← Blog

Pavel Naumov

Global Senior Security Researcher
FHP

Artem Grischenko

Junior Malware Analyst, Threat Intelligence team

Breaking down Gigabud banking malware with Group-IB Fraud Matrix

Uncover the disruptive nature of Gigabud malware and take proactive measures to mitigate the associated risks

August 14, 2023 · min to read · Fraud Protection

Banking malware Fraud Protection Gigabud

Introduction

Malware continues to evolve as a persistent threat to organizations worldwide. And while antivirus technologies strive to improve their malware detection capabilities, threat actors are actively attempting to create malicious software that can evade detection.

A powerful strategy to overcome the challenge is transitioning from traditional signature-based detection to advanced analysis techniques, which effectively prevent malware incidents. Here's a detailed analysis of how Group-IB experts recently dismantled a disruptive banking trojan.

In September 2022, the Group-IB team received a request from its customer, a Thailand-based financial organization, to investigate a malware sample targeting its clients and customers in the Asia-Pacific region. After the sample analysis, the experts concluded that the malware was a **previously undocumented Android Remote Access Trojan (RAT)**. In January 2023, cybersecurity researchers named this trojan **Gigabud** after the application's certificate issuer name.

One of **Gigabud RAT's unique features** is that it doesn't execute any malicious actions until the user is authorized into the malicious application by a fraudster, as will be shown in the Distribution section (figure 3), which makes it harder to detect. Instead of using HTML overlay attacks, Gigabud RAT gathers sensitive information primarily through screen recording.

The Group-IB team continued investigating this highly active strain and identified another malware sample within the Gigabud family that doesn't have RAT capabilities – codenamed **Gigabud.Loan**, which is a **fake loan application** that exfiltrates user-input data.

Active since at least July 2022, Gigabud.Loan has been masquerading as applications of fictional financial institutions **from Thailand, Indonesia, and Peru.** It is worth noting that the versions of Gigabud previously described by security researchers **combine the functionalities of RAT and Fake Loan.** Both Gigabud RAT and Gigabud.Loan have the same architecture and share the same certificate, which is why Group-IB researchers attribute them to the same Gigabud family.

From 2022 to 2023, Group-IB detected more than 400 Gigabud.RAT samples and more than 20 Gigabud.Loan samples based on VirusTotal hunting rules. Considering the high activity of the Gigabud malware family, the blog aims to equip organizations and the community with valuable insights into the Gigabud trojan's functionality and the topography of attacks.

The blog extends an in-depth analysis of the fraud techniques employed by Gigabud mapped using the Group-IB Fraud Matrix, which can help guide mitigation techniques enforced by different anti-fraud teams and CTI analysts.

Key findings

- Gigabud.Loan targeted account holders of more than 99 financial institutions in Thailand, Indonesia, Vietnam, the Philippines, and Peru.

The targets were individuals lured into filling out a bank card application form to obtain a low-interest loan.

The victims are convinced to provide personal information during the application process.

Gigabud.RAT targeted at least 25 companies, financial institutions, and government departments across Thailand, Peru, the Philippines, Indonesia, and Vietnam. The malware aimed to mimic these companies, possibly to deceive users.

Gigabud's feature **TouchAction,** abuses accessibility service, as shown in Figure 8. With screen capturing, Gigabud is a powerful **remote device access** tool allowing the threat actor to **access the victim's account**. It allows the threat actor to perform gestures on the user's device. This leads to the possibility of **evading defense**, **authentication** (including **two-factor authentication**), and **creating automated payments** from the victim's device.

A new password-stealing module was discovered, specifically designed to target banking applications.

Fraud Matrix: Decoding Gigabud

To facilitate the understanding of an emerging threat and its various phases, Group-IB Fraud Matrix analyzes fraudulent schemes and outlines techniques used by fraudsters at each stage. Based on the MITRE® model, the Fraud Matrix is a critical source of intelligence against fraud with deep insights into schemes, modus operandi, and recommendations for an organization's most robust defense measures.

Fraud Matrix analysis allows teams to identify, classify, and index new and existing fraud types to provide a better understanding of how this particular trojan operates, as well as its potential risks to target organizations and their customers.

Let's look at the specific tactics and techniques employed by the **Gigabud family**:

Figure 1: Visual representation of Gigabud's TTPs in the Fraud Matrix

Here's a breakdown of Gigabud techniques in **resource development, trust abuse, end-user interaction, credential access, account access,** and **defense evasion tactics**.

