PHISHLABS

Rogue Mobile Application Protection

Quickly detect and take down rogue mobile apps that abuse your brand.

Mobile applications have become a ubiquitous part of mobile computing. Online application stores are filled with mobile applications for online banking, gaming, shopping, social media and hundreds of other uses. With more than 50,000 new mobile applications being released every month just for iOS and Android devices, rogue or malicious mobile applications are an increasingly attractive attack vector for cybercriminals to carry out online fraud and distribute malware.

Rogue mobile applications often rely on recognized brands to entice mobile users into installing them. In some cases, rogue mobile applications exploit trust in popular brands to serve advertisements and profit from the victim brands. In other more malicious attacks, rogue mobile applications are used to steal account data and carry out online transaction fraud.

Cybercriminals create rogue mobile applications either by developing them themselves or by simply adding functionality to existing popular applications. The rogue mobile applications are then posted to application stores and designed to show up near the top of the list when mobile users search for the target brand. This abuse not only tarnishes your brand and associates it with poor user experience, it also distracts customers from your official applications and dilutes their value.

Most application stores do not adequately monitor for rogue mobile applications proactively. Many stores simply provide an open marketplace and assume no obligation to monitor the applications they host or their content. They rely primarily on complaints from users and legitimate companies to identify and eventually remove the rogue mobile applications. For application stores that do review mobile applications prior to posting, applications must be overtly malicious to be rejected.

Service features

Ongoing detection of rogue mobile applications

Monitoring of 75+ official and unofficial application stores

Expert assessment and analysis of suspicious mobile applications

Take down of malicious applications and associated malicious sites

Fixed-fee, unmetered service pricing

Expert protection against rogue mobile applications

PhishLabs Rogue Mobile Application Protection service protects organizations from unauthorized or malicious mobile applications that abuse their brand and/or target their customers. We actively monitor official and unofficial mobile application repositories for rogue mobile applications. When a suspicious application is detected, we confirm the abuse and analyze the threat. If malicious, we rapidly take action to shut it down and remove it from the application repositories where it is hosted.

+1.877.227.0790 info@phishlabs.com

Copyright 2015 PhishLabs. All Rights Reserved.

Rapid detection and expert analysis

PhishLabs monitors more than 75 mobile application stores and repositories for potential rogue mobile applications. This includes official stores, such as Google Play, and unofficial stores such as Cydia. Applications are analyzed to detect:

- Company and brand names
- Trademarks and service marks
- Reference images
- Other key terms

When a suspicious mobile application is detected, the PhishLabs Security Operations Center (SOC) reviews the application to confirm the abuse. Results are documented in the Client Portal, providing full visibility into threats.

Confirmed suspicious applications are immediately analyzed by mobile app threat specialists. Using static and dynamic analysis techniques, our experts determine the application's functionality and intent.

Rogue application shut down

Based on the threat analysis, the PhishLabs SOC initiates mitigation procedures. We maintain an extensive database of contacts and removal procedures for the monitored application repositories, allowing our team to quickly engage the proper administrators for removal.

Rogue mobile applications that abuse client brands and are malicious are mitigated using the following process:

- The malicious application is reported to the repository or store for removal.
- Removal is pursued until confirmed across all repositories.
- Malicious sites and communication points tied to the application are shut down.
- The malicious application and associated sites are monitored for 6 months to prevent future use.

About PhishLabs

PhishLabs is the leading provider of 24/7 cybersecurity services that protect against the exploitation of people. PhishLabs combines proprietary technology, intelligence, and human expertise to rapidly detect, analyze, and stop targeted cyberattacks before they impact organizations.

To learn more, visit www.phishlabs.com.

+1.877.227.0790 info@phishlabs.com

Copyright 2015 PhishLabs. All Rights Reserved.