Inside DanaBot's Infrastructure: In Support of Operation Endgame II

team-cymru.com/post/inside-danabots-infrastructure-in-support-of-operation-endgame-ii

S2 Research Team

5

min read

Executive Summary

DanaBot first emerged in 2018 as a banking trojan but has since evolved into a versatile and persistent threat. While it initially focused on financial credential theft, it is now used for a range of purposes including information stealing and establishing access for follow-on activity such as ransomware. Despite years of activity, DanaBot remained highly operational through 2025, until it was dealt a significant blow as part of Operation Endgame II.

DanaBot maintained an average of 150 active C2 servers per day, with roughly 1,000 daily victims across more than 40 countries. By C2-count, this was one of the largest "malware-as-a-service" platforms active in 2025, while the botnet size was relatively modest in terms of daily victims. Of these, Mexico and the United States consistently ranked among the most impacted. Its success can be partly attributed to its stealth; as of this writing, only 25 percent of its C2 servers had a VirusTotal detection score greater than zero, suggesting that a significant portion of its infrastructure remained undetected. This was likely due to selecting fewer targets than other loaders of its kind, as well as cycling operations around high profile events.

DanaBot operated with a multi-tiered architecture that Black Lotus Labs and Team Cymru assess to be separated among several users or "affiliates" that have purchased access to the malware. Depending on the affiliate and their level of access, they were assigned a dedicated "Tier 2" server or shared one with others. At any given time, at least five to six Tier 2 servers were active.

We suspect that DanaBot is likely operated from Russia with management infrastructure originating from several IPs in residential areas of Novosibirsk, Russia and what appears to be two other threat actors accessing the management infrastructure from Russian geolocated servers belonging to two separate proxy services.

During Operation Endgame I, Black Lotus Labs and Team Cymru supported the broader effort to disrupt DanaBot, working closely with industry peers and law enforcement. The recent takedown dealt a serious blow and showed how collaboration across the security community can lead to real progress against threat actors.

Introduction

First reported by Proofpoint in 2018, DanaBot has evolved into a highly successful infostealer and malware delivery platform. It has been observed delivering other threats such as Latrodectus, which is often linked to ransomware operations. While we will not delve into DanaBot's malware functionality in this post, we encourage readers to explore the many excellent writeups available on that subject.

During and since Operation Endgame I, Black Lotus Labs and Team Cymru have been collaborating behind the scenes, working closely with industry peers and law enforcement. Both of our organizations specialize in the tracking of threat actor infrastructure across the Internet. By combining our efforts, and those of several contributing teams, we strongly believe we are able to have an even greater impact than if we had acted alone, in isolation. Additionally, PQ Hosting / Stark Industries (AS44477) were a key partner and collaborator in confirming the role and activity of threat actor infrastructure and the coordinated takedown. Infrastructure identified later in this blog post which was assigned to PQ / Stark was purposefully left "online" for intelligence gathering purposes.

Over the last few years, the cybercrime landscape has evolved, with a general decline in “noisy” delivery campaigns and overt mechanisms. While several high-profile threats have been disrupted (or have simply faded away), others have opportunistically emerged to fill the void. Today, threat actors are diversifying their tactics, spreading their efforts across a wider array of malware families and delivery methods. The rise of the "initial access broker" model has further professionalized this phase of the attack lifecycle. One malware family that has endured through these changes and continues to challenge defenders is DanaBot.

Black Lotus Labs and Team Cymru will focus on DanaBot’s infrastructure, providing a view into its scale and structure based on insights gained through our collaboration during Operation Endgame II.

Global Telemetry Analysis

DanaBot consists of a diverse, multi-tiered architecture consisting of nearly 150 or more active C2 servers at any given time. Through periods of greater or lesser activity, both the upstream and backend infrastructure have remained largely static since June 2024.

A layered communications infrastructure is used between a victim and the botnet controllers, where traffic is proxied through typically two or three tiers of C2s before it reaches the final tier, which consists of the panel that the [threat actors](#) operate from. Emotet, IcedID, and Qakbot are just a few examples of other malware families that have also leveraged this setup to insulate their C2s.

