CYBLE

YEARLY ROUND-UP OF THE ANDROID THREAT LANDSCAPE

CONTENTS

EXECUTIVE SUMMARY

Android is one of the most popular operating systems, crosses over 3 billion active users worldwide, and controls 70% of the mobile market. As per a recent study, the mobile user count is expected to reach 7.5 billion by the end of 2026. As the number of mobile users increases yearly, the attacks targeting mobile devices also exponentially increase.

Cyble Research and Intelligence Labs (CRIL) has been actively monitoring prominent cyberattacks on the Android platform. This report covers the current Android Threat Landscape's strategic intelligence and highlights prevalent banking trojans, active cyber campaigns, and APT attacks.

Over the last six months, CRIL observed upticks in new banking trojans as well as existing malware variants being upgraded with new features.

- Zanubis is a new banking trojan that we identified targeting Peruvian banks
- BRATA malware discovered in 2021 has since evolved into an Advanced Persistence Threat (APT)
- A new version of SOVA malware was spotted using a ransomware module
- A few malware families, such as Sharkbot, Hydra, Joker, etc., are being distributed via the Google Play Store

We also observed and analyzed various spam campaigns distributing Android malware families in the wild. Roaming Mantis - a well-known cyber espionage group, was targeting Japanese taxpayers, which aligned with a rise in the fake e-shop scam targeting Asia. We have also discovered sophisticated phishing attacks targeting Indian bank users.

The use of Android malware by APT groups has significantly increased in the past few months. Our research indicates that various APT groups are using customized Android malware to conduct spyware operations on persons of interest.

Notable recent examples of this include:

- Bitter APT has started using a new malware variant, "Dracarys," to target south Asian countries
- APT42, an Iranian state-sponsored cyber espionage group, used PINEFLOWER Android malware in its attack
- The Scarlet Mimic group used Android malware to target the Uyghur community in China

EXECUTIVE SUMMARY

The below image showcases the top ten Android malware attacks seen since April 2022.

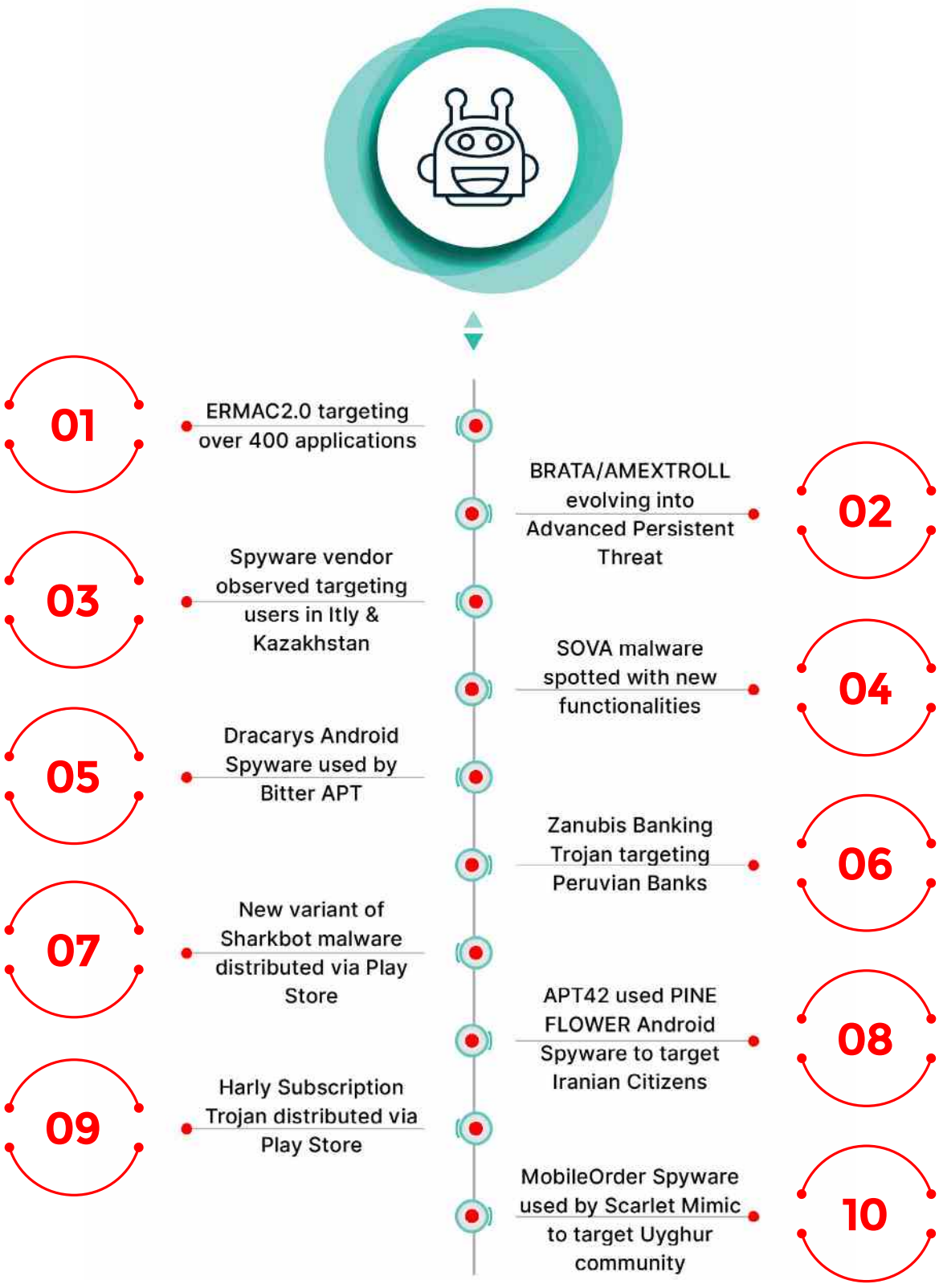


Figure 1 – Android malware attack timeline

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

Android Banking Trojans are one of the most dangerous threats for Android users as this malware uses techniques that prevent uninstallation, auto-grant permissions, etc. TAs have been developing new techniques to steal users' sensitive information by targeting different banking apps.

CRIL observed prevalent banking trojans such as BRATA, ERMAC, Hydra, SOVA, and Sharkbot constantly targeting Android users. The figure below shows the most active banking trojan statistics based on the number of malicious applications observed in the wild.

