Threat Actors Abuse Popular SaaS Products in Phishing Campaigns Targeting BFSI Customers

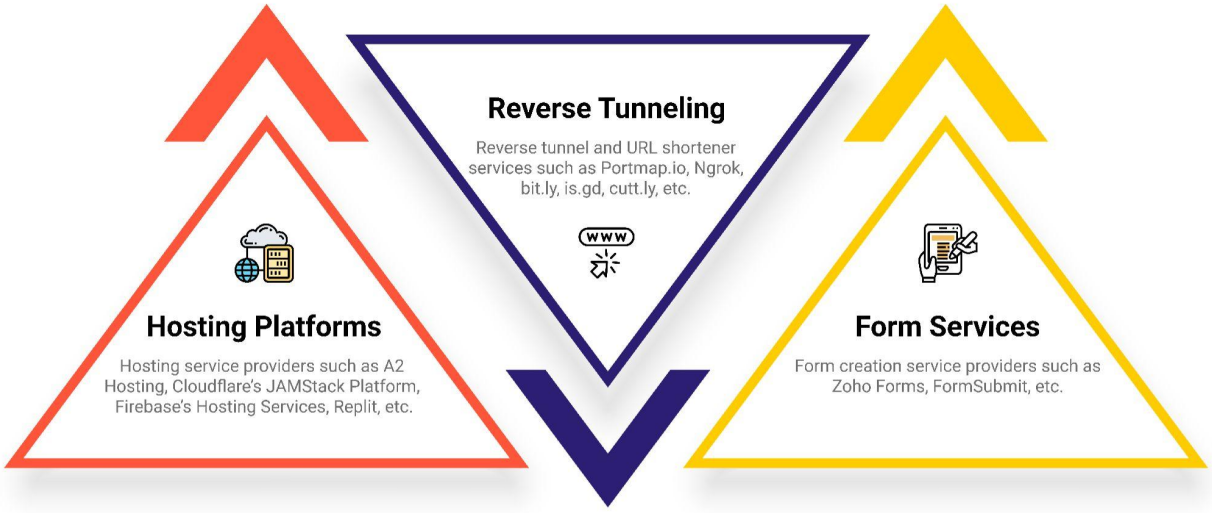
Authors: Anshuman Das
Editor : Hansika Saxena

White papers and reports can be downloaded from CloudSEK website by visiting https://cloudsek.com/whitepapers-reports or by mailing to info@cloudsek.com.

Table of Contents

Rising Popularity of SaaS Products in Phishing Campaigns

Phishing has long proved to be one of the most efficient ways to gather personal information, such as login credentials, credit card numbers, confidential customer data, and intellectual property. The individuals involved in these activities have developed advanced innovative solutions to evade detections and trick innocent users. One such solution is the use of SaaS platforms.



Three types of SaaS services exploited by cybercriminals to target the Indian BFSI sector

