Cyble ERMAC Android Malware Increasingly Active

By cybleinc

Published: 2022-10-18 · Archived: 2026-04-05 21:14:12 UTC

CRIL Investigates the resurgence of ERMAC Android Malware as an increasing number of users are falling prey to their phishing attacks.

Android Users targeted through multiple Phishing themes

Cyble Research & Intelligence Labs (CRIL) recently identified a mass phishing campaign that delivers malicious Android executables. While investigating the samples, we identified these as ERMAC Banking Trojans.

ERMAC is an Android Banking Trojan that was first discovered in late August 2021, when it was found targeting Poland. The latest version of ERMAC 2.0 targets 467 applications and Threat Actor was renting it out for **$5K/month** on a cybercrime forum.

Phishing Campaign Analysis

The campaign uses phishing websites that download fake applications that impersonate Google Wallet, PayPal, and Snapchat and trick the users into downloading and installing the malicious ERMAC APK on their Android devices.

As part of the phishing campaign, the TA has registered specific typosquatted domains of popular Android application hosting platforms such as Google PlayStore, APKPure, APKCombo, etc. The below image shows the Whois information of the IP address 103[.]109.101[.]137 hosting these phishing websites.

```
% Abuse contact for '103.109.100.0 - 103.109.103.255' is 'abuse@koddos.net'

inetnum:        103.109.100.0 - 103.109.103.255
netname:        AMARUTU-AP
descr:          102 Aarti Chambers,
descr:          Mont Fleuri,
country:        HK
org:            ORG-ATL8-AP
admin-c:        ATLA6-AP
tech-c:         ATLA6-AP
abuse-c:        AA1821-AP
status:         ALLOCATED PORTABLE
remarks:        ------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ------------------------------------------------------
mnt-by:         APNIC-HM
mnt-lower:      MAINT-AMARUTU-AP
mnt-routes:     MAINT-AMARUTU-AP
mnt-irt:        IRT-AMARUTU-AP
last-modified:  2020-07-14T13:16:34Z
source:         APNIC
```

Figure 1 – Whois Information of IP Address

The image below shows how the TA mimics the Google Play Store page, which downloads a malicious Android APK, masquerading as a Google wallet when the user clicks on the “Install” button.