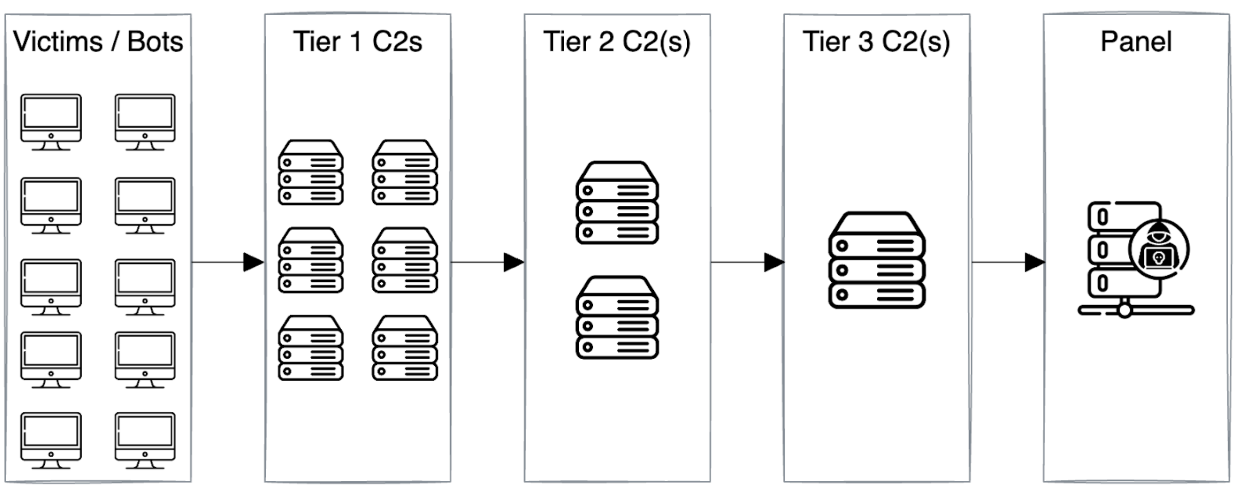

Figure 1: High-level diagram of multi-tiered C2 architecture.

When a victim is infected with DanaBot malware, they will begin to communicate with one or more Tier 1 (T1) C2s over TCP/443. We suspect that, depending on the affiliate and how they subscribe to the service, these T1 C2s will be controlled by one of several Tier 2 (T2) C2s. These T2 C2s will generally have their own individual upstream Tier 3 (T3) C2s, obfuscating the architecture infrastructure even further. The T3 C2s then communicate with what we suspect is a potential backup server, as well as with infrastructure that directly ties back to our suspected DanaBot actors. We'll dig into this more later.

At any time since we began monitoring in late 2024, a quarter to a third of all active T1 C2s in DanaBot's architecture are positioned in one single cloud service provider, and from there, on to one of two T2 servers and their T3s. The remaining T1 C2s were typically found communicating with one of three T2s, which then connected to their respective T3 servers. We suspect that between the "Cloud" architecture and the non-"Cloud" architecture, there is a mix of specific large affiliates having their own personal T2 and some smaller affiliates sharing T2s.

Below is an outline of the entire architecture we uncovered for the DanaBot pipeline and management infrastructure, but we will individually address each "section" in more detail with larger maps.

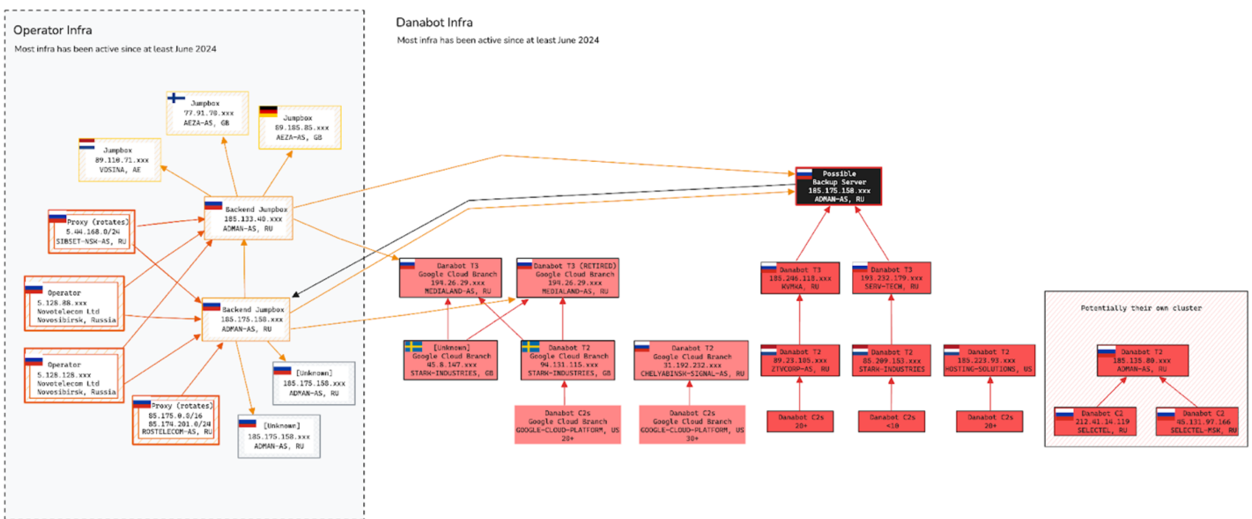

Figure 2: Overview of DanaBot pipeline and management infrastructure.

