03 June 2022

Cybercriminals Exploit Reverse Tunnel Services and URL Shorteners to Launch Large-Scale Phishing Campaigns

Category:	Industry:	Motivation:	Region:	Source*:
Adversary Intelligence	Finance & Banking	Financial	Global	A1

Executive Summary

THREAT	IMPACT	MITIGATION
• Increased malicious use of reverse tunnel services like Ngrok, and URL shorteners like bit.ly, to launch large-scale phishing campaigns. • Malicious sites are hosted from local machines that cannot be traced back to the actors. • Primary targets are banks and their customers.	• Data collected from the phishing sites can be sold on the dark web. • It can also be used to create fake bank accounts and cards. • Many of the links are live only for 24 hours, making it difficult to track the actors. • Loss of trust in banks impersonated by the sites.	• Real-time scans to identify and phishing domains, not just by name, but also by trademarks and images. • Awareness among customers regarding malicious URLs. • Policies to ensure that reverse tunnel service providers assist victims to takedown such sites.

CloudSEK's contextual AI digital risk platform XVigil has identified a surge in phishing sites hosted using reverse tunnel services. In this report, we delve into how threat actors use reverse tunnel services, along with URL shorteners, to orchestrate widespread campaigns, without leaving any traces.

Threat Actors Can Now Launch Untraceable Phishing Campaigns

Reverse tunnel services usher in a new era of phishing by making it easier for threat actors to stay under the radar.

- Threat actors can host phishing pages from their local machine and generate URLs with random names that cannot be detected by regular domain name scanning services.
- URL shorteners to further obfuscate the random domain names and evade detection.
- Since the URLs stay live only for 24 hours, it becomes difficult to track groups and their activities.
- There are no policies that mandate the service providers to monitor or takedown malicious URLs.

Analysis and Attribution

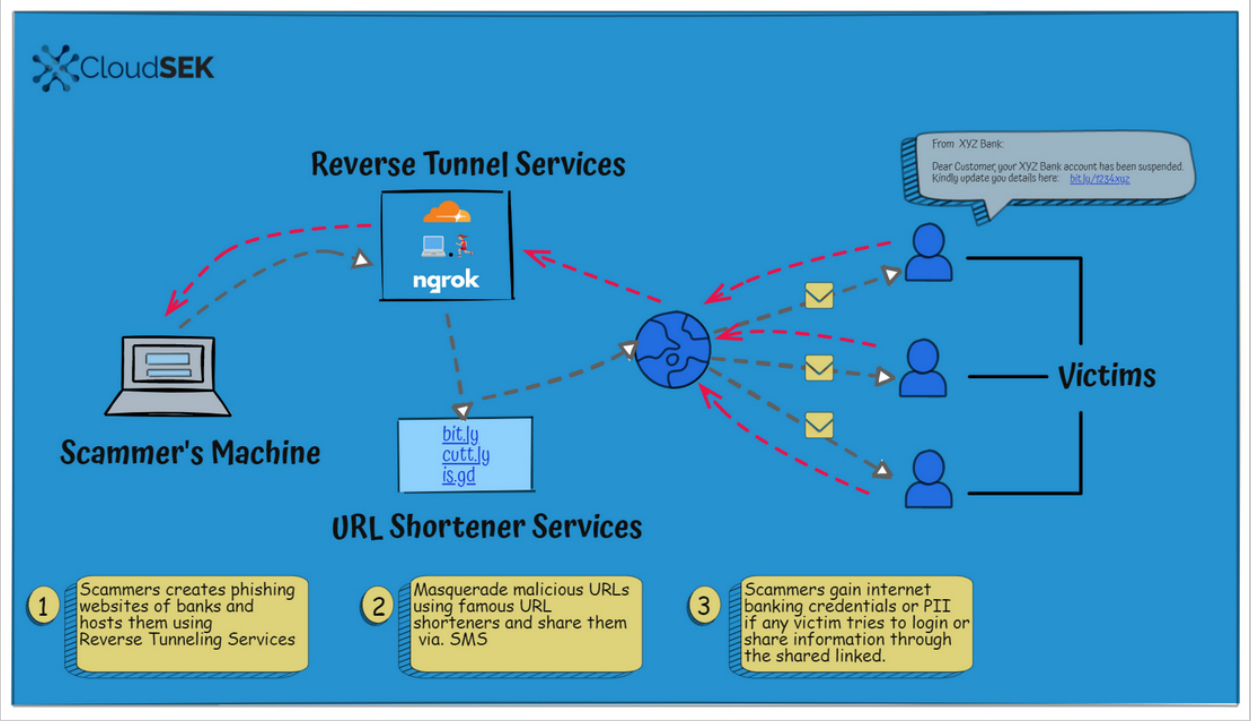
Traditional phishing campaigns require threat actors to register domains with hosting providers. This meant that when a phishing domain was detected and reported to a hosting provider, they were required to takedown the domain and cooperate with law enforcement to track threat actor groups. However, reverse tunnel service providers don't currently have any such accountability. This makes it an especially attractive channel for threat actors to launch large-scale campaigns while remaining anonymous.