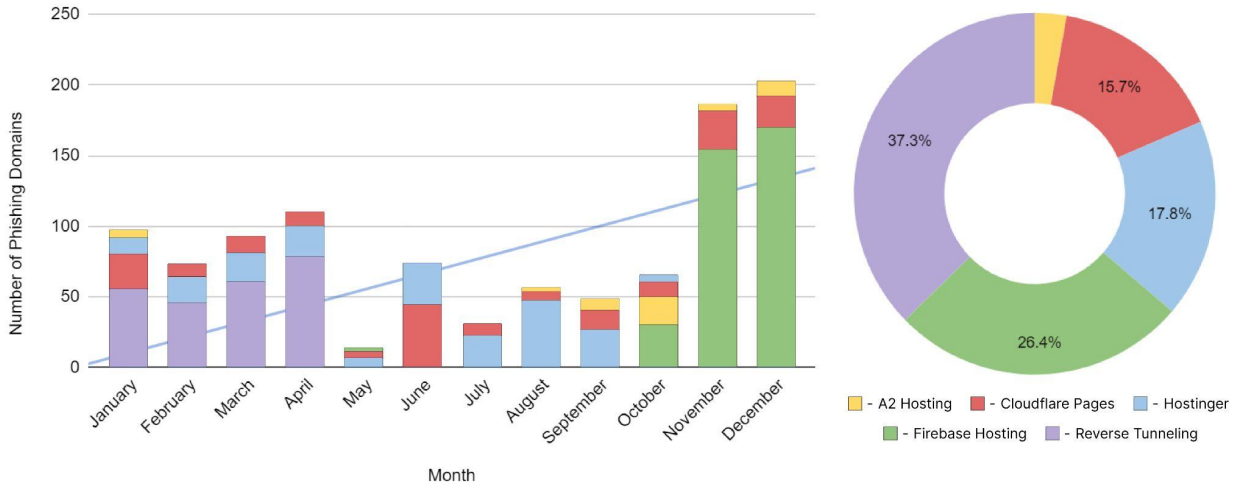
SaaS (Software as a Service) products and services usually offer free or low-cost trials. While this has allowed users across the world to try out services before subscribing or buying the products, it also provides an opportunity for threat actors to pose as legitimate users and misuse the products to defraud consumers. In 2022, researchers at CloudSEK uncovered various freemium SaaS platforms which had been abused by scammers to conduct phishing campaigns **targeting popular brands such as Amazon and Netflix.** Majority of these campaigns were aimed at the Indian BFSI customer.

As hosting providers and cybersecurity tools become sophisticated and capable of identifying phishing domains, threat actors have resorted to using legitimate SaaS* services to host phishing pages at a minimal/ no cost. These short-lived and easy-to-host phishing pages are also difficult to trace back to the actors responsible. In 2022, CloudSEK's TRIAD identified several such incidents, especially targeting banking customers, and released advisories to inform the affected SaaS companies and the public. As this trend continues, we recommend that SaaS companies and consumers stay alert to these tactics in 2023 as well.

Note: All the SaaS companies mentioned in the report are legitimate and are not responsible in any way for threat actors abusing them. Additionally, some companies like Zoho even have a disclaimer that explicitly warns users against sharing credit card details and other sensitive information.

Trends Observed in 2022

Involvement of SaaS platforms in phishing campaigns has accelerated immensely. However, this growth was distributive. While services such as reverse tunneling were constantly exploited, throughout the year, other platforms such as Firebase Hosting and A2 Hosting were more actively exploited in the second half of 2022, as depicted in the graph below*.



Stats derived from the phishing domains analyzed in 2022 by CloudSEK Researchers

***Note: The insights and distribution of SaaS services are contingent on the presence of threats relevant to our clients in 2022.**

Scammers were able to evade detection by cleverly exploiting the following user friendly services provided by each of these platforms.

Service/Platform	Techniques Used to Evade Detection
Hosting Platforms	Free domain preview & temporary domain features provided by these platforms allows scammers to evade detection as the phishing URLs are distributed during the DNS Zone Propagation time & are not available on the internet.
Reverse Tunneling & URL Shorteners	This allows scammers to host phishing pages from their local machine & generate random URLs that cannot be detected by regular domain name scanning services. URL shorteners further obfuscate these & evade detection.
Form Services	The no-code form creation service assisted scammers in creating legitimate looking webpages, hosted on a domain of a third party platform, which are usually not covered in the routine phishing domain scans.