Distribution

Both **Gigabud.Loan** and **Gigabud.RAT** spread via phishing websites in Thailand, Indonesia, Vietnam, the Philippines, and Peru. The links are delivered to the victim through **smishing** via instant messengers, SMS, or social networks where fraudsters **push the victims to visit the phishing websites**, complete a tax audit and get a tax refund. Those websites show links to download malicious Android applications and impersonate government and financial institutions (Figure 2). These applications are hosted on **consonant domains**.

Figure 2.1: Example of phishing websites spreading Gigabud malware

However, in the case of Gigabud.Loan, the threat actors use not only phishing websites but deliver the APK files directly through instant messengers as illustrated in the video, screenshot from that is shown below (Figure 3):

Figure 3: Example of phishing in messengers

Android devices allow users to install apps from third-party sources except official app stores. However, the devices have the "**Install from Unknown Sources**" setting disabled by default as a security measure that prevents app installations from unknown sources. Additionally, applications that aim to install additional applications on the device can request the **"REQUEST_INSTALL_PACKAGES"** permission, categorized as high-risk by Google. This permission allows apps to bypass the "Install from Unknown Sources" setting and allow APK installations outside the Google Play Store.

The phishing victims are frequently tricked into granting the “REQUEST_INSTALL_PACKAGES” permission for browsers, email clients, etc., on their Android devices, allowing malicious APKs to be installed. Gigabud also leverages phishing techniques to deceive users into unwittingly providing the necessary permissions for the trojan’s installation.

This combination of social engineering and permission exploitation underscores the significance of user awareness and caution when encountering unexpected or suspicious requests, safeguarding against the potential infiltration of dangerous malware.

Proactive Mitigation Steps

We advise organizations to educate their customers about not enabling “Install from Unknown Sources” and resorting to caution when granting the “REQUEST_INSTALL_PACKAGES” permission to apps, as these actions can expose Android devices to potential security risks, including malware and data privacy concerns. Group-IB Fraud Protection’s Android SDK detects these risks on users’ devices. Read more about the tool’s common malware detection techniques here.

Gigabud.RAT and Gigabud.Loan share similarities in terms of how they are distributed. Other attack stages differ. Let’s look at them more closely now.

Gigabud.RAT

The Gigabud.RAT is a trojan that mimics legitimate apps, including government and financial institution applications, and abuses **screen capturing** and **keylogger** techniques as part of the **capture credentials** technique to **access credentials** and other sensitive information.

Additionally, it can **bypass authentication** and 2nd factors, **replace bank card numbers** in clipboards, and perform **automated payments** through the victim’s **device remote access**.

When the user opens the Gigabud trojan that masquerades as a legitimate application, it presents the login activity (Figure 4).

