ISSN: 2995-326X

Research Article

Political Science International

Understanding Toxic Panda: The New Cyber Threat Targeting Data Security

Asmita Mallick[1]* and Prithwish Ganguli[2]

[1]*Student, Heritage Law College under University of Calcutta, India*

[2]*LLM (CU), MA in Sociology (SRU), MA in Criminology & Forensic Sc (NALSAR), Dip in Psychology (ALISON), Dip in Cyber Law (ASCL), Dip in International Convention & Maritime Law (ALISON) Faculty, Heritage Law College, India*

***Corresponding Author**
Asmita Mallick, Student, Heritage Law College under University of Calcutta, India.

Submitted: 2025, Sep 26; **Accepted**: 2025 Oct 23; **Published**: 2025 Oct 29

Citation: Mallick, A., Ganguli, P. (2025). Understanding Toxic Panda: The New Cyber Threat Targeting Data Security. *Politi Sci Int, 3*(2), 01-05.

Abstract

Toxic Panda is a sophisticated Android banking trojan that targets users in Europe, Latin America, and Southeast Asia. Using advanced techniques like account takeover (ATO) and one device fraud (ODF), it bypasses security mechanisms, including multi-factor authentication, to steal sensitive data and conduct unauthorized transactions. The malware's ability to manipulate user inputs and intercept one-time passwords makes it a significant threat. This paper explores the implications of Toxic Panda, highlights the evolving landscape of cybercrime, and offers insights into preventive measures and legal frameworks to combat emerging threats.

Keywords: Toxic Panda, Android Banking Trojan, On-Device Fraud, Account Takeover, Malware Prevention, Cybersecurity Threats, Mobile Banking Fraud, Multi-Factor Authentication Bypass, Cybercrime, Remote Access Trojan, Financial Institutions Security, Mobile Security Challenges, Cybercrime Prevention, Malware Detection, Banking Trojans, Cyber Law, Digital Security

1. Introduction

The "Toxic Panda" phenomenon marks the emergence of a sophisticated Android banking Trojan that is posing serious security threats to mobile users worldwide. Originating in Asia and now spreading across Europe and Latin America since October 2024, Toxic Panda has quickly become a formidable force in the realm of cybercrime. This malware, disguised as trusted apps like Google Chrome and popular banking apps, stealthily infiltrates Android devices, giving hackers unauthorized access to users' bank accounts and personal data. Its deceptive nature and rapid spread underscore the importance of vigilance and cybersecurity awareness for Android users. As Toxic Panda continues to evolve, understanding its mechanisms and adopting proactive safety measures are crucial steps in safeguarding sensitive financial information [1].

2. Method

The Toxic Panda malware operates by luring users into downloading fake apps from unofficial sources, cleverly disguised as legitimate and popular applications. Once installed, Toxic Panda grants hackers the ability to remotely control infected Android devices, allowing them to perform actions on the phone as if they were the actual owner. This dangerous capability enables the malware to deploy On-Device Fraud (ODF) tactics, bypassing typical banking security protocols by interacting directly with the device. Consequently, it becomes significantly harder for banking apps to detect any suspicious activity, as the actions appear to be initiated by the device owner.

Toxic Panda's capabilities extend to intercepting One-Time Passwords (OTPs), which are commonly used for multi-factor authentication. By intercepting these codes, hackers can bypass critical security steps, accessing and manipulating bank accounts to perform unauthorized transactions, also known as Account Takeover (ATO). This results in substantial financial losses for victims, as the malware allows intruders to transfer funds and control accounts without alerting the user.

Additionally, Toxic Panda has broad data access capabilities, extracting sensitive information from the infected device, including personal files, contacts, media, and other stored data. This data can be exploited further, either for blackmail or to compromise

additional accounts. The malware's sophisticated techniques, including ODF and ATO, make it one of the most advanced banking Trojans to date, posing a major threat to Android users globally. Awareness, caution with app downloads, and regularly updating device security are critical steps in mitigating the risks associated with this evolving cyber threat.

In short, the method involves tricking users into downloading apps from unofficial sources, often presented as legitimate but containing hidden malware. Toxic Panda can remotely control the infected devices, enabling hackers to perform actions as if they were physically holding the phone or they are the owner of that device. Then, the On-Device Fraud (ODF) technique allows the malware to bypass security measures by operating directly on the device, making it harder for banking apps to detect suspicious activity. After that Toxic Panda can intercept and used one-time passwords (OTPs) for multi-factor authentication and hackers get access to secure transactions and accounts.

