CYBER
THREAT
ANALYSIS

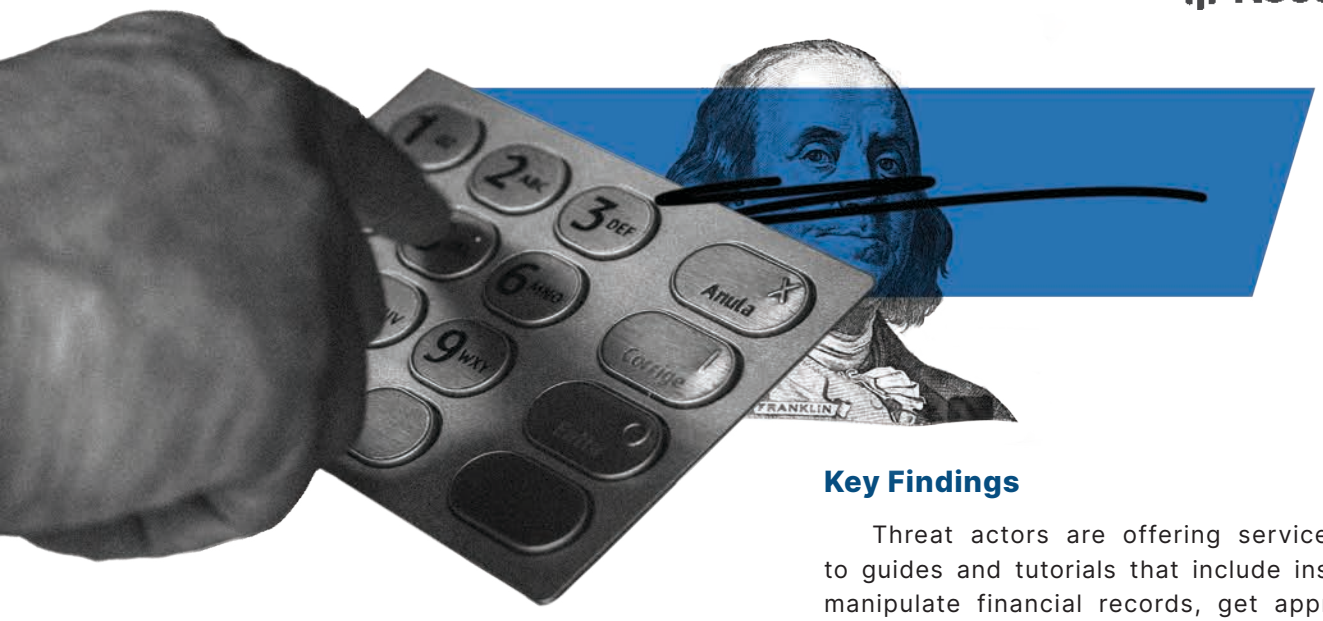
Recorded Future®

By Insikt Group®

May 24, 2022

THE BUSINESS OF FRAUD:

Bank Fraud



Recorded Future analyzed current data from the Recorded Future® Platform, dark web and special-access sources, and open-source intelligence (OSINT) between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer. This report expands upon findings addressed in the first Insikt Group Fraud Series report, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized".

Executive Summary

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution or individual by fraudulently posing as a bank, another financial institution, or another individual. As the financial sector has incorporated online and internet-connected banking into its business model, traditional means of fraudulently acquiring funds from a bank have been replicated and updated to target today's online banking employee and consumer. Throughout Recorded Future's "Business of Fraud" series of reports, we have identified many tactics, techniques, and procedures (TTPs) being used by cybercriminals to facilitate online criminal activities. Many of these same TTPs, from harvesting and using compromised personally identifiable information (PII) to social engineering, are also being used to conduct banking and online banking account fraud. In this report, we examined cybercriminal activities around the following types of bank fraud due to their often going overlooked and to identify parallels with other types of financial-related fraud: accounting, loan, check, and wire transfer.

Key Findings

Threat actors are offering services and selling how-to guides and tutorials that include instructions on how to manipulate financial records, get approval for loans, and purchase compromised accounts that contain loan application information. Hackers-for-hire include the capability of accessing and manipulating records and documentations in their advertisements.

Counterfeit checks are still in high demand and are often coupled with threat actors looking to conduct wire transfers or cash out. The means of creating a counterfeit check has become more automated and customized, with threat actors operating shops that focus on this service and whose user interface is easy to follow.

