KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Phishing campaign targeting Indian Bank Customers

Tracker ID: TN0812 **Date:** 10/Aug/2022 **Category:** Cyber Attack **Industry:** Finance, Banking **Region**: Asia

Background

A new phishing technique employed by threat actors to target customers of Indian banks using preview domains from hosting provider Hostinger has been identified. Its preview domain feature is abused to host phishing sites. Campaigns are hosted on phishing domains and are distributed via text, email, and social media. It uses Hostinger's domain preview tool to avoid discovery. Threat actors are distributing phishing URLs using this functionality throughout the DNS Zone Propagation period.

The Hostinger preview URL structure is domain-tld.preview-domain.com, and the preview domain URLs are momentary mirrors of their root domains. The activation of a new hosting order includes the automatic activation of a preview website feature. The preview URLs are accessible for 120 hours following account creation. The DNS Zone Propagation time, which for Hostinger lasts between 12 and 24 hours, is the interval from the time a domain is registered until it becomes publicly accessible. As compensation for this time, Hostinger offers the domain preview service, which enables users to create and publish their websites on the internet.

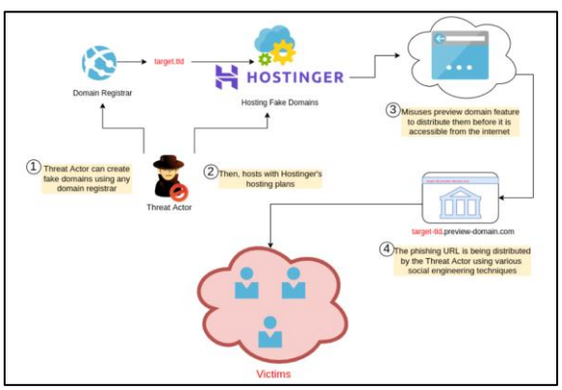

Fig1. Malicious domain hosted at Hostinger

The preview feature allows site access before it is made available globally. It allows you to browse website content without a domain (but after creating an account and adding a domain to host a website). This window of opportunity, as well as the preview domain capability, is used by the actor to distribute phishing URLs and campaigns. Threat actors have launched operations on a regular basis to deceive Indian banking customers, resulting in a loss of revenue and reputation for the impersonated firms. Victims' PII and banking information could be used in additional social engineering scams and identity theft.

Threat actors have launched operations on a regular basis to deceive Indian banking customers, resulting in a loss of revenue and reputation for the impersonated firms. Victims' PII and banking information could be used in additional social engineering scams and identity theft.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

JAESON SCHULTZ AT 8:00 AM

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Phishing campaign targeting Indian Bank Customers

Tracker ID: TN0812 **Date:** 10/Aug/2022 **Category:** Cyber Attack **Industry:** Finance, Banking **Region**: Asia

MITRE ATT&CK Tactics

Initial access, Defense Evasion and Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Validate the IOCs attached and implement the detection & prevention accordingly.
- Deploy measures to identify and take down copy-cat domains. Monitor previously taken down malicious domains.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Educate employees on how to protect themselves from the ongoing phishing threats.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

References

- Hostinger's Preview Domain Feature Abused to Launch Phishing Campaigns and Evade Detection, 04th August 2022, CloudSEK, External Link (cloudsek.com)
- Alessandro Mascellino, Hackers Exploit Hostinger's Preview Domain Feature to Launch Phishing Campaigns, 05th August 2022, InfoSecurity, External Link (infosecurity-magazine.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

JAESON SCHULTZ AT 8:00 AM

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Phishing campaign targeting Indian Bank Customers

Tracker ID: TN0812 **Date:** 10/Aug/2022 **Category:** Cyber Attack **Industry:** Finance, Banking **Region**: Asia

*

Domain
kycfrakyu-online[.]preview-domain[.]com
bankweb-de[.]preview-domain[.]com
kyc451[.]preview-domain[.]com
kycsupports-online[.]preview-domain[.]com
kycsbi-in-net[.]preview-domain[.]com
kycuserks-online[.]preview-domain[.]com
kycsbio-in-net[.]preview-domain[.]com
kycsbiko-com[.]preview-domain[.]com
kycski-online[.]preview-domain[.]com
kycsky-online[.]preview-domain[.]com
kyccsbii-online[.]preview-domain[.]com
kycsbbiyono-com[.]preview-domain[.]com
kyccsbii-com[.]preview-domain[.]com
bankweb-de[.]preview-domain[.]com
bankapp-de[.]preview-domain[.]com
bankstatements-com-au[.]preview-domain[.]com
bankingonlinebpmclient-com[.]preview-domain[.]com
bankingn26-com[.]preview-domain[.]com
bankasol-xyz[.]preview-domain[.]com
bankofamerica-upadteonline-com[.]preview-domain[.]com
bank0famerica-verification-com[.]preview-domain[.]com
Bank0famirecasurfacehelp-com[.]preview-domain[.]com
kycskii-com[.]preview-domain[.]com
kyccsbbiko-com[.]preview-domain[.]com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia