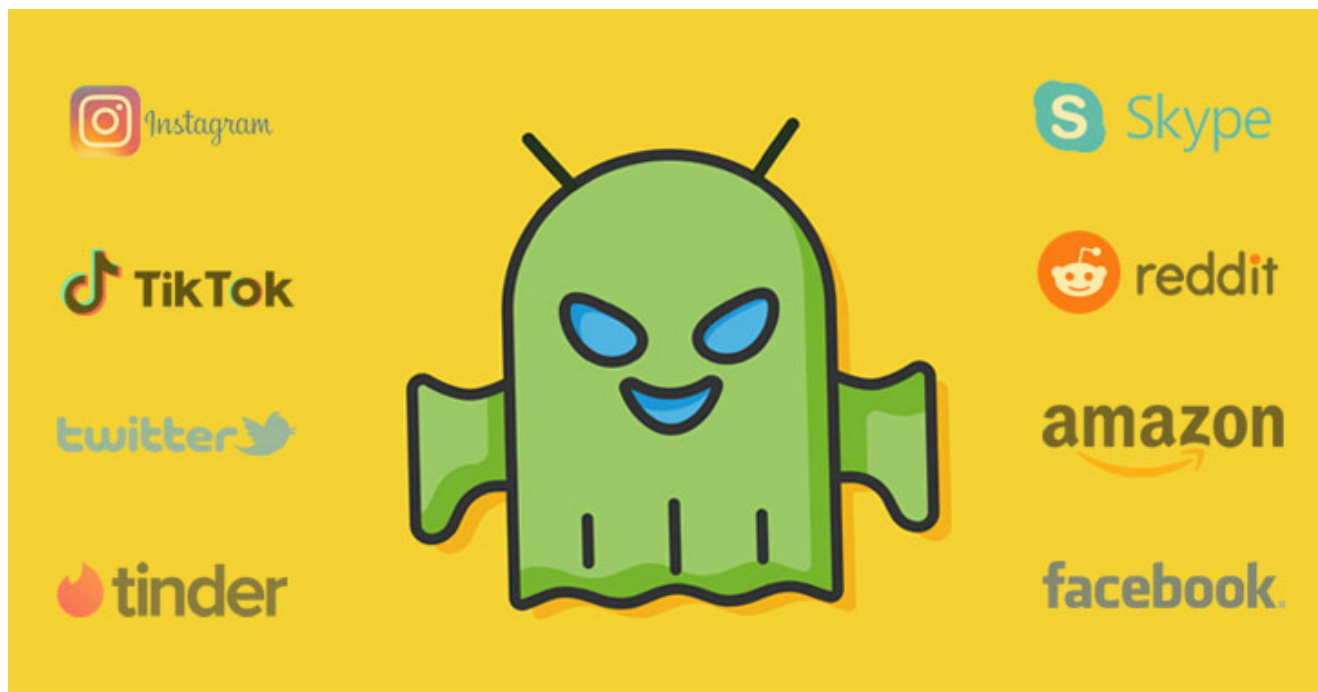


New Android Malware Now Steals Passwords For Non-Banking Apps Too

📅 July 16, 2020 👤 Ravie Lakshmanan



(<https://thehackernews.com/images/->

Nr0Ecy1ikdg/XxAZubHHdOI/AAAAAAAAA3CE/EK1ASH5tycsPG0l49ygne81GveD-4lrQwCLcBGAsYHQ/s728-e100/android-password-stealer.jpg)

Cybersecurity researchers today uncovered a new strain of banking malware that targets not only banking apps but also steals data and credentials from social networking, dating, and cryptocurrency apps—a total of 337 non-financial Android applications on its target list.

Dubbed "[BlackRock](#)

