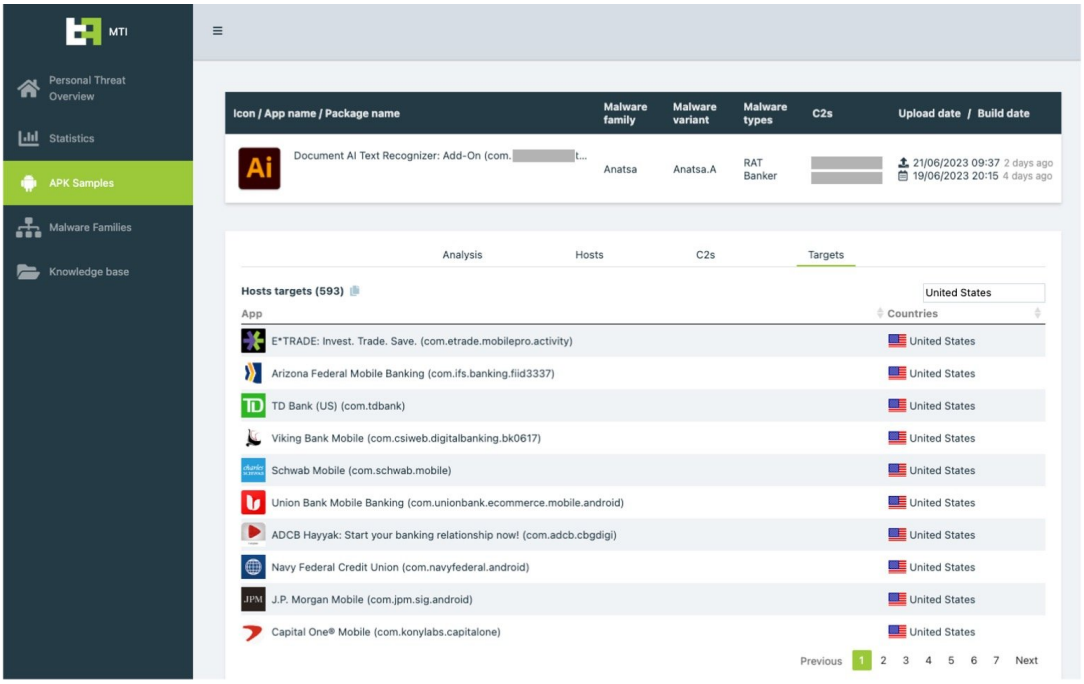
Anatsa banking Trojan hits UK, US and DACH with new campaign

threatfabric.com/blogs/anatsa-hits-uk-and-dach-with-new-campaign

Jump to

New ongoing campaign hitting banks for months

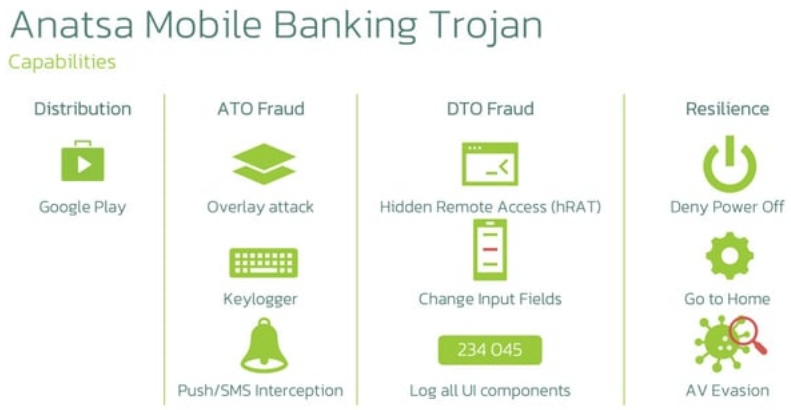
As of March 2023, ThreatFabric's cyber fraud analysts have been monitoring multiple ongoing Google Play Store dropper campaigns delivering the Android banking Trojan Anatsa, with over 30.000 installations. The threat actors behind this new wave of Anatsa showed interest in new institutions from the US, UK, and DACH region. Our fraud intelligence platform was able to confirm this dangerous malware family adding multiple Android banking apps from these regions as new targets.



Screenshot from Mobile Threat Intelligence portal

ThreatFabric is aware of multiple confirmed fraud cases, with confirmed losses caused by Anatsa, due to the Trojan's very advanced Device-Takeover capabilities, which are able to bypass a wide array of existing fraud control mechanisms.

The focus of the ongoing campaign is banks from US, UK, and DACH, while the target list of the malware contains almost 600 financial applications from all over the world. The actors behind Anatsa aim to steal credentials used to authorise customers in mobile banking applications and perform Device-Takeover Fraud (DTO) to initiate fraudulent transactions.

