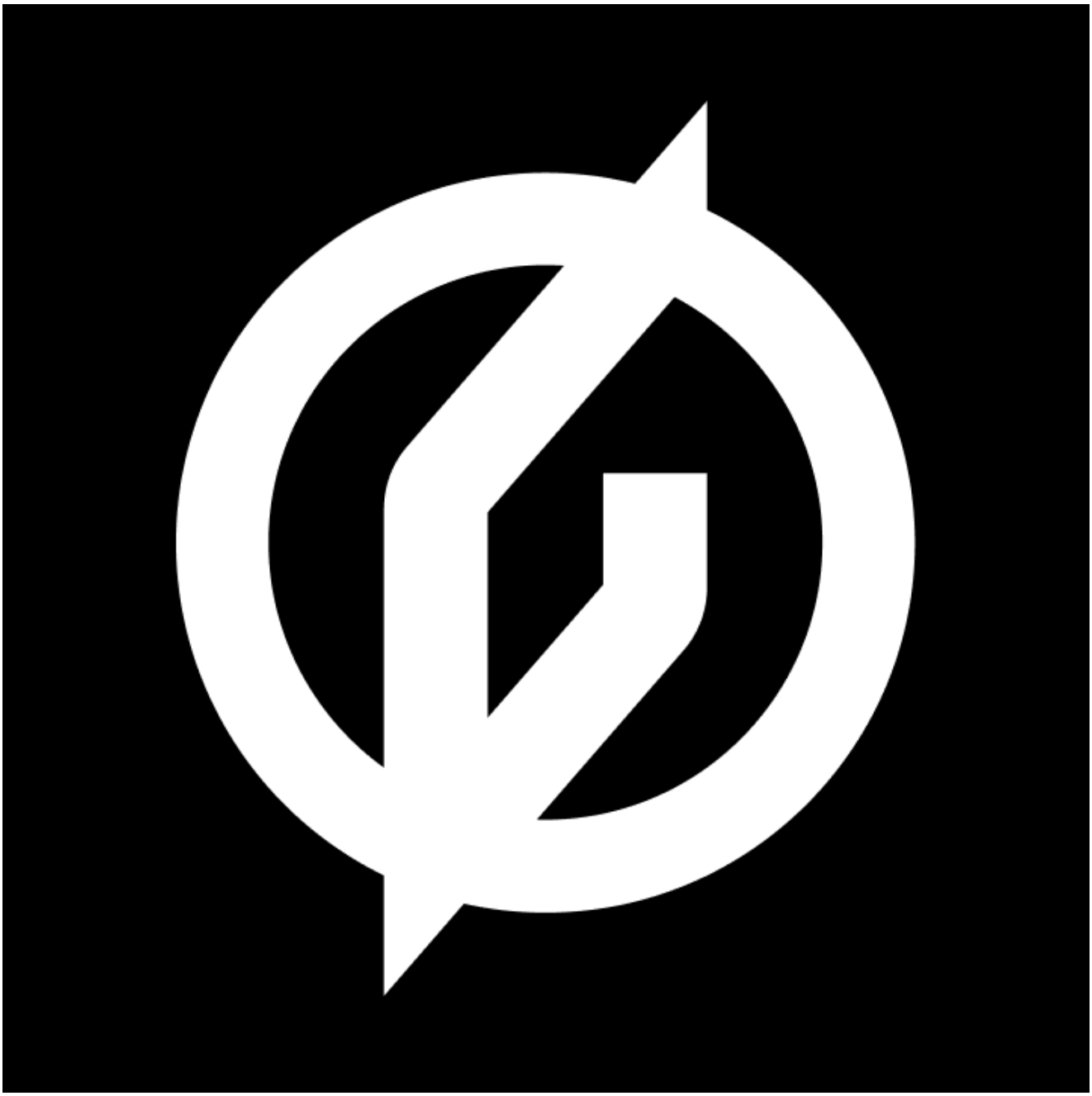
Swiss Army Knife Phishing

blog.group-ib.com/phishing-vietnam-banks

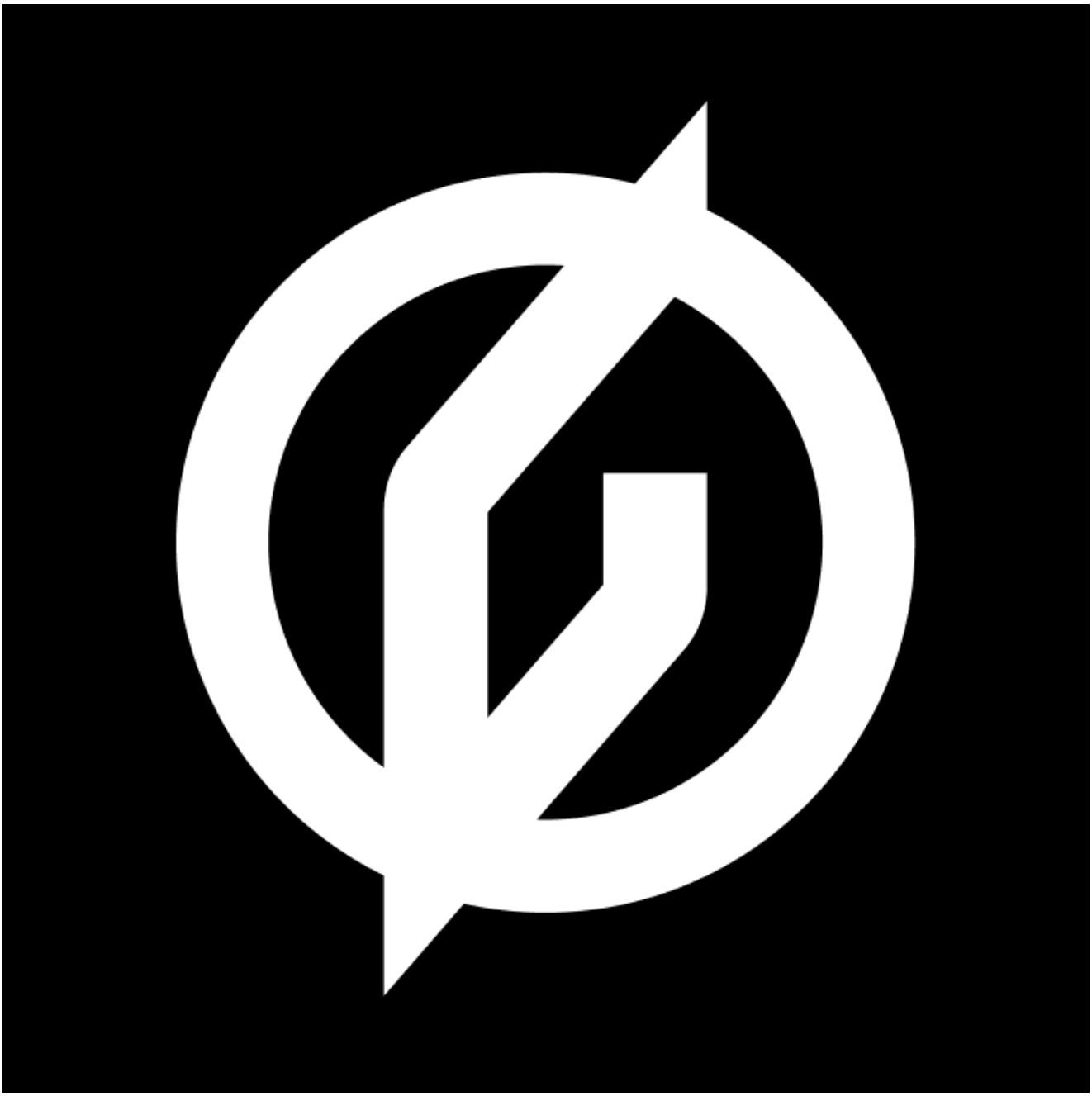
09.06.2022

Group-IB identifies massive campaign capable of targeting clients of major Vietnamese banks



Yaroslav Kargalev

Deputy Head of CERT-GIB



Ivan Lebedev

Head of CERT-GIB's Anti-phishing and global cooperation unit

Group-IB's Asia-Pacific Computer Emergency Response Team (CERT-GIB), tasked with monitoring phishing violations across the world, has spotted an unprecedented mass-scale phishing campaign impersonating Vietnamese financial institutions and targeting their clients.

According to CERT-GIB, the websites involved in the campaign mimic **27** popular financial institutions. Cybercriminals aim to steal money and banking customers' personal and payment details, such as name, address, national identity card number, phone number, DOB, and occupation.