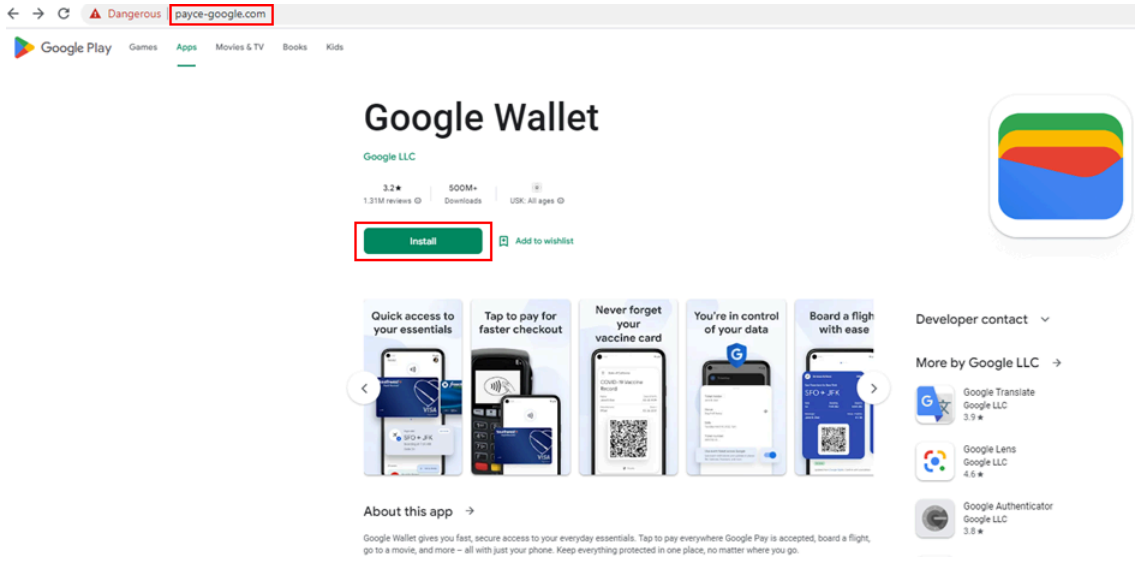

Figure 2 – Google Play Store Phishing Website

“Apkpure” is a third-party Android Application hub where Android applications can be hosted and downloaded for free. The image below mimics the Apkpure Android application Store page, which downloads a malicious Android APK, masquerading as a PayPal application.

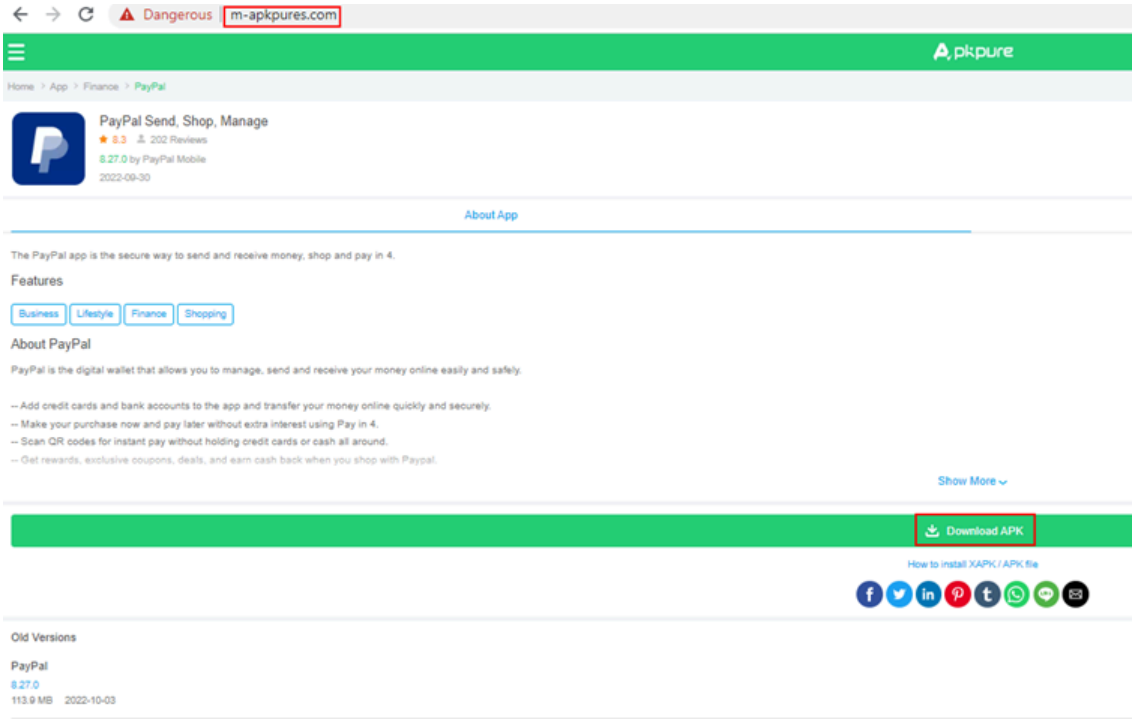

Figure 3 – Apkpure Phishing Website

Similar to Apkpure, APKCombo is also a free Android Application hosting place. The below image mimics the APKCombo Android application Store page, which downloads a malicious Android APK, masquerading as a trading application.