Threat actors continue to use instant messaging platforms to advertise, negotiate, and sell services and listings that facilitate check, loan, wire transfer, and accounting frauds. These messaging platforms are all-encompassing when compared to the traditional dark web ecosystem (forums, marketplaces, and shops) in that they provide instantaneous communication, greater control in adding and removing listings, and are more readily available.

Background

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term "bank fraud" applies to actions that employ a scheme or artifice, as opposed to bank robbery or physical theft. For this reason, bank fraud is sometimes considered a white-collar crime. Online banking services now allow customers to access bank accounts and records via personal computers and mobile devices. This convenience has not only increased the attack surface but has allowed cybercriminals to creatively leverage new and old methods for conducting nefarious activities.

Threat actors gain access to online banking accounts in multiple ways, such as using a stolen identity (identity theft) to open new accounts (application fraud) or obtaining valid credentials to existing accounts (account takeover) through phishing, credential reuse, different types of malware, or purchasing them from dark web sources. Given the previous reporting done by Recorded Future that relates to financial crimes (laundering funds, using compromised PII and counterfeit documentation to open accounts, using sniffers, bank injects/overlays, infostealers to harvest banking credentials to take over accounts and payment cards, and recruiting mules and cashout services), this report will not focus specifically on compromised payment card data or one of the aforementioned topics. Rather, this report will examine how cybercriminals are conducting operations across a variety of dark web and special-access sources to facilitate the following types of bank fraud, which are not as commonly known or popularized: check, loan, wire transfer, and accounting fraud.

Types of Bank Fraud

Many of the aspects covered throughout our Fraud Series overlap with TTPs being used by threat actors to facilitate bank fraud:

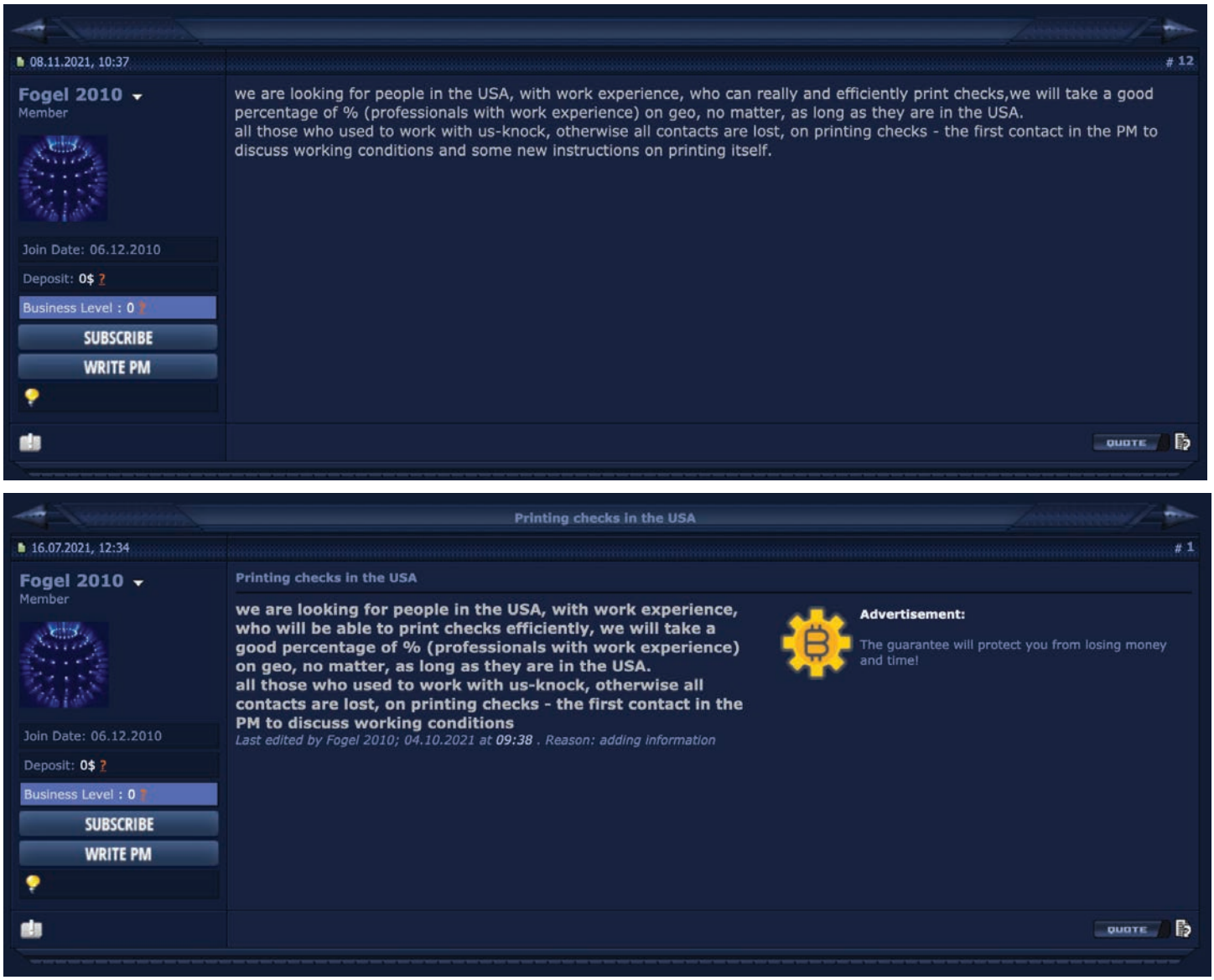
- A majority of threat actors are not specifically advertising services for the 4 types of bank fraud addressed in this report; rather, are offering services and methods that include these activities in conjunction with other types of financial fraud.
- Like with most types of fraud, compromised credentials and PII to create or gain control of accounts are the lifeblood of bank fraud. Threat actors advertising these types of compromised data are using the same forums, marketplaces, and shops (both as sellers and buyers) to facilitate other types of fraudulent cybercrimes.

