Over 100 Million Android Users Installed 'Dark Herring' Scamware

By Ionut Arghire on January 28, 2022

More than 105 million Android users downloaded and installed scamware from Google Play and third-party app stores, according to mobile security firm Zimperium.

A total of 470 malicious applications, collectively named Dark Herring, were used to target users in 70 countries in what appears to be the largest SMS scam campaign known to date. Called GriftHorse, a previous similar campaign compromised roughly 10 million users globally.

The Dark Herring campaign has been ongoing since at least March 2020, subscribing users to services that charge them with an average monthly premium of $15. With millions of dollars in recurring revenue generated monthly, the attackers caused total losses of hundreds of millions.

The campaign remained active for such a long period of time because the malicious applications provided users with the expected functionality, which allowed them to remain installed on the victims' devices.

Once installed on a device, the Dark Herring applications start communicating with the command and control (C&C) server to send over the victim's IP address, which is used to target the victim for direct carrier billing subscription.

Next, the victim is taken to a geo-specific webpage where they are prompted to provide their phone number, allegedly for verification purposes. However, unbeknown to the victim, they are in fact submitting the phone number to a premium service.

“The victim does not immediately notice the impact of the theft, and the likelihood of the billing continuing for months before detection is high, with little to no recourse to get one’s money back,” Zimperium says.

[READ: Many Security Products Fail to Detect Android Malware Variants]

The 470 Dark Herring applications were published to Google Play between March 2020 and November 2021, but all of them have been removed from the official store. However, they remain available through third-party stores.

The threat actors behind the campaign appear to have built infrastructure “to handle the communication coming from several applications with unique identifiers and responding accordingly,” Zimperium says.

Immediately after installation, the applications load into webview a first-stage endpoint hosted on Cloudfront. Links to JavaScript files that are hosted on AWS are sent in response to the initial request.

These allow the application to download resources needed to start the next stage of the process. Zimperium also observed that only individuals in specific countries are eventually subscribed to direct carrier billing.

Dark Herring, Zimperium notes, is likely the work of a well-organized group: the 470 applications are uniquely produced and not clones, a significant investment was made in developing the infrastructure needed to keep the scam operational, and the distribution of the apps was well-planned, over multiple categories.

“Due to the nature of Direct Carrier Billing, some countries might have been targeted with less success than others due to the consumer protections set in place by telcos. Based on the collected intel, the Zimperium zLabs team estimates that Dark Herring has attempted to infect over 105 million devices since March 2020,” Zimperium concludes.

Related: Tens of Thousands Download "AbstractEmu" Android Rooting Malware

Related: New ‘SharkBot’ Android Banking Malware Hitting U.S., UK and Italy Targets

Related: Android Banking Trojan 'Vultur' Abusing Accessibility Services

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Zerodium Offering $400,000 for Microsoft Outlook Zero-Day Exploits

HackerOne Bags $49 Million in Series E Funding

Xerox Quietly Patched Device-Bricking Flaw Affecting Some Printers

Over 100 Million Android Users Installed 'Dark Herring' Scamware

Outlook Security Feature Bypass Allowed Sending Malicious Links