Widespread FluBot and TeaBot Malware Campaigns Targeting Android Devices

thehackernews.com/2022/01/widespread-flubot-and-teabot-malware.html

January 27, 2022

Researchers from the Bitdefender Mobile Threats team said they have intercepted more than 100,000 malicious SMS messages attempting to distribute Flubot malware since the beginning of December.

"Findings indicate attackers are modifying their subject lines and using older yet proven scams to entice users to click," the Romanian cybersecurity firm detailed in a report published Wednesday. "Additionally, attackers are rapidly changing the countries they are targeting in this campaign."

The new wave of attacks is said to have been most active in Australia, Germany, Poland, Spain, Austria, and Italy, among others, with attacks spreading to newer countries like Romania, the Netherlands, and Thailand starting mid-January.

FluBot (aka Cabassous) campaigns use smishing as the primary delivery method to target potential victims, wherein users receive an SMS message with the question "Is this you in this video?" and are tricked into clicking a link that installs the malware.

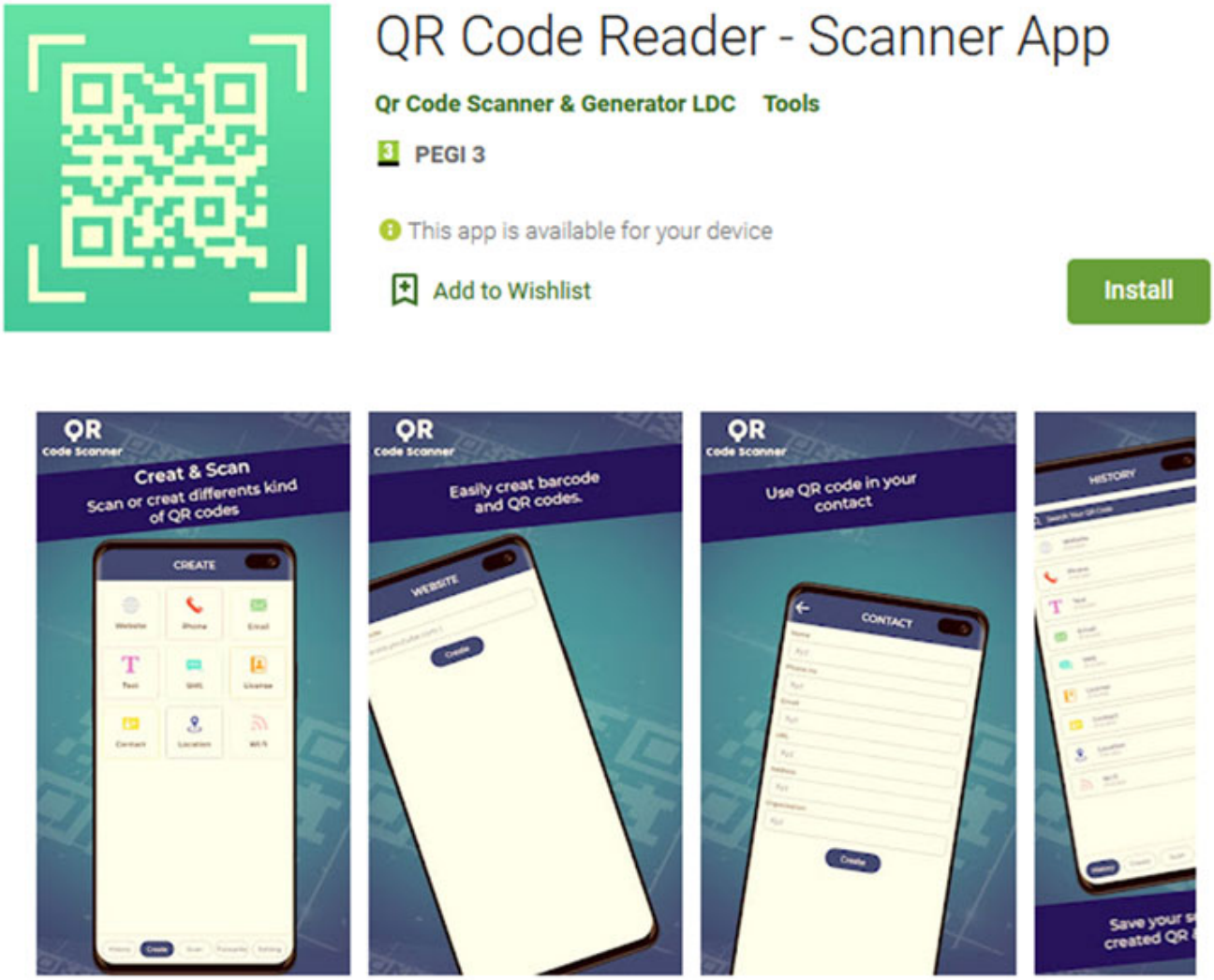
"This new vector for banking trojans shows that attackers are looking to expand past the regular malicious SMS messages," the researchers said.