Once the device is infected, the hackers can take over banking accounts to perform unauthorized transactions, which is called Account Takeover (ATO) and leading to financial loss for the victims. Toxic Panda can access all kind of sensitive data from the infected devices, including media files, which can be used for further exploitation or blackmail.

With the increasing use of mobile devices for banking and transactions, mobile malware like Toxic Panda poses a significant threat. It uses advanced techniques and making it harder for traditional security measures to detect and prevent attacks. "Toxic Panda's main goal is to initiate money transfers from compromised devices via account takeover (ATO) using a technique known as on device fraud (ODF)," Cleafy researchers reported via Hacker News.

3. Origin and Evolution

In Early 2000s, the first notable banking Trojan named ZBOT (a.k.a. Zeus) emerged in 2006. The purpose is to steal banking credentials by injecting malicious code into legitimate banking websites1. In 2007, GOZI was another early banking Trojan that used keylogging and screen capture to steal login credentials. After that, the source code for ZBOT was leaked for leading to the creation of numerous variants and inspiring other malware families in the year of 2011 [2].

Researchers have identified Toxic Panda as a financially-motivated trojan derived from the TgToxic malware family. In late October 2024, Cleafy's Threat Intelligence team noted a sharp rise in new Android malware samples initially classified under TgToxic. Upon closer examination, it was discovered that while Toxic Panda shares some bot command structures with TgToxic, its code deviates significantly, lacking several key functionalities of the original malware. Certain commands exist only as placeholders, without actual implementation, leading researchers to categorize this malware as a new variant under the name Toxic Panda. This specialized trojan is engineered to circumvent standard banking security protocols, allowing unauthorized withdrawals from users' accounts. Toxic Panda was first detected in Asia, where it spread through side-loading techniques, enticing users to download seemingly legitimate apps from unofficial sources. Its primary targets include banking institutions, utilizing advanced techniques to evade security and initiate fraudulent transactions [3].

4. Modus Operandi

The Toxic Panda trojan operates by leveraging Android's accessibility features to gain permissions, enabling cybercriminals to conduct financial fraud, including intercepting onetime passwords (OTPs) essential for multi-factor authentication. This malware primarily spreads through sideloading, where users unknowingly download apps from unofficial sources rather than from legitimate app stores like Google Play or the Galaxy Store. Cybercriminals create realistic-looking fake app pages to lure users into downloading Toxic Panda, which is commonly disguised as trusted applications such as Google Chrome or popular banking apps. By masquerading as legitimate software, the trojan bypasses bank security checks and remains undetected on users' devices.

Once installed, Toxic Panda grants attackers' remote access to infected devices, enabling them to control the devices from any location globally. This remote capability facilitates unauthorized transactions and account takeovers, often going unnoticed by victims until they see unauthorized withdrawals in their bank statements. As of now, Toxic Panda remains unavailable on official app stores, but researchers report that it is still under active development, increasing its potential threat to Android users worldwide [1].

Researchers note that what makes Toxic Panda more dangerous is that it disguises itself as trusted applications, such as Google Chrome or popular banking apps, deceiving users and bypassing bank security checks. Victims often remain unaware that their device is compromised until they notice unauthorised transactions on their bank statements.

5. Cases Reported Around the World

The Toxic Panda cybercrime campaign, a sophisticated Android malware network, has targeted banking systems across Europe and Latin America, including countries like Italy, Spain, and Portugal. The malware, primarily affecting retail banking on Android devices, operates by hijacking banking applications through unauthorized remote access. This setup enables attackers to intercept one-time passwords, bypass two-factor authentication, and execute fraudulent transactions from the victim's device directly, effectively taking control of accounts without detection by the users. Over 1,500 devices have been infected, according to security reports, with Italy experiencing over half of the detected cases [4].

Researchers found that the Chinese-speaking group behind Toxic Panda adapted techniques common in Southeast Asia to the

European banking system, indicating a new operational focus. Toxic Panda exploits Android's accessibility services to gain permissions, allowing the malware to capture sensitive data and carry out unauthorized actions such as transferring money without user consent. Notably, the malware uses social engineering for initial infection, often prompting users to download apps from untrusted sources.