Threat actors are lately interested in synthetic identities, a type of fraudulent identity that combines the proprietary PII (such as date of birth, Social Security number) of several individuals to make a single, new identity. Although this report does not specifically investigate synthetic identities, the amount of compromised PII data widely available across dark web sources coupled with the widely shared knowledge of performing fraudulent activities (social engineering, phishing, among others) makes this attack vector an attractive tactic to be used by criminals in the future, specifically those wanting to commit bank and financial-related crimes such has registering account or loan applications. According to our data sets, there are multiple tutorials and how-to guides on creating synthetic identities across different dark web and special-access sources.

Check Fraud

Check fraud involves the illegal use of banking checks to acquire the funds of the account holder. Fake checks come in many different forms that are difficult to identify; they can look like business or personal checks, cashier's checks, or electronically delivered checks. As fraud is constantly evolving and technology has made significant progress, people can produce fake checks and money orders that are difficult for consumers and even bank employees to identify as fraudulent. In addition, services such as depositing checks via mobile applications (apps) or depositing them online have recently become more widely available, making life easier for bank customers, but also for fraudsters.

An example of this activity is an advertisement posted by "Fogel 2010", a member of Verified Forum. On August 11, 2021, Fogel 2010 created a post looking for partners in the US who could print checks, likely indicating that the threat actor targets US banks and victims. Cybercriminals can cash out checks by either depositing them into self-registered online bank accounts, or via drops, who are witting and unwitting accomplices who would deposit the fraudulent checks into their own bank account and subsequently cash them out. Earlier, in October 2019, Fogel 2010 had posted an advertisement looking for drops to cash US corporate checks in the amounts of $2,000 to $5,000. Figures 1 and 2 show some of these posts.



Figures 1, 2 : Fogel 2010 looking for partners who can print checks for cashing out (Source: Verified Forum).

Criminals could also use dedicated services that offer to create counterfeit checks. An example is a dark web shop called ScanLab, which allows its customers to select the desired bank, check type, and amount. Additionally, the service offers to create counterfeit documents, such as ID cards, driver's licenses, Social Security cards, and more.

Loan Fraud

To commit loan fraud, criminals will falsify information on records and applications to loans. Like many forms of fraud, many threat actors now offer loan fraud services. Similar methods could be used to facilitate other forms of fraud, such as payment card fraud, tax fraud, and unemployment fraud. The demand of users interested in learning about how to conduct loan fraud seemed higher, in our analysis, than the supply of threat actors offering loan fraud-specific services and listings, however.

Threat actors wanting to conduct loan fraud are interested in application techniques and services related to all types of loans, including mortgages and student loans, among others. In addition to using compromised PII and sensitive data, a threat actor has at their disposal, via dark web and special-access sources, how-to guides on conducting loan fraud, services on filling out applications, and ready-to-purchase loans at set amounts. Most of these activities are occurring on low-tier forums and marketplaces, and a sample of threat actors listing services and guides follows in Table 1:

Threat Actor	Source	Intelligence
"fraudbuddy"	Hermes Market	In March 2022, the threat actor listed a tutorial for $100 on conducting bank-related fraud that includes loan applications. With the purchase, a fraudster will be provided a private point of contact to communicate directly with fraudbuddy, who will help them navigate through the application process. The threat actor is listing the same and similar fraud methods across a number of different dark web marketplaces.
"ESCO"	Carders.ws	Beginning in November 2020 and continuing to the present, the threat actor is offering a tutorial on how to acquire and get approved for loans, including bank loans. Forum users have provided positive feedback after receiving the guide and course.
"kaki09"	Altenen	In September 2021, the threat actor listed a loan scamming method. This threat actor frequently posts various how-to fraud methods, including cashing out and other types of financial-related fraud.

