GoldDigger drains your bank account: new Trojan uncovered by Group-IB targets 50+ Vietnamese banks

Media Center → Press Releases

October 5, 2023 · 4 min to read

Fraud Protection | Threat Intelligence | Trojan | Vietnam

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, has discovered a new **Android Trojan** that specifically targets users of over **50** Vietnamese banking applications, electronic wallets, and cryptocurrency wallets, with the aim of stealing their funds. Codenamed **GoldDigger** by **Group-IB's Threat Intelligence unit**, the Trojan has been active since at least **June 2023**. The malicious application impersonates a Vietnamese government portal and an energy company and abuses the Android Accessibility service to extract personal information, steal banking app credentials, intercept SMS messages, and perform various user actions. The number of infected devices and the amount stolen remains unknown.

Group-IB's Threat Intelligence customers were promptly notified upon the discovery of the threat. **Group-IB's Computer Emergency Response Team (CERT-GIB)** also issued a proactive notification to the Governmental National CERT of Vietnam (VNCERT) and continues its outreach campaign.

The malware was first spotted by Group-IB in June 2023. The company's Threat Intelligence unit identified more than **ten fake websites posing as Google Play Store** pages and fake company websites. To appear more convincing, some fake websites include user reviews and the emblem of Vietnam.

Figure 1. Fake website distributing GoldDigger

These sites were designed to deceive users into downloading the malicious GoldDigger application, named after a specific Android activity, found within the APK file, called “GoldActivity”. Group-IB was not able to establish the initial vector, but the Trojan’s operators most likely distributed the links to these websites through messengers or traditional phishing. Group-IB detected **two different strains of GoldDigger** – one that impersonated a Vietnamese governmental portal and another imitating a local energy sector company.

After being installed and launched, GoldDigger requests access to Accessibility Service, an Android feature designed to assist users with disabilities by allowing apps to interact with each other and modify the user interface. By abusing this feature, the malware can monitor and manipulate the device’s functions.

By granting the Trojan access to Accessibility Service, the user unwittingly enables GoldDigger to extract sensitive information, such as passwords, intercept SMS messages, simulate user interactions, as well as to steal login credentials. The Trojan monitors events related to **51 targeted applications of Vietnamese financial organizations, as well as e-wallets and crypto apps**. After capturing user input (such as logins and passwords), GoldDigger exfiltrates the data to command-and-control (C&C) servers.

Figure 2. GoldDigger profile

One notable feature of GoldDigger is that it uses Virbox Protector – a legitimate software that provides advanced obfuscation and encryption. Malware developers employ Virbox Protector to make it more challenging for cybersecurity researchers to analyze and reverse-engineer their malicious code and avoid detection by conventional anti-fraud solutions. Nonetheless, Group-IB's Fraud Protection can effectively detect GoldDigger.

Anh Le

Group-IB's Business Development Manager in Vietnam

"However, Group-IB's Threat Intelligence team found that, in addition to Vietnamese, the malware included language translations to Spanish and traditional Chinese. The cybercriminals may have plans to further extend GoldDigger's reach to Spanish and Chinese-speaking countries in the near

future. We continue the investigation into GoldDigger and will provide updates when they become available."

To minimize their risk of downloading banking Trojans such as GoldDigger, Group-IB recommends users always check for updates on their mobile devices, avoid downloading applications from sources outside of the Google Play Store, and check what permissions an application requests once it is downloaded. Companies seeking to safeguard their users from malware attacks might consider Group-IB's Fraud Protection solution. It monitors user sessions by leveraging machine learning algorithms to identify suspicious behavior, the latest fraud techniques, unauthorized remote sessions, as well as the presence of malware, such as GoldDigger.

Share article

About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses, citizens, and support law enforcement operations.

Group-IB's Digital Crime Resistance Centers (DCRCs) are located in the Middle East, Europe, Central Asia, and Asia-Pacific to help critically analyze and promptly mitigate regional and country-specific threats. These mission-critical units help Group-IB strengthen its contribution to global cybercrime prevention and continually expand its threat-hunting capabilities.

Group-IB's decentralized and autonomous operational structure helps it offer tailored, comprehensive support services with a high level of expertise. We map and mitigate adversaries' tactics in each region, delivering customized cybersecurity solutions tailored to risk profiles and requirements of various industries, including retail, healthcare, gambling, financial services, manufacturing, crypto, and more.

The company's global security leaders work in synergy with some of the industry's most advanced technologies to offer detection and response capabilities that eliminate cyber disruptions agilely.

Group-IB's Unified Risk Platform (URP) underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

The comprehensive suite includes the world's most trusted Threat Intelligence, The most complete Fraud Protection, AI-powered Digital Risk Protection, Multi-layered protection with Managed Extended Detection and Response (XDR), All-infrastructure Business Email Protection, and External Attack Surface Management.

Furthermore, Group-IB's full-cycle incident response and investigation capabilities have consistently elevated industry standards. This includes the 77,000+ hours of cybersecurity incident response completed by our sector-leading DFIR Laboratory, more than 1,400 successful investigations completed by the High-Tech Crime Investigations Department, and round-the-clock efforts of CERT-GIB.

Time and again, its solutions and services have been revered by leading advisory and analyst agencies such as Aite Novarica, Gartner®, Forrester, Frost & Sullivan, KuppingerCole Analysts AG, and more.

Being an active partner in global investigations, Group-IB collaborates with international law enforcement organizations such as INTERPOL, EUROPOL and AFRIPOL to create a safer

cyberspace. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, which was created to foster closer cooperation between Europol and its leading non-law enforcement partners.

Read next

March 19, 2026

Group-IB Partners with Copy Cat Group to Strengthen Intelligence-Led Cybersecurity Across East Africa

March 13, 2026

Group-IB Supports INTERPOL's Operation Synergia III, Contributing Intelligence to Global Cybercrime Takedown

March 12, 2026

Group-IB Expands into the Americas with Launch of Digital Crime Resistance Center in Chile

March 3, 2026

Group-IB and Nebrija University Strengthen Cybersecurity Education Through MOU and Threat Intelligence Integration

February 26, 2026

Group-IB Partners with Savex Technologies to Advance Predictive Threat Intelligence and Cyber Fraud Protection Across India and SAARC

February 16, 2026

National Polytechnic University of Armenia and Group-IB sign strategic partnership to strengthen cybersecurity education and research in Armenia

Go to all Press Releases →

MSSP and MDR Partner Program
Technology Partners
Partner Locator

Team
CERT-GIB
Careers
Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans →
Services →
Resource Center →

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