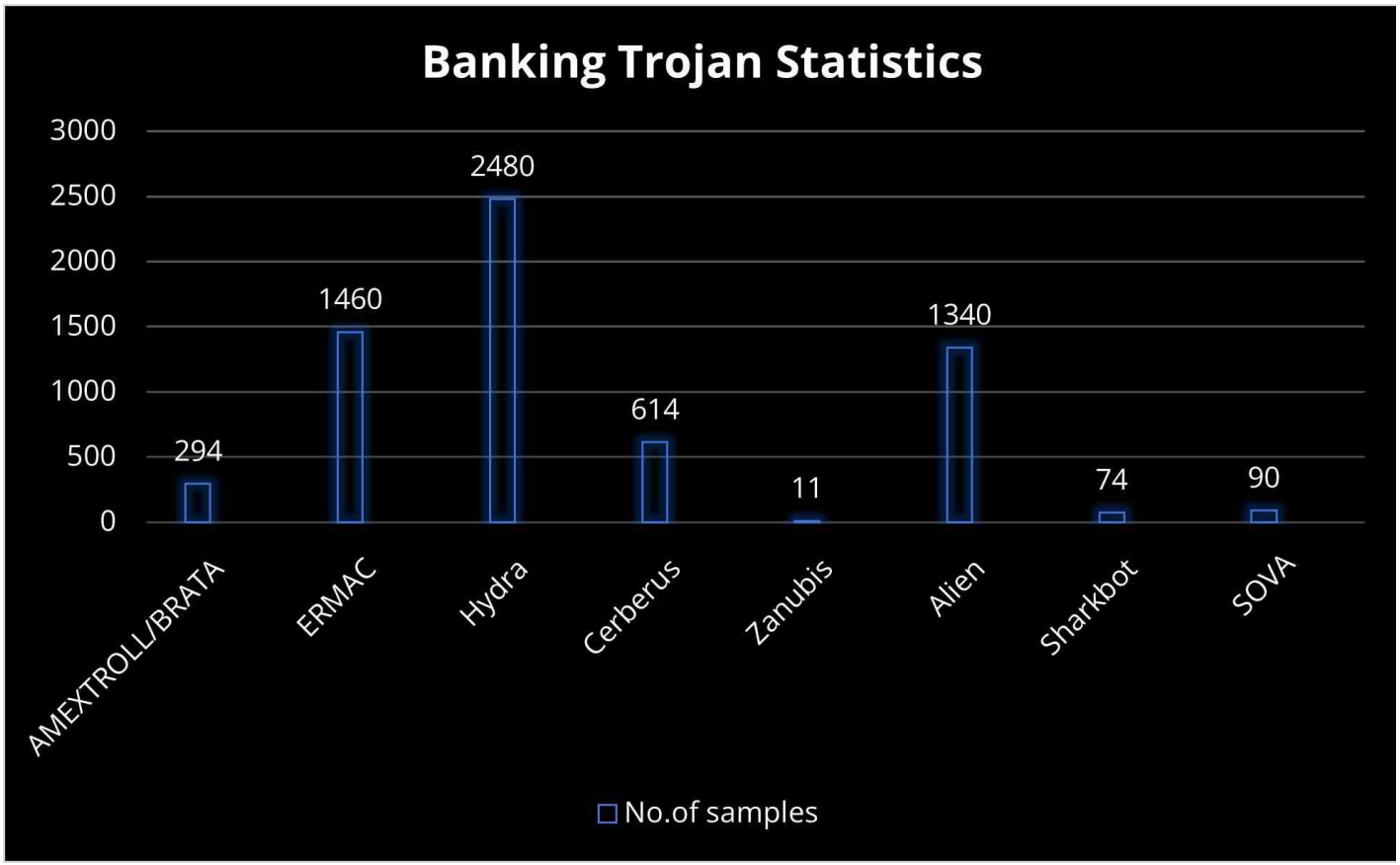


Figure 2 – Prevalent Android Banking Trojan (Based on the samples observed)

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

BRATA: EVOLVING INTO ADVANCED PERSISTENT THREAT

BRATA was initially discovered targeting Italian banks in mid-2021. After its discovery, the malware evolved and distributed new variants with different targets.

In June 2022, the new variant was observed in the wild with new capabilities targeting Italian bank users again. Our research indicated that the TA was implementing sophisticated phishing attacks for credential harvesting and downloading external payload for the keylogger functionality.

In May 2022, the TA rented AMEXTROLL Banking Trojan, aka BRATA, on an underground cybercrime forum for $3.5k/month, as shown below.

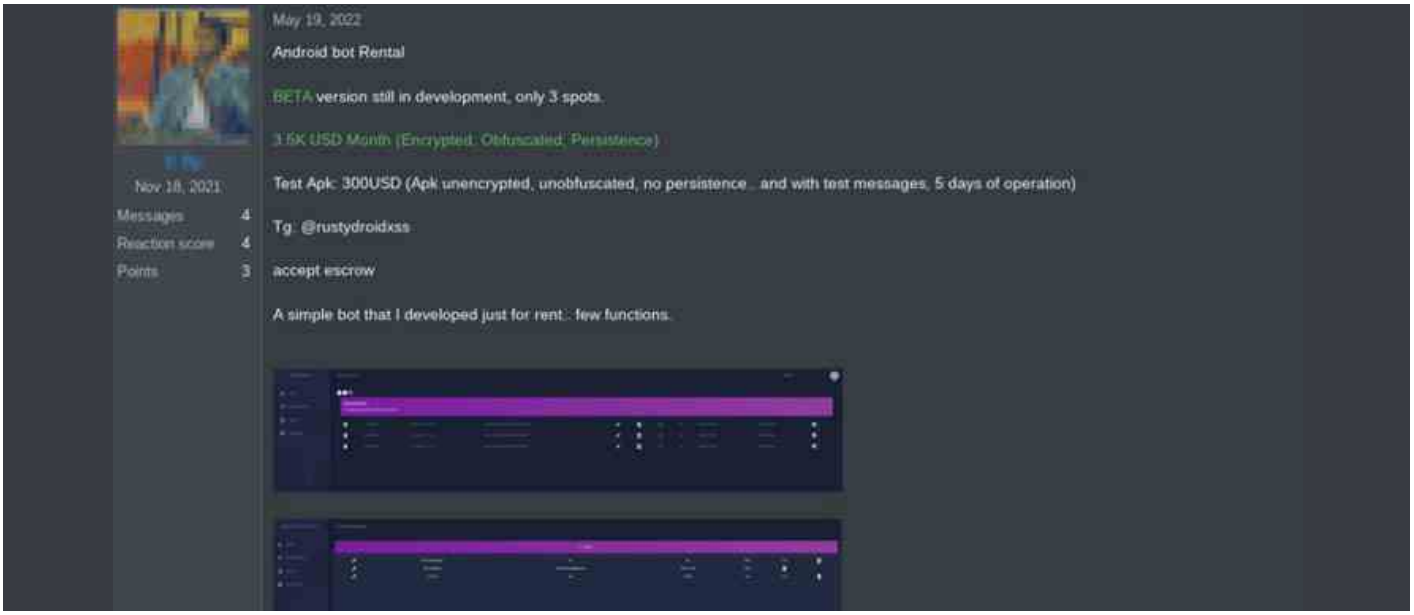


Figure 3 – AMEXTROLL/BRATA advertisement on a cybercrime forum

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

SOVA: BANKING TROJAN RETURNS WITH A RANSOMWARE MODULE

SOVA was first spotted in August 2021 when the TA advertised the Banking Trojan for sale on a cybercrime forum. The TA behind SOVA keeps updating the Trojan with new features.

Recently, new variants of SOVA malware have been observed in the wild, containing ransomware modules and cookie stealer functionality. The below figure shows the ransomware module added in the new variant.

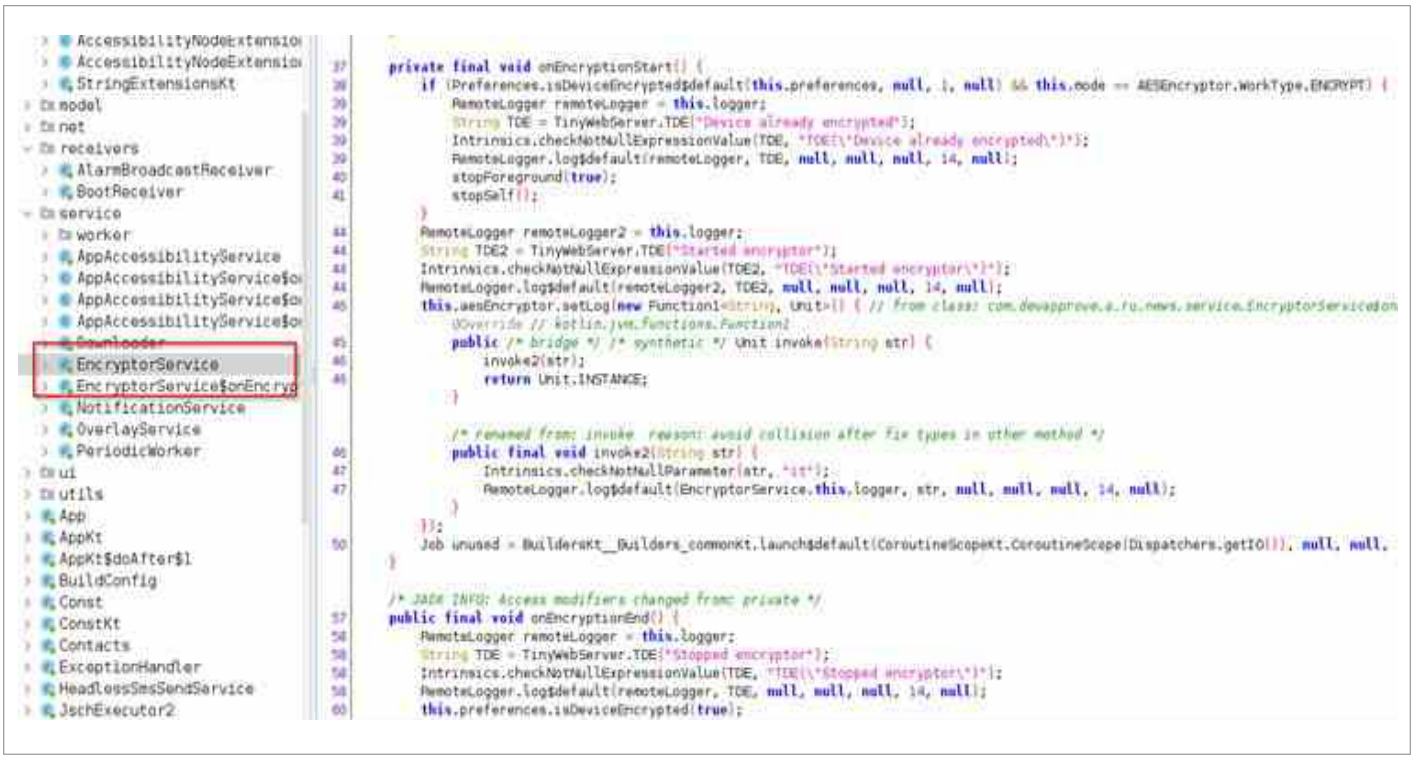


Figure 4 – Ransomware module added in new SOVA variant

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

ZANUBIS: NEWLY DISCOVERED BANKING TROJAN

Recently, CRIL released an analysis about an Android Banking Trojan called Zanubis that was observed at the end of August 2022, targeting banks from Peru.

Zanubis is an overlay-based banking trojan masquerading as a PDF Reader application. The malware receives the overlay URL from Command and Control (C&C) server, as shown in Figure 5, and creates a fake window over a targeted app to steal sensitive credentials.

We suspect that the malware is still in the development phase, and the TA behind the malware has added new banking applications to their target list in the recent version. Zanubis malware has constantly been evolving since its discovery. We may likely observe new variants with upgraded techniques and new targets in the future.

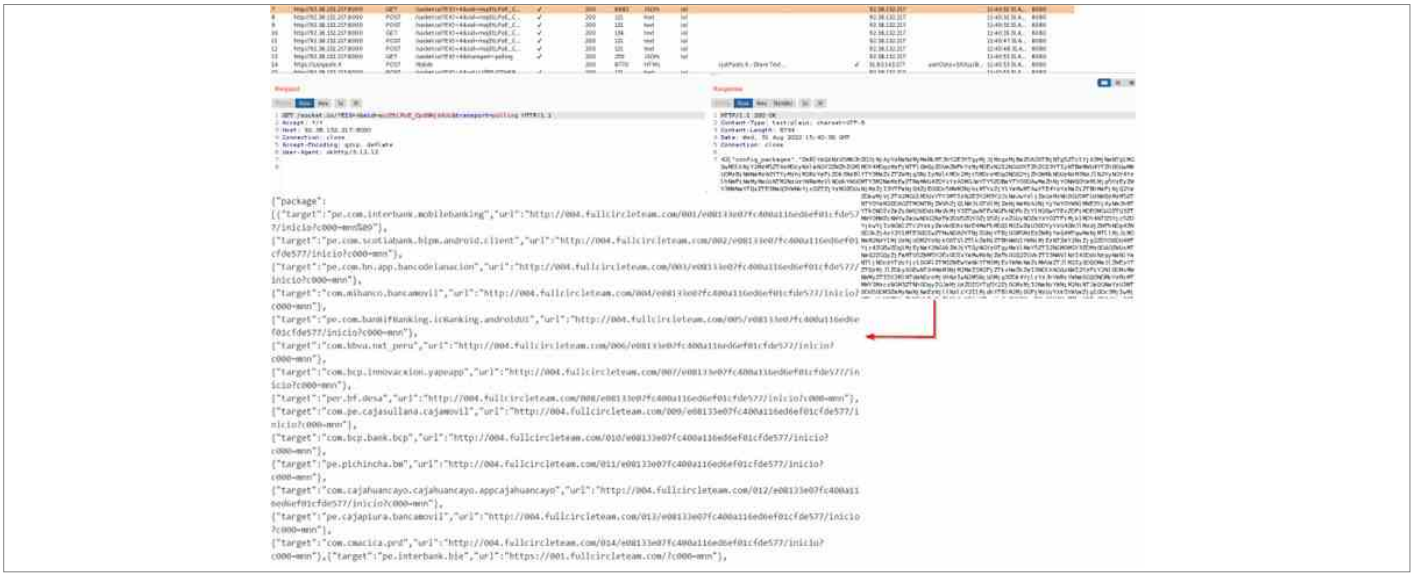


Figure 5 – Zanubis receives the targeted application list and overlays URLs

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

A NEW VARIANT OF SHARKBOT DISTRIBUTED VIA GOOGLE PLAY STORE

Sharkbot, a notorious new-generation Android banking trojan, was discovered in October 2021, targeting European banks. Sharkbot used an Automatic Transfer System (ATS) technique to transfer money from the infected device.