Table 1: Sample list of threat actors offering services that facilitate loan fraud (Source: Recorded Future)

Threat actors are also using dark web shops that specialize in selling financial-related data, such as access to compromised accounts that list loan application information and payouts. These types of listings are not reserved to just the dark web ecosystem but are also being listed on publicly accessible Telegram channels that run like shops. Some of these channels host multiple vendors selling an array of compromised financial data, including over 160 vendors operating across different channels listing and discussing loan-related products.

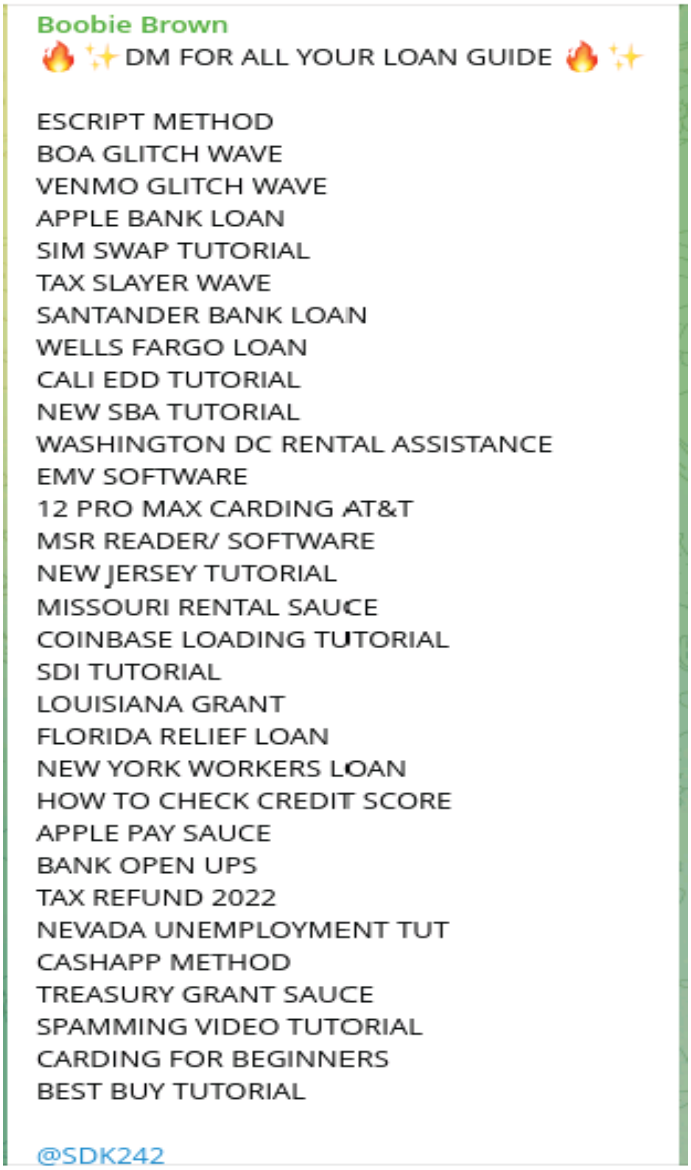


Figure 3: Listing of loan guides by "SDK242" for branded banks and companies within a public channel (Source: Telegram)

Wire Transfer Fraud

For cybercriminals, one appeal of wire transfer fraud is that once the wire goes out, it is very difficult or impossible to reverse it. In general, to conduct wire fraud, cybercriminals need to access the victim's bank account, initiate the wire transfer to an account under their control (which could be another stolen account) and then withdraw the funds. One difficulty in wire transfers is that the bank may need to verify the identity of the sender, thus requiring cybercriminals to have the victim's PII and, in some cases, forged documents.

Threat actors are using forums, marketplaces, and messaging platforms to advertise services and products that facilitate wire transfer fraud and include how-to guides on conducting wire transfers, wire transferring services that include sending, receiving, and cashing out funds, and requests for wire transfers. Cybercriminals increasingly use Telegram, as this platform offers a level of anonymity, allows for a wider customer base (as there is no need for special software to access the dark web), makes operating their own shops easier, and provides greater control of operations (such as adding or deleting listings and removing or blocking users). As most of these channels are publicly available to maximize exposure, some channels host multiple sellers where they compete for business through sales and 24/7 customer service.