TeaBot masquerades as QR Code Scanner Apps

It's not just FluBot. Another Android trojan called TeaBot (aka Anatsa) has been observed lurking on the Google Play Store in the form of an app named "QR Code Reader - Scanner App," attracting no fewer than 100,000 downloads while delivering 17 different variants of the malware between December 6, 2021, and January 17, 2022.

In a tactic that's becoming increasingly common, the app does offer the promised functionality, but it's also designed to retrieve a malicious APK file hosted on GitHub, but not before ascertaining that the country code of the current registered operator doesn't start with a "U."

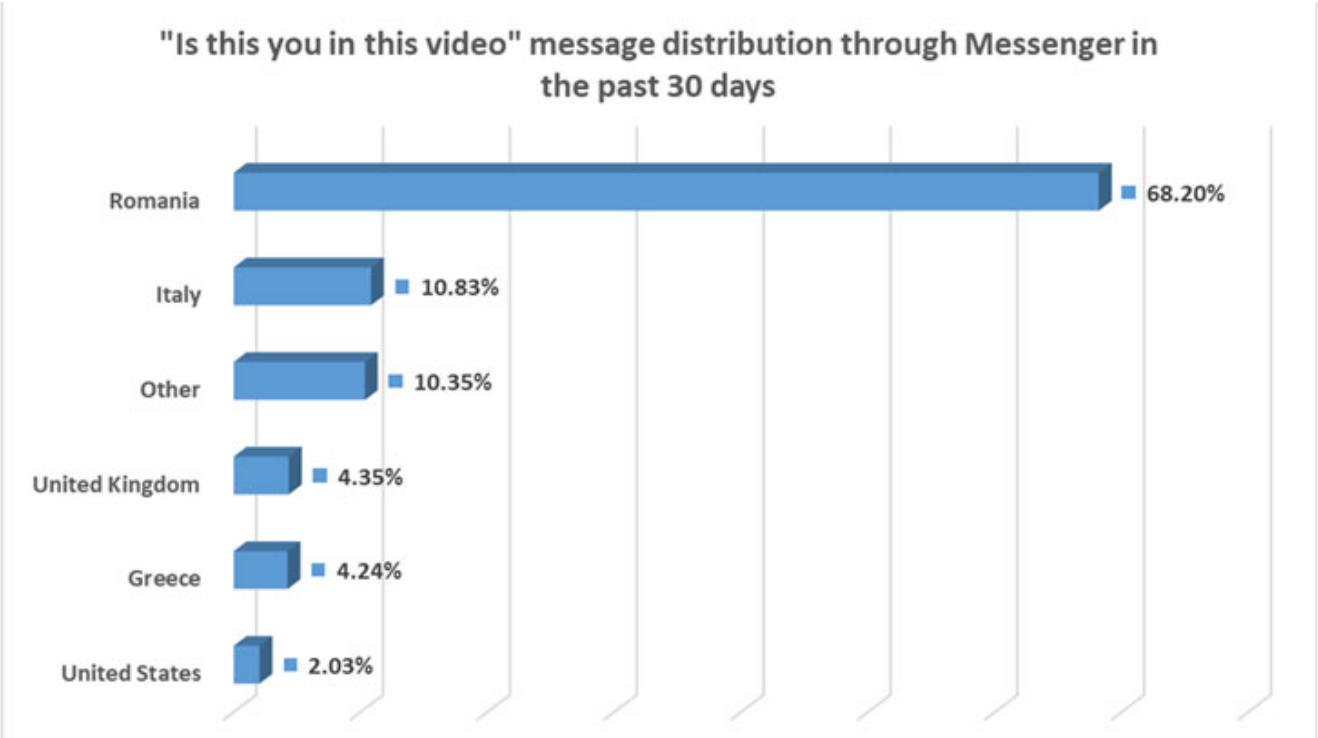
The installation of the rogue app then involves presenting a fake UI notifying the user that an add-on update is required and that the setting to allow installs from unknown sources needs to be enabled in order to apply the update.



