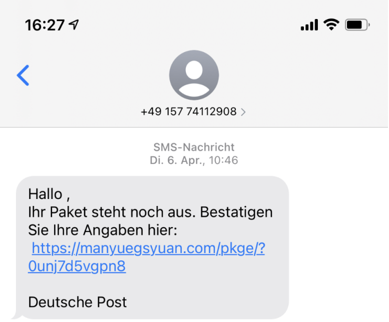
FluBot Smishing

Overview

Across Europe, particularly in Germany, mobile users are being targeted with a mobile phishing campaign that delivers the FluBot banking trojan. The attackers use phone numbers leaked in the recent Facebook data breach of 530 million users to deliver the phishing messages. To trick their victims, they use the guise of validating or providing updates about shipments from Deutsche Post & DHL, Saturn, UPS and others.

When Android users that tap the link, they're brought to a page where they are told to download an app, which is infected with FluBot, to track the package. Once the app is installed, it can intercept and send SMS messages, display screen overlays, and steal contacts. iOS users are directed to phishing pages that link to other malware or impersonate major banks in hopes of stealing that user's mobile banking login credentials.



SMS-Nachricht
Di. 6. Apr., 10:46

Hallo ,
Ihr Paket steht noch aus. Bestatigen Sie Ihre Angaben hier:
https://manyuegsyuan.com/pkge/?0unj7d5vgpn8

Deutsche Post

Lookout Analysis

Lookout data shows that in 2020, almost 80% of mobile phishing attacks intended to deliver malware like FluBot. This exemplifies how problematic Malware-as-a-Service (MaaS) like FluBot can be. Another well-known MaaS is BancamarStealer, which was discovered by Lookout researchers who observed 7,700 examples of the malware in 2018. As of March 2021, there were over 74,000 samples.

Flubot employs a domain generation algorithm (DGA), which creates slightly different variations of a given domain name in a tactic known as domain fluxing. This is similar to hiding the needle (the true Command & Control server IP) in a haystack (a long list of IPs).

Lookout Coverage and Recommendation for Admins

Lookout Phishing and Content Protection will help protect your employees from malicious phishing campaigns built to deliver malware and steal login credentials. Lookout PhishingAI constantly monitors the web for new sites built specifically for phishing purposes and implements protection against them in near real-time.

Lookout admins can force activation of Phishing and Content Protection on their employees' devices by not allowing them to access corporate resources or cloud infrastructure until the capability is enabled.

Lookout Phishing and Content Protection

As part of the broader endpoint-to-cloud security solution, Lookout provides comprehensive mobile phishing protection on both Android and iOS devices. This gives admins powerful tools for monitoring, managing and protecting mobile devices, and enables organizations to confidently embrace the use of smartphones within their organization.

Click here to learn more about Phishing and Content Protection