This campaign has also raised concerns about the limitations of current antivirus systems, which have struggled to detect Toxic Panda despite its relatively straightforward technical structure. The malware's creators use various code-hiding techniques to evade detection, challenging both banks and mobile security ecosystems [5].

Toxic Panda utilizes over 61 commands that overlap with TgToxic banking trojan as well as 33 new commands. It is also capable of accessing photo albums, converting the images to BASE64, and exfiltrating them to the Toxic Panda's command-and-control (C2) [6]. Toxic Panda uses one of three hardcoded domains for C2 and uses AES in ECB mode for C2 communication.

"ToxicPanda needs to demonstrate more advanced and unique capabilities that would complicate its analysis," the researchers said. "However, artifacts such as logging information, dead code, and debugging files suggest that the malware may either be in its early stages of development or undergoing extensive code refactoring—particularly given its similarities with TgToxic."

6. Emergence of ToxicPanda: A New Android Banking Malware Targeting Fraudulent Money Transfers

ToxicPanda is a new strain of Android banking malware that has infected over 1,500 devices. It enables attackers to hijack accounts and initiate fraudulent money transfers through ondevice fraud (ODF), bypassing banking security protocols like two-factor authentication. The malware spreads via fake apps posing as popular services, primarily affecting users in Europe and Latin America. ToxicPanda shares similarities with the TgToxic malware and is believed to be operated by a Chinese-speaking threat group.

Its command-and-control panel allows remote access to compromised devices for carrying out transactions [7]. Other Android malware in this category includes Medusa, Copybara, and BingoMod.

The discovery of ToxicPanda also follows a report from Netcraft that detailed another Android banking malware called HookBot7 (aka Hook) that also exploits Android's accessibility services to conduct overlay attacks in order to display bogus login pages on top of legitimate banking apps and steal credentials or other personal data.

Some of the popular institutions targeted using the malware include Airbnb, Bank of Queensland, Citibank, Coinbase, PayPal, Tesco, and TransferWise, among others. Besides harvesting sensitive data, a notable feature of the trojan is its ability to spread in a worm-like fashion by sending links to malware-laced apps via WhatsApp messages.

"HookBot can also log keystrokes and capture screenshots to steal sensitive data while the user interacts with their device," the company said. "It can also intercept SMS messages, including those used for two-factor authentication (2FA), enabling threat actors to gain full access to the victim's accounts."

HookBot is offered for sale on Telegram to other criminal actors under a malware-as-a-service (MaaS) model, costing anywhere from $80 for a weekly subscription to $640 for six months. It also comes with a builder that allows the customers to generate new malware samples and build dropper apps.

7. Android Banking Trojan Toxic Panda Targets Europe

The Cleafy threat intelligence team identified a new Android banking trojan, named ToxicPanda, which primarily targets users in Europe, particularly in Italy, Portugal, and Spain, as well as some regions in Latin America. ToxicPanda is believed to be a variant of TgToxic, a malware linked to Chinese-speaking threat actors. The malware uses on-device fraud (ODF) techniques to bypass security mechanisms, intercepting one-time passwords and manipulating user inputs. ToxicPanda is still under development, with more than 1,500 infected devices discovered. It highlights the growing challenges in mobile security, especially in the face of expanding cybercrime operations [8].

7.1 Targets of Toxic Panda: Who Is Most at Risk?

- **Android Users:** Since Toxic Panda is an Android malware, users of this operating system are the primary targets.
- **Banking Customers:** every individual person who use mobile banking apps are at higher risk, as the malware aims to steal banking credentials and perform unauthorized transactions.
- **Regions with High Infection Rates:** Users in Italy, Spain, Portugal, France, and Peru are particularly vulnerable, as these regions have seen the highest number of infections.
- **Users of Older Android Versions:** Devices running older versions of Android (such as Android 7 and earlier) are more susceptible due to known security vulnerabilities.
- **Users Downloading Apps from Unofficial Sources:** Those who download apps from unofficial sources or click on suspicious links are at higher risk of inadvertently installing the malware.

The reports further reveal that till date hundreds of users have already come into contact for this trojan and majority of these victims are reported from countries like Italy (56.8 per cent), followed by Portugal (18.7 per cent, Hong Kong (4.6 per cent), Spain (3.9 per cent, and Peru (3.4 per cent) [9,10] .