In March 2022, a new variant of Sharkbot was identified in the wild and distributed via the Google Play Store.

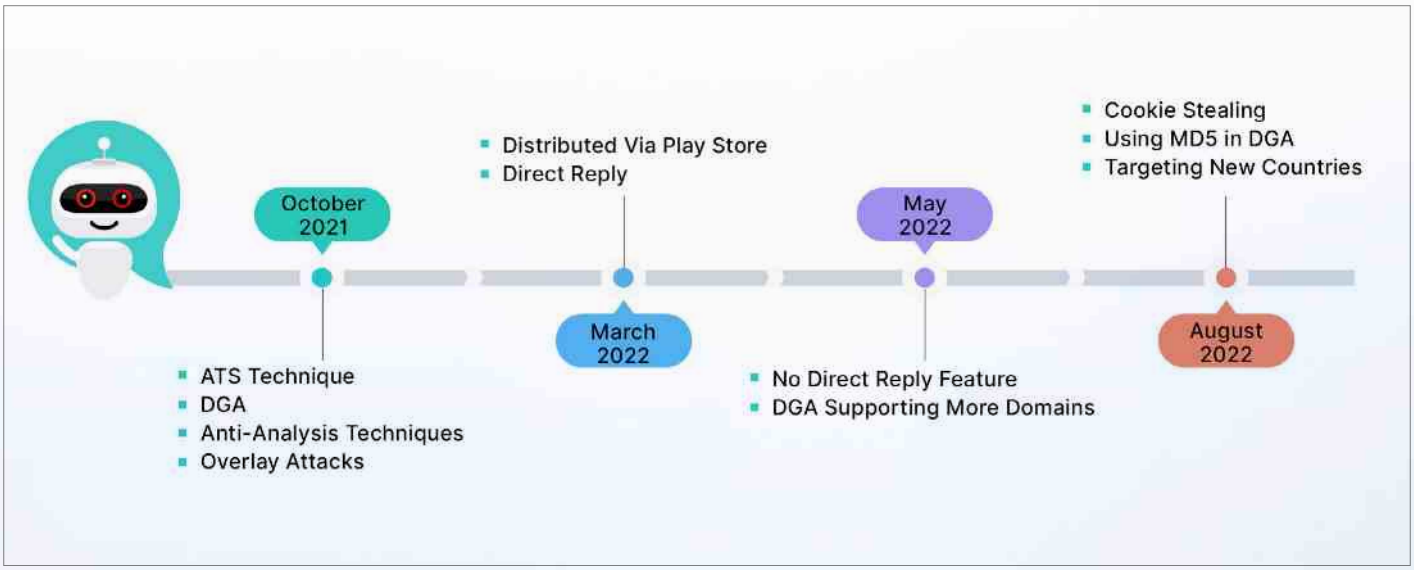


Figure 6 – Timeline of Sharkbot malware attack

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

In September 2022, new variants of Sharkbot malware - v2.25 and v2.26 - were distributed via the Google Play Store. The TA has added the cookie stealer feature in the new variants and removed the feature allowing automatic replies to notifications.

In the latest variant, the malware uses the **logsCookie** command to receive the URL and loads it into WebView. Then, using the **onPageFinished** method, the malware collects the cookies of the loaded URLs and sends them to the attacker's C&C server.

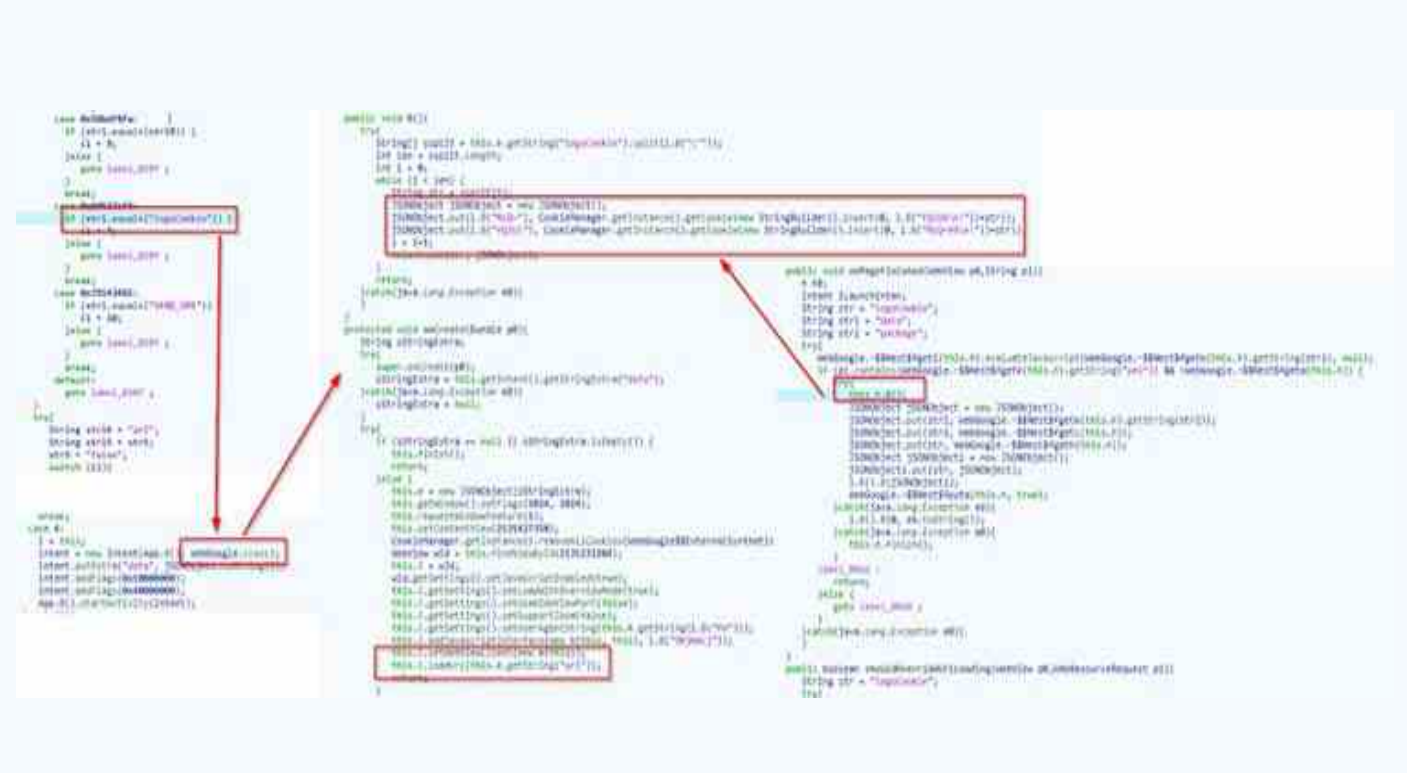


Figure 7 – Cookie-stealing feature in Sharkbot

PREVALENT BANKING TROJANS TARGETING THE ANDROID PLATFORM

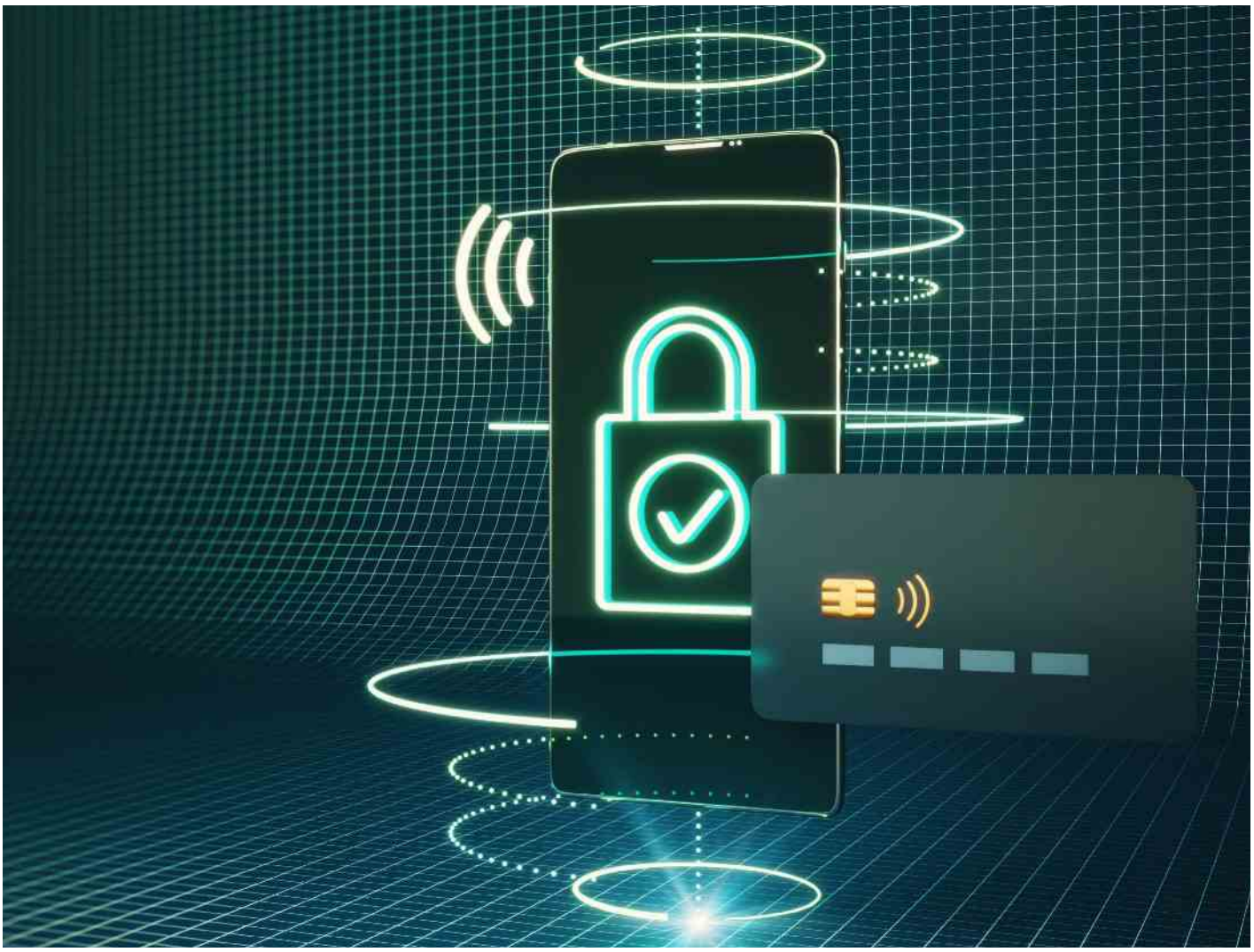
END OF FLUBOT BANKING TROJAN

Flubot Android Banking Trojan was identified in late 2020 and distributed via fake FedEx and Correos text messages targeting European, Asian, and Oceania countries.

Flubot abuses the Accessibility Service to steal victims' credentials by creating an overlay window on top of genuine banking or cryptocurrency applications. The distribution strategy of Flubot malware is unique and different from other banking trojans. Flubot malware spreads predominantly via smishing messages sent to the contacts of the compromised device.

Though the Flubot malware variant was actively distributed through various campaigns between late 2020 to April 2022, the journey of Flubot came to an end in June 2022 as a result of Law Enforcement Agency activities.

Europol – A Law Enforcement Agency declared the takedown of Flubot malware in an operation involving 11 countries, and the Dutch Police took down its infrastructure in May 2022.



ACTIVE SPAM CAMPAIGNS DISTRIBUTING ANDROID MALWARE

CRIL constantly monitors all spam campaigns which we identify targeting Android users in the wild. These campaigns use sophisticated phishing and smishing techniques to distribute Android malware.

The identified campaigns in the last six months have primarily targeted countries such as Japan, India, Malaysia, Vietnam, France, and others.

ROAMING MANTIS SMISHING CAMPAIGN

The Roaming Mantis campaign has been targeting Asian countries for a long time using Android malware.

During our research, we observed that this campaign actively targets Japan and sends SMSs with phishing links impersonating the Japan Post service to distribute the malicious APK file "japanpost.apk".

Over 24,000 malicious samples related to this campaign have been identified over the past 2 months. We have positively identified these samples as the backdoor "Wroba" malware variant.

Figure 8 – Roaming Mantis Japan Post Campaign

ACTIVE SPAM CAMPAIGNS DISTRIBUTING ANDROID MALWARE

In July 2022, the Roaming Mantis campaign was observed targeting France using MoqHao, aka Wroba malware. Around the same time, it also started targeting Japan through a smishing campaign impersonating the National Tax Agency.

The victim receives the malicious shortened URL, which further downloads the FakeCop malware on Android and iOS devices. The URL redirects users to the fake Japanese Nation Tax Agency site, as shown below.

Figure 9 – Roaming Mantis National Tax Agency campaign

ACTIVE SPAM CAMPAIGNS DISTRIBUTING ANDROID MALWARE

FAKE E-SHOP SCAM TARGETING MALAYSIA AND VIETNAM

The Fake e-shop campaign started at the end of 2021, targeting Malaysia by impersonating well-known cleaning services. The TA used Facebook pages and ads to lure the victim into downloading malicious applications.

Recently, we observed the rise in Fake e-shop scams, and the TA seems to be targeting 10 Malaysian banks as well as targets in Vietnam. According to our statistics, the rise in these fake e-shop scam incidents was primarily observed in August 2022.

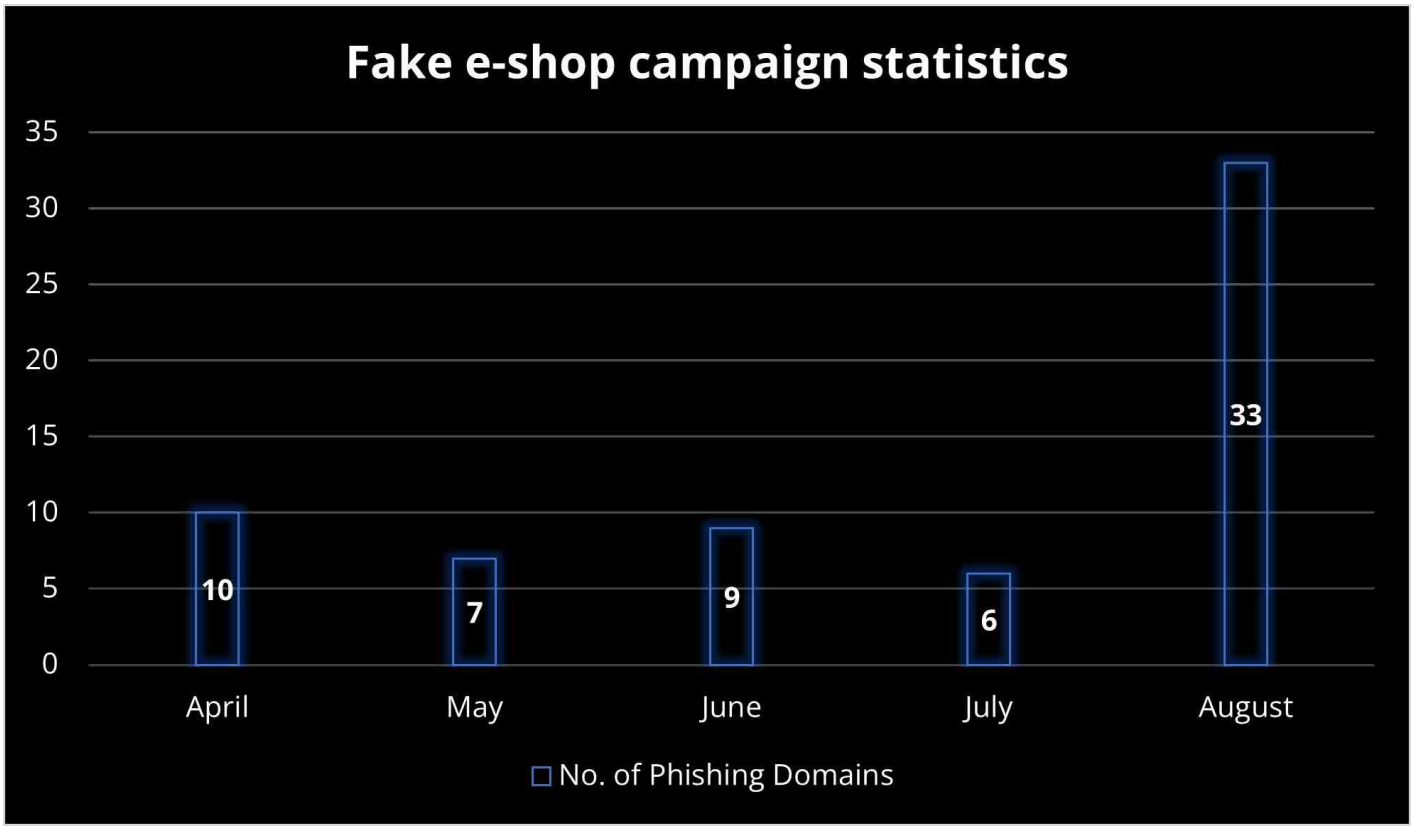


Figure 10 – Fake e-shop campaign statistics

ACTIVE SPAM CAMPAIGNS DISTRIBUTING ANDROID MALWARE

SOPHISTICATED PHISHING ATTACK TARGETING INDIAN BANK CONSUMERS

CRIL witnessed a spike in spam campaigns that target Indian banking users. The attacker targets Indian bank users via a sophisticated SMS-based phishing technique, where the user receives a smishing message on their mobile device containing a malicious application URL.

In some cases, the user receives a call from an attacker who pretends to be a bank representative, asking users to redeem credit card points and convincing them to download malicious applications from the phishing link.

Upon opening the link and installing the malicious application, it prompts the user to submit netbanking credentials and credit card details, as shown in Figure 11.

Further, the malware sends the stolen information to the attacker's C&C server. Recently, the same campaign was observed using an info-stealing RAT to target potential victims.

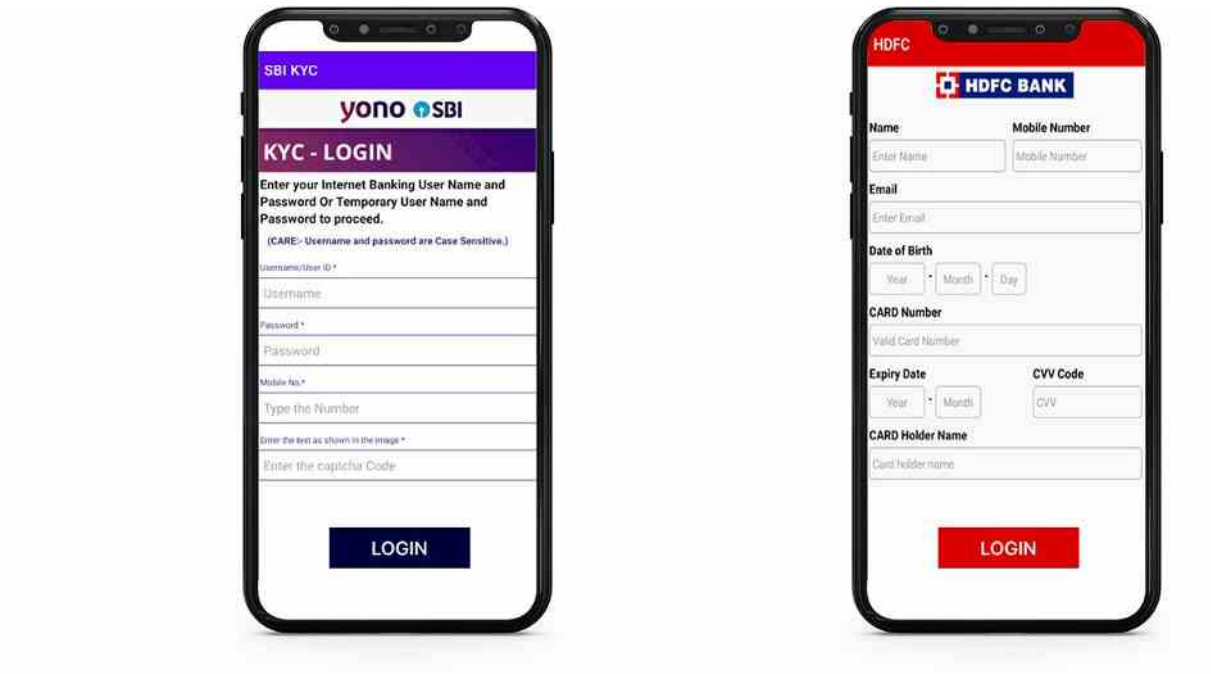


Figure 11 – Credit Card phishing pages used by malware

MALWARE DISTRIBUTION VIA GOOGLE PLAY STORE

The Google Play Store is the most trusted source for Android app downloads because of its Play Protect feature. Despite implementing comprehensive security features, attackers still find alternate ways to host Android malware.

A good example of this is how TAs publish Hostile Downloader apps and use the Dropper as a Service (DaaS) to download malicious payloads after installation.

Sharkbot, HiddenAds, Crypto phishing apps, Joker variants, Hydra, and other banking trojans were found hosted on the Google Play Store and compromised several users. The below image shows Android malware hosted in the Google Play Store.

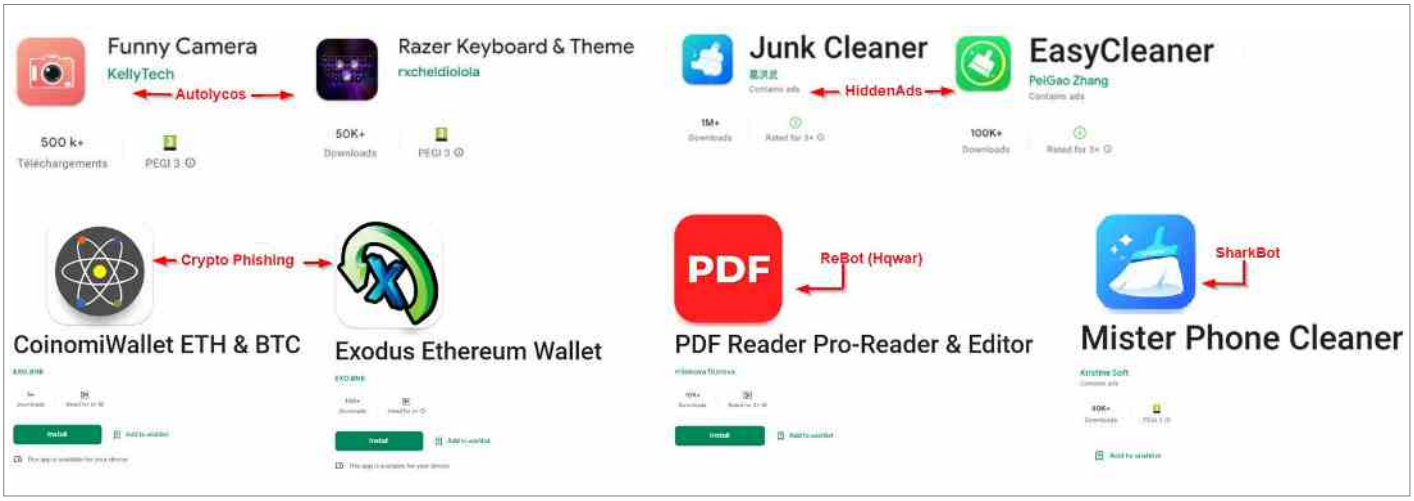
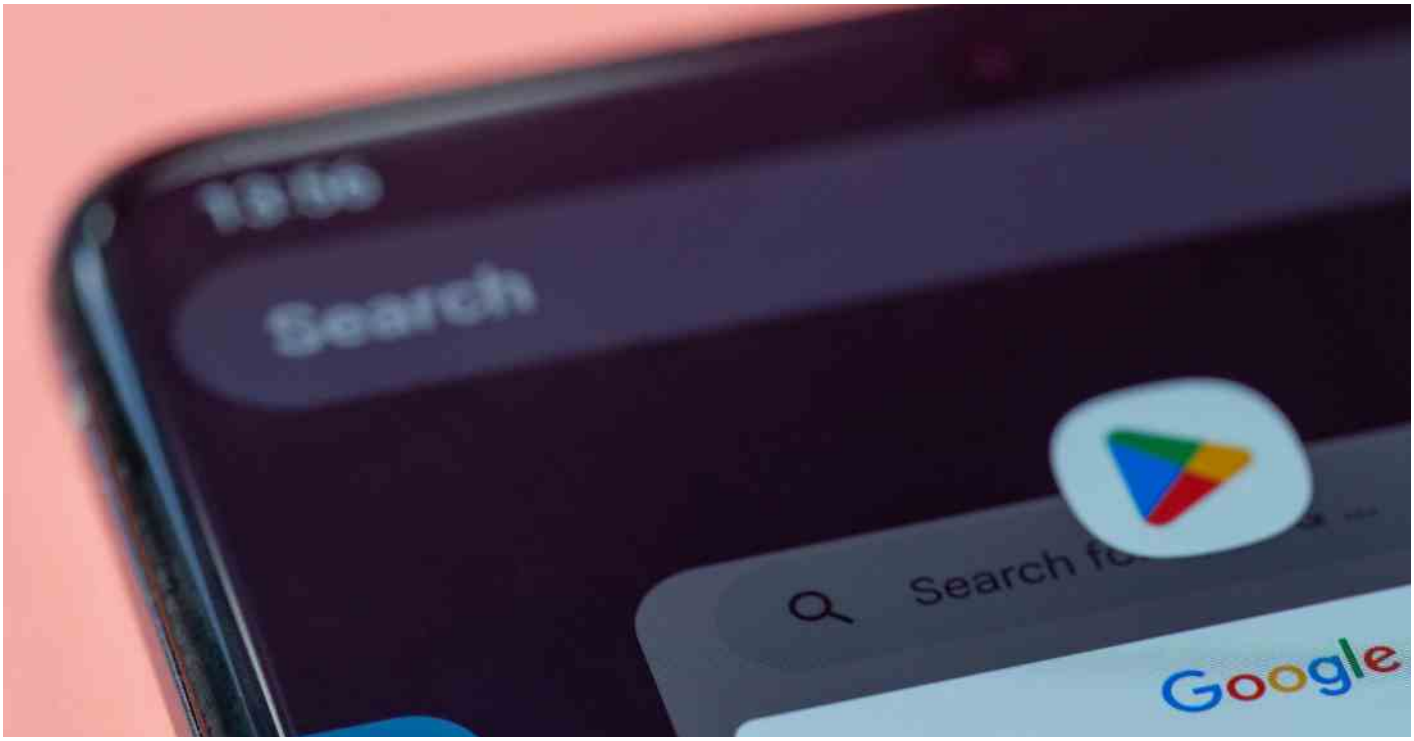


Figure 12 – Android malware distributed via Google Play Store



APT ATTACKS OBSERVED USING ANDROID MALWARE

CRIL noticed many APT groups actively using Android malware, especially spyware, to target their victims. We also observed that APT groups are creating new and customized spyware with enhanced capabilities to suit their requirements.

BITTER APT USES DRACARYS SPYWARE VARIANT TO TARGET SOUTH ASIAN COUNTRIES

Bitter, aka T-APT-17, is a well-known Advanced Persistent Threat (APT) group active since 2013 and has primarily operated in South Asia. It has been observed targeting China, India, Bangladesh, Pakistan, and other countries in South Asia.

Recently, we noticed the Bitter APT group using Dracarys malware, which injected malicious code into the legitimate Signal app's Android code to perform spyware activities.

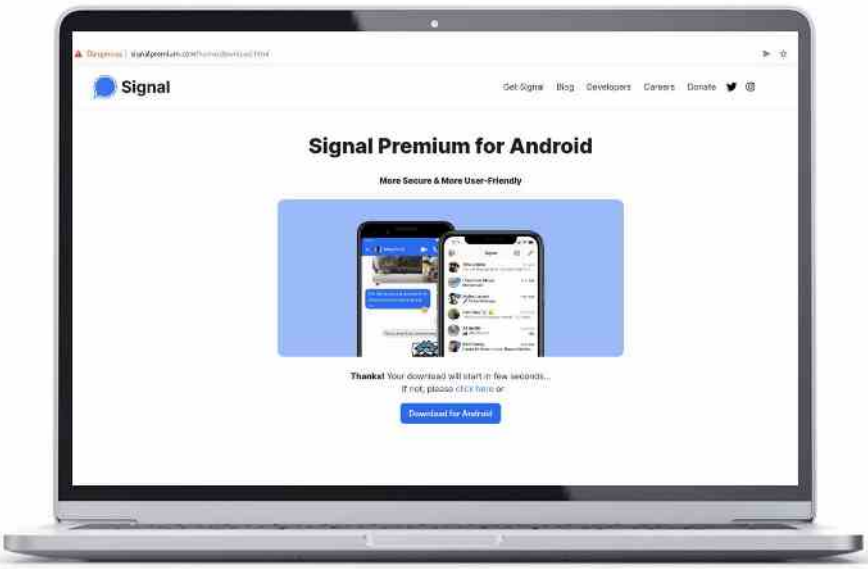


Figure 13 – Phishing Page Delivering Dracarys Android App

APT ATTACKS OBSERVED USING ANDROID MALWARE

APT 42 USING PINEFLOWER MALWARE TO TARGET THEIR VICTIMS

APT 42 is an Iranian state-sponsored cyber espionage group that operates against individuals and organizations under the command of the Iranian government.

APT 42 is known for using techniques such as targeted spear-phishing and social engineering to perform malicious activities such as Credential Harvesting, Surveillance Operations, and Malware Deployment.

Its primary targets are foreign policy officials, commentators, and journalists, particularly from the United States, the United Kingdom, and Israel, who are working on Iran-related projects.

The group was also behind the spyware attack on Iran-based individuals with ties to universities, reformist political groups, and human rights activists using the Android spyware known as PINEFLOWER.

Figure 14 – PINEFLOWER Android Malware Information

ANDROID MALWARE USED TO TARGET UYGHURS

Scarlet Mimic is a cyber espionage group that operates against minority rights activists in China. This Threat Actor's group has not been directly linked to a government source, but its goals seem to be aligned with the Chinese government. Scarlet Mimic was first seen in 2015 when it was primarily targeting Uyghur and Tibetan activists, including individuals who are sympathetic to these causes.

Recently, Scarlet Mimic was observed using malware impersonating a book reader app for a popular book – "The China Freedom Trap" by Dolkun Isa - to target Uyghurs and was stealing several sensitive information such as SMSs, contacts data, call logs, neighboring cell information, etc. from user's device.

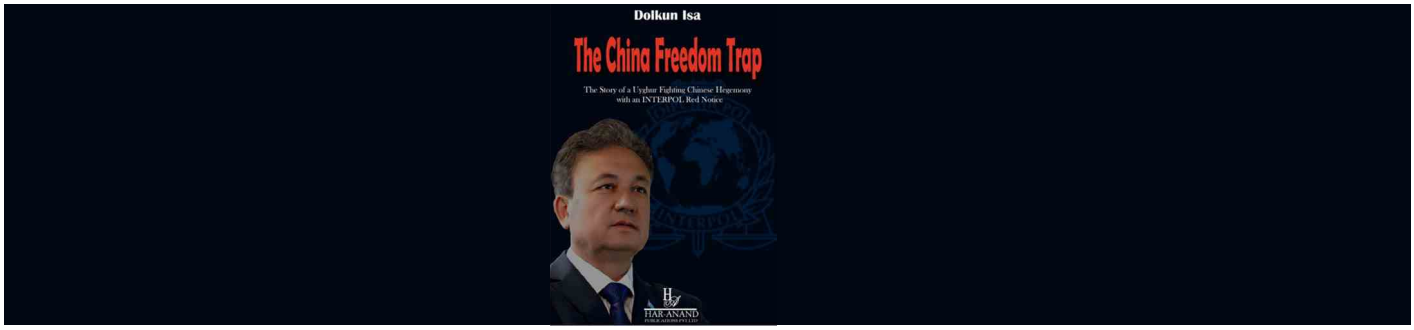


Figure 15 – Book's Cover Page Used by the Malware

OUR PREDICTIONS

One study shows that there are 2 billion mobile banking app users worldwide, and 70% of all smartphone users use mobile banking services. The active use of mobile banking apps incentivizes Threat Actors to develop advanced baking trojans targeting bank users worldwide.

As the number of mobile banking users increases annually, we may see the return of existing banking trojans such as Sharkbot, SOVA, Hydra, etc., with new capabilities and targets alongside newly-developed banking trojans such as Zanubis.

Another study shows that around 378,509,197 phishing SMSs are sent/received daily. Smishing plays a major role and is an effective way for cyber criminals to deliver Android malware successfully since the click rate and responsiveness to smishing messages is relatively high.

We observed major scams that actively use smishing to deliver Android malware targeting Japanese taxpayers, Indian banking users, etc. The spike in campaigns that use smishing to deliver Android malware is only expected to grow in the future.

With the release of Android 13, several privacy and security features were implemented that restrict existing malware variants from carrying out malicious activities on the latest SDK versions. Android 13 introduced a "Restricted Setting" feature that prevents any sideloaded apps from abusing the Accessibility Service.

In the coming days, we may observe Android malware trying to bypass newly implemented security features to continue to target their victims.

OUR RECOMMENDATIONS

- Download and install software only from official app stores like Google Play Store or the iOS App Store
- Use a reputed anti-virus and internet security software package on your connected devices, such as PCs, laptops, and mobile devices
- Use strong passwords and enforce multi-factor authentication wherever possible
- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device where possible
- Be wary of opening any links received via SMS or emails delivered to your phone
- Ensure that Google Play Protect is enabled on Android devices
- Be careful while enabling any permissions
- Keep your devices, operating systems, and applications updated

ABOUT US

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, Dubai and India, Cyble has a global presence.

To learn more about Cyble, visit www.cyble.com