Bots and Tier 1 C2s

DanaBot maintained a daily average of over 150 active T1 C2s throughout our study. What becomes interesting is where we see peaks and troughs. We noticed a surge of almost 50 C2s leading up to the November 2024 election in the US, followed by a lull in activity before ramping up to all-time highs during the December 2024 holidays. This pattern suggests the DanaBot actors may use newsworthy events to their advantage, luring more victims to download malicious software, open a phishing email, and more.

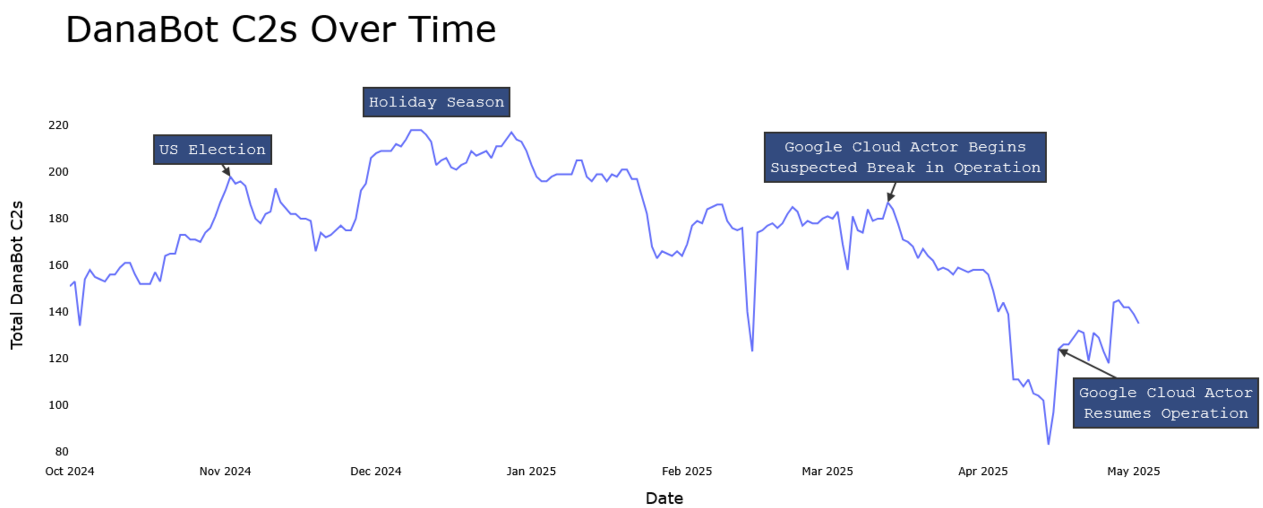

Figure 3: Total Number of DanaBot C2s over time

We also observed that the actor(s) who use the "Cloud" C2s seem to take the greater part of their architecture offline for extended periods. Throughout April 2025, we tracked most of the "Cloud" architecture as it went dark, only to have both the T1s and one of the T2s reappear towards the end of April into May. The other T2 remained active during this period, though it had far fewer C2s communicating with it, and those connections occurred infrequently. We suspect this atypical period was either the actor taking a break from DanaBot activities, or they were updating their servers during this time.

Black Lotus Labs and Team Cymru have noticed close to 400 distinct IPs acting as DanaBot C2s thus far in 2025, still a considerable number given the December 2024 peak of 230. Regardless of the numbers, their C2s are well distributed in many different countries and maintain a robust lifecycle.

