Darth Vidar: The Aesir Strike Back

team-cymru.com/post/darth-vidar-the-aesir-strike-back

S2 Research Team June 15, 2023

At the beginning of this year, we released a detailed publication on Vidar infrastructure, encompassing both the primary administrative aspects, and the underlying backend. In that publication, we highlighted three key insights:

1. Russian VPN gateways had the potential to confer anonymity to Vidar operators and customers, thereby rendering it more arduous for analysts to attain a comprehensive understanding of the threat. These gateways were observed to be transitioning towards Tor.

2. There were indications of Vidar operators expanding their infrastructure, necessitating continued vigilance from analysts. We anticipated an influx of new customers and consequently a surge in campaigns in forthcoming weeks.

3. The analysis revealed that Vidar operators had segregated their infrastructure into two distinct components: one dedicated to regular customers and the other specifically catering to the management team, as well as potentially serving premium or high-priority users.

As a refresher, Vidar is an info-stealer malware, which was first spotted in the wild in late 2018 by the security researcher Fumik0. Upon initial inspection, the identified sample appeared to be Arkei (another info-stealer), however differences in both the sample's code and C2 communications were observed. The name itself (Vidar) is derived from a string found in the malware's code, alluding to the Norse god Víðarr. Vidar is considered to be a distinct fork of the Arkei malware family.

As of the end of January 2023 (and as described in our previous blog), Vidar’s administration and backend infrastructure was configured as follows:

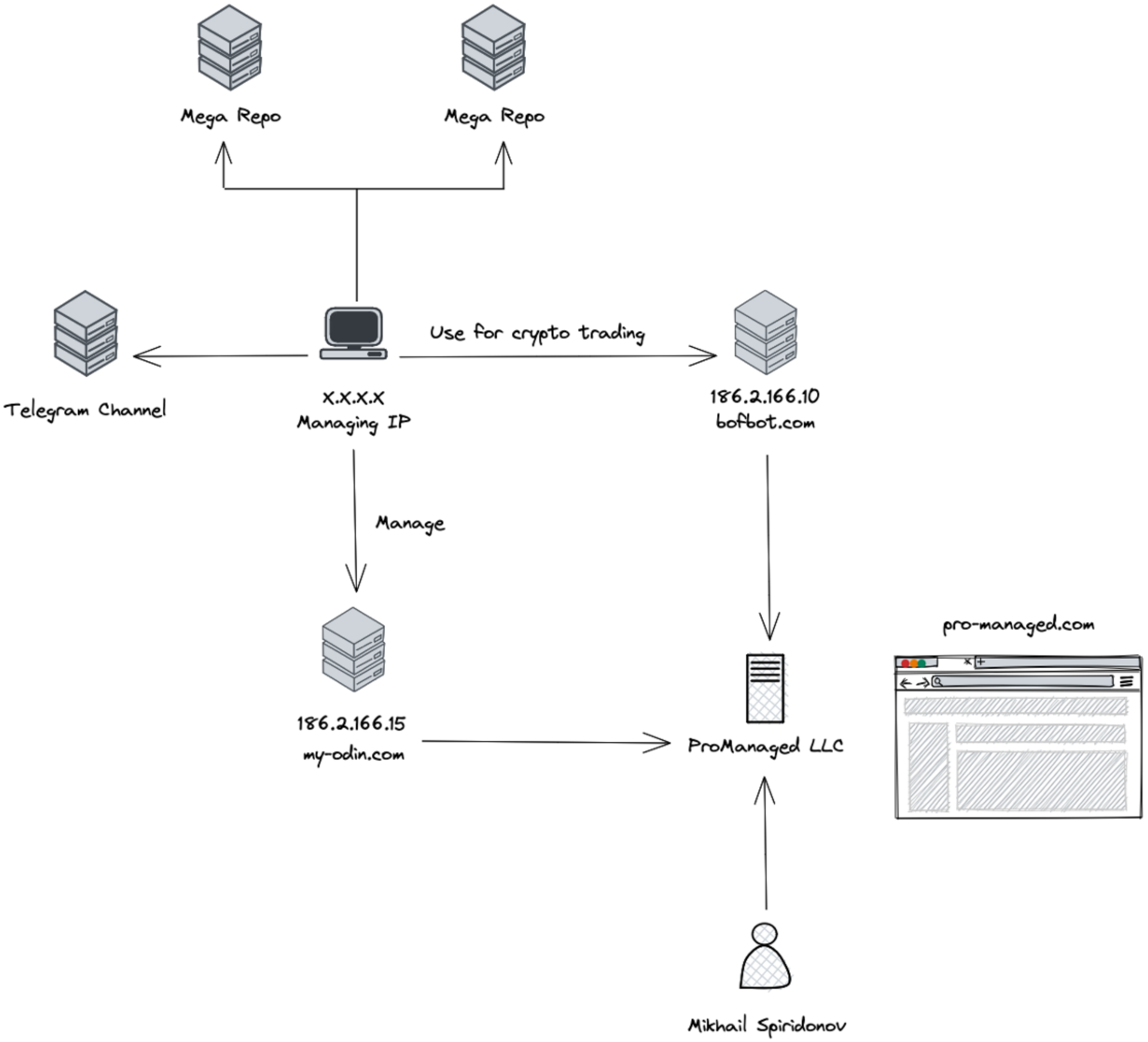


Figure 1: Vidar Infrastructure as of January 2023

Over the past four months, several changes have occurred within this infrastructure configuration. Therefore, the intention of this blog post is to provide a comprehensive update on how Vidar is administered / operated today.

Key Findings

- Vidar threat actors continue to rotate their backend IP infrastructure, favoring providers in Moldova and Russia.

- Evidence suggests that since our last blog post, the threat actors have taken steps to anonymize their activities using public VPN services.
- By tracking the hosting of the main Vidar site (presently **my-odin[.]com**), we are able to monitor other aspects of the threat actors infrastructure, potentially illuminating both affiliates and victims.

Vidar’s Spring Makeover(s)

Since August 2022, Vidar threat actors have utilized the domain **my-odin[.]com** as the primary location for managing various elements of their operation, including affiliate authentication, file sharing, and panel administration. Previously, it was possible to download any files hosted on the URL path /private, such as the bash script responsible for installing the necessary components for a new Vidar campaign, making it possible to monitor malware updates. However, more recently, changes were made whereby if an unauthenticated attempt to download a file occurs, the user is redirected to the Vidar affiliate login page.

In the period since our previous blog post was published, there were two updates to the IP address used to host **my-odin[.]com**. In parallel with these changes, updates were also made to the background infrastructure supporting the Vidar operation, which we will detail below.

Technically speaking, the IP address for **my-odin[.]com** was updated three times, however in the case of the update from **186.2.166.15** (ProManaged LLC) to **5.252.179.201** (MivoCloud SRL) very little else changed, with the infrastructure remaining largely as described in our previous blog post (Figure 1).

March 2023

At the end of March 2023 the IP address was updated from **5.252.179.201** to **5.252.176.49**, with the threat actors continuing their use of MivoCloud SRL-assigned infrastructure. With this transition, other alterations were also made behind the scenes.

The primary IP address (the ‘Managing IP’ in Figure 1) used to manage **5.252.176.49** was accessed via ‘new’ peers, utilizing the Remote Desktop Protocol (RDP). As far as we can tell, this server was previously accessed directly.

From mid-March 2023 onwards, the RDP management activity was sourced from ProtonVPN relays which appeared to be used more broadly by other users, mainly for benign activities.

By using VPN infrastructure, which in at least part was also utilized by numerous other benign users, it is apparent that the Vidar threat actors may be taking steps to anonymize their management activities by hiding in general Internet noise.

In addition to the changes in how the management IP is accessed, we also observed ‘new’ outbound connections from the IP (**5.252.176.49**) hosting **my-odin[.]com**.

Communications with infrastructure associated with ‘**blonk[.]co**’; Blonk is a recruitment platform which utilizes AI to match candidates with opportunities, in the way that dating applications match potential partners. The precise reason for these communications being observed from Vidar management infrastructure is uncertain, however it is plausible that the threat actors may use this platform in their operations; for identifying targets / victims, or perhaps even for recruitment.

Finally, we continued to observe outbound connections to **185.173.93.98**:443, a host located in Russia assigned to Adman LLC. In addition to the TCP/443 traffic it was also observed in GRE tunnelling activity with **5.252.176.49**. This IP (**185.173.93.98**) operates as a conduit between Vidar’s **my-odin[.]com** and *proxy_pass* infrastructure (we detailed *proxy_pass* in our previous blog post).

Figure 2 below summarizes the Vidar infrastructure as of the end of April 2023, as detailed above.

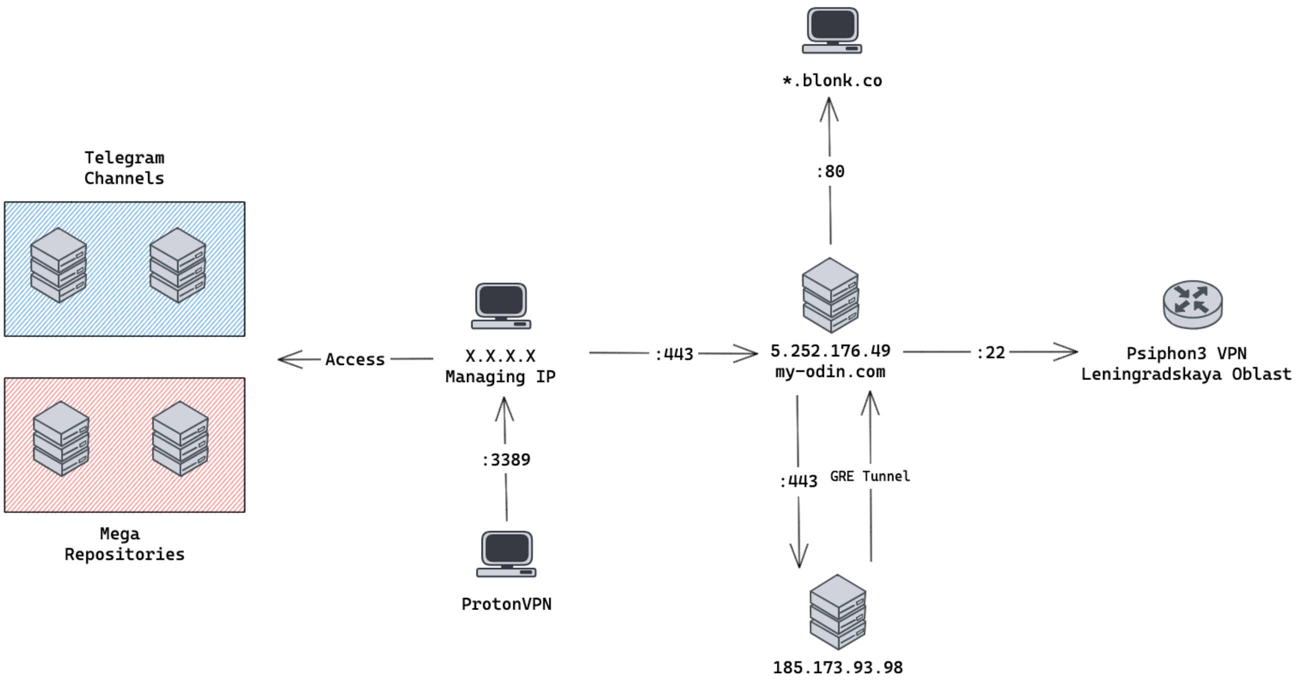
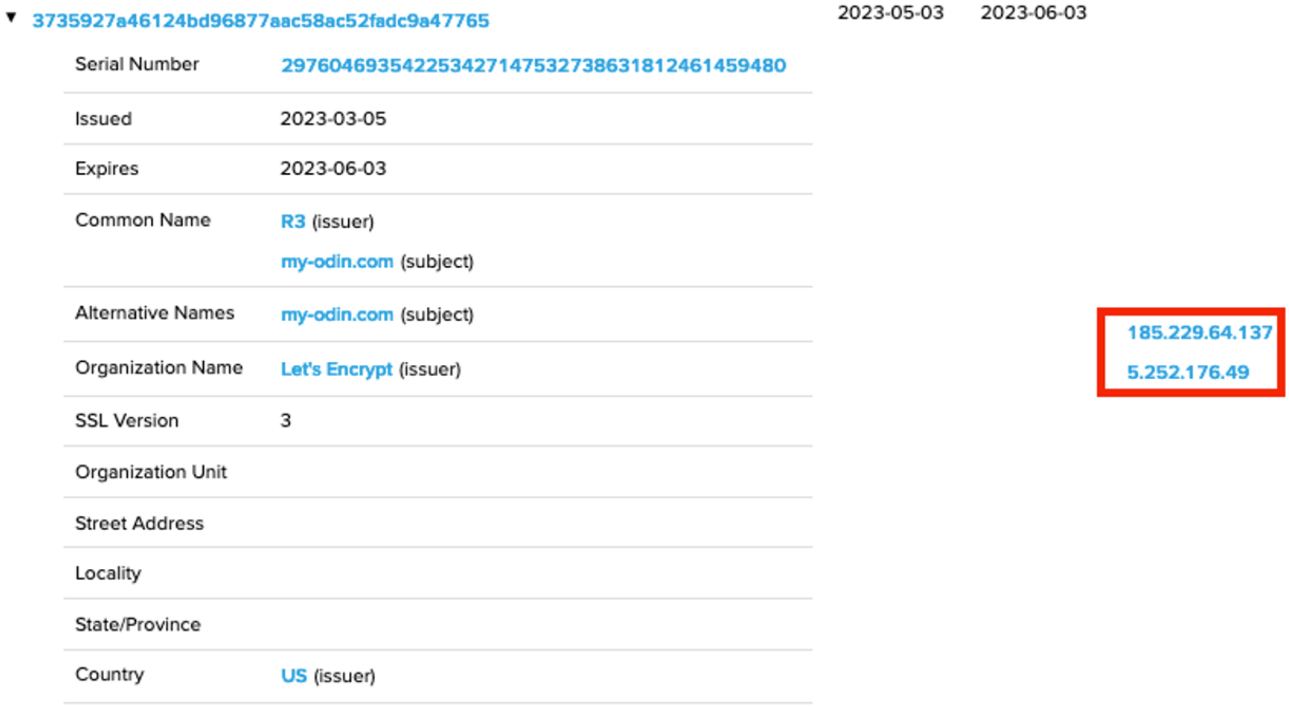