BitDefender said it identified four more dropper apps — 2FA Authenticator, QR Scanner APK, QR Code Scan, and Smart Cleaner — that were available on the Play Store and distributed the TeaBot malware since at least April 2021.

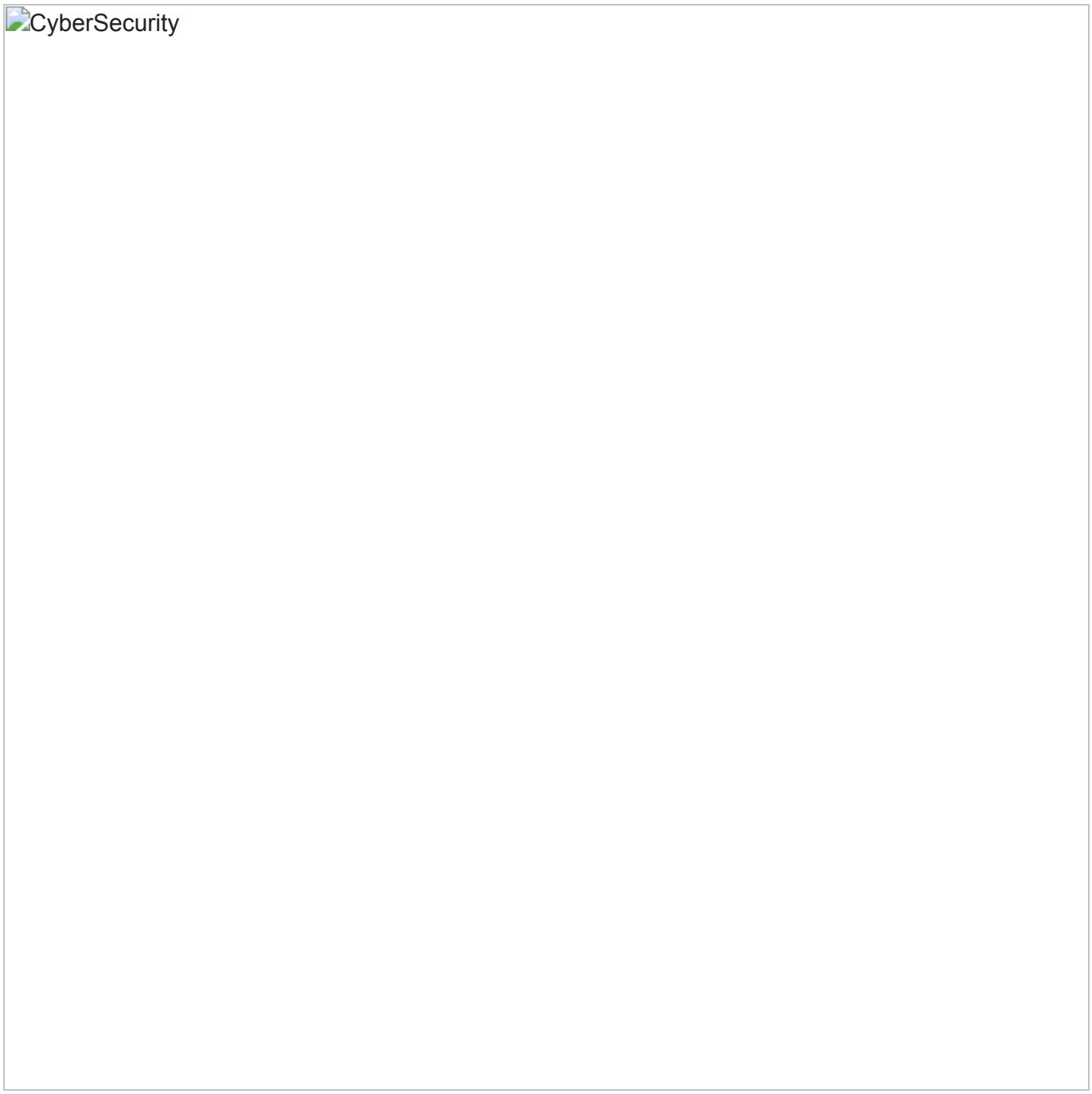
Another technique of interest adopted by the operators is versioning, which works by submitting a benign version of an app to the app store for purposes of evading the review process put in place by Google, only to replace the codebase over time with additional malicious functionality through updates at a later date.

Beyond circumventing the Play Store protections to reach a wider infection pool, the malware authors are believed to have paid to appear in Google Ads served within other legitimate applications and games, "giving them screen time in an app that could have millions of users."



The analysis also corroborates a previous report from Dutch cybersecurity firm ThreatFabric, which found six Anatsa droppers on the Play Store since June 2021. The apps were programmed to download an "update" followed by prompting users to grant them Accessibility Service privileges and permissions to install apps from unknown third-party sources.

In a related development, researchers from Pradeo found that a two-factor authenticator app called "2FA Authenticator" distributed through the Google Play store and downloaded more than 10,000 times was saddled with a banking trojan named Vultr, which targets financial services to steal users' banking information.



"The application called 2FA Authenticator is a dropper leveraged to spread malware on its users' devices," the researchers said. "It has been developed to look legitimate and provide a real service. To do so, its developers used the open-source code of the official Aegis authentication application to which they injected malicious code."

"Malicious actors treat malware like a product, with development and versioning, working hard to circumvent security technologies and gain more victims," Richard Melick, director of product strategy for endpoint security at Zimperium, said.

"When one version gets disrupted, the malicious actors go back to developing the next version, especially when the outcomes have been effective. And the mobile endpoint is an incredibly lucrative target for attackers," Melick added.

From GriftHorse to Dark Herring

The development comes as Zimperium zLabs disclosed details of yet another premium service abuse campaign along the lines of GriftHorse that leveraged as many as 470 innocuous-looking apps to subscribe users to paid services costing $15 per month without their knowledge.

The billing fraud, also categorized as "fleeceware," is said to have affected upwards of 105 million users across more than 70 countries, with most victims located in Egypt, Finland, India, Pakistan, and Sweden.

The mammoth operation, which the mobile security company codenamed "Dark Herring," has been backtraced to March 2020, making it one of the longest-running mobile SMS scams discovered to date.

While the huge nest of trojan apps have since been purged from the Play Store, they are still available on third-party app stores, once again underscoring the potential dangers when it comes to sideloading applications onto mobile devices.

"In addition to over 470 Android applications, the distribution of the applications was extremely well-planned, spreading their apps across multiple, varied categories, widening the range of potential victims," Zimperium researcher Aazim Yaswant said. "The apps themselves also functioned as advertised, increasing the false sense of confidence."