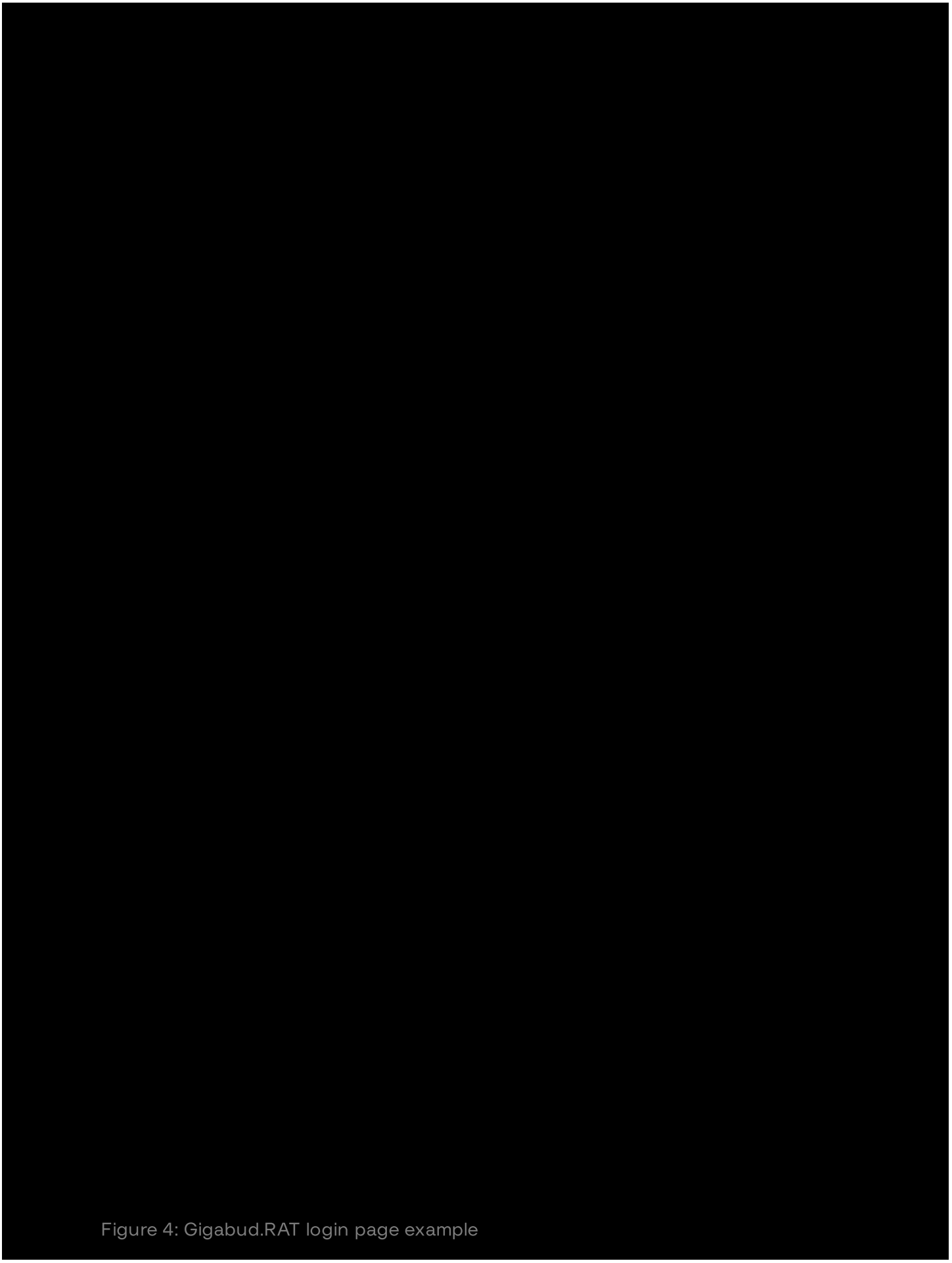

Figure 4: Gigabud.RAT login page example

When the user passes the Login form, Gigabud requests two 6-digit invitation codes that are mentioned on Figure 3 from the user as shown below. With this extra step, fraudsters can verify the victim, making it more difficult for research by malware analysts, and seek to trick users into believing that they are dealing with a legitimate application.

Figure 5: 6-digit invitation code pages example

As a result, Gigabud opens a fake “Activation” page. This activity contains one button, which only functions to pass on the “Permission Request” page (Figure 6). There are several options on the “Permission Request” page, and the exact number depends on the sample. They are primarily used for:

- installing the Add-On application
- **granting permission to use Accessibility Service**

granting permission to Start Screen Recording

granting permission to display the application over other apps

When the user grants these permissions, the Gigabud can then perform all its malware capabilities.

Figure 6: Gigabud.RAT Activation and Permissions request pages

When all the necessary permissions are granted, the “Wait” page is opened. This activity contains an endless loading animation and the text “Please Wait for Information.”

