 2022

There are a number of hypothesized reasons for these changes and each one is not independent of the others (nor is the following list exhaustive):

- Greater awareness of BC infrastructure has resulted in faster response times; both in reporting to hosting providers and mitigation activities; leading to a shorter C2 shelf-life.
- An increase in the use of the BC protocol by IcedID threat actors and their affiliates has required additional infrastructure to be stood up.
- Disruption / changes to activities has increased the need for additional back-up / fall-over C2 servers.
- General evolution of threat actor modus operandi - e.g. “statistics show that an individual C2 server reaches its peak potential on day N (<28 days), so why not rotate them more often?”. We know from analyzing other IcedID infrastructure that the admins run a metrics-influenced operation.

Since IcedID returned from its winter hiatus on 23 January 2023 through the end of June 2023, we have identified 34 medium (50-75%) and high (75-99%) confidence BC C2 servers. In the case of the four medium confidence C2 servers, we (Team Cymru) were not able to confirm their usage with the same veracity, but on the balance of probabilities are likely connected to IcedID BC activity; indeed some were reported by other researchers.

Management Infrastructure

In this section we will provide background context on the IP addresses we have observed accessing the BC C2s on particular ports of interest; namely TCP/8082, TCP/8083, and TCP/8101.

We assess that TCP/8082 relates to the BC SOCKS proxy, TCP/8083 to VNC (screen sharing), however at this stage it is unclear what the use of TCP/8101 relates to. We began to observe this port (TCP/8081) open on BC C2 servers over the past few months.

The two IP addresses we detailed in our previous blog post (see Figure 2) continue to be used to access BC C2 servers, however they are no longer observed in every single case.

> The **VNC Management IP** continues to be accessed from IP addresses assigned to MOLDTELECOM-AS and was last observed communicating with BC C2 servers in early July 2023.

> The **SOCKS Management IP** continues to be accessed from an IP address assigned to a Ukrainian ISP, interspersed with irregular connections from Starlink infrastructure. Communications with BC C2 servers was last observed in early June 2023.

Over the past six months, we have observed other IPs accessing the BC C2 servers. By following the activities of a number of these IPs we are able to fill in the blanks where we don’t see communications from those two originally identified management nodes.

It is unclear why the IPs accessing the C2s vary depending on C2, ; although it is plausible to assess that the activity originates from both IcedID operators and their affiliates.

The recently identified management IPs fall into three distinct categories:

Private VPN Nodes

These IPs appear to be utilized in the same way as the initial two management IPs, with a limited number of inbound peers. Outbound traffic is broadly limited to IcedID BC-related infrastructure, with connections occurring on all three ports of interest.

German Node 🇩🇪

This IP connects to BC C2 servers on TCP/8101 and is currently active at the time of writing. Aside from connections to BC C2 servers, we also observe inbound connections from Tor relays - hinting at how this node is accessed.

Latvian Node 🇱🇻

This IP connects to BC C2 servers on TCP/8082 and TCP/8083 and is also currently active at the time of writing. This IP is observed in traffic indicative of blockchain/cryptocurrency trading and the use of Tor and Tox messenger. TCP/1194, commonly associated with OpenVPN, is open on this IP - again hinting at how this node is accessed.

Russian Node 🇷🇺

This IP connects to BC C2 servers on TCP/8082 and TCP/8101 and is also currently active at the time of writing. Aside from connections to BC C2 servers, we also observe outbound connections utilizing common mail ports (25, 143, 468, 993, etc).