8. Future Risk

The future risks posed by ToxicPanda include increased sophistication in bypassing multifactor authentication and enhanced

targeting of financial institutions globally. As its infrastructure evolves, the malware may expand to infect more devices and regions, complicating cybersecurity efforts. Additionally, its ability to hijack financial apps and manipulate transactions could lead to significant financial losses for individuals and institutions. Given its ongoing development, ToxicPanda could also introduce new capabilities, further challenging existing security measures and posing a growing threat to mobile banking and online transactions.

8.1 Impact on Cybersecurity

• **Increased Threat Level:** Toxic Panda has raised the threat level for Android users, as it uses advanced techniques like On-Device Fraud (ODF) and Remote Access Trojan (RAT) capabilities to bypass security measures of mobile banking.
• **Need for Advanced Defences:** The sophistication of Toxic Panda has highlighted the need for more advanced and proactive cybersecurity measures to detect and prevent such threats.
• **Global Spread:** The breakdown of Toxic Panda malware has shown the global nature of cyber threats and the importance of international cooperation in cybersecurity efforts.
• **Evolving Tactics:** The cybercriminals are constantly refining their tactics because of the continuous development and evolution of Toxic Panda indicate. It is requiring cybersecurity professionals to stay vigilant and adapt their strategies.

8.2 Impact on Society

• **Financial Losses:** Victims have suffered financial losses due to unauthorized transactions and account takeovers.
• **Loss of Trust:** The spread of such malware can lead to a loss of trust in mobile banking i.e. UPI and financial institutions, as users become wary of potential security breaches.
• **Privacy Concerns:** The malware's ability to access and exfiltrate sensitive data raises concerns about privacy and data protection for individuals and organizations.
• **Increased Awareness:** The incidents involving Toxic Panda have raised awareness about the importance of cybersecurity practices, such as downloading apps from trusted sources and keeping devices updated with the latest security patches.
Overall, the impact of Toxic Panda underscores the need for robust cybersecurity measures and increased vigilance to protect against emerging threats.

9. Case Study

• **Asian Countries:** While there haven't been many detailed case studies specifically about Toxic Panda, but it was first identified in Asia, where it began spreading to other regions [1,11].
• **Hong Kong:** Toxic Panda has also shown signs of spreading to Hong Kong, indicating a potential expansion into Asia through China.
• **Europe and Latin America:** Toxic Panda has infected over 1,500 devices globally, with a significant focus on Europe (Italy, Spain, Portugal, France) and also Latin American countries like Peru. There are some cases.
• **Italy:** In early November 2024, the malware targeted users through side-loading techniques, disguising as popular apps like Google Chrome. It was a significant outbreak of Toxic Panda. Over 500 devices were affected and leaded to substantial financial losses for users and banking institutions.
• **Portugal:** In Portugal, the malware spreading through phishing campaigns and side-loading techniques. The attackers used RAT capabilities to remotely control devices and capture OTPs, leading to unauthorized transactions and steals everything.
• **Spain:** Spain experienced a similar attack, with over 300 devices infected. The malware spread through phishing campaigns and side-loading techniques, allowing attackers to perform account takeovers and steal funds.
• **France:** While there have been fewer reported cases in France also, the malware has still managed to infect several devices. The attackers used similar techniques to those in other European countries, targeting banking institutions and users through phishing and sideloading.
• **Latin America (Peru):** In other side Peru saw over 300 devices infected by Toxic Panda at the same time. The malware spread through phishing campaigns that tricked users into downloading malicious apps from unofficial sources. To remotely control devices attackers used RAT capabilities and capture OTPs to lead the account takeovers and fund theft

9.1 Role of Law in Combating the Situation

The role of law in combating the ToxicPanda malware involves implementing robust cybersecurity regulations, enforcing stricter data protection laws, and promoting cooperation between international law enforcement agencies to tackle cybercrime. Legal frameworks should also ensure that victims of such malware have access to legal recourse, compensation, and support. Moreover, laws should push for stricter penalties for cybercriminals and compel financial institutions to adopt advanced fraud detection technologies to prevent malware attacks like ToxicPanda. Strengthening the legal infrastructure can deter cybercriminal activities and help mitigate future risks.