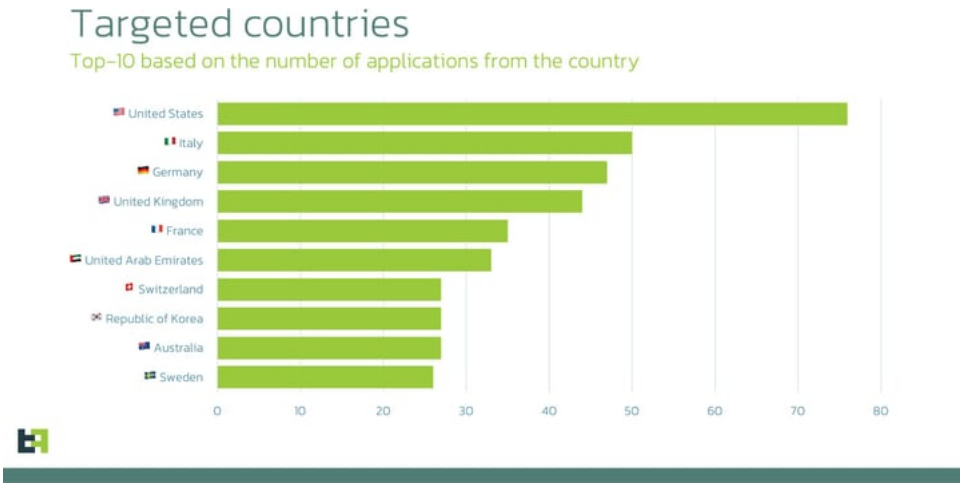


New targets, new focus

ThreatFabric has been monitoring Anatsa's activity since its discovery in 2020. We have seen multiple changes in the actor's areas of interest over the years, with continuous updates in target lists. This campaign is no exception: we see a strong shift towards targeting banking institutions in the DACH region, specifically in Germany. This focus is mirrored by the regions where the droppers used for distribution are released.

In the latest iteration of the campaign, with the introduction of the new dropper, our Fraud Intelligence portal identified 3 new German banking applications that were added to Anatsa's overlay target list, which once again proves the current focus of the actors.

However, Anatsa remains active in the US and UK, just like in previous campaigns. Analysing the list of targeted applications, we see more than 90 new targeted applications compared to the last of last year, in August 2022. Anatsa's actors added targets from Germany, Spain, Finland, South Korea, Singapore. While the droppers are not distributed in all of these countries, it definitely reveals plans to target those regions. It is likely part of the initial reconnaissance that will give the actors more insights into the internal structure of banking applications and the way apps need to interact in order to perform transfers; in addition, it can be possible that actors are trying to also target significant minorities that live in countries targeted by these droppers.



If you are interested in the full list of Anatsa's targeted banking applications and a personal briefing, please, contact us.

The campaign we report in this blog is not a usual one - it serves as an example of efforts actors make to deliver the malware to victims, at the same time increasing infection conversion and maintaining long-lasting campaigns. In the following sections, we explain our observations on the latest (still ongoing at the moment of writing this blog) Anatsa campaign.

