TsarBot Trojan Hits 750+ Banking & Crypto Apps!

cyble.com/blog/tsarbot-using-overlay-attacks-targeting-bfsi-sector/

March 28, 2025

TsarBot: A New Android Banking Trojan Targeting Over 750 Banking, Finance, and Cryptocurrency Applications

Cyble analyzes TsarBot, a newly identified Android banking Trojan that employs overlay attacks to target over 750 banking, financial, and cryptocurrency applications worldwide.

Key Takeaways

- A new Android Banking Trojan, TsarBot, targets over 750 applications globally, including banking, finance, cryptocurrency, and e-commerce apps.
- TsarBot spreads via phishing sites masquerading as legitimate financial platforms and is installed through a dropper disguised as Google Play Services.
- It uses overlay attacks to steal banking credentials, credit card details, and login credentials by displaying fake login pages over legitimate apps.
- TsarBot can record and remotely control the screen, executing fraud by simulating user actions such as swiping, tapping, and entering credentials while hiding malicious activities using a black overlay screen.
- It captures device lock credentials using a fake lock screen to gain full control.
- TsarBot communicates with its C&C server using WebSocket across multiple ports to receive commands, send stolen data, and dynamically execute on-device fraud.

Overview

Cyble Research and Intelligence Labs (CRIL) discovered a new Android banking trojan that uses an overlay attack to target over 750 applications, including banking, finance, cryptocurrency, payment, social media, and e-commerce applications, across multiple regions.

While the malware mainly utilizes overlay attacks to steal credentials, it also carries out various other malicious actions. It is capable of recording and remotely controlling the screen, enabling attackers to monitor and manipulate the device. Additionally, it employs lock-grabbing techniques, keylogging, and intercepting SMS messages.

The analyzed samples indicate the presence of a newly discovered banking trojan, which we are internally tracking as "TsarBot," a name chosen due to the threat actor's suspected Russian origin. During our investigation, we identified multiple log entries in Russian within the malicious application, suggesting that a Russian-speaking threat actor likely developed the malware.

Figure 1 – Logs in the Russian Language

TsarBot has been observed spreading through a phishing site that impersonates the official Photon Sol website. The phishing site deceptively offers a download option for an application to start trading, whereas the legitimate website lacks such an option.

The following phishing sites impersonate legitimate entities and distribute dropper applications that, once installed on the targeted device, will deploy TsarBot.

- hxxps://solphoton[.]io
- hxxps://solphoton[.]app
- hxxps://cashraven[.]online

Figure 2 – Phishing site distributing TsarBot

Figure 3 – Phishing site distributing TsarBot

Technical Details

As previously mentioned, the phishing site delivers a dropper application that stores the TsarBot APK file, implant.apk, in the “res/raw” folder. The dropper utilizes a session-based package installer to deploy the TsarBot malware on the device.

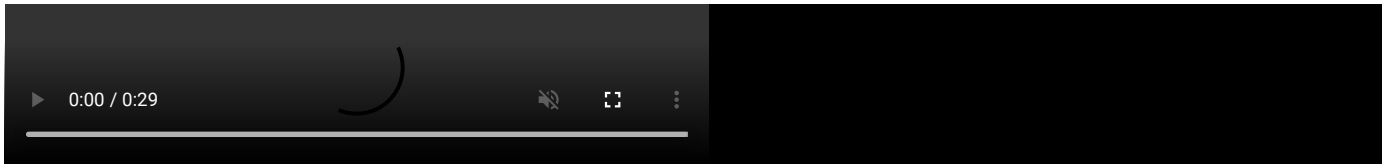

Figure 4 – Dropper installing TsarBot

TsarBot conceals itself as the Google Play Service app and does not display a launcher icon. Upon installation, it presents a fake Google Play Service update page, prompting the user to enable Accessibility services.

Figure 5 – Malware prompting victims to enable Accessibility services

WebSocket Connection

After the victim enables the Accessibility service, the malware establishes a socket connection with the C&C server **“hxxp://95.181[.]173.76”** using four different ports listed below:

- 9001 – To receive commands
- 9002 – To send captured screen content
- 9004 – To receive different sets of commands
- 9030 – To send data to the server

TsarBot can receive various commands from the server, primarily focused on-screen control, enabling it to carry out on-device fraud.

Command	Description
Command Received from 9001 Port	
REQUEST_CAPTURE	Prompt to start screen capturing and initiates screen recording
CLICK_DESCRIPTION	Click on the screen containing the mentioned description
CLICK_TEXT	Clicks on the text present on the screen
SWIPE_RIGHT	Makes a swipe-right gesture
TAP	Taps on the screen
BACK	Take the user to the back screen
HOME	Take the user to the home screen
RECENT_APPS	Takes to the recent app
CLICK_NEAR_TEXT	Click on the button near the mentioned text
CLICK_INDEX	Check the clickable object on the given index and perform a click
ZOOM_IN	Zoom in screen
TAP_COORDINATES	Taps on the mentioned co-ordinates on the screen
SWIPE_UP	Makes swipe-up gesture
SWIPE_DOWN	Makes swipe-down gesture
SWIPE_LEFT	Makes swipe-left gesture
LAUNCH_APP	Launch app
ZOOM_OUT	Zoom out screen
Commands Received from 9004 Port	
click_by_text	Clicks on the element matching text
stop_sending_tree	Stops sending ketlogs
swipe_up	Make a swipe-up gesture
tap	Makes a tap gesture
home	Takes to the home screen
hide_black_overlay	Remove the black overlay from the screen
swipe_down	Makes a swipe-down gesture
swipe_left	Makes a swipe left gesture
show_black_overlay	Displays a black overlay on the screen
swipe_right	Make a swipe-right gesture
recents	Take to the recent screen
start_sending_tree	Starts sending keylogs
paste_text	Paste text into the edit field on the screen

Screen Recording

As outlined in the command table, when TsarBot receives the **"REQUEST_CAPTURE"** command, it prompts the user to enable screen capture permissions. Once granted, the malware initiates the screen capture service, transmitting the captured screen content to the C&C server via a WebSocket connection on port 9002.

Figure 6 – Screen capture service

By capturing screen content and executing server-issued screen control commands, TsarBot can carry out fraudulent transactions on the targeted device by concealing this fraud activity with a black overlay screen.

Lock Grabber

TsarBot incorporates the LockTypeDetector feature to determine the device's lock type using the Accessibility service. It detects specific on-screen text or descriptions, such as "PIN area," "Device password," or a pattern, to identify the lock method. Once identified, it saves the lock type status for future use in lock-grabbing operations.

Figure 7 – Lock type detection code

When TsarBot receives the "USER_PRESENT" action for the first time, it loads a fake lock screen based on the detected lock type from "hxxps://xdjhgfgjh[.]run/injects/htmlPIN/android.PinCode.html" and captures the user's lock password, PIN, or pattern.

Figure 8 – Malware loading fake lock screen

Overlay Attack

TsarBot connects to the URL **“**hxxps://xdjhgfgjh[.]run/injects/ServiceName.txt**“** to retrieve a list of targeted application package names. Most of these belong to banking apps from various regions, including France, Poland, the UK, India, the UAE, and Australia. The remaining package names are associated with e-commerce, social media, messaging apps, cryptocurrency, and other categories.

Figure 9 – TsarBot receiving the target application package names

TsarBot collects the installed applications on the infected device and compares them against the package names received from the server, maintaining a target list for overlay attacks.

Figure 10 – Malware comparing the installed application package names with the target list received from the server

When the victim interacts with an application, TsarBot checks its package name against the maintained target list. If the application is found in the targeted list, it then retrieves the corresponding injection page from **“**hxxps://xdjhgfgjh[.]run/injects/html/{packagename}.html**“** and loads it into a WebView.

Figure 11 – Creating an overlay window on top of the targeted application

The injection page mimics a legitimate application, tricking users into entering sensitive information such as net banking credentials, log in details, and credit card information. The figure below shows the injection pages for one of the target applications.

Figure 12 – Injection page for Indian Bank prompting to enter login and credit card details

The data entered into the injection phishing pages is sent to the C&C server over port 9030. After transmitting the stolen sensitive information, TsarBot removes the targeted application's package name from the list to prevent the overlay from being triggered again for the same app.

Figure 13 – Sends collected login and credit card information from overlay activity to the C&C server

Figure 14 – Removing application package name from target list

The image below shows the injection pages used by TsarBot to trick the victims into submitting sensitive information while attempting to access genuine applications.

Figure 15 – Injection pages for different applications

Conclusion

TsarBot is yet another addition to the growing list of Android banking trojans, relying on familiar yet effective tactics such as overlay attacks, screen recording, and lock grabbing. By abusing Accessibility services and WebSocket communication, it enables on-device fraud while maintaining a low profile. With its ability to target over 750 applications across multiple sectors, TsarBot underscores the persistent threat posed by banking malware. Users should exercise caution when installing apps, avoid untrusted sources, and remain vigilant against phishing sites distributing such threats.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Download and install software exclusively from official application stores, such as the Google Play Store or the iOS App Store.

- Utilize a reputable antivirus and internet security software package on all connected devices, including personal computers, laptops, and mobile devices.
- Implement strong passwords and enforce multi-factor authentication wherever feasible.
- Activate biometric security features, such as fingerprint or facial recognition, for unlocking mobile devices when available.
- Exercise caution while opening links that have been sent via SMS or emails on your mobile device.
- Ensure that Google Play Protect is enabled on Android devices.
- Be judicious when granting permissions to applications.
- Maintain updated versions of your devices, operating systems, and applications.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Procedure
Initial Access (TA0027)	Phishing (T1660)	Malware is distributed via phishing sites
Persistence (TA0028)	Event-Triggered Execution: Broadcast Receivers (T1624.001)	TsarBot listens for the BOOT_COMPLETED intent to automatically launch after the device restarts.
Defense Evasion (TA0030)	Masquerading: Match Legitimate Name or Location (T1655.001)	Malware pretending to be a genuine application
Defense Evasion (TA0030)	Application Discovery (T1418)	Collects the installed application package name list to identify the target
Defense Evasion (TA0030)	Hide Artifacts: Suppress Application Icon (T1628.001)	Hides the application icon
Defense Evasion (TA0030)	Input Injection (T1516)	Malware can mimic user interaction, perform clicks and various gestures, and input data
Credential Access (TA0031)	Input Capture: Keylogging (T1417.001)	TsarBot can collect credentials via keylogging
Collection (TA0035)	Protected User Data: SMS Messages (T1636.004)	Collects SMSs
Collection (TA0035)	Screen Capture (T1513)	Malware records screen using Media Projection
Command and Control (TA0037)	Application Layer Protocol: Web Protocols (T1437.001)	TsarBot uses HTTP to communicate with the C&C server
Exfiltration (TA0036)	Exfiltration Over C2 Channel (T1646)	Sending exfiltrated data over C&C server

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
13c30f24504cb83c8f90747a51aebc0f8fb7ed8c41fb87419b7300376cfbd7f2 1a41ae507d6f67385e2e10f106cedf80632f1eb42b864e722ad4c2e0d2b91aca 291f807cc1d9a26a04da128f3de6d136fd0974a66c38694d0559ca884bd0d359 2c4574fb07eb254e845eb86f76d8e353d13d671ba71b6e79c1e55485664d666c	SHA256	Dropper file hashes
8d2e3f46c71ba5f3dcb4e7a0359693765bf4d8e0152ad82906c42d9f7573c88f 73a6ae8331cd01dd59b8c526df2a90771dcf9d74048dc7ea51d75a3beacbd95b 0e8569ec252caf58f72c43358472f22786cd32685d23c882b4b2e38409cf2e47 957df5b8998780c50ee630ad70926bdd4ee83748ee89c3a7916e8eace9b95d88	SHA256	TsarBot
hxxps://cashraven[.]online/ hxxps://solphoton[.]app/ hxxps://solphoton[.]io/	URL	Phishing sites
hxxps://solphoton[.]io/PhotonSol.apk hxxps://cashraven[.]online/CashRaven.apk	URL	Malware distribution URLs
95.181.173[.]76	IP	C&C server
hxxps://xdjhgfgjh[.]run/injects/ServiceName[.]txt hxxps://xdjhgfgjh[.]run/injects/html/ hxxps://xdjhgfgjh[.]run/injects/htmlPIN/android[.]Passcode[.]html hxxps://xdjhgfgjh[.]run/injects/htmlPIN/android[.]Pattern[.]html hxxps://xdjhgfgjh[.]run/injects/htmlPIN/android[.]PinCode[.]html	URL	URL hosting injections

Disclaimer: This blog is based on our research and the information available at the time of writing. It is for informational purposes only and does not constitute legal, financial, or professional advice. While we strive for accuracy, we do not guarantee the completeness or reliability of the content. If any sensitive information has been inadvertently included, please contact us for correction. Cyble is not responsible for any errors, omissions, or decisions made based on this content. Readers should verify findings and seek expert advice where necessary. All trademarks, logos, and third-party content belong to their respective owners and do not imply endorsement or affiliation. All content is presented “as is” without any guarantee that it is free of confidential, proprietary, or otherwise sensitive information. If you believe any portion of this content contains inadvertently shared or sensitive data, please contact us immediately so that we may address and rectify the issue. No Liability for Errors or Omissions Due to the dynamic nature of cyber threat activity, this [blog/report/article] may include partial, outdated, or otherwise incorrect information due to unverified sources, evolving security threats, or human error. We expressly disclaim any liability for errors or omissions or any potential consequences arising from the use, misuse, or reliance on this information.