CloudSEK's TRIAD (Threat Research & Information Analytics Division) researchers have performed an in-depth analysis of 500+ sites that were hosted and distributed using the following popular reverse tunnel services and URL shorteners:

Reverse Tunnel Services		
Ngrok	LocalhostRun	Try CloudFlare
URL Shortener Services		
Bit[.]Ly	is[.]gd	cutt[.]ly

Our analysis shows that popular Indian banks such as SBI are particularly targeted by threat actors using reverse tunnel services.

Modus Operandi



Modus Operandi of phishing sites hosted using reverse tunnel services

Step 1: A threat actor hosts phishing pages impersonating popular banks from their local machine. They then run reverse tunnel services to make the URLs available to users. The URLs typically have randomized names such as: http://776f-2401-4900-3625-4c7e-540a-4ac4-d992-7867[.]in[.]ngrok[.]io/.

Step 2: The URLs are then simplified using URL shorteners to something innocuous, such as: http://ibit[.]ly/oMwK.

Step 3: Threat actors distribute the simplified URLs via email, text messages, WhatsApp, Telegram, fake social media pages, etc.

> Dear user, your <The Target Bank Name> Account will be suspended! today please update your PAN CARD click here to link https://cutt.ly/ODO2tvB Thank you.

SMS Template displaying message with shortened URL

Step 4: Victims who land on the phishing pages are directed to share sensitive information such as:

- Banking credentials
- Aadhaar card numbers
- PAN card numbers

Step 5: Since most reverse tunnel URLs are live only for 24 hours, threat actors keep the same template, but generate new URLs on a daily basis. Even if a URL is reported or blocked, threat actors can easily host another page, using the same template.

Overview of Popular Reverse Tunnel Services

Cloudflare Reverse Tunnel Service

- Cloudflare's reverse tunnel, named Argo Tunnel, lets anyone expose a server or local system to the internet without opening any ports.
- The reverse tunnel service runs a lightweight process on the user's server that is responsible for creating outbound tunnels to the Cloudflare network.
- Anyone with a Cloudflare account can use this service for free.
- Detailed tutorial and documentation is available on their official website regarding how to set up the Argo Tunnel on a local system.
- Example of a phishing domain hosted using Cloudflare:
    - Submitted URL: https://cutt[.]ly/UDbpGhs
    - Effective URL: http://ultimate-boy-bacterial-generates[.]trycloudflare[.]com/sbi/