5 droppers on Google Play in 4 months

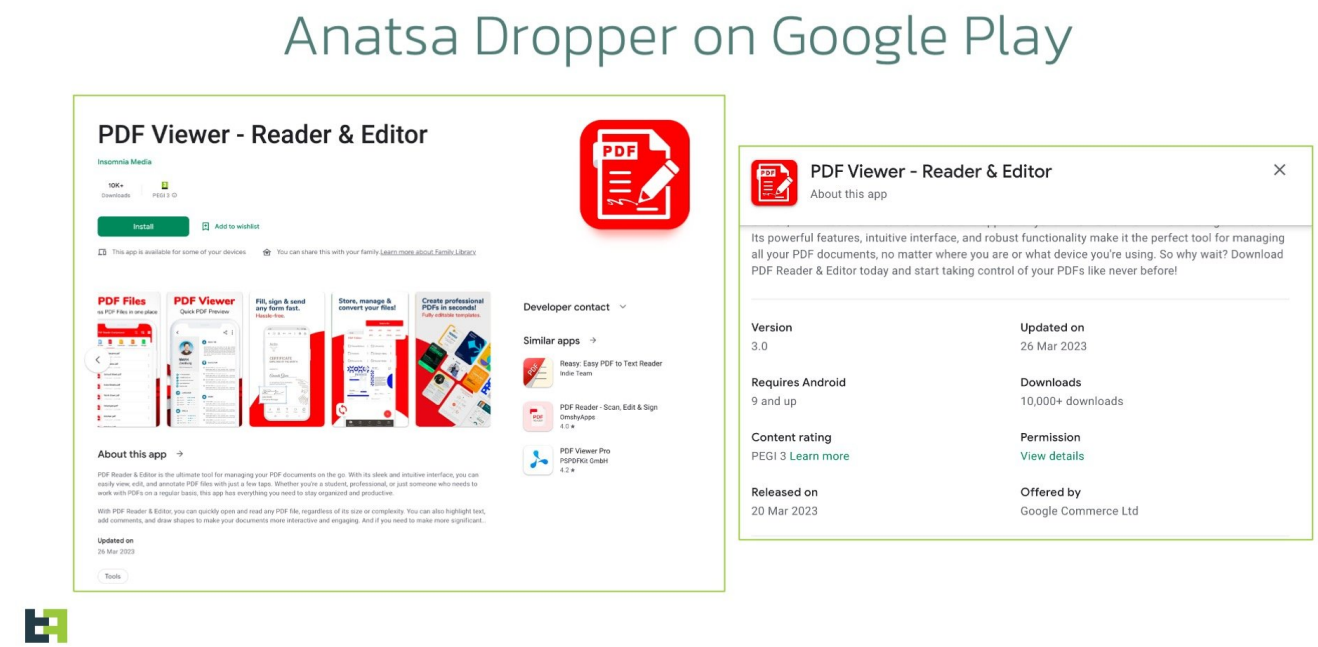
It all started at the beginning of March 2023, when ThreatFabric detected the start of a new campaign by Anatsa after an approximate half-year hiatus. Our analysts were able to identify a dropper application on the Google Play Store used to deliver Anatsa on infected devices, posing as a PDF-reader application.

Once installed, such an application would make a request to a page hosted on GitHub, where the dropper would get the URL to download the payload (also hosted on GitHub). The payloads would masquerade as an add-on to the original application (similar to what we have seen in previous campaigns).

Screenshot from Mobile Threat Intelligence portal

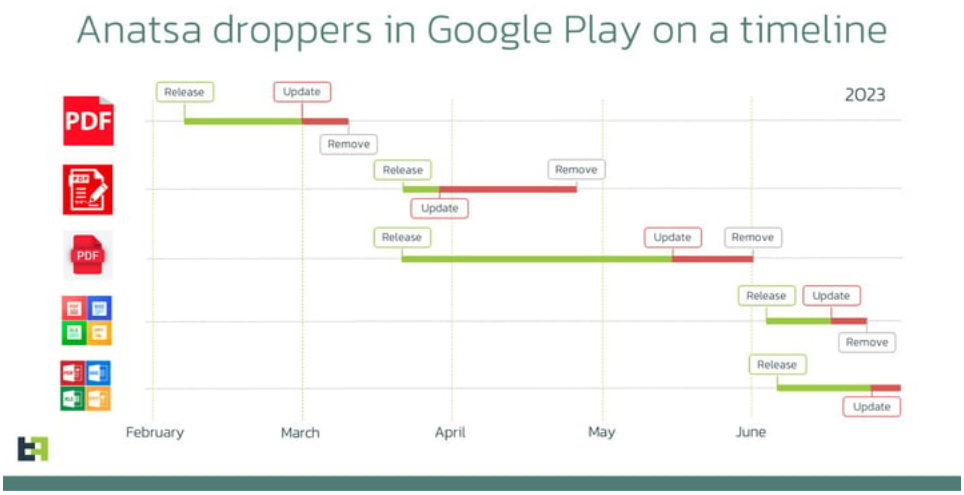
Shortly after this dropper was reported to Google, it was removed from the store. However, one month after the discovery of the first dropper, the actors published another one, once again posing as PDF-viewer. It was the continuation of the same campaign, as the payloads used in it were the same, still masquerading as an add-on. The choice of disguise for these malicious applications observed confirms the trend we see for droppers on Google Play: after the restriction of "*REQUEST_INSTALL_PACKAGES*" permission, droppers tend to impersonate file-management-related applications.

These types of apps are more likely to already havethis permission, as they need it for their functionality: the addition of the code responsible for installing a payload does not result in an increase of permissions to the original trojanized application.



This second dropper was reported to Google by our team and it was removed from the store. Nevertheless, the same repeated twice: another dropper appeared within a month after the previous one was removed. Our team discovered 3 more droppers in May and June, 2023.

The timeline of the dropper's releases and removals is shown in the picture below.



We want to highlight the speed with which the actors return with a new dropper after the previous one is removed: it takes anywhere from a couple of days to a couple of weeks to publish a new dropper application on the store. Moreover, at the time of writing this blog, a new Anatsa dropper was discovered by our analysts and it is still online.

