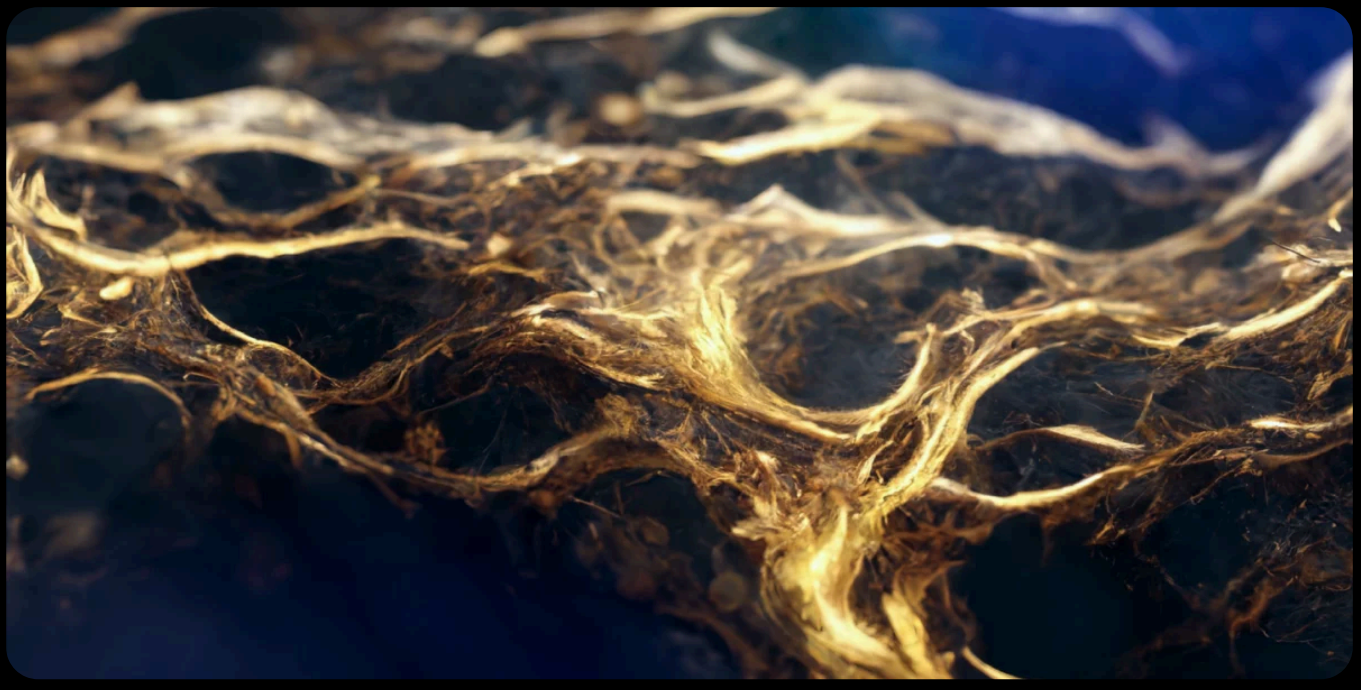
GROUP-IB

← Blog

Let's dig deeper: dissecting the new Android Trojan GoldDigger with Group-IB Fraud Matrix

Delve into the tactics of the GoldDigger Trojan and discover ways to safeguard your customers

October 5, 2023 · min to read · Fraud Protection



Fraud Protection GoldDigger Trojan

In August, Group-IB's Threat Intelligence researchers detected a previously unknown **Android Trojan** targeting financial organizations in Vietnam. We codenamed it **GoldDigger** in reference to a particular GoldActivity activity within the APK.

We promptly informed our clients in Vietnam and beyond about our findings. Additionally, our 24/7 **CERT-GIB** (Group-IB Computer Emergency Response Team) proactively reached out to **VNCERT** (Vietnam Computer Emergency Response Team), in accordance with the data-sharing agreement among APCERT members. CERT-GIB shared the necessary technical information, including indicators of compromise, so that VNCERT was equipped to take appropriate risk mitigation measures.

This particular Trojan has been active since at least June 2023. GoldDigger disguises itself as a fake Android application and can impersonate both a Vietnamese government portal and a local energy company. Its main goal is to steal banking credentials. Like many Android Trojans, the malware abuses Accessibility Service to extract personal information, intercept SMS messages, and perform various user actions. The Trojan also has a remote access capability.

One of the main features of GoldDigger is its **use of an advanced protection mechanism**. **Virbox Protector**, a legitimate software identified in all discovered samples of GoldDigger, allows the Trojan to significantly complicate both static and dynamic malware analysis and evade detection. This presents a challenge in triggering malicious activity in sandboxes or emulators.

The use of VirBox by banking Trojans is a recent trend. According to Group-IB's Threat Intelligence team, three Android Trojans currently active in the Asia Pacific region, including GoldDigger, are using this evasion technique.

As a result, dynamic analysis of each VirBox-protected sample takes significant time and requires manual intervention. Regular updates to VirBox make static analysis of such malware inefficient. The main goal of banking Trojans is to infect as many devices as possible and gain access to user accounts. The most effective way to combat them is with client-side fraud protection solutions that offer multiple benefits. These include real-time protection, adaptability to evolving threats and, most importantly, the ability to rely on behavioral indicators to protect customers.

Figure 1. GoldDigger Profile

As discovered by Group-IB researchers, the GoldDigger Trojan uses fake applications in Vietnamese to attack its victims. It has also been found that the Trojan includes language translations for Spanish and traditional Chinese, which implies that these attacks may potentially extend their reach beyond Vietnam, encompassing Spanish-speaking nations and other countries in the APAC region.