Figure 2: Vidar Infrastructure as of April 2023

May 2023

During May 2023, we observed the initiation of the process to update the hosting IP for **my-odin[.]com** once more. Again (this finding was also documented in our previous blog post) the Vidar threat actors reused the same SSL certificate when transferring infrastructure, revealing the new IP address; **185.229.64.137** (S.C. INFOTECH-GRUP S.R.L.).



▼ 3735927a46124bd96877aac58ac52fadc9a47765 2023-05-03 2023-06-03

Serial Number	297604693542253427147532738631812461459480
Issued	2023-03-05
Expires	2023-06-03
Common Name	R3 (issuer) my-odin.com (subject)
Alternative Names	my-odin.com (subject)
Organization Name	Let's Encrypt (issuer)
SSL Version	3
Organization Unit	
Street Address	
Locality	
State/Province	
Country	US (issuer)

185.229.64.137
5.252.176.49

Figure 3: SSL Certificate for my-odin[.]com

Based on our network telemetry data, we can see that communications with **185.229.64.137** commenced on 03 May 2023; this aligns with other open source passive DNS information for the domain resolution.

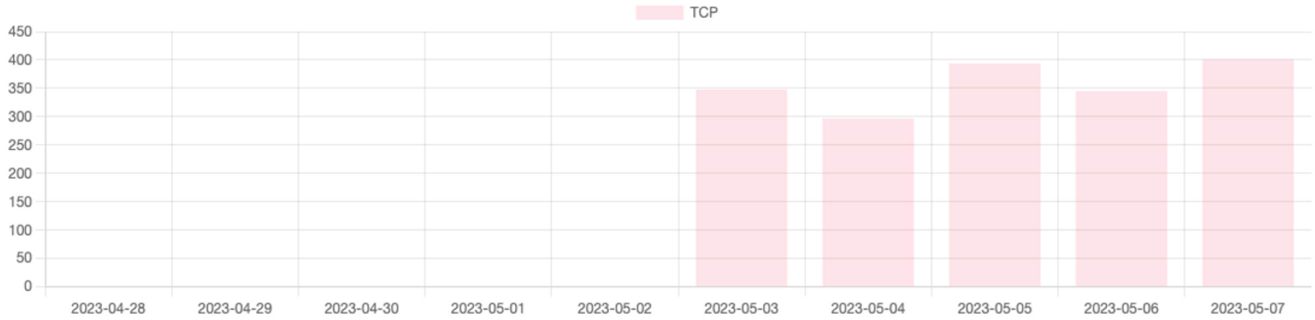


Figure 4: Summarized Communications Involving 185.229.64.137

The behaviour of the new IP address hosting **my-odin[.]com** remains broadly consistent with previous (**5.252.176.49**), however we also observe inbound connections from Tor relays; potentially evidence of Vidar affiliates accessing their accounts / malware repositories.

The change in infrastructure detailed above is summarized in Figure 5 below.

