KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Typosquat Campaign
Targeting Windows and Android Users

Tracker ID: TN1102 **Date:** 07/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

Over 200 typosquatting domains that mimic 27 different brands are identified in a large-scale, malicious operation that deceives victims into downloading malware for Windows and Android. Typosquatting is the time-honored practice of registering a domain name that is identical to those of legitimate brands to trick visitors into accessing a fraudulent website. This campaign includes over 90 websites that appear to be from well-known businesses. The campaign's aims include the dissemination of Windows and Android malware, along with the theft of cryptocurrency recovery keys.

The domains employed in this campaign are quite similar to the genuine ones, with only a single letter modified or an extra "s," making them challenging for individuals to notice. It's not uncommon for victims to mistype the URLs into their browsers, leading them to these sites. However, phishing emails, SMS, direct messaging, malicious social media and forum posts, and other tactics could steer individuals to such websites.

Malicious websites impersonating well-known Android app stores, such as Google Play, APKCombo, and APKPure, were found along with the download pages for PayPal, VidMate, Snapchat, and TikTok. There are websites that imitate the well-known Microsoft Visual Studio Code, the open-source Thunderbird email client, and the Brave web browser to remove Vidar Stealer. In most of these instances, ERMAC, a banking trojan was found. It targets banking accounts and cryptocurrency wallets and infects individuals attempting to download the APKs.

The range of malware families distributed to victims indicates that campaign operators try different strains to determine which one performs best. The typosquat website for the well-known Notepad++ text editor is also idenfied. It uses the domain "notepads-plus-plus[.]org," which is only one character different from the actual site's domain "notepad-plus-plus.org." Furthermore, the downloads from this website install the Vidar Stealer, an information-stealing malware that has inflated to 700MB to evade detection. Another website uncovered by the researchers impersonates the Tor Project that uses the "tocproject.com" name, and the website disables the RAT and keylogger from Agent Tesla.

Other sites in the campaign spoof well-known cryptocurrency wallets, trading apps, and NFT sites in an attempt to attract cryptocurrency owners and digital asset investors. These domains are only a fraction of the whole network of domains used in the campaign because threat actors use multiple variations of each name to cover as many mistypes as possible. Some browsers, including Microsoft Edge and Google Chrome, have typosquatting prevention. To avoid typosquatting domains, the simplest method for identifying a reputable site is to use a search engine to look for a specific brand. Furthermore, visitors should be cautions and avoid clicking on adverts displayed in search results as fraudulent ads could have been generated to spoof a legitimate site.

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.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Typosquat Campaign
Targeting Windows and Android Users

Tracker ID: TN1102 **Date:** 07/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Indicators of Compromise

Please refer to the attached sheet for IOCs.

MITRE ATT&CK Tactics

Initial Access, Delivery, Defense Evasion, Data Exfiltration and Execution.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Be wary of opening any links received via SMS or emails delivered to you and be careful while enabling any permissions.
- Download and install software only from official app stores or websites like Play Store or the iOS App Store.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Turn on the automatic software update feature on your computer, mobile, and other connected device.
- Regularly monitor your financial transactions and contact your bank immediately if you notice any suspicious activity.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Bill Toulas, Typosquat campaign mimics 27 brands to push Windows, Android malware, Bleeping Computer, 23rd October 2022, External Link (bleepingcomputer.com)
- ERMAC Android Malware Increasingly Active, Cyble, 18th October 2022, External Link (blog.cyble.com)

KPMG in India Cyber Response Hotline : +91 9176471471

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.

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.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

Tracker ID: TN1102 **Date:** 07/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

*

URL	SHA256 Hash	MD5	IP
hxxp://apk-combos[.]com/	8e9a45e5ac00332d83afa5efb5c5ed92e38280c7da7b7a5f6ae5577e2271cb26	8692e3212dc590c254020450bdee7003	103[.]109.101[.]137
hxxps://paltpal-apk[.]com/		1b9600d9ba73aeb09bd8d75bd1ae73d75eac6232	
hxxps://m-apkpures[.]com/			
hxxps://payce-google[.]com/			
hxxp://payse-google[.]com/			
hxxps://vidmates-app[.]com/			
hxxps://app-vidmates[.]com/			
hxxp://www.app-vidmates[.]link/			
hxxp://app-vidmate[.]com/			
hxxps://snacpchat-apk[.]com/			
hxxp://193.106.191[.]121:3434/yy.php/			
hxxp://193.106.191[.]121/			

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.

This document is for e-communication only.