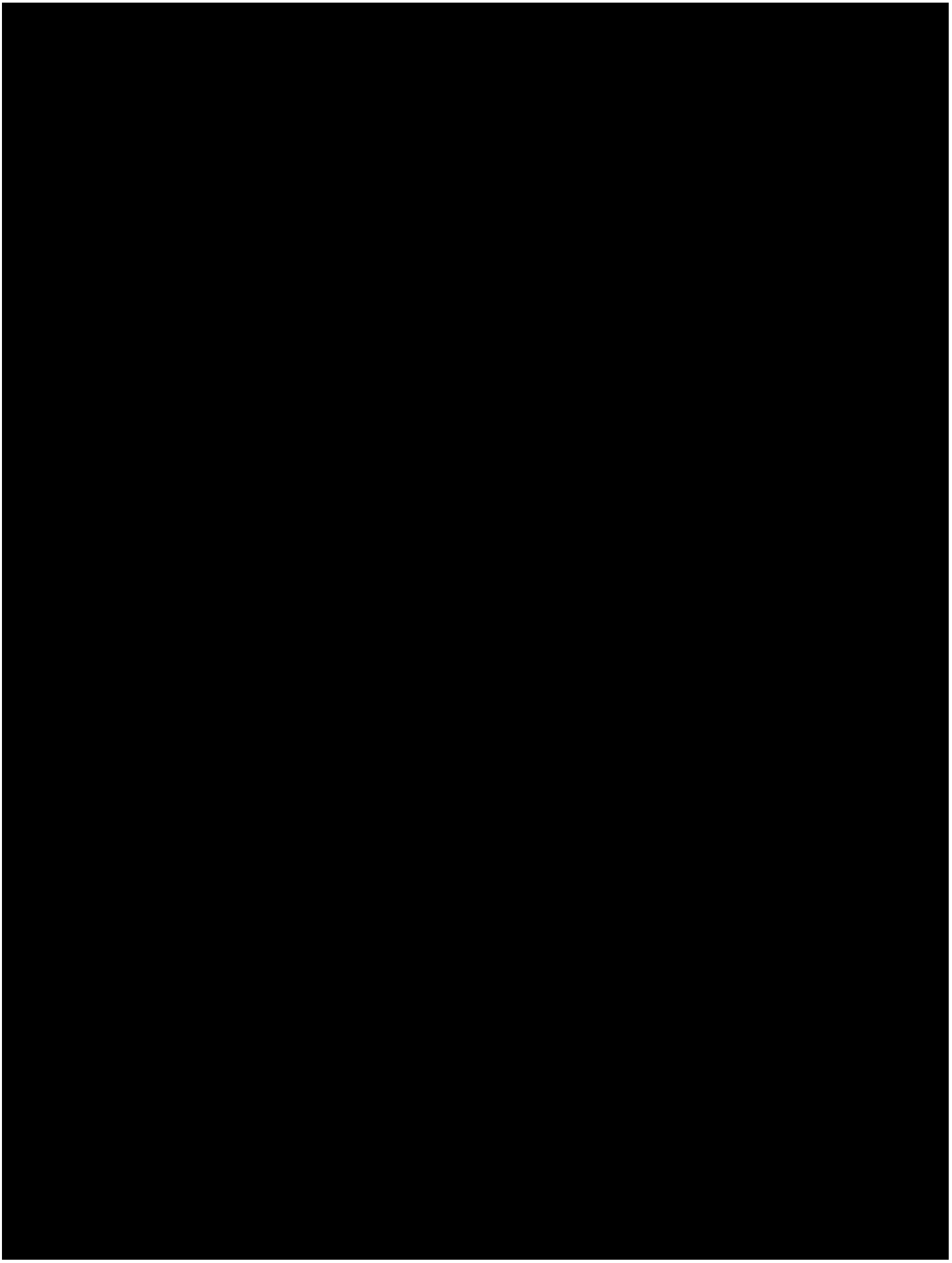

Figure 7: Gigabud.RAT “Wait” page example

Screen Capture

Screen capturing has been used in legitimate software applications and malware. Legitimate use cases include screen recording apps, remote access apps, and productivity tools that allow users to capture and share their screen activity for various purposes – from content creation to troubleshooting and remote support. These applications often utilize high-level libraries, but ultimately, screen capturing is implemented using the underlying mechanisms of Android, such as virtual displays and MediaProjection API.

However, this same feature is also exploited by malware to steal sensitive user information, such as login credentials and personal data. To mitigate this risk, Android has implemented **runtime permission** that requires users to grant access to screen recorders, enabling users to control and monitor screen-capturing activities on their devices.

Group-IB Fraud Protection’s SDK can detect active screen capturing on Android devices, as shown in the video below. Group-IB’s Threat Intelligence team found a Gigabud sample with some debug activities and patched it to show one of them instead of the login activity.

Accessibility Service to perform gestures

Accessibility services, in the context of Android, refers to a system feature designed to assist users with disabilities in effectively interacting with their devices. Accessibility services provide enhanced functionalities and modifications to the user interface, allowing individuals with visual, auditory, physical, or cognitive impairments to navigate, interact, and utilize their Android devices more easily.

These services can offer features like screen reading, magnification, gesture-based controls, speech-to-text, haptic feedback, and more. Accessibility services are crucial in promoting inclusivity, empowering users with disabilities to access and engage with their devices, applications, and digital content, thereby fostering greater independence and usability.

However, accessibility services, similar to screen capturing, are now being leveraged as a means of exploitation by threat actors by several banking trojans, such as Gustuff and Gigabud. From the banking anti-fraud point of view, devices with accessibility services should be marked because they can be treated as an indicator of compromise.

One of Gigabud's features **TouchAction,** abuses accessibility service, as shown in Figure 8. With screen capturing, Gigabud is a powerful **remote device access** tool allowing the threat actor to **access the victim's account**. It allows the threat actor to perform gestures on the user's device. This leads to the possibility of **evading defense**, **authentication** (including **two-factor authentication**), and **creating automated payments** from the victim's device.

