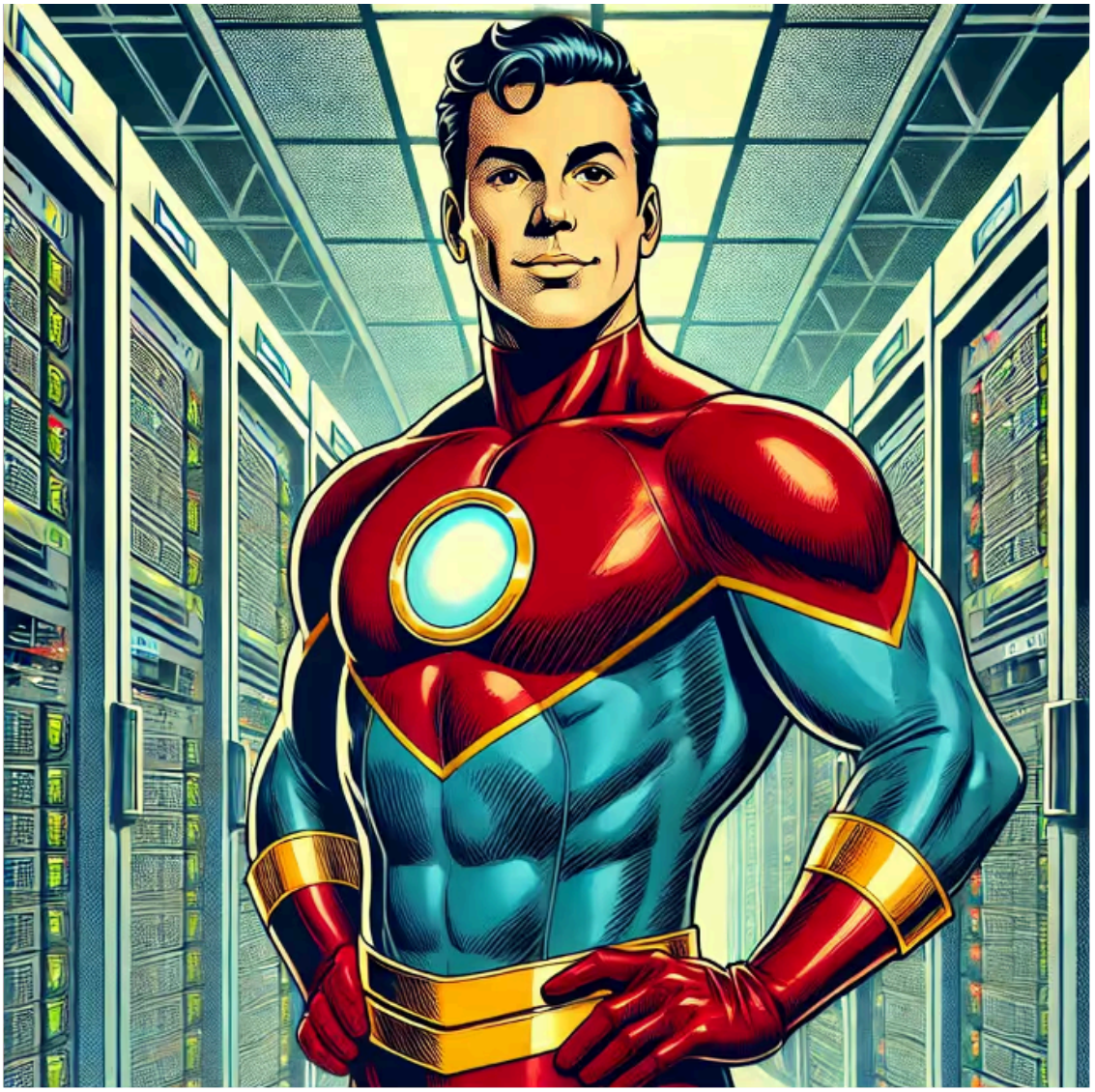
FIN7: The Truth Doesn't Need to be so STARK

By Team Cymru

Published: 2025-04-08 · Archived: 2026-04-05 16:03:41 UTC

First and foremost, our thanks go to the threat research team at Silent Push and the security team at Stark Industries Solutions (referred to as "Stark" from this point forwards) for their enthusiastic cooperation in the 'behind the scenes' efforts of this blog post.



Introduction

In our opening statement, we also introduce the subject of this post: the cross-team and cross-organization collaborative efforts of Silent Push, Stark, and Team Cymru in taking action against a common and well-known adversary, FIN7.

FIN7 is a financially motivated threat group that has been active for more than a decade, targeting a wide variety of sectors during that time. Although disruptive actions have previously been taken against the group, current reports within the CTI community indicate that it remains active today.

Recent research by Silent Push has identified upwards of 4,000 domains that they believe are attributable to either FIN7 or other threat actors mimicking the group's established TTPs (Tactics, Techniques, and Procedures). One notable subsection of their research highlighted the apparent use of infrastructure assigned to Stark for hosting a significant proportion of these domains. This particular finding was picked up by cybersecurity media outlets, notably including KrebsonSecurity, whose post inspired this blog's title.

At this juncture, it is important to note that we have been working directly with Stark for several months to assist in their objective of identifying and reducing abuse activity on their networks.

To ensure appropriate action can be taken, activity that breaches the terms of service outlined by Stark should be reported via email to abuse@stark-industries[.]solutions. We can confirm that there is a human reviewing this mailbox! If direct contact with Stark is not feasible, Team Cymru is happy to act as an intermediary to ensure the requests reach the right people.

The following is an expanded analysis of the findings shared by Silent Push, undertaken in tandem with the security team at Stark.

Key Findings

- Identification of two clusters of potential FIN7 activity, derived from collaborative analysis of indicators originally shared by Silent Push.
- The two clusters indicate communications inbound to FIN7 infrastructure from IP addresses assigned to Post Ltd (Russia) and Smart Ape (Estonia), respectively.
- Identification of 25 Stark-assigned IP addresses used to host domains associated with FIN7 activities.

"Seed" Infrastructure

In support of their research, Silent Push provided 70 indicators (67 domains and 3 IP addresses) of FIN7-related activity. Passive DNS data for the domains showed them resolving to 116 distinct IPs in the 30 days prior to the research's publication. Notably, the majority of the IPs (74%) were assigned to Cloudflare, US, indicating the "true" hosting IPs were likely obscured behind Cloudflare services.

From the overall list, we extracted nine Stark-assigned IPs as follows:

- **103.113.70.142**
- **103.35.189.39** - 2024sharepoint[.]lat, sharepoint2024[.]one
- **103.35.189.46** - ariba[.]business, ariba[.]one
- **103.35.189.90** - dr1v3[.]one, dr1v3[.]top, dr1ve[.]xyz
- **103.35.191.112** - multyimap[.]com
- **103.35.191.28**
- **103.35.191.87** - netepadtee[.]com

- **141.98.168.183** - hotnotepad[.]com
- **86.104.72.16** - thomsonreuter[.]info, thomsonreuter[.]pro, westlaw[.]top

Our first step was to share this information with the security team at Stark, who were able to take prompt action to suspend any services that were still active. Some were no longer being operated by the threat actors at the time of publication.

The initial feedback we received from Stark indicated that the hosts identified by Silent Push were likely procured by the threat actors from one of Stark's resellers. "Stark Industries Solutions" acts as a white label brand under which services are sold, including by distinct entities acting as resellers.

Reseller programs are common in the hosting industry; many of the largest VPS (virtual private server) providers offer such services. Customers procuring infrastructure via resellers generally must follow the terms of service outlined by the "parent" entity.

The nine IPs shared with Stark served as the "seeds" for our investigation to identify and disrupt further FIN7 infrastructure. Using these initial seeds, we expanded our efforts to trace and mitigate additional malicious activities associated with these threat actors.

Infrastructure Discovery

Based on a combination of insights shared by the Stark security team and our own network telemetry data, we were able to identify two clusters of potential upstream activity. This led to the discovery of further FIN7 infrastructure, similar in nature to that shared by Silent Push.

Post Ltd (AS12494)

The first cluster involved four IP addresses assigned to Post Ltd, a broadband provider operating in the Northern Caucasus region in Southern Russia.

Over the past 30 days, we observed these IP addresses communicating with at least 15 Stark-assigned hosts, which we associate with the TTPs referenced in the research by Silent Push. These hosts included **86.104.72.16**, which was in the original list of indicators from Silent Push.

Figure 1 below shows the Stark-assigned IPs identified within this cluster, including resolving domains which we attribute to the same threat actor.

Figure 1 - Post Ltd Cluster

Communications occurred outbound from the Post Ltd IPs to remote TCP/22 on the Stark-assigned hosts. Reviewing metadata for these communications confirmed them to be established connections. This assessment is based on an evaluation of observed TCP flags and sampled data transfer volumes.

Open port information for all 15 Stark-assigned hosts indicated that they had a version of OpenSSH listening on TCP/22 during the time of observed communications. This activity is therefore indicative of potential management activity of the Stark-assigned hosts, initiated via SSH from user(s) of the Post Ltd IPs.

SmartApe (AS62212)

The second cluster involved three IP addresses assigned to SmartApe, a cloud hosting provider operating from Estonia.

Over the past 30 days, we observed these IP addresses communicating with at least 16 Stark-assigned hosts, which we associate with the TTPs referenced in the research by Silent Push. Again, these hosts included **86.104.72.16**.

In addition, 12 of the hosts identified in the Post Ltd cluster were also observed in the SmartApe cluster.

Figure 2 below shows the Stark-assigned IPs identified within this cluster, including resolving domains that we attribute to the same threat actor.

Figure 2 - SmartApe Cluster

Communications occurred outbound from the SmartApe IPs to remote TCP/443 on the Stark-assigned hosts. Again, metadata for these communications confirmed them to be established connections.

Given the nature of the content likely hosted on the Stark-assigned IPs, which in many cases may be some form of spoofed website, it is possible that this cluster is tied to threat researcher activities, accessing potential FIN7 hosts (via TCP/443) to collect information. Alternatively, it is also possible that the SmartApe IPs are used in some capacity for testing purposes, such as verifying if the correct content is delivered when visiting the target site.

For the purposes of our investigation, regardless of the case, the SmartApe IPs provided a vantage point from which to identify potential FIN7-linked activity.

Note: In the case of both clusters, the identified hosts were reported to Stark and the customers' services were suspended.

In addition to the 19 hosts identified in the two clusters described above, insights from Stark's security team led to the discovery of a further six hosts, which we assess to be connected to the same activity.

Details of all identified hosts are provided in the IOC section at the end of this post.

Conclusion

The purpose of this blog post is not to exhaustively identify FIN7 infrastructure; rather, it represents a snapshot in time of activity hosted on the infrastructure of one hosting provider (Stark).

The purpose is twofold:

- To highlight the value of collaboration in expanding our knowledge and understanding of threat activities.
- To demonstrate that efforts can be made to communicate directly with hosting providers who may previously have been considered facilitators of the same threat activities.

Moving forward, we will continue to work closely with Stark to combat FIN7 activities and other threat groups, with a shared goal of reducing abuse of their networks. Similarly, we encourage other threat intelligence organizations to remain proactive in reporting suspicious activities to hosting providers.

As a final point, in the spirit of this blog post we also reported our findings to the other hosting providers mentioned in advance of publication.

Recommendations

- The usual advice applies in relation to the IOCs shared in this blog post - block, hunt, mitigate, remediate.
- It goes without saying that malicious activities should be reported to relevant authorities and hosting providers. As a specific reminder, abuse complaints can be sent to abuse@stark-industries[.]solutions for Stark-related matters.

Indicators of Compromise (IoCs)

IP Address	Domain Name	Cluster
103.35.188.245	2bonmai[.]buzz	Post Ltd
103.35.189.143	ttlpcs[.]lat	Both
103.35.189.38	clio[.]lat	None
103.35.189.38	clio2024[.]top	None
103.35.189.40	ariba[.]lat	Both
103.35.190.215	2024-7zip[.]pw	None
103.35.190.215	7zip2024[.]info	None
103.35.190.40	gogogononono[.]top	Both
103.35.190.40	gogogononono[.]xyz	Both
103.35.190.40	lexisnexis[.]lat	Both
103.35.190.51	dhlpost[.]lat	None
103.35.190.51	dhlpost[.]nl	None
103.35.190.51	dhlpost[.]sbs	None
103.35.191.137	lexis2024[.]info	SmartApe
103.35.191.137	lexis2024[.]pro	SmartApe
103.35.191.137	lexisnex[.]pro	SmartApe
103.35.191.137	lexisnex[.]team	SmartApe
103.35.191.137	lexisnex[.]top	SmartApe

IP Address	Domain Name	Cluster
103.35.191.137	lexisnexis[.]one	SmartApe
103.35.191.137	lexisnexis[.]pro	SmartApe
103.35.191.137	lexisnexis[.]top	SmartApe
176.120.75.99	antispam-ms[.]pro	Post Ltd
45.150.65.100	blackrock-alladin[.]pro	Both
45.150.65.100	wilandsabim[.]info	Both
45.150.65.46	wuriye[.]com	Post Ltd
45.150.67.143	-	None
45.89.53.175	2024aimp[.]info	Both
45.89.53.243	gl-meet2024[.]com	None
45.89.53.243	meet-gl[.]com	None
45.89.53.243	meet-goo[.]net	None
45.89.53.243	meet-goo[.]org	None
45.89.53.243	meet[.]com[.]de	None
45.89.53.243	meet2024[.]com	None
5.180.24.27	gogogogogotests[.]xyz	Both
5.252.22.213	edankhk[.]top	SmartApe
5.252.22.213	miles-and-mroe[.]com	SmartApe
5.252.22.213	otpdank24[.]top	SmartApe
5.252.22.213	unicrebitdank[.]top	SmartApe
5.252.22.213	unicredibank[.]top	SmartApe
86.104.72.125	2024clio[.]one	Both
86.104.72.125	2024clio[.]top	Both

Source: https://www.team-cymru.com/post/fin7-the-truth-doesn-t-need-to-be-so-stark