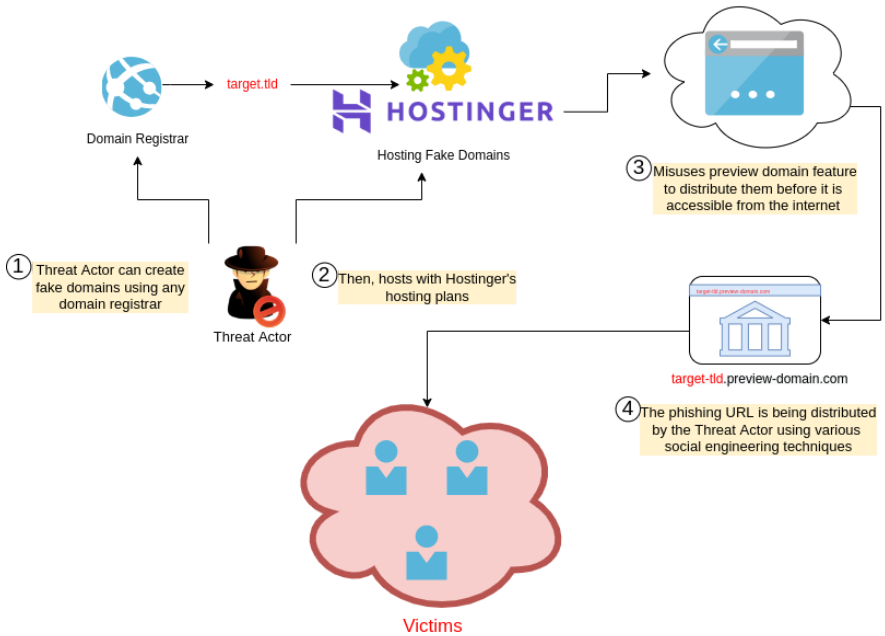
Hosting Platforms

Hosting platforms allow users to build and manage websites that are accessible via the Internet. Threat actors operating phishing campaigns often utilize the services offered by various web hosting platforms to create phishing pages. The methods and modules used from these platforms may vary, a few of which are discussed below.

Abusing Freemium Features

Most web hosting platforms provide certain free-of-cost services as their USP. One such platform is A2 Hosting's temporary domain feature and Hostinger's preview domain feature, where a user can host any kind of website without registering a new domain. Scammers have taken advantage of this feature to host phishing websites that target customers across multiple industries, with a primary focus on the banking sector.

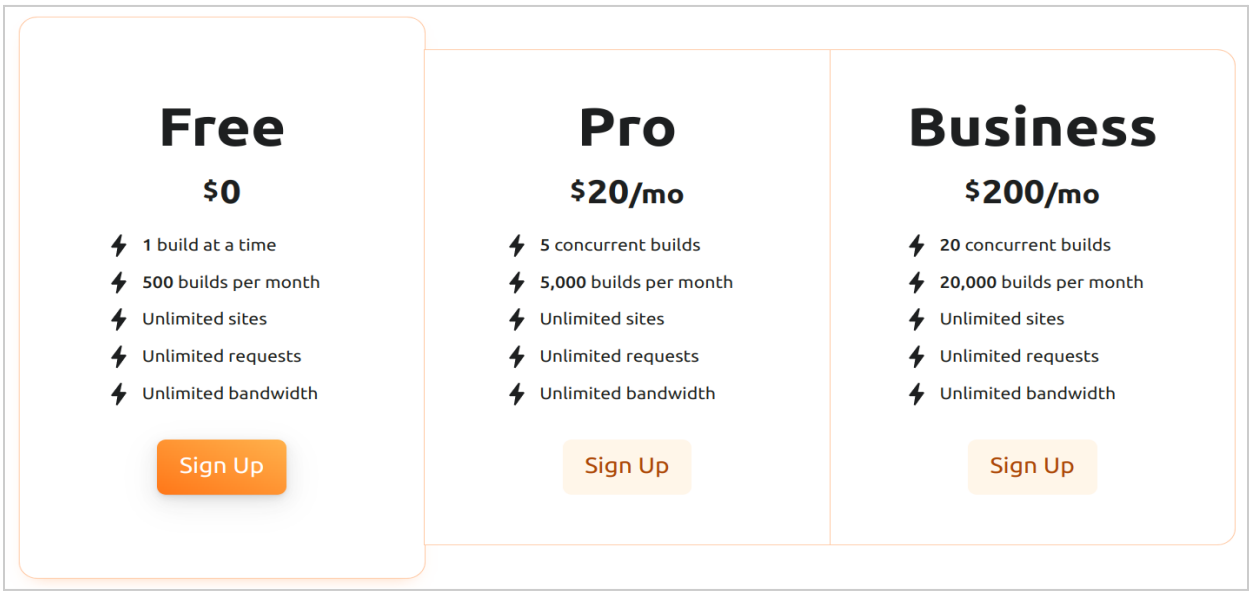
By creating these phishing websites, scammers are able to evade detection and steal individuals' net banking credentials and other PII information like Aadhar card, PAN card, etc. This technique is particularly interesting as it can be challenging to classify the links before a campaign begins on a large scale, as many of them may not be available on the Internet. In 2022, CloudSEK TRIAD conducted an in-depth analysis of **300 such domains** out of which 40 domains were hosted using A2 Hosting's temporary domain functionality and 260 domains were hosted using the Hostinger's preview domain feature.