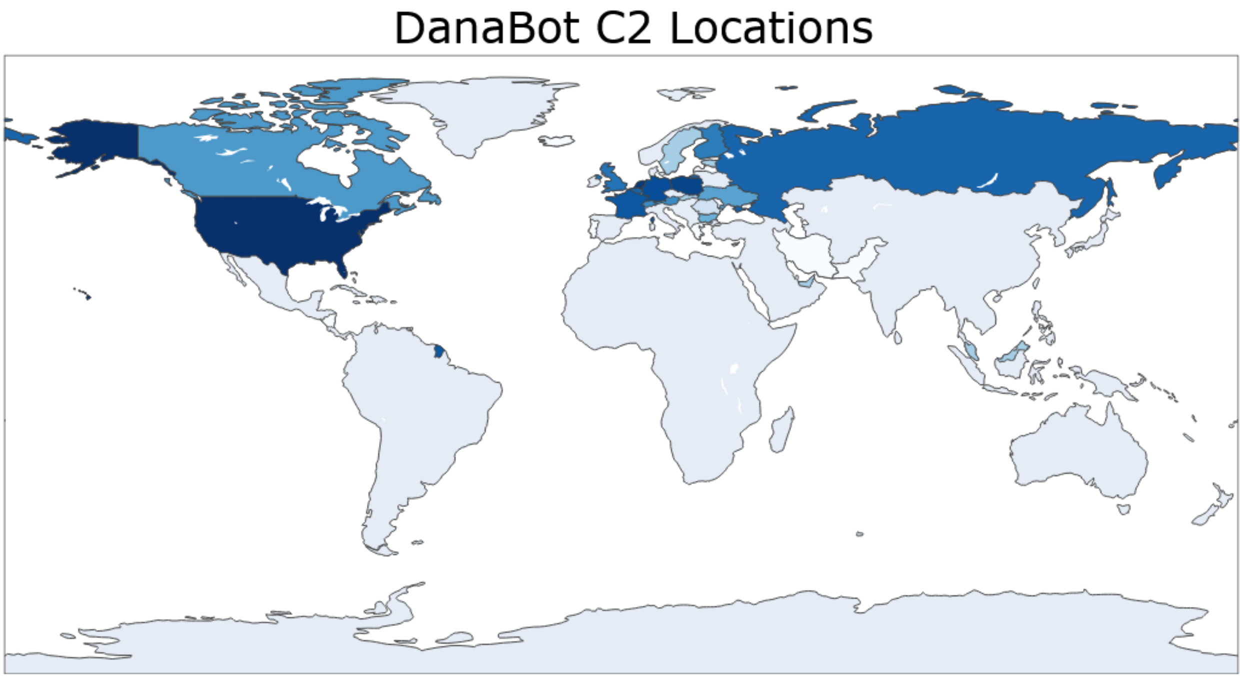

Figure 4: DanaBot C2 Distribution during 2025 where dark blue represents more C2s

We have observed the average C2 is active for over one month, and close to 25% stay engaged for over two months. While normally this wouldn't be a successful operating model as it would allow network defenders to discover and easily block these IPs, DanaBot has somehow remained stealthy. For the C2s that were active in the last month, only 25% of them have a score of greater than 0 in VirusTotal. Of greater concern, 65% have a score of 0 and no associated malicious files meaning actors who are using these DanaBot C2s are remaining very quiet and likely performing more targeted attacks.

When we investigate the bot population, Black Lotus Labs and Team Cymru have found victims in over 40 countries with Brazil, Mexico, and the United States having the most.