Localhost Reverse Tunnel Service

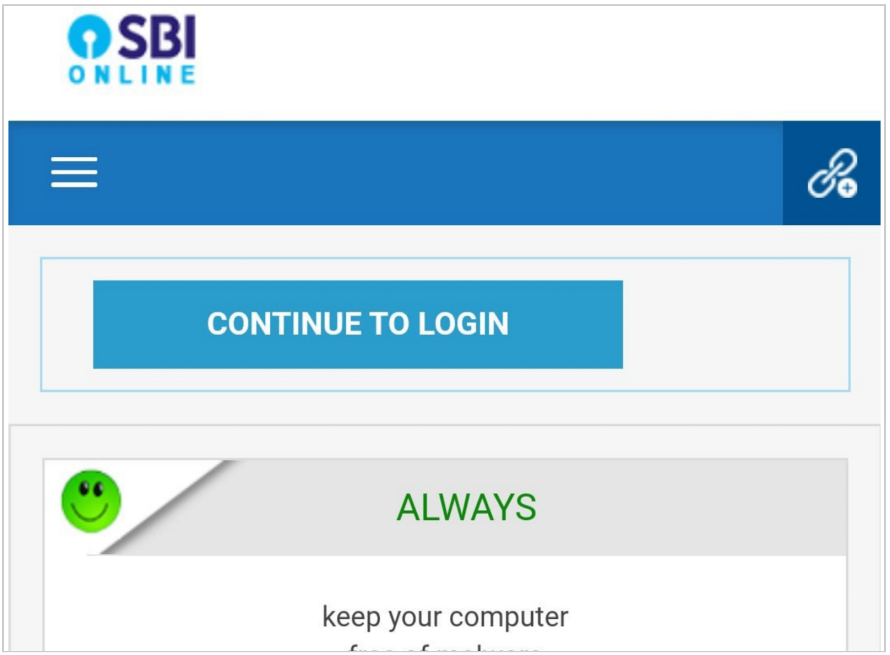
- localhost[.]run is a client-less tool that makes a locally running application available on the internet through a URL.
- This reverse tunnel uses SSH as a client, so no download is necessary to use the service without setting up an account.
- It is capable of forwarding HTTP traffic down to the locally hosted app and automatically adds

encrypted HTTPS endpoints.

- This service comes with Freemium plans and detailed documentation.
- Example of a phishing domain hosted using Localhost:
    - Submitted URL: http://bit[.]ly/3pkBIUn
    - Effective URL: https://585928ab103a05[.]localhost[.]run/

Ngrok Reverse Tunnel Service

- Ngrok is used to expose local servers behind NATs and firewalls to the public internet over a secure reverse tunnel.
- This is a program that can be downloaded on a local machine and run to provide it the port of a network service, generally a web server.
- This service is used for running personal cloud services, hosting demo websites without deploying, for building webhooks, etc.
- It can create a public HTTPS URL for a website running locally on a development machine.
- This service also has Freemium plans that gives users the flexibility to use customized subdomains to End-to-End TLS Tunnels.
- Despite the core logic behind Cloudflare, LocalHost, and Ngrok reverse tunnels' being the same, due to extensive misuse, Ngrok requires a registered account to host HTML content. And the traffic is redirected through dynamically generated subdomain by the reverse tunnel services.
- Example of a phishing domain hosted using Localhost:
    - Submitted URL: http://ibit[.]ly/oMwK
    - Effective URL: http://776f-2401-4900-3625-4c7e-540a-4ac4-d992-7867[.]in[.]ngrok[.]io/



Next Steps

CloudSEK will continue monitoring and deploying proactive scripts to capture publicly submitted URLs that are generated for the subdomains - *.trycloudflare.com, *.ngrok.io, and *.localhost.run/ *.lhr.run and report the malicious activity for the takedown. We will also proactively notify URL shortening services such as cutt.ly, bit.ly, byrl.me, is.gd, shrtco.de, and bitly.ws about malicious URLs using their services.

Impact & Mitigation

Impact	Mitigation
• Data collected from the phishing sites can be sold on the dark web. It can also be used to create fake bank accounts and cards. • Many of the links are live only for 24 hours, making it difficult to track the actors. • Commonly used passwords or weak passwords could lead to brute force attacks. • Loss of trust in organizations impersonated by the phishing pages. • It would equip malicious actors with the details required to launch sophisticated ransomware attacks.	• Awareness among customers should be raised to alert them on clicking only correct URLs and not indistinguishable URLs. • Real-time scans to identify and phishing domains, not just by name, but also by trademarks and images. • Create awareness among customers regarding malicious URLs. • Implementation of policies that ensure reverse tunnel service providers assist victims to takedown such sites.

References

- *https://en.wikipedia.org/wiki/Intelligence_source_and_information_reliability
- #https://en.wikipedia.org/wiki/Traffic_Light_Protocol