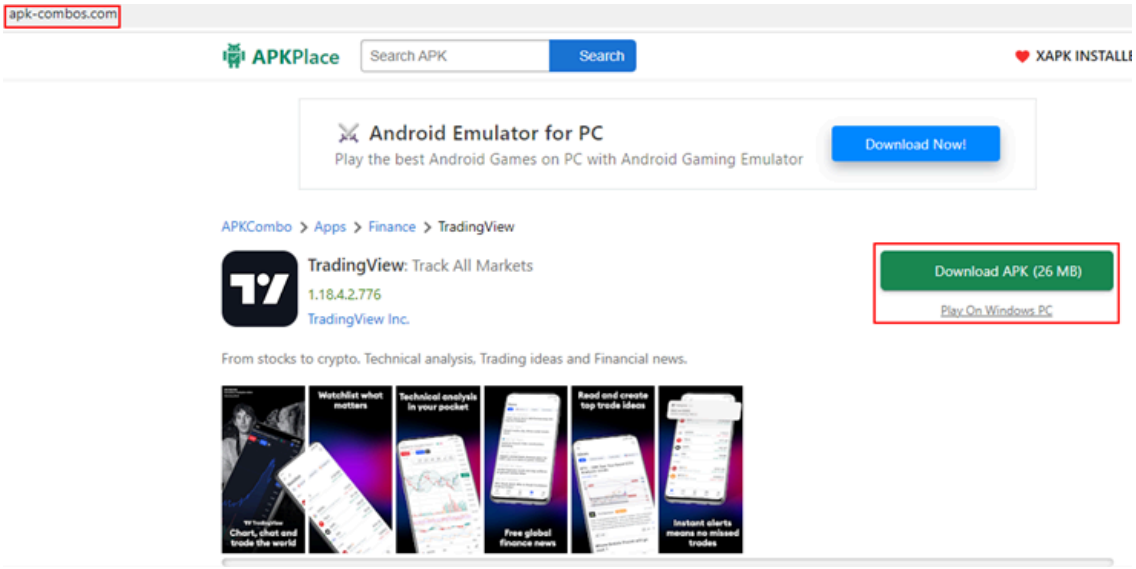

Figure 4 – APKCombo Phishing Website

The TA also created a phishing website to target PayPal users. The below image shows a fake website that downloads a malicious Android APK, masquerading as a PayPal application when the user clicks on the "*Download*" button.

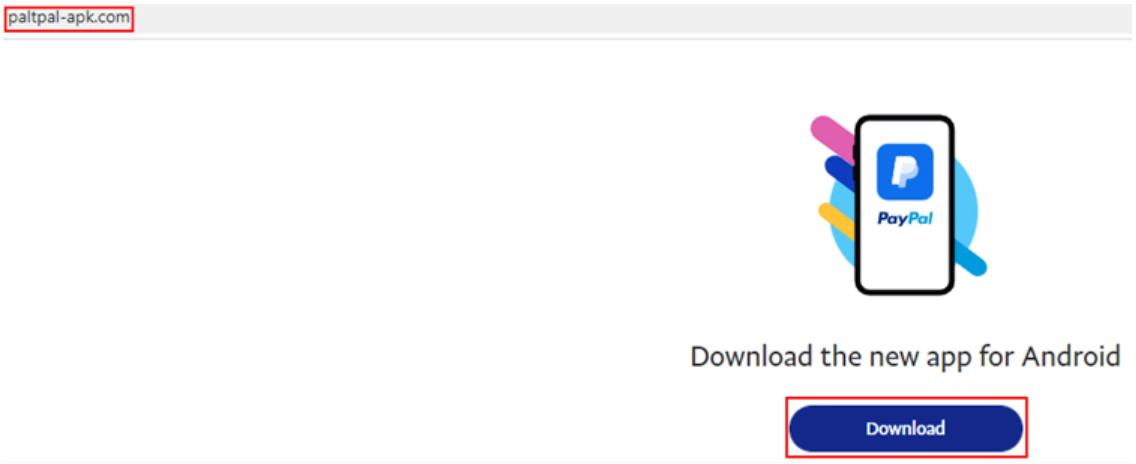

Figure 5 – PayPal Phishing Website

The TA even targets the users of "VidMate." The VidMate application downloads multimedia files hosted on various popular websites, including YouTube, Facebook, Instagram, etc. The below image shows a fake website that downloads a malicious Android APK, masquerading as the official VidMate application.