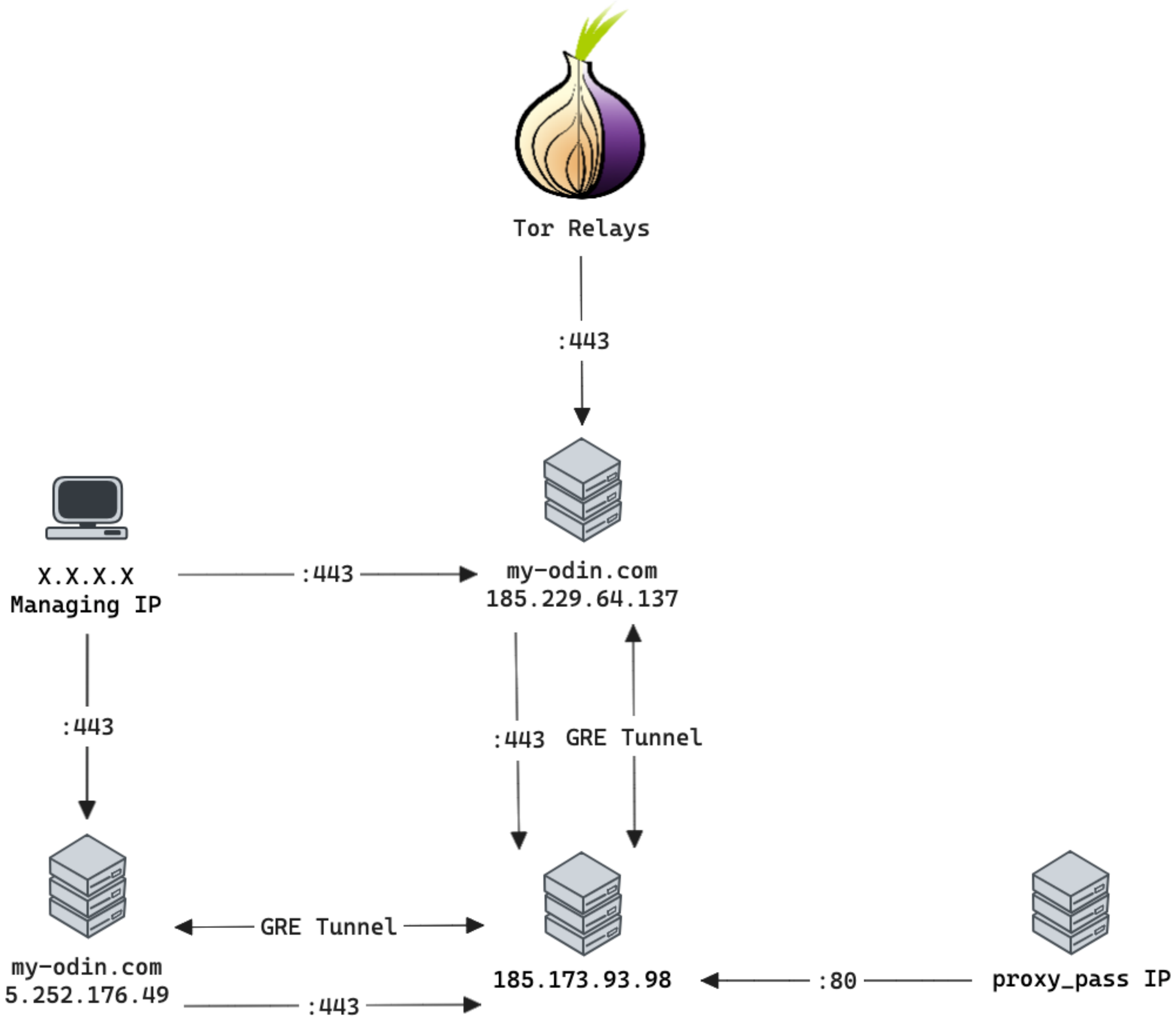


Figure 5: Vidar Infrastructure as of June 2023

Conclusion

This short update provides further insight into the ‘behind-the-scenes’ operation of Vidar, demonstrating the evolution of its management infrastructure as well as evidence of steps taken by the threat actors to potentially cover their tracks. By continuing to track this infrastructure we are able to identify future changes, as well as uncovering evidence which may support victim and/or affiliate identification.

Elements of the infrastructure were redacted from this blog post as investigations are currently ongoing; lower confidence aspects will be shared in the future once confirmation of findings have taken place.

As ever, we will continue to update the community on any new or emergent findings related to Vidar and other connected threats.

Recommendations

> Users of Pure SignalTM Recon and Scout are able to track Vidar management infrastructure by querying for **my-odin[.]com** or the associated hosting IP addresses referenced in this blog post.