KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Drinik Android trojan impersonating Income Tax Department of India

Tracker ID: TN1101 **Date:** 02/Nov/2022 **Category:** Malware **Industry:** Finance **Region**: Asia

Background

A new Drinik Android trojan has emerged that targets customers of at least 18 Indian banks while masquerading as India's official tax management app to capture victims' PII data and login information. Drinik has been circulating in India as an SMS thief since 2016, and in September 2021, it added banking trojan characteristics targeting 27 financial institutions by redirecting victims to phishing pages. Its developers have upgraded it into a full-fledged Android banking trojan, equipped with keylogging, screen recording, exploitation of accessibility functions, and overlay attack capability.

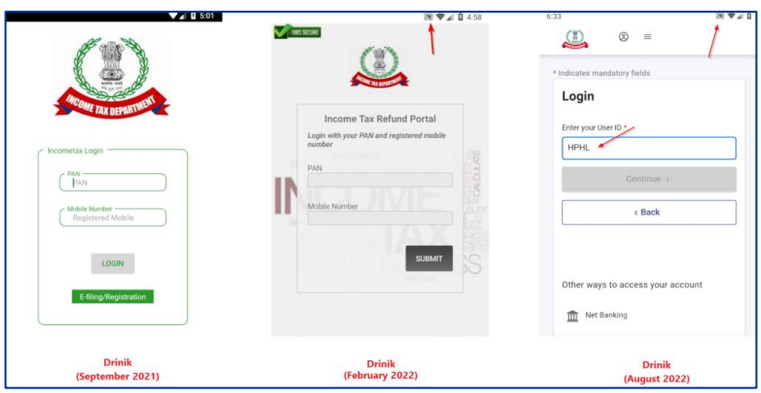

Figure 1: Login Page Drinik malware versions | Source: Cyble

For initial infection, the attacker sends a malicious SMS or email containing a link to a phishing website (similar to the website of the India's Income Tax Department), where the victim is asked to enter personal information and download and install the malicious APK file to complete verification. The malware's latest APK variant, "iAssist," masquerades as the official tax administration tool for India's Income Tax Department.

In an identified incident, it requested permission to read the user's call history, read and write to external storage, and receive, read, and send SMS upon installation. The victim is prompted to allow the app permission to (ab)use the Accessibility Service. If enabled, it deactivates Google Play Protect and uses it to capture the screen, keystrokes, and navigational motions. Rather than launching phishing sites, as earlier versions did, the app eventually accesses the legitimate Indian income tax website using WebView and then steals user credentials by recording the user's screen and employing a keylogger.

Drinik evaluates whether the victim landed at a URL that indicates a successful login to confirm the accuracy of the exfiltrated information (user ID, PAN, and AADHAR). At this point, the victim is presented with a phony dialogue box in which the tax authorities claim they are entitled to a refund of Rs 57,100 ($700) due to earlier tax computation errors and urge them to click the "Apply" button to do so. Victims are then asked to submit financial information, such as account numbers, credit card numbers, CVVs, and card PINs, on a phishing page that looks remarkably like the official Income Tax Department website.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Drinik Android trojan impersonating Income Tax Department of India

Tracker ID: TN1101 **Date:** 02/Nov/2022 **Category:** Malware **Industry:** Finance **Region**: Asia

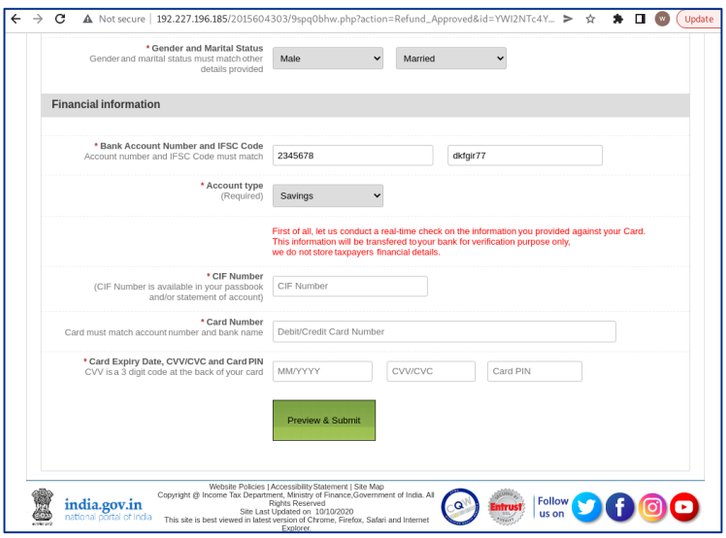

Figure 2 Phishing site asking for financial information Page | Source: Cyble

It continuously searches the Accessibility Service for events related to banking apps to be targeted. If a match is found, the malware extracts user credentials from keylogging data and transfers them to the C2 server. During this assault, Drinik uses the "CallScreeningService" to prevent incoming calls from interfering with the login process and data-stealing procedure. SBI (State Bank of India) is one of the targeted banks.

Drinik isn't as sophisticated or advanced as other banking trojans, but its developers are continuously adding capabilities that make it harder to detect. Considering Drinik targets Indian taxpayers and banking clients, each new successful feature could result in huge financial rewards for the malware's developers. As, malware is constantly evolving, a novel variation with new targets and techniques is almost certain to arise. We highly advise users not to download or install software from unauthorized sources and to be cautious when opening links sent by SMS or email.

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Discovery, Impact, Collection, Persistence, Impact, Credential Access, Exfiltration.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Drinik Android trojan impersonating Income Tax Department of India

Tracker ID: TN1101 **Date:** 02/Nov/2022 **Category:** Malware **Industry:** Finance **Region**: Asia

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.
- Download and install software only from official app stores or websites like Play Store or the iOS App Store.
- Be wary of opening any links received via SMS or emails delivered to you and be careful while enabling any permissions
- Never share your Card Details, CVV number, Card PIN, and Net Banking Credentials with an untrusted source.
- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device to avoid unauthorized access obtained using malicious activities such as keylogging and screen recording.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Cyble, Drinik Malware Returns With Advanced Capabilities Targeting Indian Taxpayers, Cyble Blogs, 27th October 2022, External Link (blog.cyble.com).
- Cyble, Fake Income Tax Application Targets Indian Taxpayers, Cyble Blogs, 07th September 2021, External Link (blog.cyble.com).
- Cert-IN, Drinik Android malware targeting Indian banking users, masquerades as Income Tax refund, 21st September 2021, External Link (www.cert-in.org.in).
- Bill Toulas, Drinik Android malware now targets users of 18 Indian banks, Bleeping Computer, 27th October 2022, External Link (www.bleepingcomputer.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 9176471471

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Drinik Android trojan impersonating Income Tax Department of India

Tracker ID: TN1101 **Date:** 02/Nov/2022 **Category:** Malware **Industry:** Finance **Region**: Asia

*

SHA256 Hash	MD5 Hash	URL	IP
86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523	0c6257e385f33e46c1839f59bc4b53d7	hxxp://gia.3utilities[.]com	198[.]12.107[.]13
		hxxp://192[.]227.196.185	