Anatsa Trojan Returns: Targeting Europe and Expanding Its Reach

threatfabric.com/blogs/anatsa-trojan-returns-targeting-europe-and-expanding-its-reach

Jump to

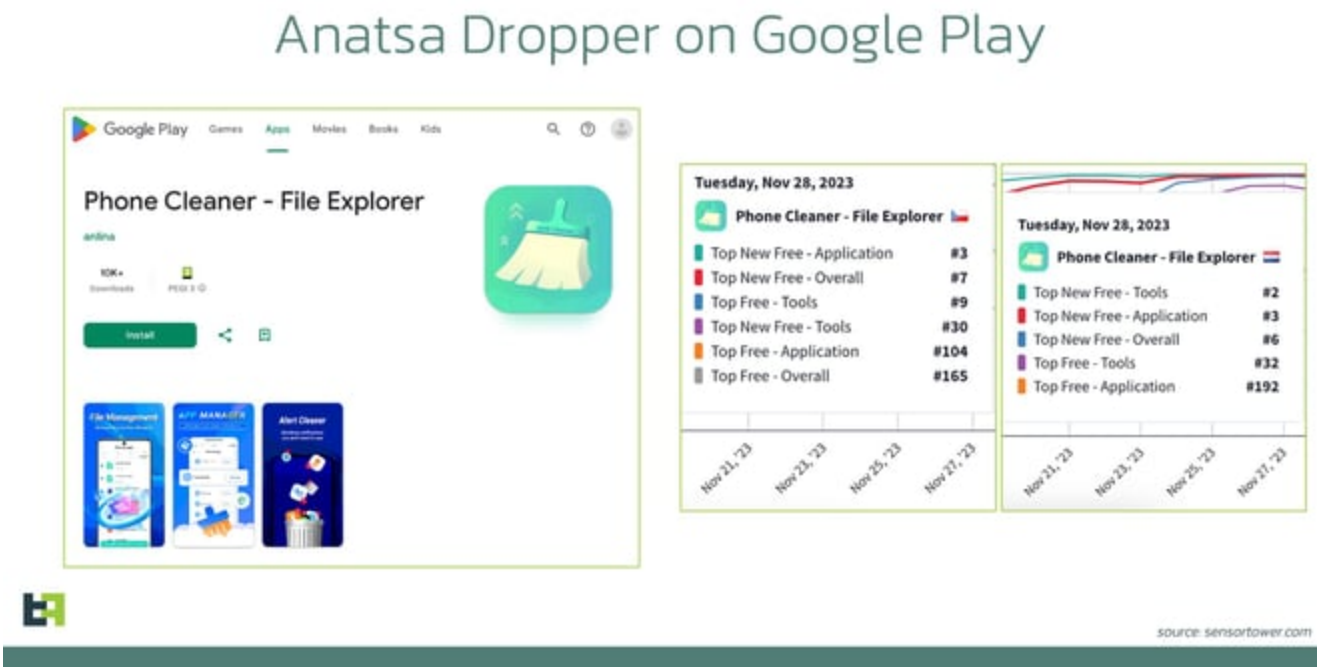
Introduction

In the dynamic world of mobile banking, the security landscape is constantly shifting, posing new challenges for banks and financial institutions. It is therefore imperative to stay ahead of emerging threats. Our latest findings on the Anatsa banking Trojan campaign highlight the evolving nature of these threats and the need for robust mobile threat intelligence.

Campaign overview

In November 2023, our Mobile Threat Intelligence (MTI) team detected a resurgence of the Anatsa banking Trojan campaign, marking a significant shift since our last update in June 2023. Over the past four months, we have observed five distinct waves of this campaign, each focusing on different regions. While Anatsa has previously targeted the UK, Germany, and Spain, its expansion into Slovakia, Slovenia, and Czechia signals a new phase in its operational strategy.

Our analysis reveals that Anatsa's activity can be classified as "targeted," with threat actors focusing on 3-5 regions at a time while promoting dropper applications on Google Play in these specific areas. These applications often reach the Top-3 in the "Top New Free" category, enhancing their credibility and lowering the guard of potential victims while increasing the chances of successful infiltration.



Throughout this campaign, Anatsa's Modus Operandi has evolved, displaying more sophisticated tactics such as AccessibilityService abuse, a multi-staged infection process, and the ability to bypass Android 13's restricted settings.

New droppers: technical details

- Some of the droppers in the campaign successfully exploited the AccessibilityService, despite Google Play's enhanced detection and protection mechanisms.
- To evade detection, all droppers employed a multi-staged approach, dynamically downloading configuration and malicious executable files from their command and control (C2) server, allowing the threat actors to modify them as needed.

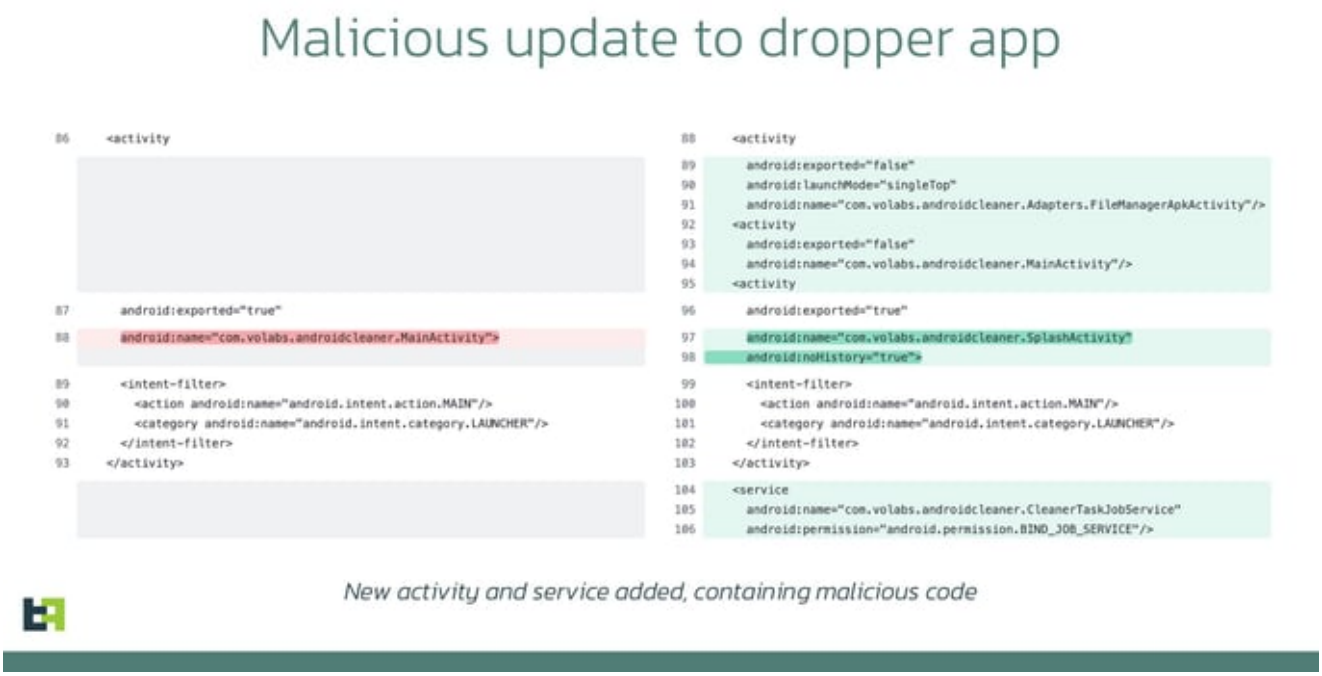
- As reported in previous blogs, all droppers in this campaign have demonstrated the capability to bypass the restricted settings for AccessibilityService in Android 13.

Forbidden techniques: abusing Accessibility Service

AccessibilityService is a feature frequently exploited by mobile malware to carry out harmful activities. Historically, malicious droppers on official app stores used AccessibilityService to automate the installation of payloads, enabling them to complete the installation process without user interaction and thereby increasing the success rate of converting dropper installations into actual payload deployments.

However, this tactic saw a decline after 2017, when Google updated its policy for apps on Google Play using AccessibilityService. Under the new policy, apps must provide a clear explanation for requiring AccessibilityService. This led to a noticeable decrease in its misuse by malicious droppers, which prompted a change in its operational methods.

Recent policy updates on Google Play have imposed even stricter restrictions on the use of AccessibilityService. For an app to now use this service and be published on Google Play, it requires additional approval, significantly reducing the likelihood of malicious apps exploiting this feature.