The campaign was launched back in 2019 with the first domain having been registered in May 2019. Since the start of the fraudulent operations, Group-IB has identified **240 interconnected domains**. All 240 domains were taken down following CERT-GIB and other local authorities' efforts.

Cybercriminals' phishing infrastructure. Source: Group-IB Network Graph Analysis Tool

However, the operation remains active up until now: the latest phishing domain, that is part of the cybercriminals' infrastructure, was activated on **June 1, 2022**. New domains come and go regularly. They do not live long by design to complicate detection and takedown. Group-IB continues to cooperate with domain registrars and other authorities to take down new domains identified to contain further financial loss for banking customers and to protect banks from reputation damage.

CERT-GIB was able to retrieve the number of visitors to 44 out of 240 websites identified, where web counters were installed. Just since the beginning of 2021, at least **7,800** potential victims visited these 44 phishing resources. The overall number of visitors and affected users is unknown but is believed to be significantly higher, taking into account the scale, duration of the fraudulent operations and the degree of sophistication in the methods used by the cybercriminals. The campaign is directed at major financial institutions of Vietnam with every phishing website, it uses an OTP hijacking scheme, and their communications tactics are highly customized and targeted.

Upon detection of the phishing campaign, CERT-GIB immediately notified Vietnam's national computer emergency response team VNCERT. Group-IB team also continues its outreach across the banks that the scammers impersonate.

Key characteristics of the phishing campaign:

Targets several major financial institution of Vietnam and its customers with every phishing website.

Two main objectives of the campaign: control of users online banking transactions; gather PII data (name, address, national identity card details, phone number, DOB, and occupation)

To trick the victims into phishing websites cybercriminals distribute customized messages/emails disguised as legitimate banks to apply for loans, quick cash, or to claim gift vouchers from famous ecommerce brands.

Cybercriminals use OTP hijacking techniques that allow them to bypass verification.

These phishing websites contain the logos of 27 highly reputed banks and financial institutes in the form of a single page or as a drop down option where victims can pick their registered bank.

This campaign has not been seen in public targeting financial institutions in other countries apart from Vietnam.

