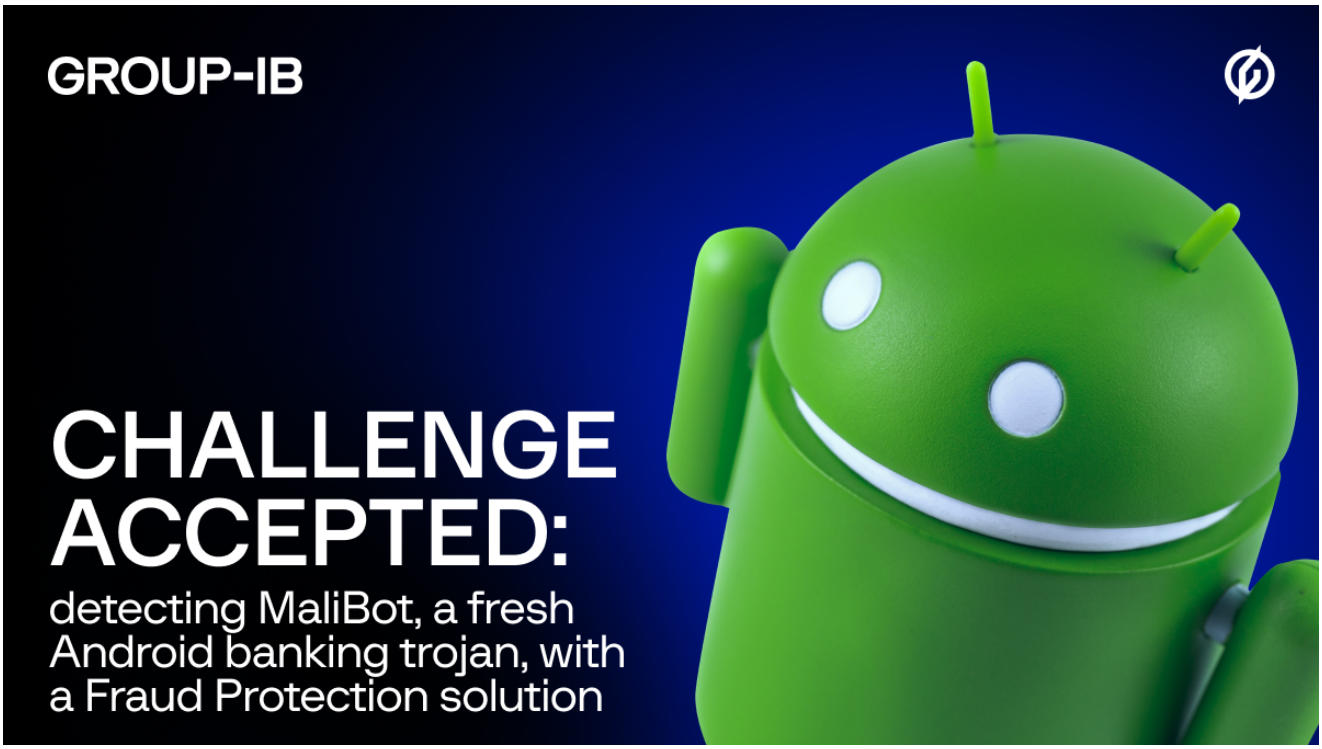
Challenge accepted

blog.group-ib.com/malibot



11.08.2022

Detecting MaliBot, a fresh Android banking trojan, with a Fraud Protection solution

Flubot is dead, and the new evil is detected and crowned, the first of his name – MaliBot. Well, in fact this new MaliBot is a revised follower of another Android banking trojan – S.O.V.A. MaliBot malware, usually disguised as a cryptocurrency mining application, targets Android devices and uses overlay attacks to outfox MFA/2FA, capture messages and SMS, and steal banking and crypto credentials.

By this moment, it has mainly threatened financial sector companies in Spain and Italy. Obviously, it has an ominous ambition and surely still untapped potential to infuse into other industries and conquer new territories.

In this article we will tell in more detail what techniques exist against such attacks, and give you a live demonstration of how Group-IB Fraud Protection stops MaliBot or other similar threats.

WHAT IT IS	MaliBot, banking trojan, camouflaged as a cryptocurrency mining app
HOW IT ACTS	Mostly focused on web injection / overlay attacks
HOW IT HARMS	• Steals cryptocurrency wallets, MFA/2FA codes, cookies, or SMS; • Bypasses Google Authenticator; • Gets VNC access to the infected device and captures the screen; • Manages apps on demand; • Sends messages; • Collects device data (IP, Android ID, model, OS language etc.)
WHO IS CONCERNED	Financial industry and beyond
WHERE IT HEADS	Spain, Italy and beyond

MaliBot fraud dossier

Challenging anti-fraud professionals

As you can clearly see, this malware is powerful and tricky, which makes it a real challenge to detect this attack and other similar to MaliBot malwares with an average anti-fraud tool. That's actually why the financial sector is such fertile soil for threat actors successfully stealing money from banking and cryptocurrency accounts.

MaliBot operators harness a variety of distribution campaigns: they promote cryptocurrency applications in the form of APKs that victims are supposed to download and install manually; they clone real projects like TheCryptoApp (1M+ downloads on Google Play Store); operators also use smishing (SMS phishing) and other methods to multiply their chances to succeed.

Even though the overall context looks scary, fear not because advanced solutions and tactics, developed to respond to similar web injection threats and this particular one, do exist, and one of them is almost at your doorstep.

Proven tactics to respond

There are at least two major countermeasures to leverage against such fraud attacks. According to your case, you have a choice between fraud intelligence and behavioral analysis. Let us explain to you what's the difference and how it works.

The signature-based analysis utilizes the abilities of **fraud intelligence** to collect information about the application and compare its certification deviation to other application certificates. Once information about installed applications is gathered, it is essential to match them with already known trojan signatures.
Here are some examples of suspicious Android permissions:

PROCESS_OUTGOING_CALLS

SEND_SMS

WRITE_EXTERNAL_STORAGE

READ_EXTERNAL_STORAGE

RECEIVE_SMS

Another way to thwart such attacks is a so-called **behavioral analysis** that

- comprises overlay or accessibility service detections;
- realizes default SMS application monitoring;
- captures the slightest deviations in the user's behavior routine.

Every tiny derogation matters here: the speed of movement, pressure on the screen while using the app, and other factors that could drop an alert about anomalies.

Where intelligence meets analysis

Group-IB Fraud Protection is a solution that combines device fingerprinting, fraud intelligence, and behavioral analysis and already protects more than 300M+ web and mobile apps users worldwide against advanced digital threats, malware, payment fraud, social engineering attacks, and bad bots. The solution acts in real-time and across all digital channels.

Group-IB Fraud Protection utilizes the threat intelligence insights collected by the Unified Risk Platform by Group-IB giving us the full fraud landscape visibility, and our professional expertise turns these insights into actionable anti-fraud strategies.

Better to see something once, so please check out this video demonstration of how MaliBot typically acts and what signals Group-IB Fraud Protection solution collects to detect the threat: