Turla APT Targets Albania With Backdooor in Ongoing Campaign to Breach European Organizations

Prior to public reporting, infrastructure tied to the Russia-based Turla APT group was present in an organization possibly located in Albania.

File: 7aa5a936a67cf367c0f1e0a22f3290ae57d8af01679daa811bb975c2978ca8a3 contains IP address 91[.]193[.]18[.]120, which is a key indicator of compromise recently described by Cisco Talos as a command and control server used in parallel with the “TinyTurla-NG” (TTNG) backdoor. The file was uploaded manually to the VirusTotal web interface by a user located in Albania, dated March 26.

Analysis reveals the file is indeed a list of IP addresses in a plain text file. It is named “Firewall_Bllok_IP.txt.txt”. Every IP address within is currently listed as malicious, and all but one IP address are registered on multiple Antivirus vendors. The file has no further OSINT links, further suggesting authenticity.

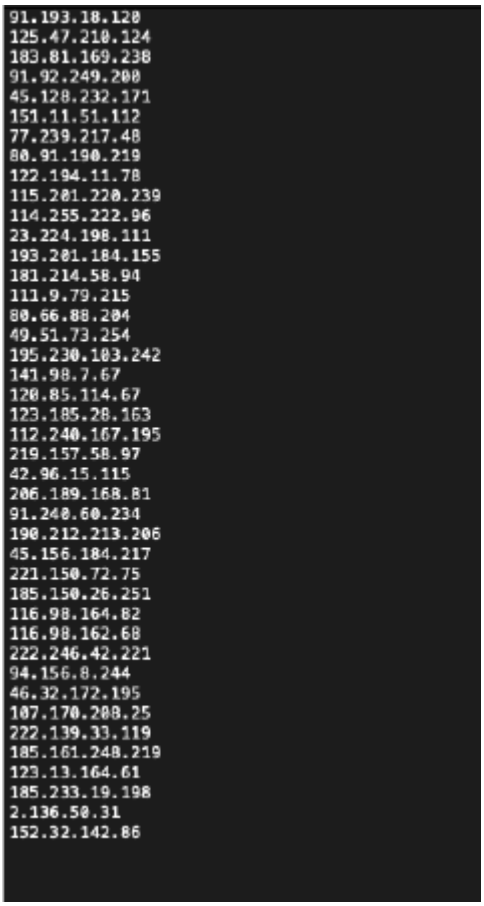

Figure 1 - The plaintext file only lists IP addresses *(click on image to open in separate tab)*.

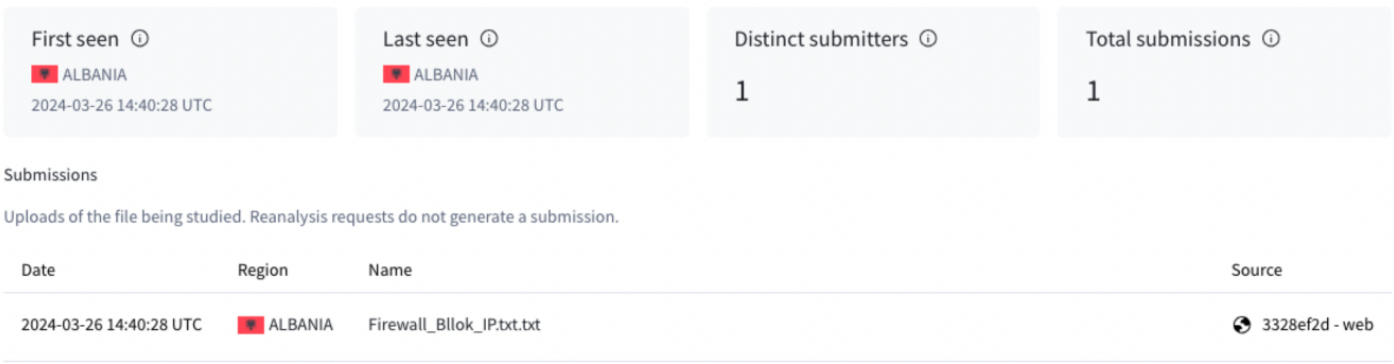

Figure 2 – Unique file uploaded manually from Albania-based IP address on March 26 to the VirusTotal user web interface with ”bllok”(block) written in Albanian.

The upload time falls within two Cisco reports regarding Tiny Turla activity, [1, 2] but prior to IP address 91[.]193[.]18[.]120 being made public. The targeting of Albania aligns with the regional interests of the APT campaign first described mid-February. This new activity provides additional intelligence into the possible scope of Russia-based APT operations, which has also included Poland in this campaign.

Baltic and Eastern European-based organizations with links to government are likely to continue to be high-value targets for cyberattacks throughout 2024 as they provide espionage channels for APT groups aligned to Russian interests in the broader context of the war in Ukraine.

References

[1] Cisco Talos, “TinyTurla Next Generation - Turla APT spies on Polish NGOs.” Accessed: Apr. 2, 2024. [Online]. Available: https://blog.talosintelligence.com/tinyturla-next-generation/

[2] Cisco Talos “New details on TinyTurla’s post-compromise activity reveal full kill chain.” Accessed: Apr. 3, 2024. [Online]. Available: https://blog.talosintelligence.com/tinyturla-full-kill-chain/