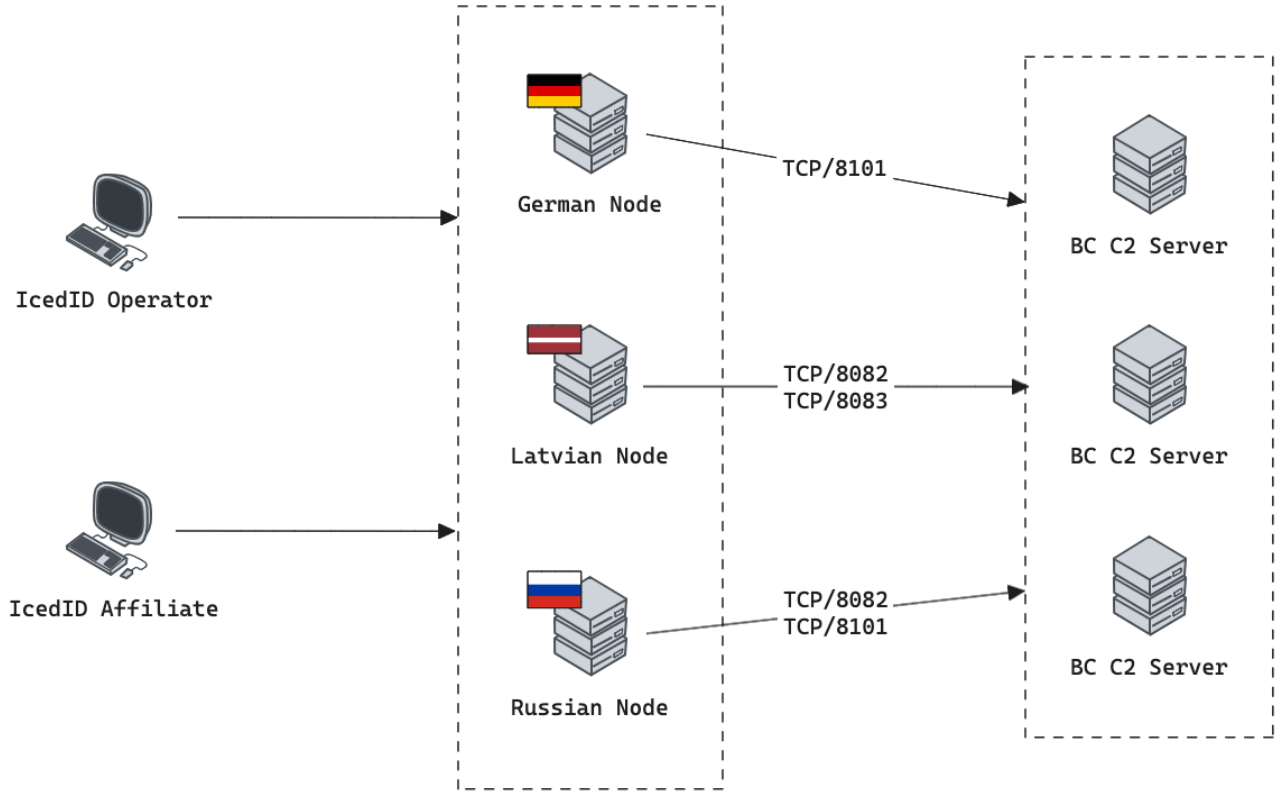

Figure 6: Private VPN Nodes - Hypothesized Management Access

Jump Boxes

In February we published a blog post stemming from an investigation into an IP address which was observed connecting to various elements/levels of the IcedID infrastructure, including BC C2 servers. This IP was geolocated to Chile, but there was clear evidence that it was utilized by a Russian-speaking operator.

Since our last post, we have observed the Chilean jump box was accessed via an OpenVPN connection from an IP geolocated to Switzerland - assigned to Private Layer Inc, a Panamanian-registered VPS provider.

We have continued to monitor this Swiss IP, which has led to the identification of further jump boxes, utilized in much the same way as we described in the blog.