Despite being considered outdated, old tactics occasionally resurface in official app stores. In November 2023 we identified a dropper on Google Play distributing the Anatsa malware. This dropper, disguised as a cleaner app, claimed to require AccessibilityService as a means

to "hibernate draining apps." Initially, the app appeared harmless, with no malicious code and its AccessibilityService not engaging in any harmful activities. However, a week after its release, an update introduced malicious code. This update altered the AccessibilityService functionality, enabling it to execute malicious actions such as automatically clicking buttons once it received a configuration from the C2 server.

A unique aspect of this dropper was its malicious code, specifically targeting Samsung devices. The malicious AccessibilityService was tailored to interact with the UI elements of Samsung devices, meaning only Samsung users were impacted in this phase of the campaign. This suggests that the threat actors initially developed and tested their code exclusively for Samsung devices.

Based on our findings, we believe there is potential for future adaptations to target other manufacturers. In contrast, other droppers in the campaign did not contain such manufacturer-specific code, posing a threat to all devices regardless of the vendor.

The following code snippet shows how dropper filters work for the manufacturer and Android version, as well as the location (once again showing the highly targeted approach of the actors).

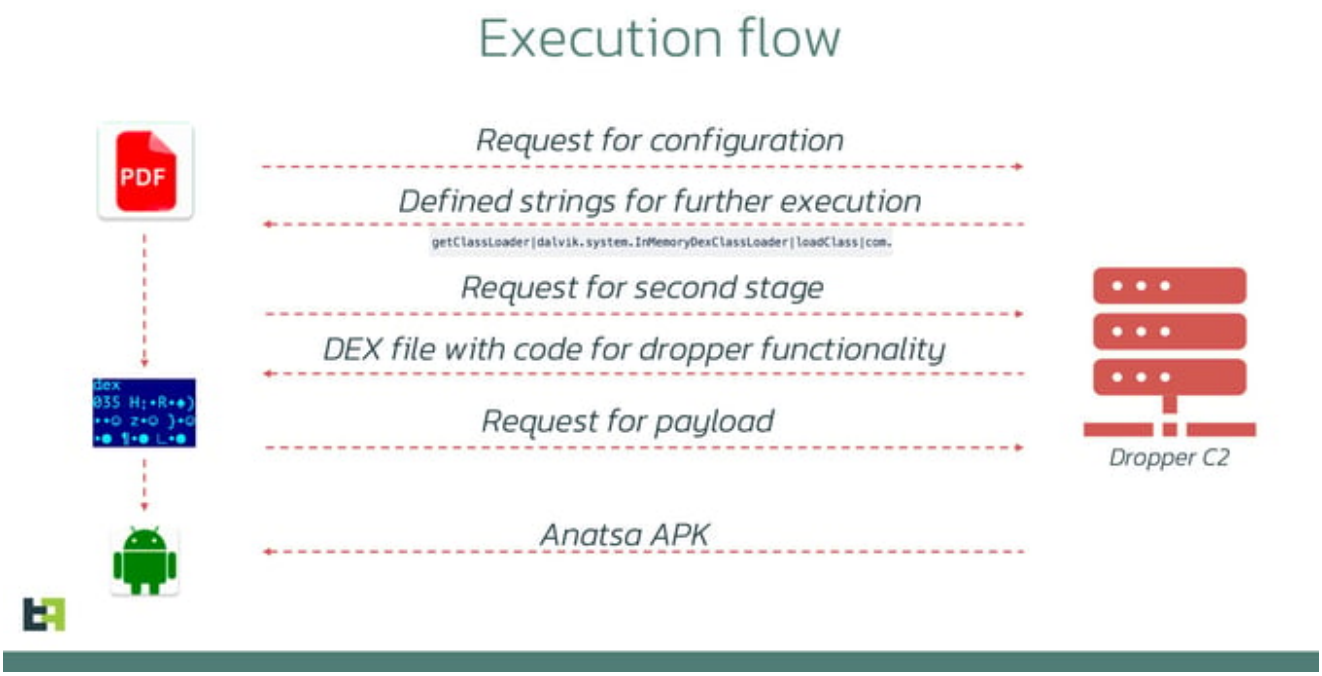
```
if(!Build.MANUFACTURER.equalsIgnoreCase("samsung") || Build.VERSION.SDK_INT != 33) {
    Intent intent0 = new Intent(context0, class0);
    intent0.addFlags(0x10000000);
    context0.startActivity(intent0);
    return;
}
TelephonyManager telephonyManager0 =
(TelephonyManager)context0.getSystemService("phone");
String s = telephonyManager0.getNetworkCountryIso().isEmpty() ? "uat" :
telephonyManager0.getNetworkCountryIso();
if(!s.startsWith("de") && !s.startsWith("nl") &&
!s.startsWith("es") && !s.startsWith("gb") &&
!s.startsWith("hk") && !s.startsWith("cz") &&
!s.startsWith("sk")) {
    Intent intent1 = new Intent(context0, class0);
    intent1.addFlags(0x10000000);
    context0.startActivity(intent1);
    return;
}
```

Interestingly, the malicious code that handles accessibility events is located in an additional stage (DEX file) that is downloaded from the C2 and dynamically loaded into memory.