It is also important to highlight that every dropper was updated sometime after the publication date, very likely adding malicious functionality at that point in time (we marked that moment with the “Update” tag on the timeline above). Our analysis also reveals that the actors can have several apps published in the store at the same time under different developer accounts, however, only one is acting as malicious, while the other is a backup to be used after takedown.

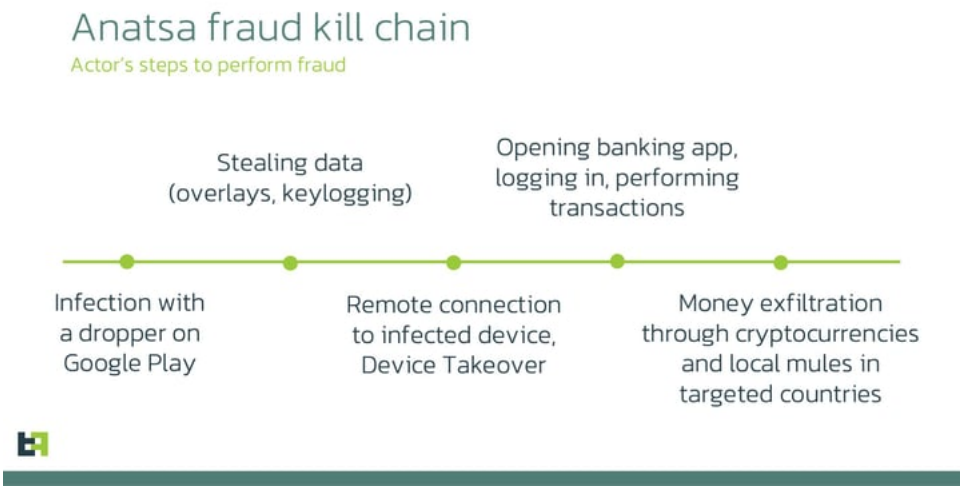
Such a tactic helps actors to maintain very long campaigns, minimising the time needed to publish another dropper and continue the distribution campaign.

Anatsa fraud kill chain

The analysis of Anatsa's activity and its capabilities allows us to draw a fraud "kill chain" for Anatsa, highlighting the way in which actors may act in order to perform fraud.

It all starts with the distribution phase where the payload is delivered through malicious apps on Google Play Store. Victims are routed there through advertisements, which look less suspicious to them as they lead to the official store.

Once the device is infected, Anatsa is able to collect sensitive information (credentials, credit card details, balance and payment information) via overlay attacks and keylogging. This information will be later used by the criminals to perform fraud. Anatsa provides them with the capability to perform Device-Takeover Fraud (DTO), which then leads to performing actions (transactions) on the victim's behalf. Since transactions are initiated from the same device that targeted bank customers regularly use, it has been reported that is very challenging for banking anti-fraud systems to detect it.



Conclusions

The latest campaign by Anatsa reveals the evolving threat landscape that banks and financial institutions face in today's digital world. The recent Google Play Store distribution campaigns targeting US, DACH, and UK regions demonstrate the immense potential for mobile fraud and the need for proactive measures to counter such threats.

In this rapidly evolving landscape of cyber fraud, the battle against mobile banking Trojans like Anatsa requires client-side visibility and adaptability before the customer journey (powered by fraud intelligence) and directly during it with the help of SDK built-in banking applications.

Fraud Risk Suite

ThreatFabric's Fraud Risk Suite enables safe and frictionless online customer journeys by integrating industry-leading mobile threat intel, behavioural analytics, advanced device fingerprinting and over 10.000 adaptive fraud indicators. This will give you and your customers peace of mind in an age of ever-changing fraud.

Appendix

Anatsa droppers

App name	Package name	SHA-256
PDF Reader - Edit & View PDF	lsstudio.pdfreader.powerfultool.allinonepdf.goodpdftools	ecce34c0ba83120ccf1f8e1640cd867fbfeb490dbc8a41d1cf8c577d508819c
PDF Reader & Editor	com.proderstarler.pdfsignature	128820e1c5d62523f675042da9d1e11af3191217afe308bcc17e51ad8c2ec

PDF Reader & Editor	moh.filemanagerrespdf	7231546ee377738cbe9075791eb6e76b7bc163c1b91831e05e81b4756fff4
All Document Reader & Editor	com.mikijaki.documents.pdfreader.xlsx.csv.ppt.docs	3740e6b4d259efe6a72f503429fb67db96363935a29f7428ccab5b78fa9bee
All Document Reader and Viewer	com.muchlensoka.pdfcreator	db7df65f2699817fa3ebfb3ebef106a3801a96b9da1ba6d88e727a253ae34c