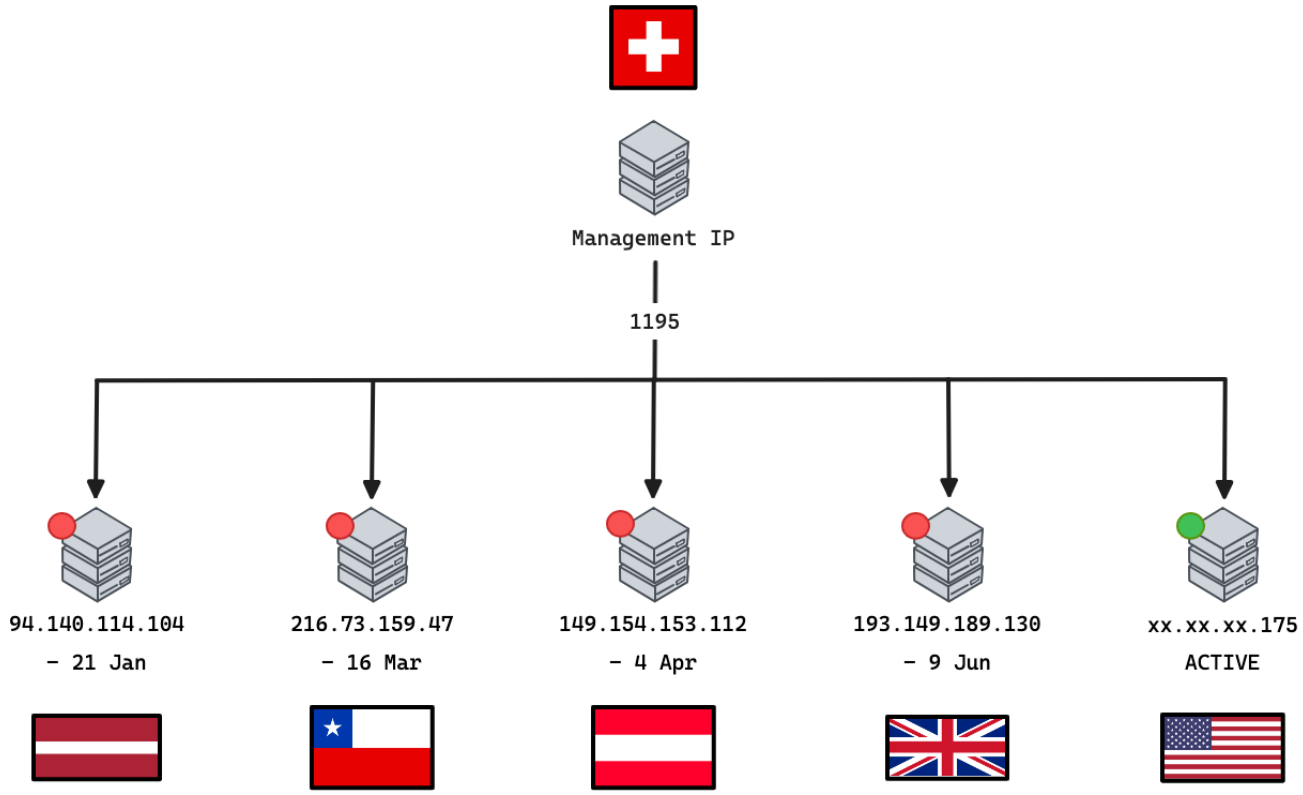

Figure 7: Jump Box Management and Identification

Since June, an IP geolocated to the United States has been used as the current jump box and again this has included access to BC C2 servers.

We continue to assess that this infrastructure is associated with IcedID administration.

Russian Telecommunications (Rostelecom)

These appear to be consumer IPs which, based on data from Spur Intelligence, are utilized as small gateways for a limited number of concurrent users. We have observed numerous IPs (with no cross-over in usage) assigned to Rostelecom, Russia's largest ISP, in communication with BC C2 servers using port TCP/8083.

Whois information for these IPs is consistent in identifying them as previous VolgaTelecom infrastructure for the Mari El region of Russia. VolgaTelecom was absorbed by Rostelecom in 2011; it is unclear if this infrastructure continues to serve Mari El, however this may provide an indication of the end user's location if so.

Outside of the connections to BC C2 servers, we observe general Internet usage, BitTorrent activity, and evidence of the use of crypto-mining software.

Victimology

In simple terms, victimology refers to the practice of understanding and studying the characteristics of victims versus focusing on the perpetrators. In cyber threat research we can use victim to C2 communications, at a large scale, to understand trends in threat activity.