GoldDigger is just one of numerous Android malware strains currently active in the Asia-Pacific region. Other noteworthy Android malware families currently targeting the region include the Gigabud family, SpyNote, HookBot, PWNDROID4, CraxsRAT, TgToxic, and Anubis (Godfather's predecessor), etc. Most of them share common characteristics and tactics that can be analyzed and categorized using **Group-IB's proprietary Fraud Matrix,** which is an essential element of **Group-IB Fraud Protection.**

In light of GoldDigger's current activity and potential expansion, we have decided to take a close look at the Trojan's tactics, in accordance with **Group-IB's Fraud Matrix**. Based on the MITRE® model, Group-IB Fraud Matrix is a unique framework that analyzes and categorizes fraudulent schemes and outlines techniques used by fraudsters at each stage. The Matrix is a critical intelligence source against fraud with deep insights into schemes, modus operandi, as well as recommendations that can ensure your organization is equipped with the most robust defense measures.

In addition to an in-depth analysis of GoldDigger's fraud techniques, the post includes a list of indicators of compromise (IOCs), making it a valuable resource for anti-fraud teams and CTI analysts.

Let's look at GoldDigger's fraud techniques more closely.

Figure 2. Visual representation of GoldDigger's TTPs in the Fraud Matrix of the Group-IB Fraud Protection interface

Distribution of malware

GoldDigger spreads via fake websites masquerading as **Google Play** pages and fake corporate websites in Vietnam. The Trojan's operators most likely distributed the links to these websites through *smishing* or *traditional phishing*. Those websites include links to download malicious Android applications (Figure 3).

Figure 3. Fake website distributing GoldDigger

All Android devices have an "**Install from Unknown Sources**" setting disabled by default to prevent app installations from third-party sources. If the "Install from Unknown Sources" setting is enabled, APKs from sources other than the Google Play Store can be installed.

GoldDigger requires that the "Install from Unknown Sources" function is enabled on a victim's device to be downloaded and installed.

Proactive Mitigation Steps

We advise organizations to educate their customers about not enabling the "Install from Unknown Sources" function as these actions can expose Android devices to potential security risks. Group-IB Fraud Protection's Android SDK detects applications installed from unauthorized and unknown sources that request suspicious permissions. Read more about the tool's powerful malware detection techniques here.

Let's look at GoldDigger's other techniques now.

Trust Abuse Tactic: Accessibility Service

When launched, the GoldDigger Trojan asks the user to *enable Accessibility Service*.

Android's accessibility services are intended to assist users with disabilities in operating their devices. These services offer capabilities such as screen reading, magnification, gesture-based controls, speech-to-text, haptic feedback, and others. Regrettably, certain banking Trojans, such as Gustuff and Gigabud, are exploiting this feature.

Granting Accessibility Service permissions to GoldDigger enables it to gain full visibility into user actions and interact with user interface elements. This means it can see the *victim's balance*, *harvest the second credential issued for two-factor authentication,* and implement *keylogging* functions, allowing it to *capture credentials*. GoldDigger monitors **51 financial apps, e-wallets, and crypto apps i**n Vietnam. All this data is exfiltrated to command-and-control (C&C) servers. An example is shown in Figure 4 below.

Figure 4. Implementing Capture Credentials in GoldDigger

By abusing the Accessibility Service, GoldDigger ensures a range of intrusive capabilities. We have not confirmed that the Trojan operators use these capabilities at the time of writing. However, based on the behavior of other known Trojans similar to GoldDigger, we don't think they differ significantly. This includes the ability to simulate user interactions enabling *device remote access*, essentially providing it with a backdoor into the user's system. Figure 5 is a code snippet from the gestures dispatcher, which performs device screen unlock. Additionally, it enables *authentication bypass,* including the *2nd-factor bypass*, allowing GoldDigger to perform *payment creation from a legitimate device*.

Figure 5. Automated device screen unlock

Conclusion

Banking malware such as GoldDigger often exploits accessibility services or permissions to carry out fraudulent activities. To combat this, Group-IB Fraud Protection's SDK is able to detect GoldDigger using a combination of rules, including the detection of accessibility service abuse, remote access capabilities, and abnormal behavior, as well as spotting applications installed from unauthorized sources that request suspicious permissions, and a range of other relevant indicators.

Group-IB Fraud Protection's SDK can be easily added to any application to prevent fraud schemes that rely on this popular technique, whether they are known or zero-day malware on end-user devices.

User Behavior Monitoring can be employed to recognize an imposter by gaining a deep understanding of the way genuine users interact with your applications. The system monitors key user behavior indicators such as speed of movement and pressure on-screen navigation. Incorporating these capabilities can strengthen your defenses against most malware attacks.

Figure 6. Malware detection with User Behavior Monitoring by Group-IB Fraud Protection

Find out more on how to detect different types of banking malware old or new on our malware detection blog.

Indicators of Compromise

File SHA256

Network

IOC	Description
cskh[.]evnspa[.]cc	Malware delivery site

cskh[.]evnspc[.]cc	Malware delivery site
cskh[.]evnspe[.]cc	Malware delivery site
cskh[.]evnspo[.]cc	Malware delivery site
cskh[.]evnspr[.]cc	Malware delivery site
viet[.]cgovn[.]cc	Malware delivery site
viet[.]egovn[.]cc	Malware delivery site
viet[.]gdtgovn[.]com	Malware delivery site

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends