BLACKROCK THREAT ADVISORY

What is it?

BlackRock – an advanced Android malware derived from Xeres malware – evades detection and steals login credentials or credit card data from 337 different mobile banking, shopping, lifestyle, and video apps. BlackRock was disclosed in July 2020 by ThreatFabric. The Zimperium z9 engine had begun detecting early variants of BlackRock in the weeks prior to the full public disclosure with our patented on-device engine.

How it works

1. Your mobile app user first installs a utility app containing connections to the BlackRock malware server. These apps are often handy currency conversion, stock information, or trading apps. (The BlackRock malware is not present on the device yet, to evade detection from Google Play.)

2. Days later, the malicious utility app updates itself to deliver the BlackRock malware files to your user's device.

3. Once installed, the malware then launches and hides from the user so as not to cause concern.

4. The malware then cleverly achieves device access to the user's Accessibility Service by tricking your user into clicking on and agreeing to a fake Google update. This phony update allows the malware to gain more privileges on your user's device.

5. BlackRock then automatically grants itself additional permissions after receiving the requested Accessibility Service privilege and communicates with its command and control server.

6. BlackRock then abuses the Accessibility Service (provided by your user) to display a malicious overlay screen that exactly mimics your app's login screen. Your users cannot detect this fake overlay screen on top of your app running in the foreground. Your user will unknowingly provide her banking login credentials or credit card information directly to the attackers. The malware also contains functions to capture incoming SMS messages to record second-factor authentication information.

7. Captured credit card numbers and account credentials can be used for fraud payments, transfers, or sold on the Black Market.

Who is targeted?

BlackRock contains instructions to provide credit card overlays on 111 different apps. Half of the apps targeted (55) are Books and Reference apps, a third (33) are Communication apps, and the remainder constitutes Dating, Lifestyle, and Video player apps. Many of these apps are new targets since the coronavirus pandemic changed mobile usage and user habits. According to App Annie, the average weekly time spent in Android mobile apps increased by 25% during the first half of 2020 compared to 2019. A large portion of the increase constitutes dating and business video apps as users are limited to connecting online vs. in person.

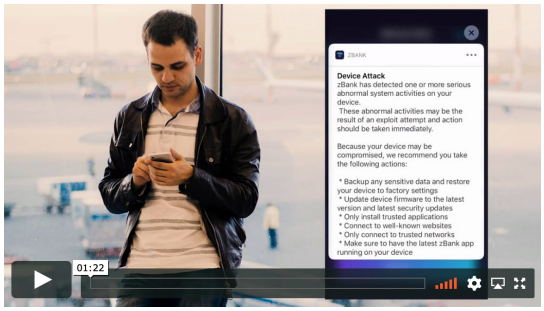
BlackRock also contains code to phish credentials using display overlays from 198 different Finance apps. It targets eight (8) shopping apps and the remainder from Auto, Communication, and Entertainment categories (Full list linked below). The first half of 2020 saw mobile commerce eclipse that of 2019's holiday shopping season. Again, this is caused by the coronavirus pandemic and why this malware is targeting these app categories.

How is it detected?
Zimperium maintains the market-leading machine-learning-based mobile malware detection solution. Our malware detection found BlackRock exhibited similar characteristics to known malware, and therefore, our detection engine classifies it as malware without signatures. Detecting malware behavior and not relying on signatures is particularly important since BlackRock forces users to different screens if a signature-based malware detection app is present on the same device.

How do app developers defend against it?
BlackRock is constructed to capture login credentials or credit card information from 337 targeted apps while attempting to evade detection. Zimperium's zDefend mobile threat defense SDK detects BlackRock and other malware that abuse privileges to become persistent and phish your users.

Mobile app developers install zDefend into mobile apps to detect mobile malware, compromised devices, and network attacks threatening your mobile app users. zDefend provides mobile risk, threat, and attack data to your security and fraud teams. The information enables your teams to make informed decisions to limit fraud and protect your users and brand.

It is essential to defend against BlackRock and other malware variants to limit fraudulent transactions initiated from your customers' accounts or having their data stolen. According to RSA's Q1 2020 Fraud report, 72 percent of fraudulent transactions originate from mobile devices. Mobile devices are valuable targets since fraudulent transactions initiated from mobile devices are more than two times as costly at $767 per transaction vs. $364 for all others.



How do mobile device managers defend against it?
BlackRock is designed to capture login credentials or credit card information from 337 targeted apps your employees may have on their devices. If zIPS (or one of our partner's mobile threat defense apps) is active on your employees' devices, our core machine learning-based engine, z9, will detect BlackRock or other malware installed on your employees' devices. When detected, your mobile security administrator will have the option to remediate the threat and create compliance policies to remediate future instances. It is essential to identify and remediate this threat to keep your employees safe and protect company assets. Further complications could arise if employees reuse credentials and passwords to login to company systems.

Install Zimperium to detect BlackRock and other mobile malware
Contact us for a custom mobile threat briefing or to obtain trial mobile security software.

Sources:
https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html
https://www.zdnet.com/article/new-blackrock-android-malware-can-steal-passwords-and-card-data-from-337-applications/
https://thehackernews.com/2020/07/android-password-hacker.html
https://www.appannie.com/en/insights/market-data/coronavirus-impact-mobile-economy/