BlackRock Android Malware (CSB20-12)

BlackRock Malware is a banking Trojan derived from the code of the existing Xerxes malware that is known strain of the LokiBot Android Trojan. However, despite being a banking Trojan, the malicious code is said to target non-financial apps.

It targets a total of 337 apps, which is significantly higher than any of the already known malicious code. The list of 226 targeted apps specifically for BlackRock's credential theft include Amazon, Google Play Services, Gmail, Microsoft Outlook, and Netflix, among others. Similarly, there are also 111 credit card theft target apps that include popular names such as Facebook, Instagram, Skype, Twitter, and WhatsApp.

The malware is capable of deflecting usage of an antivirus software such as Avst, AVG, BitDefender, Eset, Trend Micro, Kaspersky, or McAfee.

It can steal information like passwords and credit card information.

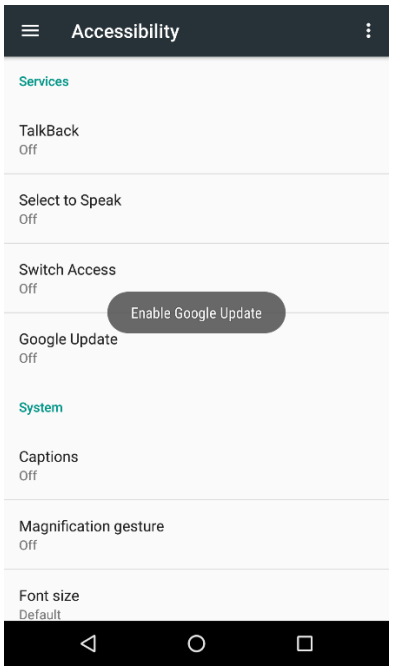
How it works

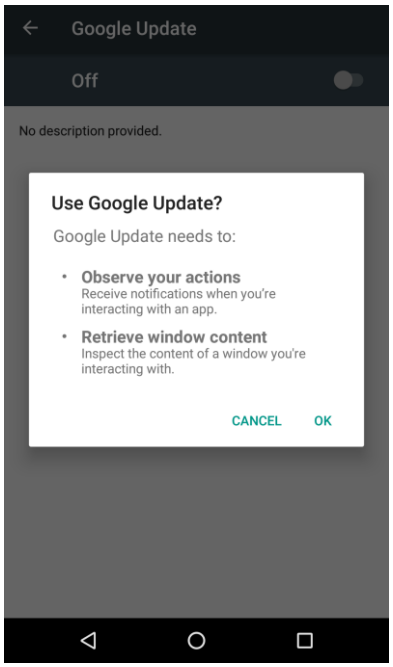
Any form of phishing

Hide its icon from the app drawer, making it invisible to the end-user

Asks the victim for the Accessibility Service privileges. Posing as fake Google updates

Access granted by the user





BlackRock grants itself additional permissions for the bot to fully functional without having to interact any further with the victim and to receive commands from the C2 server and perform the overlay attacks

BlackRock collects user information **by abusing the Accessibility Service of Android and overlaying a fake screen on top of a genuine app**. One of the overlay screens used for malicious activities is a generic card grabber view that could help attackers gain credit card details of the victim. It can also bring a specific per-targeted app for credential phishing, asks users to grant access to the Accessibility Service feature after surfacing as a Google Update. Once granted, it hides its app icon from the app drawer and starts the malicious process in the background. Then **grant other permissions itself** and use Android work profiles to control a compromised device.

Commands

Command	Description
Send_SMS	Sends an SMS
Flood_SMS	Sends an SMS to a specific number every 5 seconds
Download_SMS	Sends a copy of SMS messages to C2
Spam_on_contacts	Sends an SMS to each of the contacts present on the infected device
Change_SMS_Manager	Set malware as default SMS manager (command is repeated every 30 seconds until action is achieved)
Run_App	Starts a specific app on the bot
StartKeyLogs	Logs text content shown on the screen from targets and sends it to the C2
StopKeyLogs	Stops logging the accessibility events from targets
StartPush	Send a copy of all notifications content to the C2
StopPush	Stops sending a copy of all notifications content to the C2
Hide_Screen_Lock	Keeps the device on the HOME screen

Unlock_Hide_Screen	Unlocks the device from the HOME screen
Admin	Makes the both request admin privileges
Profile	Adds a managed admin profile for the malware on the device
Start_clean_Push	Dismisses (hiding) all push notifications
Stop_clean_Push	Stops dismissing push notifications

Impact

- Intercept SMS messages;
- Perform SMS floods;
- Spam contacts with predefined SMS;
- Start specific apps;
- Log key taps (keylogger functionality);
- Show custom push notifications;
- Sabotage mobile antivirus apps; and
- Identity theft

How to Secure

- Download apps only from the Google Play stores;
- Use strong passwords;
- Beware of spam and phishing emails;
- Verify the owner of the app; and
- Always check app permissions

References

https://gadgets.ndtv.com/apps/news/blackrock-android-malware-banking-trojan-lokbot-user-credentials-credit-card-information-2264633#:~:text=The%20malware%2C%20called%20BlackRock%2C%20is,to%20target%20non%2Dfinancial%20apps;

https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html;

https://indianexpress.com/article/explained/blackrock-android-malware-337-apps-data-privacy-6513223/#:~:text=BlackRock%20works%20like%20most%20Android%20malware.&text=BlackRock%20uses%20the%20phone's%20Accessibility,invisible%20to%20the%20end%2Duser