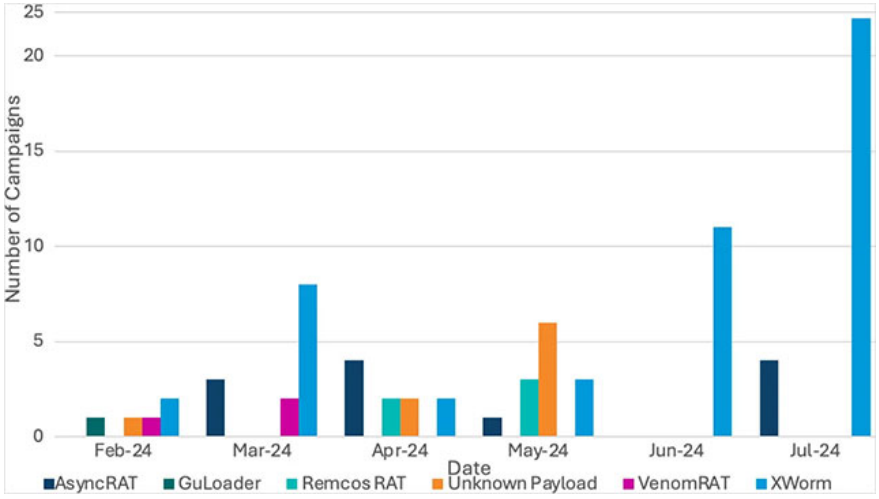
Warning: TryCloudflare is being abused to distribute remote access malware

This cybercriminal activity was first discovered in February this year, taking advantage of the free service TryCloudflare to spread many different RAT strains.

International security researchers are warning that hackers are increasingly abusing the Cloudflare Tunnel service in extremely serious malware campaigns that spread remote access trojans (RAT). .

This cybercriminal activity was first discovered in February this year, taking advantage of the free service TryCloudflare to spread many different RAT strains. We can mention names labeled as highly dangerous such as AsyncRAT, GuLoader, VenomRAT, Remcos RAT and Xworm.

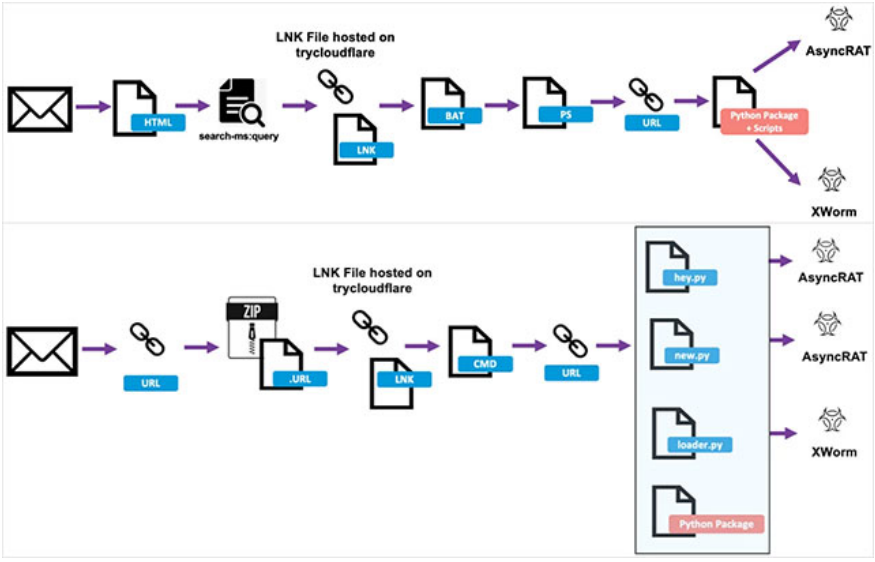


The Cloudflare Tunnel service allows proxying traffic through an encrypted tunnel to access local services and servers over the internet without exposing your IP address. This will come with added security and convenience as there is no need to open any public gateways or establish VPN connections.

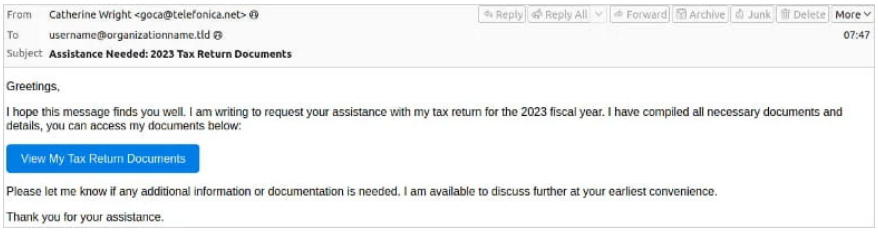
With TryCloudflare, users can create a temporary tunnel to a local server and test the service without needing a Cloudflare account. Each tunnel creates a temporary random subdomain on the trycloudflare.com domain, which is used to route traffic across Cloudflare's network to the local server. In the past, hackers have taken advantage of this feature to remotely access compromised systems while still being able to avoid detection.

A new report from cybersecurity firm Proofpoint says it observed malware activity targeting law, finance, manufacturing, and technology organizations with malicious .LNK files hosted on domains TryCloudflare is legit.

Threat actors are luring targets with tax-themed emails with URLs or attachments leading to the LNK payload. When launched, the payload will run BAT or CMD scripts that deploy PowerShell.



At the final stage of the attack, the Python installer is downloaded for the final payload. Proofpoint reports that the email distribution began on July 11, and distributed more than 1,500 malicious messages.



Hosting LNK files on Cloudflare offers several benefits, including making traffic appear legitimate thanks to the service's reputation. Furthermore, TryCloudflare Tunnel provides anonymity and the subdomains that serve LNK are only temporary, so blocking them doesn't really help much.

Finally, the service is free and reliable, so cybercriminals don't need to incur the costs of setting up their own infrastructure. If automation is used to avoid being blocked by Cloudflare, hackers can exploit those tunnels even for large-scale operations.