Modus Operandi of phishing sites hosted using Hostinger's preview domain feature

Abusing Developer-Friendly Features

Cybercriminals always try to use free services for phishing campaigns to maximize their profits. Developer-focused platforms like Cloudflare Pages and Firebase Hosting provide certain features such as GitHub integration, which are easily abused to create phishing domains. In these campaigns also the main motive of the scammers remains the same, i.e. stealing sensitive banking information or PII and then using this information to generate fake KYC accounts or to carry out fraudulent activities via pretexting or vishing techniques. In 2022, CloudSEK TRIAD conducted an in-depth analysis of **57 such domains** targeting the BFSI sector and **over 200 domains** targeting Netflix and Amazon.



Plans for Cloudflare Pages

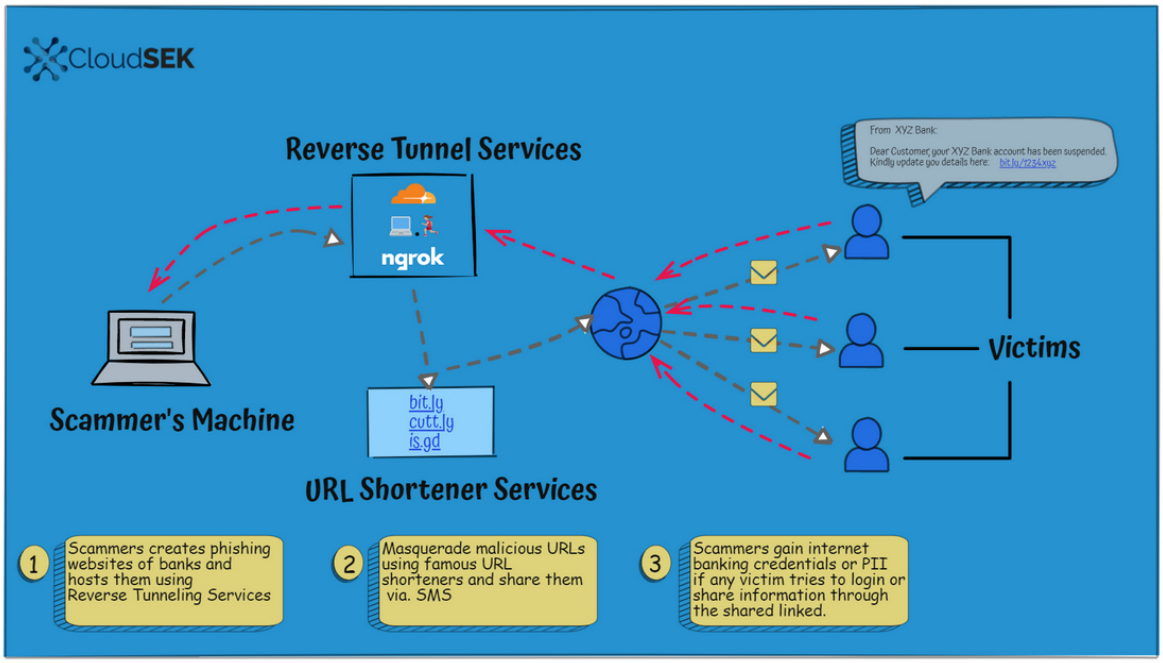
Reverse Tunneling Service Providers

Reverse tunnel services enable threat actors to expose their local server ports to the Internet and serve malicious content to customers. Based on a brief investigation conducted on data collected by XVigil, and across a variety of open-source research feeds that share phishing URLs on a daily basis, CloudSEK

researchers 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	Portmap.io	Try CloudFlare
URL Shortener Services			
Bit[.]Ly	is[.]gd		cutt[.]ly