9.2 Unchecked Cybercrime Innovation: The Role of Law Enforcement in the Rise of Toxic Panda

The evolution of ToxicPanda malware highlights a disturbing trend where parallel research and development efforts are dedicated to advancing cybercrime techniques in line with emerging technologies. This progression is fueled, in part, by the failure of law enforcement and the judicial system to adequately address the growing threat of cybercrime. The lack of timely intervention, the slow pace of adapting to new technological threats, and the inadequate response mechanisms from police and judicial bodies allow cybercriminals to innovate and exploit vulnerabilities, exacerbating the risk to individuals and institutions alike.

9.3 Precautionary Measures Against Toxic Panda Malware: Safeguarding Your Devices and Finances

To protect against ToxicPanda malware, users should avoid sideloading apps from untrusted sources and only download applications from official app stores. Enabling two-factor

authentication (2FA), being cautious of phishing attempts, and regularly updating device software can also help mitigate risks. Additionally, using mobile security software that can detect malicious activities and monitoring bank accounts for suspicious transactions are key preventive measures.

Recently, a group of researchers from the Georgia Institute of Technology, German International University, and Kyung Hee University has discovered a backend malware analysis service called DVa – short for Detector of Victim-specific Accessibility, to flag malware exploiting accessibility features on Android devices.

"Using dynamic execution traces, DVa further utilizes an abusevector-guided symbolic execution strategy to identify and attribute abuse routines to victims," they said. "Finally, DVa detects [accessibility]-empowered persistence mechanisms to understand how malware obstructs legal queries or removal attempts."

10. Conclusion

According to Cleafy, Toxic Panda still appears to be in the early stages of development. For this reason, Poly Swarm analysts consider Toxic Panda to be an emerging threat. Cleafy researchers noted ToxicPanda appears to be associated with the TgToxic banking trojan, which was previously observed targeting Android users in Southeast Asia. Toxic Panda was originally mistaken for TgToxic until further analysis discovered a considerable divergence between the source code of each family. The threat actors behind both TgToxic and Toxic Panda are thought to be the same group and are likely Chinese speakers.

In conclusion, the emergence of Toxic Panda underscores the growing sophistication of cybercrime, with threat actors continually adapting to new technologies. As this malware continues to evolve, it highlights the critical need for proactive cybersecurity measures, public awareness, and more effective legal frameworks. The collaboration between law enforcement, judiciary, and cybersecurity experts will be essential in mitigating the risks posed by threats like Toxic Panda, ensuring better protection for individuals and financial institutions alike.

*** ToxicPanda is an emerging cybercrime technique, still under investigation by security experts. As this malware continues to evolve, its full capabilities and reach remain unclear. Given the rapid technological advancements and the growing threat, this paper will be regularly updated to reflect the latest findings and developments on ToxicPanda, its impact on mobile banking, and emerging countermeasures. Ongoing research will shed light on the complexities of combating such advanced cybercrime tactics.

References

1. India Today, *ToxicPanda is the new threat for Android phones and your bank account. Here is how you can be safe.
2. Zeus/ZBOT Overview: Trojan. Malwarebytes Labs.
3. new-threat-for-android-phones-and-your-bank-account-here-is-how-you-can-be-safe-2629036-2024-11-06.
4. Mascellino, Alessandro. (2024). "ToxicPanda Malware Targets Banking Apps on Android Devices." Infosecurity Magazine.
5. Vulnera. "ToxicPanda Android Botnet Attacks Banks in Europe and Latin America." Vulnera, 8Michele Roviello, Alessandro Strino & Federico Valentini, New Android Banking Malware 'ToxicPanda' Targets Users with Fraudulent Money Transfers, THE HACKER NEWS.
6. ToxicPanda Android Banking Trojan.
7. New Android Banking Malware 'ToxicPanda' Targets Users with Fraudulent Money Transfers.
8. SecurityWeek, "Android Banking Trojan ToxicPanda Targets Europe".
9. ToxicPanda Banking Trojan Infects Over 1,500 Android Smartphones, Targets 16 Banks: Report Technology News.
10. Android Banking Trojan ToxicPanda Targets Europe SecurityWeek.
11. Indian Express, "ToxicPanda Android Malware Remotely Takes Over Your Phone to Steal Money," Indian Express.