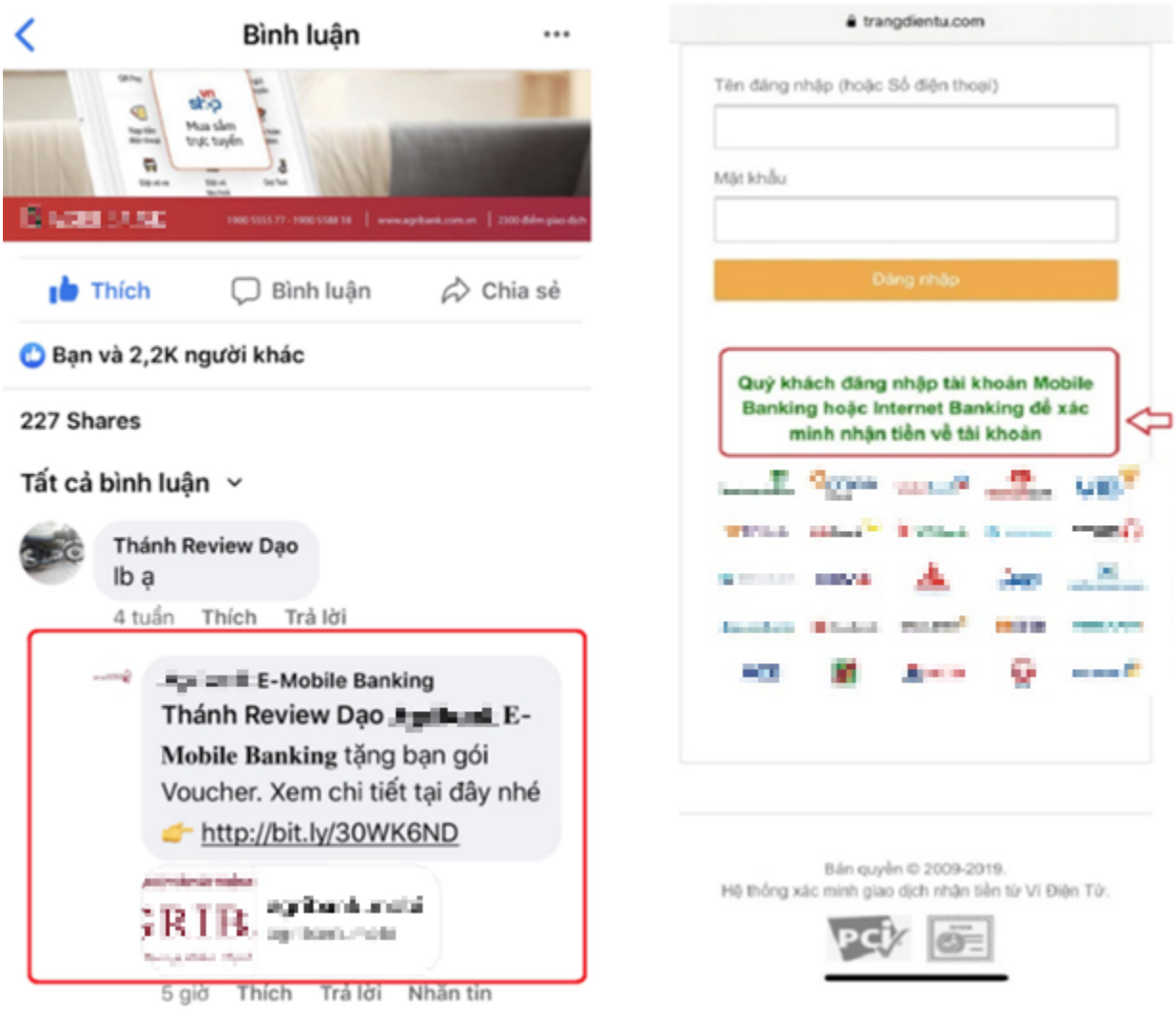
Victim journey

Cybercriminals behind this campaign leverage rogue SMS, Telegram and What's App messages, and even comments on Facebook pages of legitimate Vietnamese financial service companies to drive traffic to their phishing resources.

Such comments, observed by CERT-GIB, included the link which takes the victims to the phishing site. One of the tactics used by the operators of the campaign is the usage of shortened URLs where an average user would be unable to differentiate the legitimacy of the

URL.

Upon clicking on the link, the victims will be forwarded to a fake web page which is identical to the bank mobile login page where they are prompted to enter their credentials.

