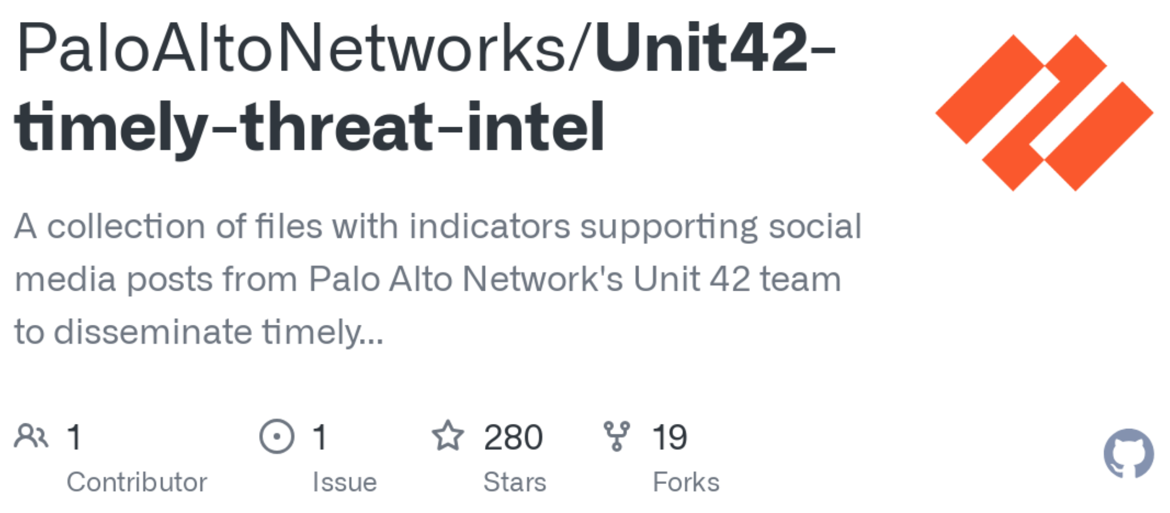
2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt

github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt

PaloAltoNetworks



PaloAltoNetworks/**Unit42-timely-threat-intel**

A collection of files with indicators supporting social media posts from Palo Alto Network's Unit 42 team to disseminate timely...

1 Contributor · 1 Issue · 280 Stars · 19 Forks

CLUSTER OF INFRASTRUCTURE LIKELY USED BY AFFILIATE OF DARK SCORPIUS (BLACK BASTA)

2025-01-21 update: Added 5 additional IP addresses to the C2 server list.

AUTHOR:

- Richard Emerson

REFERENCES:

- https://www.linkedin.com/posts/unit42_darkscorpius-blackbasta-infrastructure-activity-7286133953743241216-4f_O/

- https://x.com/Unit42_Intel/status/1880368272610050459

ORIGINAL REFERENCES:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

- https://www.reliaquest.com/blog/black-basta-social-engineering-technique-microsoft-teams/

SUMMARY:

- In the past 3 months, we've observed a campaign with an infrastructure likely used by an affiliate of Dark Scorpius (the Black Basta ransomware group).

- We have identified 20 IP addresses associated with this attack infrastructure.

DETAILS:

- Since October 2024, we've observed several instances of "email bombing" against different organizations in this campaign.

- Email bombing is a denial of service attack that floods a target's inbox with emails.

- Email bombing is generally used to potentially hide security alerts or other notifications.

- However, these attacks use email bombing to create an IT issue by making targeted email clients unusable.

- After email bombing, attackers initiate a Microsoft Teams chat session pretending to be the victim's help desk or IT department.

- Offering to fix the email problem, attackers instruct victims to install a remote management tool like Microsoft Quick Assist.

- If successful, attackers download a zip archive to the targeted host and extract its contents using Tar for Windows.

- The zip archive contains a copy of Microsoft's Onedrive Standalone Updater, Onedrivestandaloneupdater.exe, and other files that include a malicious DLL named winhttp.dll.

- In an example of DLL side loading, Onedrivestandaloneupdater.exe loads the malicious file named winhttp.dll.

- This malware potentially beacons out to multiple C2 IP addresses.

- We have also observed an added registry key at HKCU\SOFTWARE\TitanPlus storing these C2 IP addresses.

- In at least one instance, this activity led to the deployment of Black Basta ransomware.

IP ADDRESSES ASSOCIATED WITH THE ATTACK INFRASTRUCTURE:

- Our analysis reveals at least 20 IP addresses associated with the infrastructure behind these attacks.

- The following are 25 IP addresses that we believe are used for this campaign.

- 5.78.41[.]255

- 5.181.3[.]164

- 5.181.159[.]48

- 38.180.25[.]3

- 38.180.135[.]232

- 38.180.138[.]15

- 38.180.192[.]243

- 45.8.157[.]146

- 45.8.157[.]158

- 45.8.157[.]162

- 45.8.157[.]199

- 45.128.149[.]32

- 89.185.80[.]86

- 89.185.80[.]170

- 89.185.80[.]251

- 91.90.195[.]91

- 178.236.247[.]173

- 185.190.251[.]16

- 195.123.233[.]19

- 195.123.233[.]148

- 195.123.241[.]24

- 195.211.96[.]135

- 207.90.238[.]46

- 207.90.238[.]52

- 207.90.238[.]67