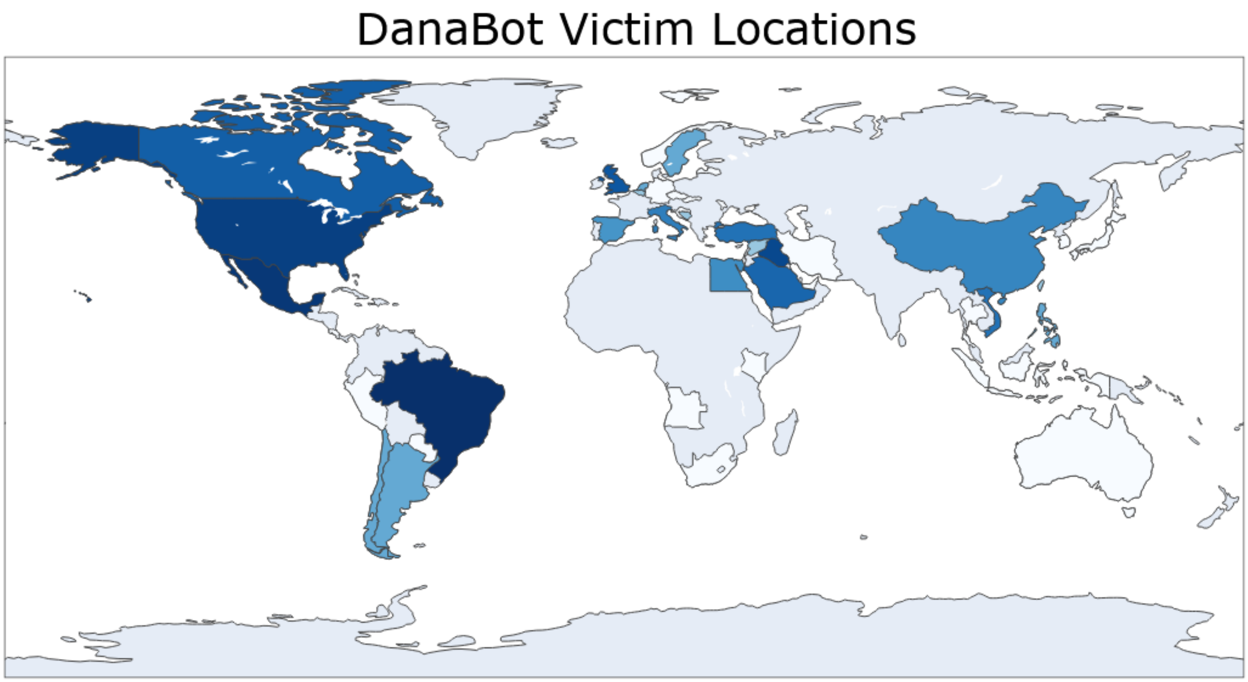

Figure 5: DanaBot Victim breakdown by country where dark blue represents more victims

On the low end we see around 1,000 victims per week, ranging as high as 3,000 victims, all in residential IP space. It’s important to note that DanaBot has the functionality to transit victim data through Tor instead of using a direct connection between the victim and the C2, so the true bot population is likely larger than what we can see. Aside from just residential victims, we have seen multiple higher value targets infected including law firms and universities among others.

It appears the actors who purchase DanaBot likely use it for different purposes. A small handful of C2s control the vast majority of the bot population where most of the C2s have relatively small amounts of victims, likely indicating some actors are using DanaBot for scale and others have specific victims they are trying to infect. A second reason for the difference in the number of victims infected by some C2s we observe is likely connected to the aforementioned usage of Tor. Just under half of the C2s we track appear to route at least some portion of their victim populations via this method, making victim enumeration more complex.

Although the DanaBot C2s are active for extended periods of time, 50% of the infected victims only communicate with the DanaBot C2 for a single day, and 75% of infections last less than three days. This leads us to believe that, in general, actors who are using DanaBot quickly get the information they need from the infected victims and move quickly to downstream activities. Aside from information stealing and banking fraud, actors likely use DanaBot as a precursor to download other malware such as Latrodectus, or pass off access to a ransomware group.

Tier 2 C2s

Black Lotus Labs and Team Cymru tracked the daily average of 150 T1 C2s, to a select few T2 C2s. Apart from one instance, T1s only talk to one T2, typically over TCP/443. We believe this is due to the infrastructure being siloed based on actor and subscription packages.

A pair of potential T2s were of interest as they did not fall into any specific pockets of activity. One T2 server, 185.135.80.xxx, was located in Russia and only interacted with two identified Russia T1 C2s, each with very small victim volumes. This communication occurred over TCP/23213, rather than the typical TCP/443 used by the other clusters. We suspect this was the actors' personal siloed architecture, which they used with their own malware and aligns with the hosting they generally maintain for backend management. However, it became inactive at the end of March 2025.

Another host, 45.8.147.xxx, appeared to function as a T2 based on its upstream communication with both the retired and current T3 for one of the "Cloud" clusters, although no activity with T1 C2s was observed. We were not able to confirm its exact purpose, but one theory is that it could be related to testing.