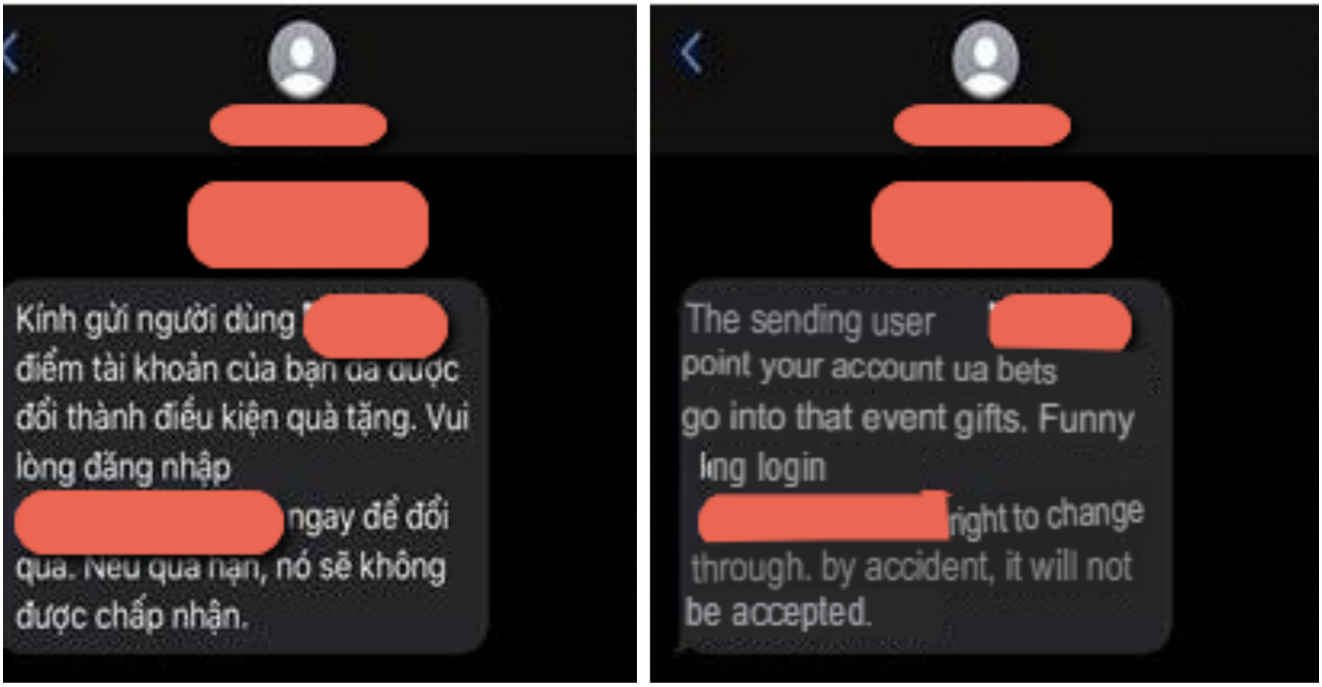


Automated machine translation form Vietnamese to English

Other channels that cybercriminals tap into are SMS and What's App. They send out rogue messages purporting to come from legitimate banks or ecommerce companies. The fraudulent What's App message below informs the recipient about the possibility to receive about 200 million VNĐ. To claim the award, the victim is prompted to click on the link to fill the banking account details.

Source: scamvn.com

Another SMS, obtained by CERT-GIB informs the victim that they have been awarded a gift and need to login to their banking portal to receive it. The message says that the offer is set to expire soon. By doing so the scammers create a sense of urgency.



Automated machine translation form Vietnamese to English

Upon clicking on such links, the victims are forwarded to a fake web page featuring the logos of Vietnamese leading banks.

The legitimate companies' logos have been blurred to minimize further reputational damage for the organizations affected with the campaign

Once the victim chooses its bank from the list, they are redirected to another phishing page disguised as a legitimate banking portal.

After the username and password are filled, the victims are once again redirected to a fake web page where a One Time Password (OTP) is requested. At the same time the fraudsters use already stolen credentials to login into the victim's real account. After the victim receives an OTP from their bank (requested by fraudsters) and submits it via a fake authentication page, the cybercriminals gain full access to the victim’s bank account.

After the “log in”, the victim is shown a message that says that the transaction is still processing.

Having this information allows cybercriminals to steal funds from victims' accounts. With this data they can also initiate unauthorized illicit transactions. Additionally, scammers harvest a vast amount of personal data. Such data is traded actively in the cybercriminal underground and can be purchased by other threat actors for further targeted follow-up attacks on the victims.

Group-IB has observed offers to sell Vietnamese citizens’ information harvested as a result of phishing campaigns on underground markets. While it is unknown whether the information is authentic and is sourced directly from this phishing campaign or not, CERT-GIB’s analysts have seen first-hand instances of offers to sell data about holders of bank accounts in Vietnam.

CERT-GIB is closely monitoring the campaign and its infrastructure for the appearance of new phishing. Group-IB team continues to work with registrars, hosting providers, and competent organizations in Vietnam to action phishing domains in a timely manner to to contain further financial loss for banking users and to protect banks from reputation damage.

Recommendations

For users

The communications that create a sense of urgency and intimidation are always red flags.

Users should pay attention to the URL in the browser. They should also be wary of malfunctioning websites and long chains of redirection. Users should also avoid purchasing from unauthorized resellers and clicking on links in fraudulent discount articles. It’s important to confirm the credibility of the resource. It takes some time to find the company’s official website, look for reviews, and call customer support but it’s worth it.

Enabling 2FA where possible is a must. Changing passwords from time to time is also a good habit.

For companies

Cybercriminals exploit the lack of decent monitoring and blocking efforts to create fake sites that misuse legitimate brand names. Companies need to be swift in taking actions against such complex threats. Detection at early stages is the key to minimizing the digital risks to the affected brands and to safeguarding the potential victims. Mapping and attributing newly registered domains can help to reveal patterns to improve the quality and scope of detection. Effective monitoring and blockage should involve an automated machine-learning digital risk protection system fuelled by regular updates to its knowledge base about cybercriminals' infrastructure, tactics, tools.