We looked for potential victims by identifying activity that matched typical C2 communication over TCP/443, excluding traffic that was likely researcher or scanner related. Eventually a sample of eight candidate victim IPs from various ASNs and geographical regions was collected, all of which communicated with three or more BC C2s over a relatively long period of time. We found there were many other potential victims connections to the C2 servers, but the majority communicated with only one or two, and for shorter time periods.

In the timeline below, connections with the BC C2 servers for each victim is indicated by a line next to the geolocation of the victim. Each box on a line represents the start and end date of communication between the victim and the C2 server listed within the box. Underneath the x-axis of the timeline are flags showing when we first spotted the C2 in the management infrastructure we monitor (a replication of Figure 4).

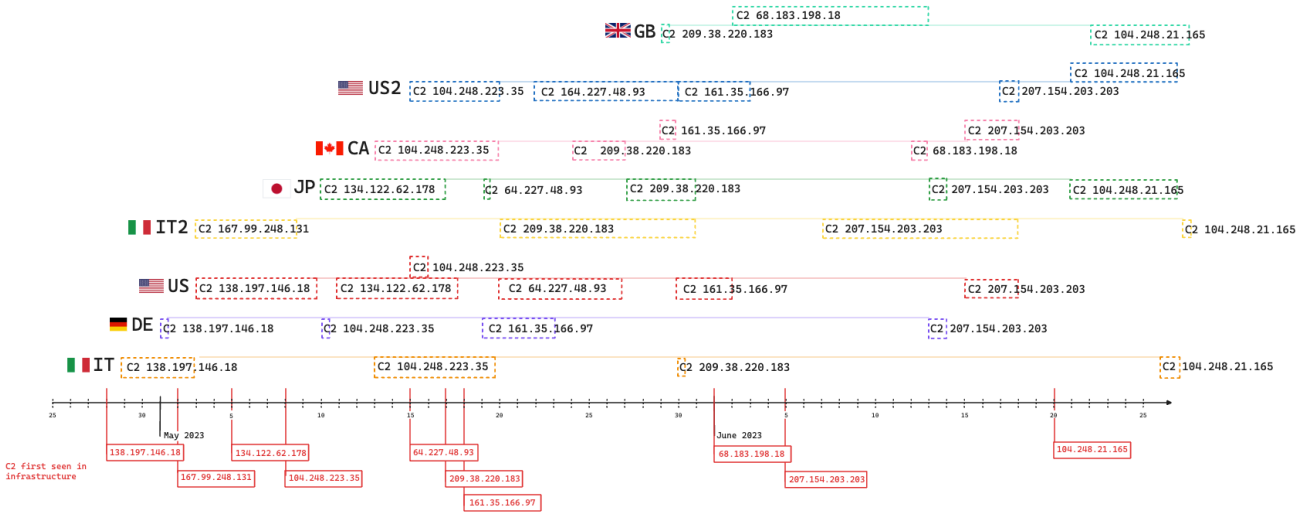

Figure 8: BC Victim Timeline

For all of the victims in our sample, first connections to a new BC C2 server began after we identified the C2 via monitoring the management related IPs mentioned in the section above. The two management nodes we originally wrote about in our previous blog only communicated with five of the BC C2 servers, and in some cases this only occurred after victim traffic had commenced.

This is a good example of why we continuously update our tracking of upstream threat actor infrastructure, whilst it might remain static for a duration, this infrastructure can change or be superseded by other key hosts. In the case of IcedID BC infrastructure we were able to adapt our insights by continuing to pivot from NetFlow data for known BC C2 servers.

We see that victims can communicate with multiple BC C2s over time while they remain infected, but not every victim communicates with every new C2. In fact, there is no discernable pattern around how long a victim communicates with a C2, when victims switch to a new C2, or which C2 servers a victim communicates with.

However, when we pivot to analyzing the volume of traffic between victims and C2s, we finally see a pattern emerge.