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. Whereas URL shorteners can further obfuscate the random domain names and evade detection. Since these URLs stay live only for 24 hours, it becomes difficult to track groups and their activities. There are no policies that mandate the reverse tunnel service providers to monitor or takedown malicious URLs. Hence, these have become an attractive channel for threat actors to launch large-scale campaigns.

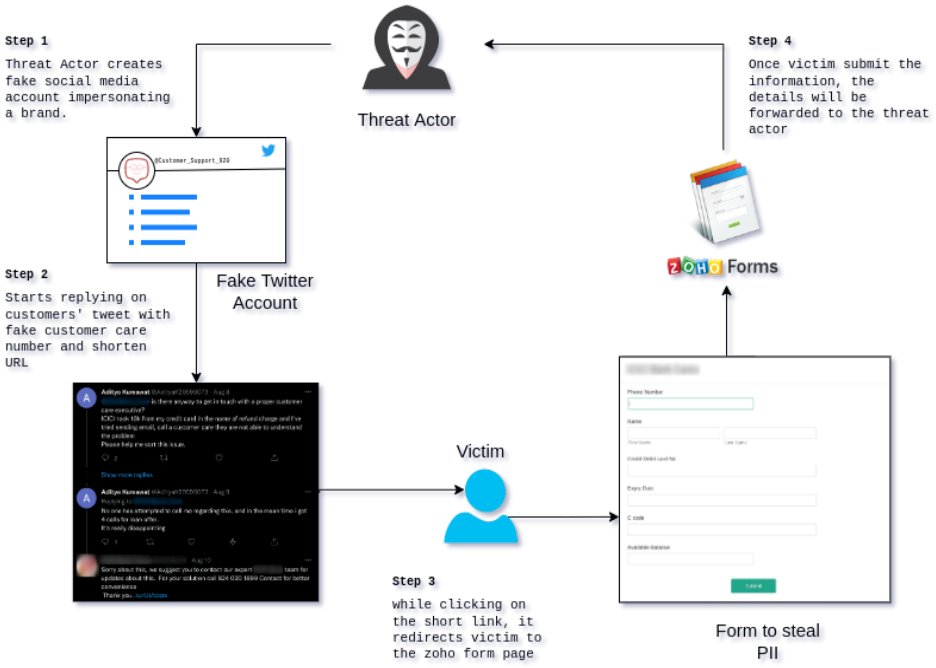


Modus Operandi of phishing sites hosted using reverse tunnel services

Form Services

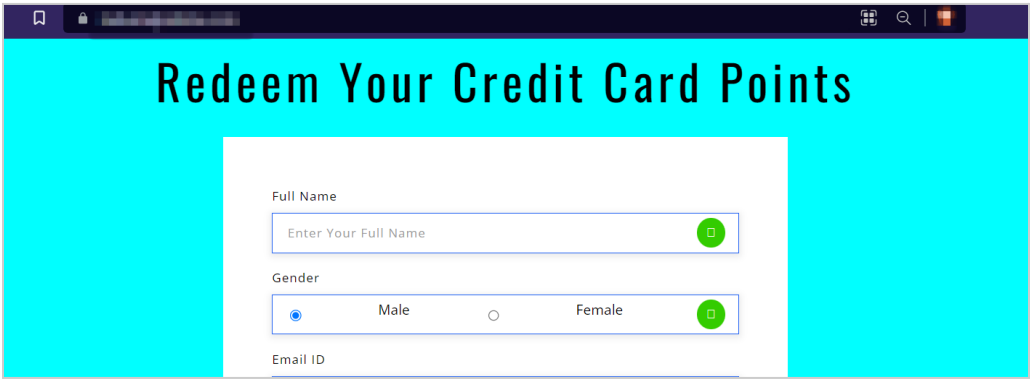
SaaS platforms such as Zoho, FormSubmit, etc., provide no-code form creation services which are designed to send input data from an HTML form straight to a specified email address. During the routine security scans XVigil discovered a Twitter account involved in a new type of phishing campaign where