Figure 8: "TouchAction" service

Real-time detection of accessibility service abuse is one key feature of Group-IB Fraud Protection's SDK that can easily be added to any application. This helps prevent fraud schemes that rely on this popular technique by known and zero-day malware on end-user devices.

Accessibility Service as a keylogger

The latest Gigabud versions contain another feature that abuses accessibility services – a new **keylogging** module that allows preparing the specific password-stealing scheme for each targeted banking application. Our Threat Intelligence team suggests that this module is being tested by the malware developers now, and Gigabud will contain more modules to steal data from different banking applications. The identified Gigabud samples currently have a password-stealing handler for only one banking app.

Figure 9: Fragment of keylogger implementation

As we can see in the Figure 9 screenshot, the keylogger feature is implemented using an accessibility service. Group-IB Fraud Protection's SDK can be leveraged to detect if the accessibility service is enabled on the user's device.

Gigabud.Loan

The Gigabud.Loan is a **fake loan version** of Gigabud that only exfiltrates user-input data and has no RAT capabilities. It **abuses the user's trust** by impersonating a non-existing financial institution to collect personal information such as full name, identity number, national identity document photo, digital sign, education, income info, bank card information, and phone number to obtain a loan.

The **fake loan request** is a fraud technique where fraudsters pose as lenders and request money from individuals disguised as loan providers. Fraudsters typically use various methods to target victims, such as sending unsolicited emails or making phone calls, and other deceptive tactics to convince their victims to send them money.

In a typical fake loan request fraud scenario, the fraudster may ask victims to pay upfront fees or provide personal information, such as bank account numbers or social security numbers to process the loan application. They may promise low-interest rates or guaranteed approval to entice victims into sending money or providing sensitive information. However, once the victims take action, the scammers disappear, and the victims are left without a loan and may suffer financial losses.

After the user opens Gigabud.Loan, the application shows activity with login and registration forms (Figure 10, Screen – 1). The user can register with a phone number and an SMS invite code. Then Gigabud shows activity with a credit offer (Figure 10, Screen 2) and requests the user's personal information (Figure 10, Screen – 3, 4) before providing a fake loan contract. After all personal data is submitted, the credit contract can be received. Gigabud.Loan views formatted contract as a loan request result presented in Figure 7.

Figure 10: Fake loan request stages

Figure 11. Fake loan contract example

Detect and defend against Gigabud malware

With the Gigabud malware getting more adaptive and effective in its attack tactics, and expanding its target range, adding new modules in recent samples, building advanced evasion techniques; it is imperative to stay vigilant and have proactive cybersecurity measures to defend against the malware.

For financial organizations

- Implement a user session monitoring system such as Fraud Protection to detect the presence of malware and block anomalous sessions before the user enters any personal information.
- Educate your clients about the risks of Gigabud malware. This includes teaching them to spot fake websites and malicious apps and protecting their passwords and personal information.
- As for **fake loan requests,** actively inform your customers through educational materials, such as brochures, website content, and FAQs to verify the legitimacy of loan offers and lenders.
- Use a Digital Risk Protection platform that detects the illegitimate use of your logos, trademarks, content, and design layouts across your digital surface.

For end-users

- Be careful about the links you click on. Gigabud malware is often spread through malicious links in emails, text messages, and social media posts.
- Tread with caution when downloading third-party applications
- Check what permissions an application requests before installing it.
- Use a VPN when connecting to public Wi-Fi. This will help protect your device from malware that may be lurking on public networks.
- Back up your data regularly to minimize the damage if your device is infected with malware.
- Use reputable antivirus software to detect and remove Gigabud malware if it does manage to infect your device.

If your device has been infected, do the following:

- Disable network access.
- Freeze any bank accounts that your device has accessed.
- Contact experts to receive detailed information about the risks that the malware could pose to your device.

In cases of fake loan request fraud, users can take the following steps.

- Verify the lender’s legitimacy before you apply for a loan. You can check the lender’s website for a physical address and phone number, and also check with Ombudsman Services to see if any

complaints have been filed against the lender.

Avoid paying the fees upfront. it is less likely for legitimate lenders to ask you to pay any upfront fees before you receive a loan.

Legitimate lenders will not use high-pressure tactics to pressure you into taking out a loan. It is likely a scam if a lender pressures you to take out a loan.

More on malware:

Gigabud RAT: New Android RAT Masquerading as Government Agencies

Bad behaviour: How to detect banking malware

Hi-tech Crime Trends 2022/2023

Godfather: A banking Trojan that is impossible to refuse

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