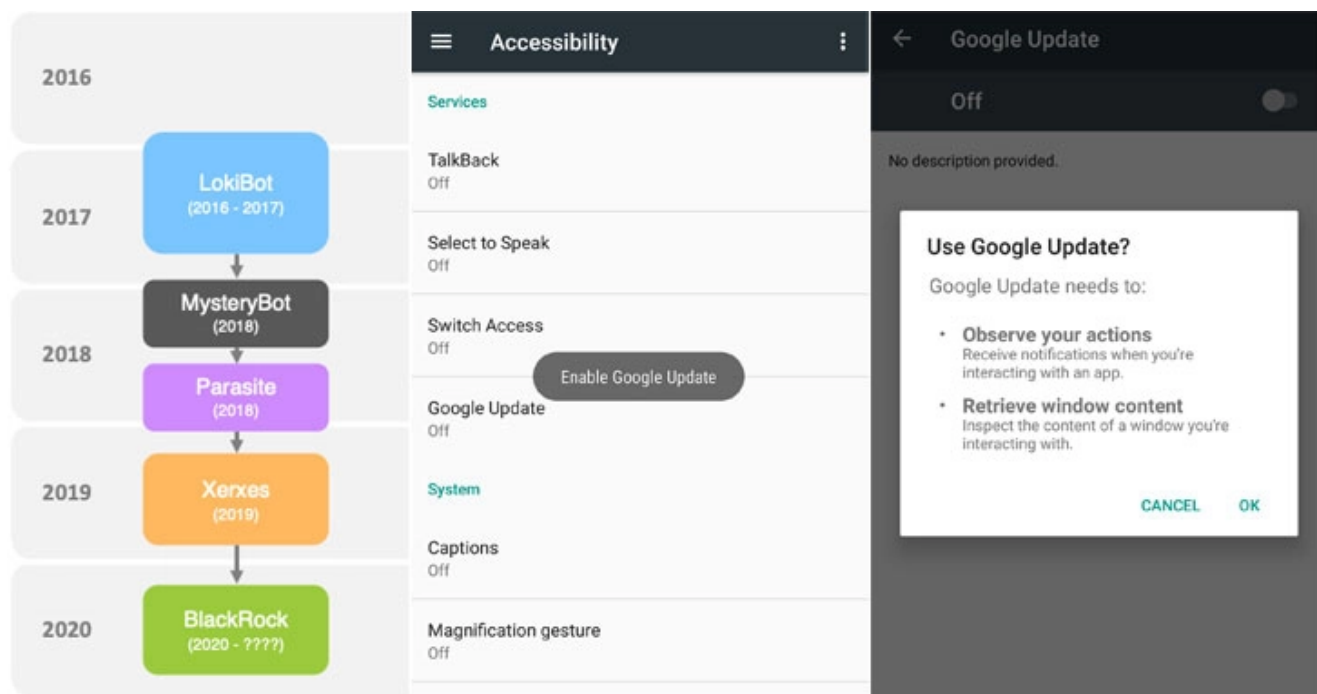
(https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html) " by

ThreatFabric researchers, which discovered the trojan in May, its source code is derived from a leaked version of Xerxes banking malware, which itself is a strain of the [LokiBot Android banking trojan](#) (<https://thehackernews.com/2017/03/android-malware-apps.html>) that was first observed during 2016-2017.

Chief among its features are stealing user credentials, intercepting SMS messages, hijacking notifications, and even recording keystrokes from the targeted apps, in addition to being capable of hiding from antivirus software.

"Not only did the [BlackRock] Trojan undergo changes in its code, but also comes with an increased target list and has been ongoing for a longer period," ThreatFabric said.

"It contains an important number of social, networking, communication and dating applications [that] haven't been observed in target lists for other existing banking Trojans."

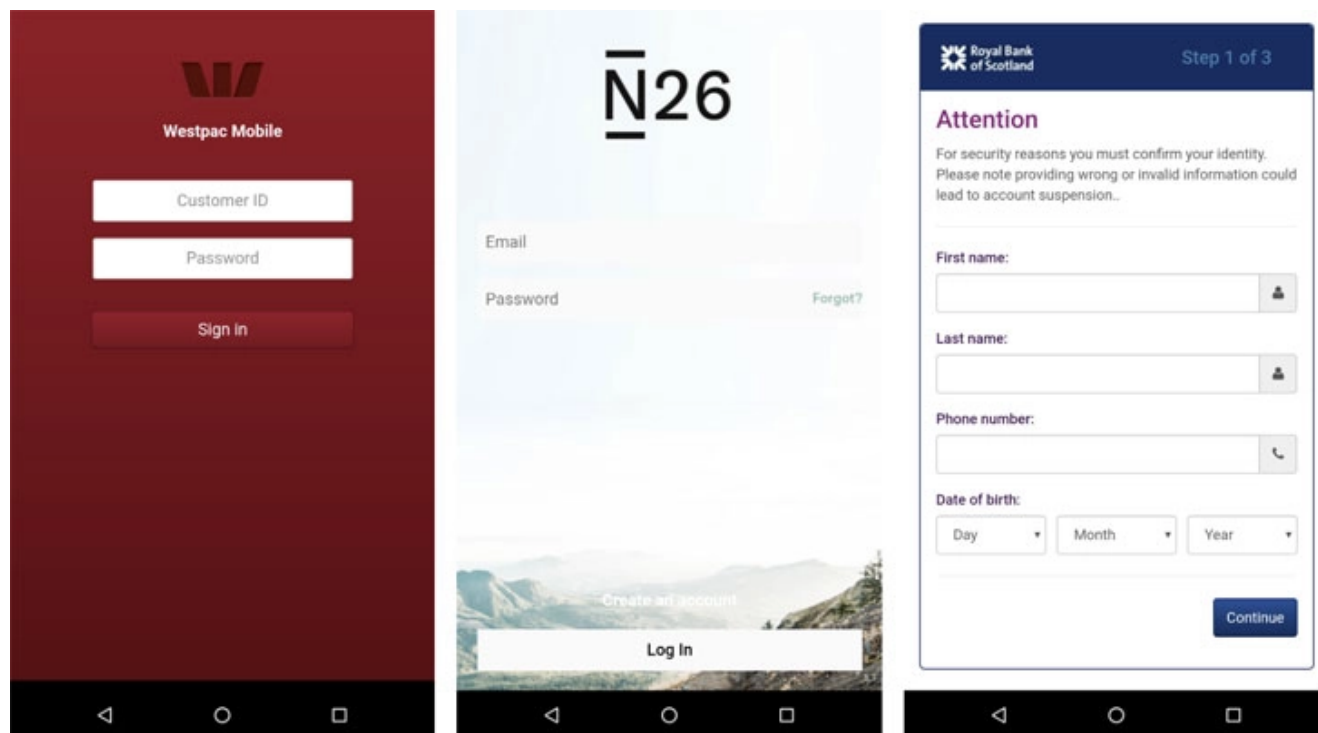


(<https://thehackernews.com/images/-0gNHAZtQMqc/XxAG5wn5dzl/AAAAAAAAAAkY/gaMOuMB2maMYZyXlgHs6-ASoUAp536yKACLCBGAsYHQ/s728-e100/android-banking-malware.jpg>)

BlackRock does the data collection by abusing Android's Accessibility Service privileges, for which it seeks users' permissions under the guise of fake Google updates when it's launched for the first time on the device, as shown in the shared screenshots.

Subsequently, it goes on to grant itself additional permissions and establish a connection with a remote command-and-control (C2) server to carry out its malicious activities by injecting overlays atop the login and payment screens of the targeted apps.

These credential-stealing overlays have been found on banking apps operating in Europe, Australia, the US, and Canada, as well as shopping, communication, and business apps.



([https://thehackernews.com/images/-](https://thehackernews.com/images/-vutbNApkgPo/XxAHlaqHIUI/AAAAAAAAAAkg/t746HeOxq1A9Hsnd4gvTollQvrghBtiCwCLcBGAsYHQ/s728-e100/android-banking-malware.jpg)

[vutbNApkgPo/XxAHlaqHIUI/AAAAAAAAAAkg/t746HeOxq1A9Hsnd4gvTollQvrghBtiCwCLcBGAsYHQ/s728-e100/android-banking-malware.jpg](https://thehackernews.com/images/-vutbNApkgPo/XxAHlaqHIUI/AAAAAAAAAAkg/t746HeOxq1A9Hsnd4gvTollQvrghBtiCwCLcBGAsYHQ/s728-e100/android-banking-malware.jpg))

"The target list of non-financial apps contains famous applications such as but not limited to Tinder, TikTok, PlayStation, Facebook, Instagram, Skype, Snapchat, Twitter, Grinder, VK, Netflix, Uber, eBay, Amazon, Reddit and Tumblr," the researchers told The Hacker News.

This is not the first time mobile malware has abused Android's accessibility features.

Earlier this year, IBM X-Force researchers detailed a new TrickBot campaign, called [TrickMo](https://thehackernews.com/2020/03/trickbot-two-factor-mobile-malware.html) (<https://thehackernews.com/2020/03/trickbot-two-factor-mobile-malware.html>), that was found exclusively targeting German users with malware that misused accessibility features to intercept one-time passwords (OTP), mobile TAN (mTAN), and pushTAN authentication codes.


Then in April, Cybereason uncovered a different class of banking malware known as [EventBot](https://thehackernews.com/2020/04/android-banking-keylogger.html) (<https://thehackernews.com/2020/04/android-banking-keylogger.html>) that leveraged the same feature

to exfiltrate sensitive data from financial applications, read user SMS messages, and hijack SMS-based two-factor authentication codes.

What makes BlackRock's campaign different is the sheer breadth of the applications targeted, which go beyond the mobile banking apps that are typically singled out.

"After Alien, Eventbot, and BlackRock we can expect that financially motivated threat actors will build new banking Trojans and continue improving the existing ones," ThreatFabric researchers concluded.

"With the changes that we expect to be made to mobile banking Trojans, the line between banking malware and spyware becomes thinner, [and] banking malware will pose a threat for more organizations."

Found this article interesting? Follow THN on [Facebook](https://www.facebook.com/thehackernews) (<https://www.facebook.com/thehackernews>) , [Twitter](https://twitter.com/thehackersnews)  (<https://twitter.com/thehackersnews>) and [LinkedIn](https://www.linkedin.com/company/thehackernews/) (<https://www.linkedin.com/company/thehackernews/>) to read more exclusive content we post.