scammers were misusing Zoho Forms to steal confidential information from banking customers. Further investigation into the incident revealed a series of phishing campaigns operating on a similar modus operandi, as shown below.



The flow of the modus operandi of the scam

Phishing campaigns operated in this manner majorly exploited form services provided by Zoho Form and FormSubmit, primarily to target banking customers. These forms were designed to look legitimate and trick people into entering their PII, such as their name, address, and financial information.



Screenshot of the phishing website used by scammers to steal customers' PII details

Conclusion

Phishing scams are a common sighting in the banking and e-commerce industry. Threat actors behind such campaigns are always on the lookout for festive sale seasons and any new guidelines issued by banks, such as linking Aadhaar details, which can be manipulated to their advantage. With the various

advances in technology, scammers have also begun implementing improvised modus operandi to mislead victims into giving away sensitive information. However, their end goal still remains the same, i.e. to use the stolen information for malicious purposes such as selling it on the dark web, using it to conduct additional social engineering attacks, etc. Oftentimes these details are exploited to carry out unauthorized financial transactions as well.

Most phishing domains nowadays do not contain any keywords which could hint at a particular entity. This helps scammers to evade detection on the basis of keyword searches. Thus, users are required to think proactively before clicking or entering their data into any site. In case of any doubts about a particular detail asked on any website, make sure to contact the concerned company directly and clarify the reason for the required input. In general, it is always important to be vigilant and to practice safe online habits to protect yourself from phishing and other types of cyber fraud.

References

- Scammers Misuse A2 Hosting's Services to Target Indian Banking Customers | Threat Intelligence | CloudSEK
- Cloudflare Pages Misused in a Phishing Campaign Against Indian Banking Customers | Threat Intelligence | CloudSEK
- Hostinger's Preview Domain Feature Abused to Launch Phishing Campaigns and Evade Detection | Threat Intelligence | CloudSEK
- Cybercriminals Exploit Reverse Tunnel Services and URL Shorteners to Launch Large-Scale Phishing Campaigns | CloudSEK
- Scammers Misuse FormSubmit SaaS Platform to Steal PII of Indian Banking Customers | Threat Intelligence | CloudSEK
- Zoho Form Service Leveraged to Exfiltrate Sensitive PII from Banking Customers | Threat Intelligence | CloudSEK
- Free Vector | Triangle shape three steps infographics template
- Hosting Icons & Symbols
- Online registration Icons
- Url Icons & Symbols

Request for a Guided Walkthrough : **Schedule a Demo**

CloudSEK

We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in **2015**

150+ *CloudSters*

2 Offices *HQ in Singapore and R&D in India*

170+ *Clients Globally*

4 *Products*

We secure some of the Fortune 500 and Unicorns

tokopedia · CISION · Reliance Industries Limited · SulAmérica · Olam · NPCI · Fullerton India · certin · TATA COMMUNICATIONS · Paytm · NCR · OLA

... And we are backed by eminent investors

Omidyar Network India · MassMutual Ventures · IDFC Parampara · Startup Xseed · exfinity Venture Partners

Accelerated by

NVIDIA Inception Program

NetApp Excellerator

CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services.

NetApp Excellerator Best Growth Strategy 2019 · ISO 27001 · ISO 22301 · Nasscom Emerge 50 Awards 2020 · Security Product Company of the Year 2020 · Gartner Rated 4.5+ peerinsights · Gartner Peer Insights Customer First

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.

Request a Guided Walkthrough **Schedule a Demo**

CloudSEK

www.cloudsek.com
info@cloudsek.com