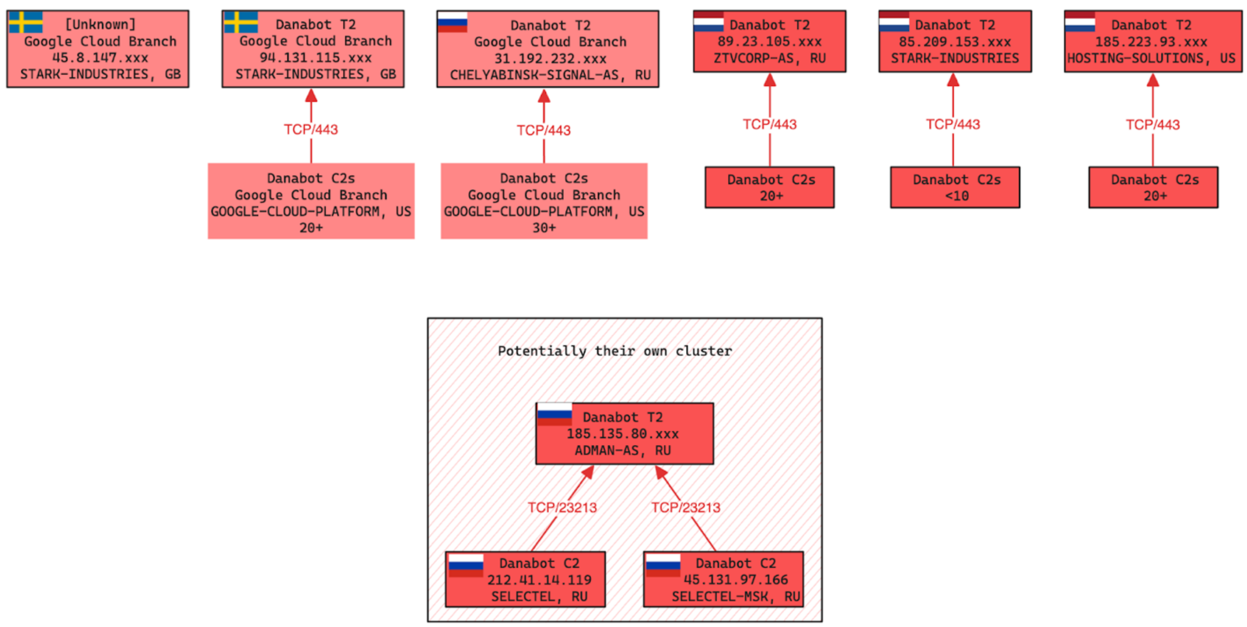

Figure 6: DanaBot C2-to-Tier 2 infrastructure with associated port usage.

Tier 3 and Above

We identified most of the upstream T3s that each T2 communicated with, all of which were located in Russia. The T2 to T3 communication for one of the two "Cloud" clusters was over TCP/15643, while the non-"Clouds" were over TCP/443.

The unidentified T3s included the other "Cloud" cluster, and one T2 suspected to belong to the core DanaBot team or developer. An additional T2 was involved in the only observed instance of a T1 being shared with a second T2, which showed significantly higher activity.

This may indicate that the cluster used two T2s, with one acting as a backup, both connected to the same T3.

At least two of the identified T3s were observed sending large volumes of data to the same Russian server (185.175.158.xxx) on a monthly basis over TCP/2048, typically around the same time. This behavior pattern is commonly associated with backup server activity. Given that no additional upstream infrastructure was identified and all known T3s were found in Russia, it is likely that the T3s represented the final tier and hosted the panels for each DanaBot cluster.