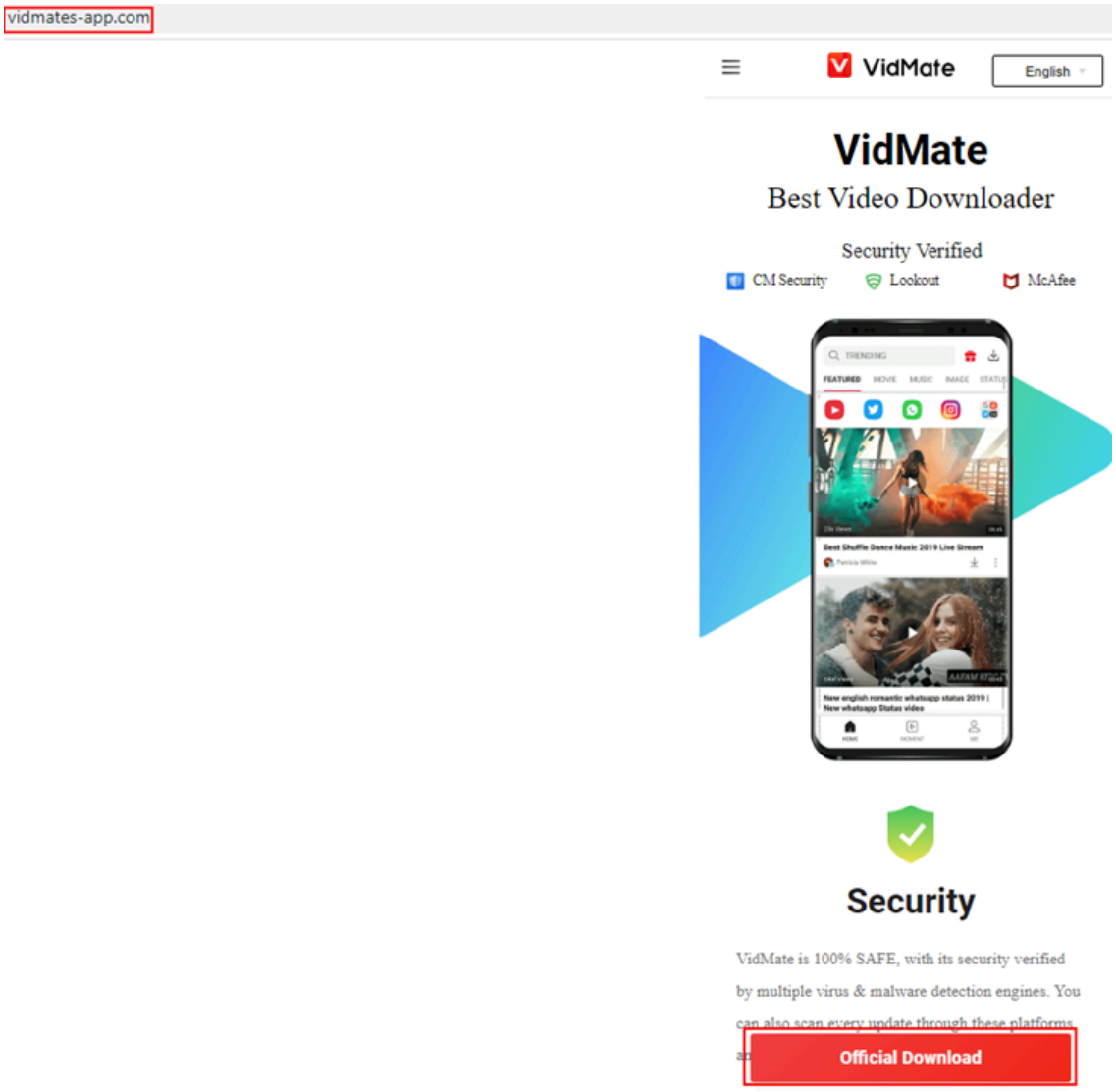

Figure 6 – VidMate Phishing Website

The TA also targets popular chat application users. The below

image depicts a fake Snapchat website that downloads a malicious APK file.