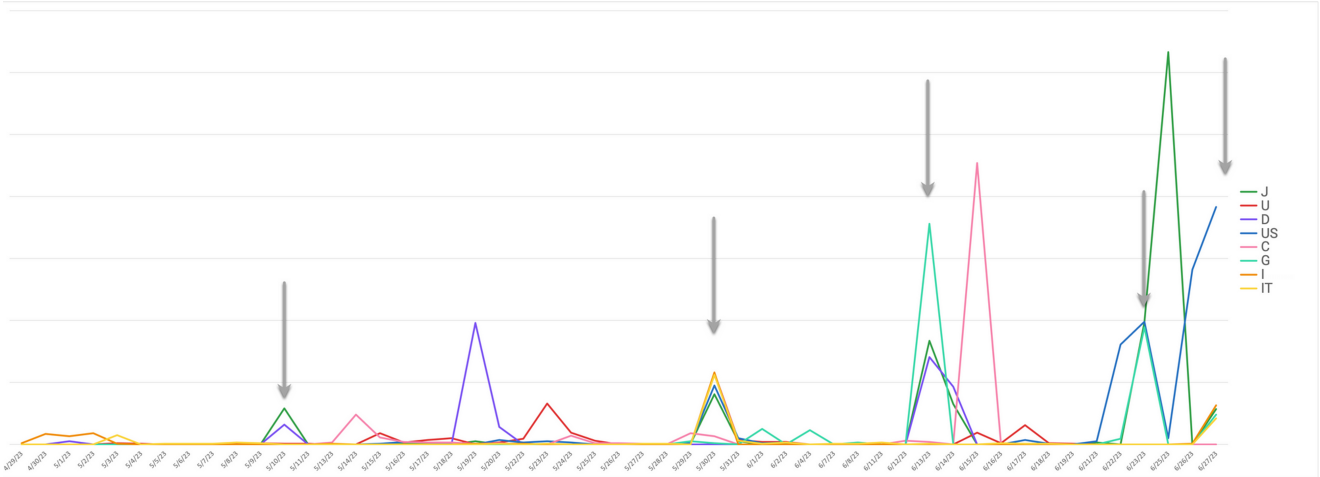

Figure 9: Spikes in BC Victim Traffic Volume

Regardless of C2, some days show jumps in traffic volume between the victims and C2 servers. For example, on 13 June 2023 there was a spike for the British, Japanese, and German victims, but they were not communicating with the same C2. The German and Japanese victims were communicating with C2 **207.154.203.203**, while the British victim was communicating with C2 **68.183.198.18**.

This is potentially indicative of the overall coordination of IcedID victims interacted with using the BC protocol. Whilst victims may be communicating with separate C2 servers, we see peaks in activity within the same time parameters. This points to the same IcedID operator or affiliate accessing multiple victims for a specific purpose, likely via a panel which consolidates all victims together regardless of specific C2 server.

TCP/587 and TCP/465 Activity

While analyzing victim NetFlow data, we found that all eight victims from our sample group shared outbound connections to some of the same obscure mail servers over TCP/465 and TCP/587, typically in bursts on the same day. We hypothesize these communications may be connected to IcedID delivery / spam operations.

Often we observe the victims connecting to the same mail servers concurrently, or scenarios when victims switch between mail servers which are ultimately in the same pool. Essentially, there is a lot of overlap which appears more than just coincidental, where batches of victim machines are used, presumably using the SOCKS element of BC, to access mail servers. When we look back into our data, we observe this pattern of activity occurring as far back as March 2023, and potentially even before.

Additionally, the bursts of activity coincide quite clearly with the previous line chart showing the volume of connections between victims and BC C2s, specifically on:

- 10, 19, and 30 May 2023

- 13, 23, and 24 June (and an uptick at the end of the research window, 26/27 June) 2023

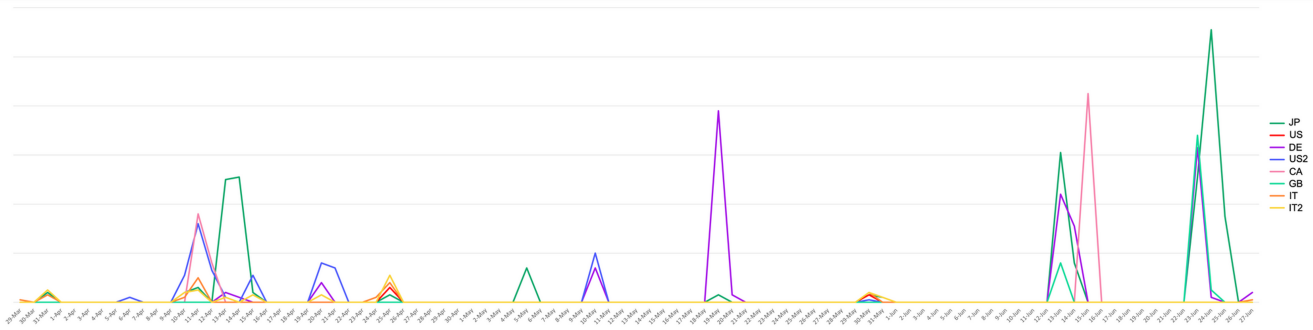

Figure 10: BC Victim Mail Server Traffic

Are they related? Based on the comparison of the two charts, it seems likely. On the days where victims had a spike in BC C2 traffic, there was also a burst of activity from victims sending outbound connections to mail servers over TCP/587 (and sometimes TCP/465). It is unlikely that such a random group of victims would coincidently have the same type of activity on the same days, repeatedly over months. It's far more unlikely that it would also coincidently align with victim/BC C2 activity.

Whilst we have no definitive proof at this point in time, our current hypothesis, based on the findings described above, is that BC is used (at least in part) to enable spamming operations associated with IcedID and their affiliates. Specifically, the SOCKS element of BC is used to proxy connections to mail servers via a subset of IcedID victims.

Conclusion

In this blog post we have outlined how IcedID BC infrastructure has expanded over the first half of 2023; with an increase in C2 servers observed in total, and in parallel use at any point in time.

We have also discussed some of our techniques for tracking emergent C2 infrastructure, often on a timeline whereby identification occurs before victim traffic is observed. Early identification is key to preventing future compromise, threat actor-victim interaction and eventual data / financial loss.

In examining management infrastructure associated with IcedID BC, we are also able to discern a pattern of multiple distinct accesses from users we assess to be both associated with the day to day operations of IcedID, and their affiliates who interact with victim hosts post-compromise.

Through victimology analysis we are also able to provide a hypothesized purpose for the BC protocol; we would assume one of several purposes. The evidence in our NetFlow data suggests that certain IcedID victims are used as proxies in spamming operations, enabled by BC's SOCKS capabilities.

This is a potential double blow for victims, not only are they compromised and incurring data / financial loss, but they are also further exploited for the purposes of spreading further IcedID campaigns.

Recommendations

- Users of Pure SignalTM Recon and Scout can follow this activity by pivoting from the BC C2 servers provided in the IOCs section at the end of this blog post.
- In general we would recommend that the IOCs are used for cyber defense measures; both proactive blocking and reactive threat hunting. Threatfox is an excellent open-source resource for up to date IOCs relating to IcedID and many other threat campaigns.

Indicators of Compromise

BC C2 Servers

5.196.196.252

135.148.217.85

80.66.88.71

45.61.137.220

193.239.85.16

185.99.132.16

167.99.235.95 (Medium)

162.33.179.145

46.21.153.153

193.149.176.100

45.61.139.144

45.61.137.159 (Medium)

45.61.139.235 (Medium)

193.149.176.198

192.153.57.134

193.149.187.7

162.33.179.218

139.59.33.128

138.197.146.18

167.99.248.131

134.122.62.178

104.248.223.35

64.227.48.93

209.38.220.183

161.35.166.97

138.68.244.54

68.183.198.18

207.154.203.203

64.227.146.71

116.203.30.206 (Medium)

139.59.186.140

139.59.72.105

104.248.21.165

159.89.116.11