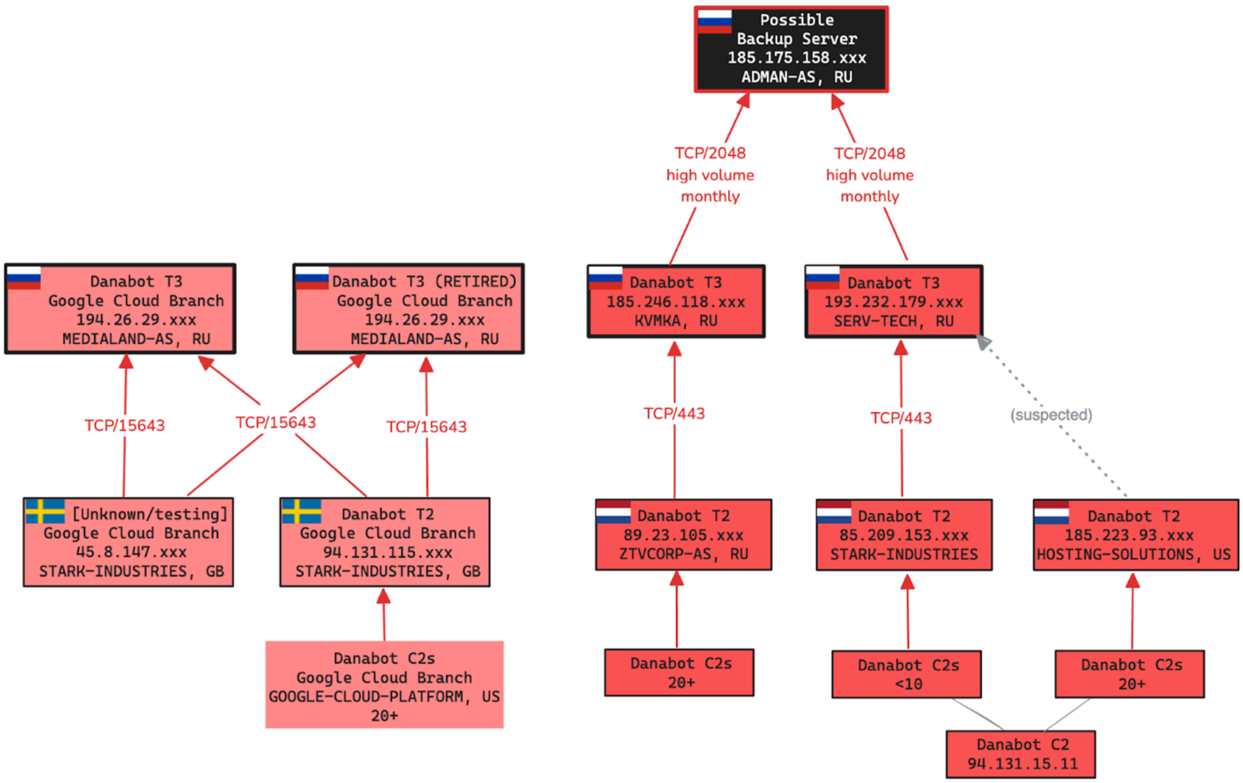

Figure 7: DanaBot Tier 2-to-Tier 3 infrastructure with associated port usage.

Management Infrastructure

Russian management infrastructure was observed connecting over RDP and VNC to what appeared to be the backup server, as well as to both the current and retired T3s associated with one of the “Cloud” clusters. It possibly interacted with other T3s as well, but visibility into connections between various Russian providers is limited.

This activity originated from two ADMAN-AS, RU servers that appeared to serve as “jumpboxes” used for backend management. A jumpbox in this context served as a relay point for operators, enabling access to internal infrastructure and external services without connecting directly from their own systems. Notably, one of these servers, 185.175.158.xxx, connected to the other, 185.133.40.xxx, over OpenVPN and VNC.

In addition to communicating with the backup server and some of the T3s, both jumpboxes interacted with other suspected DanaBot-related infrastructure. 185.175.158.xxx connected to two additional ADMAN-AS, RU servers: one over SSH and VNC, and the other over TCP/8080. The purpose of these two hosts could not be determined based on the available data.

185.133.40.xxx connected to three other jumpboxes that were used for external activities commonly associated with threat actor infrastructure, including cryptocurrency services and use of tools like Tox and Telegram. One of these jumpboxes was observed connecting over RDP to a host that interacted with DanaBot C2s. During the same time period, a host used for SmartApeSG backend management was also seen connecting over RDP to that same host. This overlap was notable, suggesting a single operator may have been involved in both efforts and that the same group was managing multiple operations. Still, it was the only strong link observed and not enough to draw a firm conclusion.

At least three separate operators were determined to have connected to both backend jumpboxes over OpenVPN. One IP based in Novosibirsk, Russia (5.128.128.xxx) frequently connected to the jumpboxes from at least June 2024 until recently. Even during periods of inactivity across other parts of the infrastructure, this IP continued to connect occasionally.

At the end of February, another IP from the same provider and location (5.128.88.xxx) also began connecting to the jumpboxes, with some overlap in timing. This may have represented a separate operator or the same individual using a different IP.

The two other operators used proxies and connected far less frequently. One consistently used a proxy in the 5.44.168.0/24 range belonging to SIBSET-NSK-AS, RU, changing IP addresses only every few months. This operator connected frequently, though far less often than the one previously described. The remaining operator was the least active, and always used IP space from ROSTELECOM-AS, RU, changing addresses after each burst of activity. These bursts typically occurred every few weeks and lasted only a day or two.

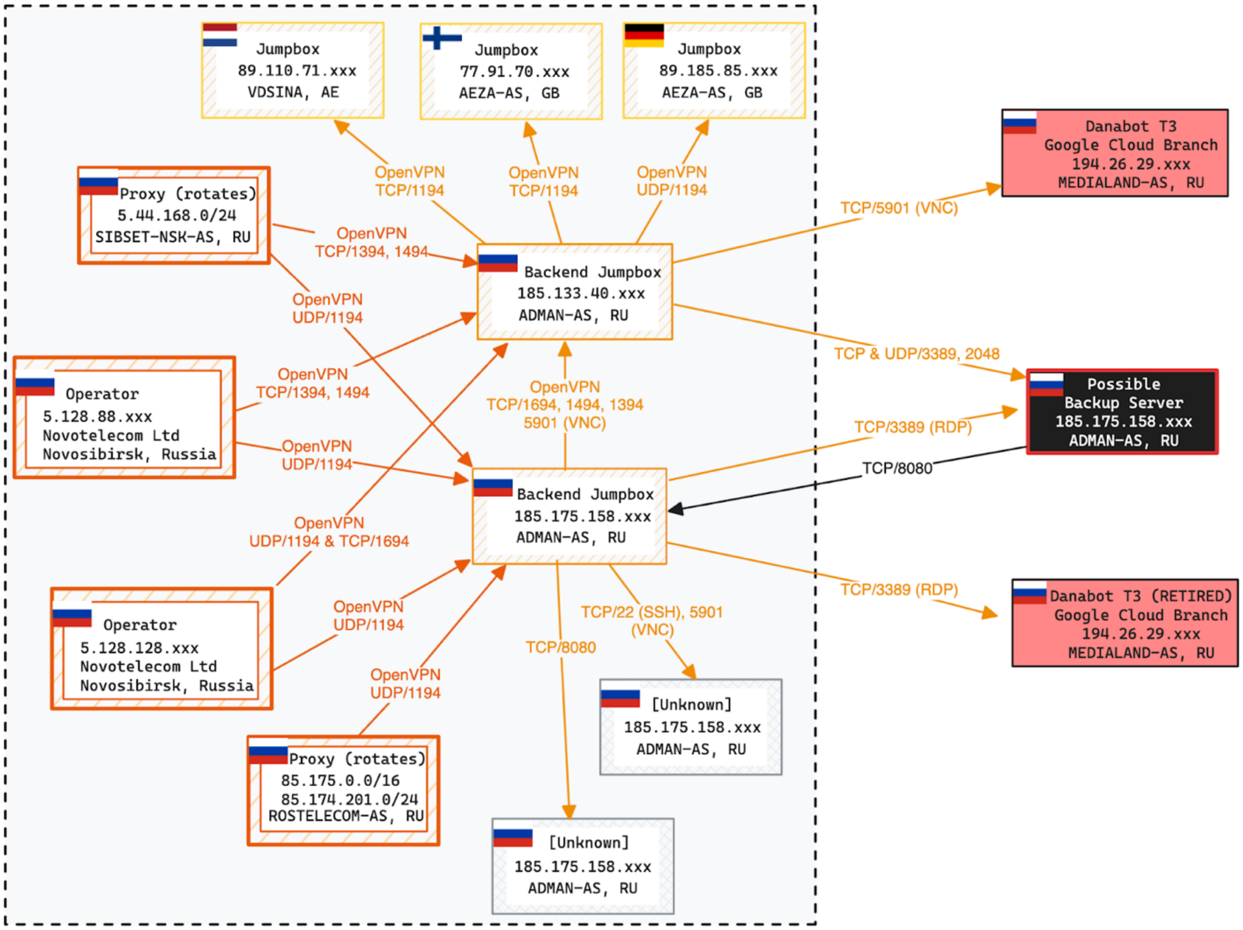

Figure 8: DanaBot backend infrastructure with associated port usage.

Conclusion

It is clear that since emerging in 2018, DanaBot has continued to evolve and persist where many other malware families have not. The operators have shown their commitment to their craft, adapted to detection and changes in enterprise defense, and with later iterations, insulating the C2s in tiers to obfuscate tracking. Throughout this time, they have made the bot more user-friendly with structured pricing and customer support. Black Lotus Labs and Team Cymru, alongside others in the security community, contributed insight into its layered infrastructure through close collaboration with each other and with law enforcement. Operation Endgame II is the most thorough and direct action taken against the botnet to date, and our hope is to show that continued attention by the security community along with collaborative efforts such as these can have an impact in the fight against cybercrime.

A list of C2s is available in the Black Lotus Labs GitHub. We encourage the community to monitor and alert on these and any similar IoCs. Because DanaBot's malware was used by such an array of criminal interests including ransom groups, we advise readers to bolster defenses against phishing as an initial access vector by fully monitoring network resources, ensuring proper patch management and conducting ongoing phishing and social engineering training for employees. We also advise the following:

Corporate Network Defenders:

- Continue to look for attacks on weak credentials and suspicious login attempts, even when they originate from residential IP addresses which bypass geofencing and ASN-based blocking.
- Protect cloud assets from communicating with bots that are attempting to perform password spraying attacks and begin blocking IoCs with Web Application Firewalls.
- Leveraging sophisticated network perimeter countermeasures, which are updated continuously to proactively stop traffic from malicious points from interacting with corporate networks.

Copy Link

Threat Research

The latest articles straight to your inbox

Thank you! You're Subscribed!

Oops! Something went wrong while submitting the form.