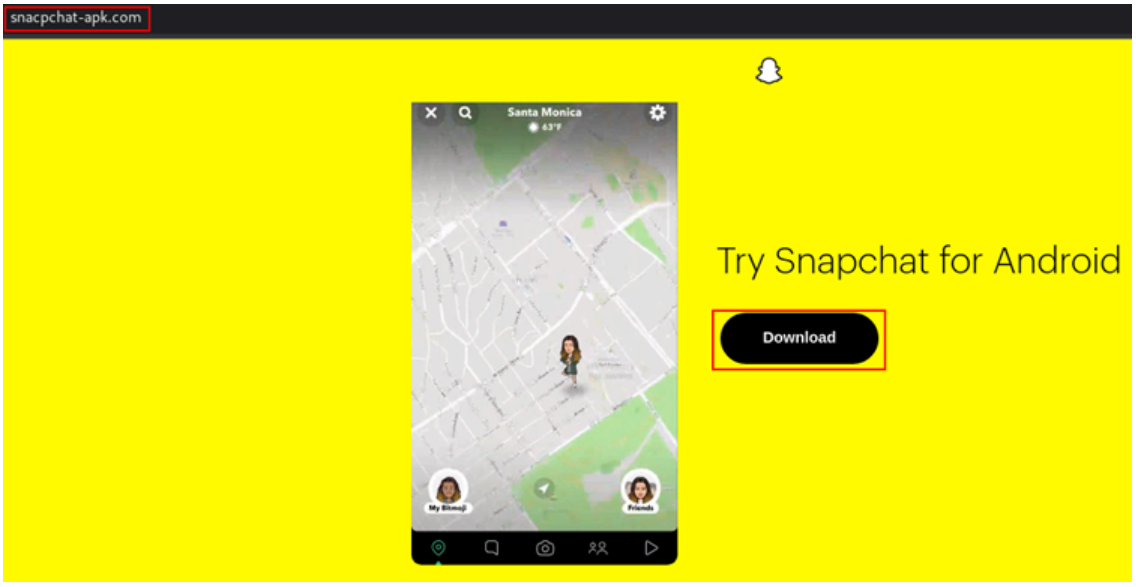

Figure 7 – Snapchat Phishing Website

Upon successful execution of the executable, ERMAC Android malware steals sensitive data such as contacts and SMSs, and a list of installed applications from the user's device.

The malware captures the list of installed applications to steal credentials by loading phishing pages on the victim's device screen. During infection, the malware connects the Command and Control (C&C) server using a POST request, as shown below.

Figure 8 – Communication with C&C

We observed the ERMAC admin panel hosted on the same IP as shown in the figure below.

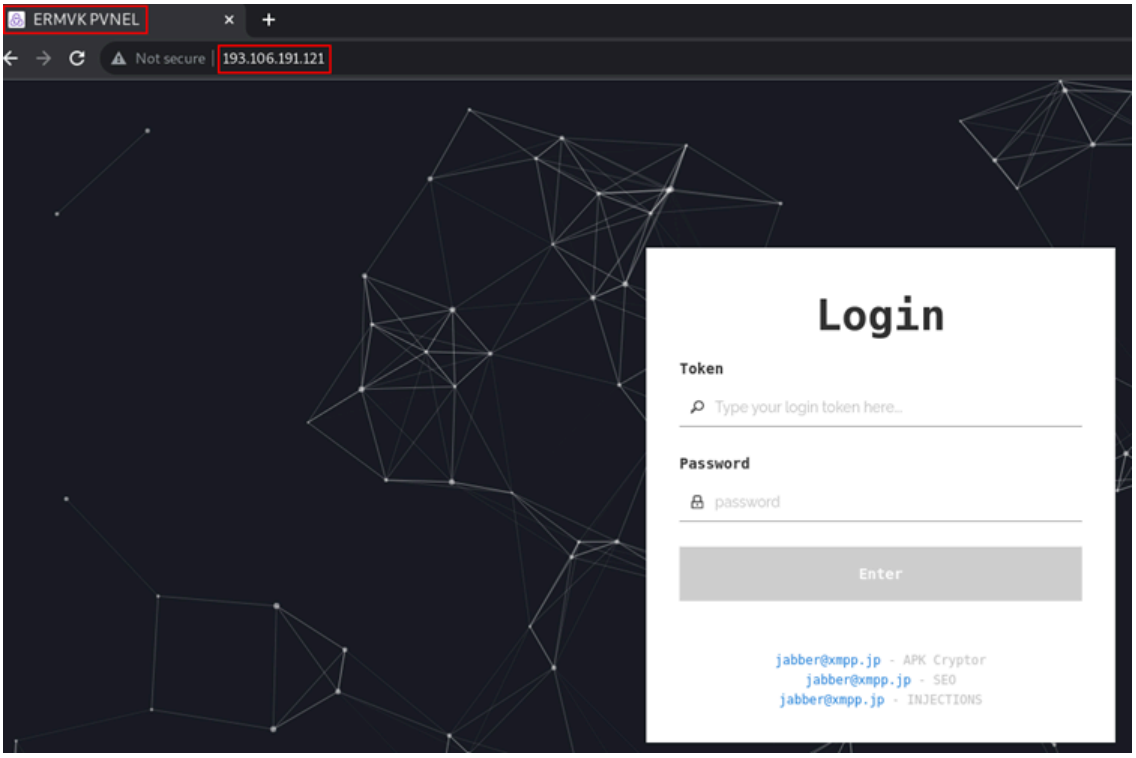

Figure 9 – ERMAC Admin Panel

Conclusion

Since over 70% of mobile users use Android devices, attacks on Android devices have proportionally scaled with the importance and widespread use of Android OS. This is the primary reason that TAs use various sophisticated techniques to deliver malicious Android payloads.

In this case, the TAs use phishing techniques by mimicking several popular and legitimate websites to deliver the ERMAC Android payload.

Cyble Research & Intelligence Labs constantly monitors active phishing campaigns and keeps our readers updated with our latest findings about phishing and other types of data-stealing attacks.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Regularly monitor your financial transactions, and contact your bank immediately if you notice any suspicious activity.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
8692e3212dc590c254020450bdee7003	MD5	ERMAC APK
1b9600d9ba73aeb09bd8d75bd1ae73d75eac6232	SHA1	ERMAC APK
8e9a45e5ac00332d83afa5efb5c5ed92e38280c7da7b7a5f6ae5577e2271cb26	SHA256	ERMAC APK
hxxp://apk-combos[.]com/	URL	Phishing site
hxxps://paltpal-apk[.]com/	URL	Phishing site
hxxps://m-apkpures[.]com/	URL	Phishing site
hxxps://payce-google[.]com/	URL	Phishing site
hxxp://payse-google[.]com/	URL	Phishing site
hxxps://vidmates-app[.]com/	URL	Phishing site
hxxps://app-vidmates[.]com/	URL	Phishing site
hxxp://www.app-vidmates[.]link/	URL	Phishing site
hxxp://app-vidmate[.]com/	URL	Phishing site
hxxps://snacpchat-apk[.]com/	URL	Phishing site
hxxp://193.106.191[.]121:3434/yy.php/	URL	C&C URL
hxxp://193.106.191[.]121/	URL	ERMAC Admin

		Panel
103[.]109.101[.]137	URL	IP hosting phishing sites

Source: https://blog.cyble.com/2022/10/18/ermac-android-malware-increasingly-active/