Malicious puzzle: multiple stages to avoid detection

To avoid immediate detection, the actors strategically spread the malicious indicators across several stages. Our analysts observed that the latest version of the dropper showed improvement, dynamically retrieving the following files from the command-and-control server:

1. Configuration for the malicious DEX file. It contains strings necessary for malicious code, which might trigger the detection mechanisms if they were placed in the dropper itself. The strings contain suspicious class names like "dalvik.system.InMemoryDexClassLoader", the presence of which indicates the suspicious intent to load the DEX file directly from the memory.
2. DEX file containing malicious code responsible for payload installation. Having downloaded strings in the previous step, the control flow is redirected to the loaded DEX file.
3. Configuration with a payload URL. It allows cybercriminals to dynamically change the payload URL if the previous one gets taken down.
4. Payload. As a final step, the code in the DEX file loaded in step 2 downloads Anatsa, installs it and launches it.



Bypassing Android 13 restrictions

The droppers in the latest Anatsa campaign effectively install payloads, circumventing the AccessibilityService restrictions of Android 13. This technique, capable of bypassing certain restrictions and previously covered in our discussion on several actors providing Dropper-as-a-Service, is increasingly being adopted by various actors. It ensures that the droppers can install malicious payloads without having their access to AccessibilityService functionalities disabled.

In this campaign, all three droppers observed use this method and employ dynamically loaded DEX files, further enhancing their ability to evade detection by security engines.

Impact: Device Takeover hits European banks

- Financial organisations are advised to alert and educate their customers about the risks of installing applications from official stores and enabling AccessibilityService for applications that do not require them.
- Implementing effective detection and monitoring for malicious applications and unusual customer account activity is crucial in identifying fraud cases linked to device-takeover mobile malware such as Anatsa.

As of this report, the current campaign involves five droppers with over 100,000 total installations. Each installation poses a potential risk for Anatsa installation and subsequent fraud. In comparison, the previous campaign in the first half of 2023 featured six different droppers, accumulating over 130,000 total installations. Based on this pattern, we anticipate the continuation of this campaign, with new droppers appearing in the official store and an expansion into additional targeted regions. The threat actors have a history of shifting focus between regions within a single campaign.

The distribution strategy and remote access capabilities of Anatsa classify it as a critical threat in the targeted regions. Our threat intelligence indicates that these actors prefer concentrated attacks on specific regions rather than a global spread, periodically shifting their focus. This targeted approach enables them to concentrate on a limited number of financial organisations, leading to a high number of fraud cases in a short time. This not only increases the burden on fraud analysts but also places significant strain on customer support teams.

Anatsa is a banking Trojan with Device Takeover (DTO) capabilities that can gain full control over an infected device and execute actions on a victim’s behalf. Financial organisations should urgently educate their customers about the risks of installing applications, even from official stores, and caution against enabling AccessibilityService for apps that don't require it for their supposed operations. In cases where customers report unusual device behaviour or unrecognised transactions, we advise institutions to inquire about recent activities such as newly installed applications and any permissions granted, particularly regarding AccessibilityService.

Effective detection and monitoring of malicious applications, along with observing unusual customer account behaviour, are crucial for identifying and investigating potential fraud cases linked to device-takeover mobile malware like Anatsa.

Conclusion

In the ever-changing threat landscape, staying informed is the first step. Proactive measures are essential to safeguarding your institution's mobile banking infrastructure. ThreatFabric's Mobile Threat Intelligence service is designed to provide actionable intelligence that can be integrated into your security strategy.

Our continuous monitoring and analysis of threats such as Anatsa equips you with the knowledge needed to anticipate and mitigate these evolving risks. By partnering with ThreatFabric, you gain access to cutting-edge threat intelligence, empowering you to protect your assets and maintain the trust of your customers in an increasingly digital banking environment.

Stay vigilant, stay informed, and stay ahead with ThreatFabric.