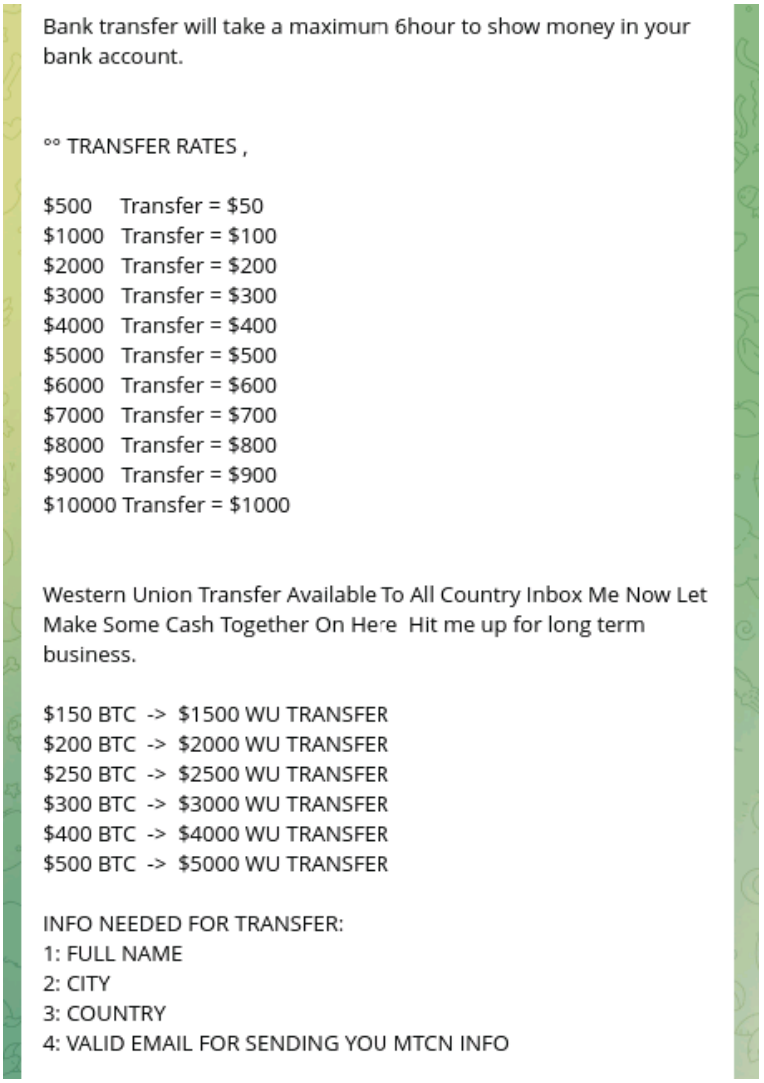
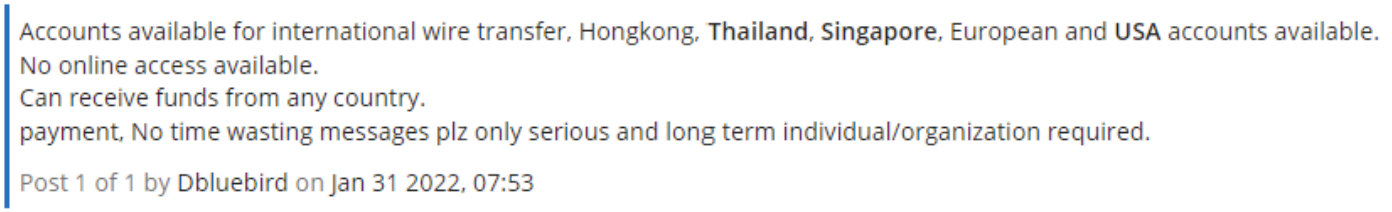


Figure 4: Wire transferring services and rates by "[Trusted] Panda" (@TrustedPanda) (Source: Telegram)

Another service in which threat actors are seeking out methods for hiding financial activities is the use of offshore banks and institutions that bypass international sanctions and do not divulge financial or account information to the US or other countries. This topic has had a renewed interest following the release of the Pandora Papers at the end of 2021, as well as Russians wanting to transfer their funds, typically through wire transfers, to countries that do not cooperate or abide by economic and fiscal sanctions imposed by the US and Western European countries following the invasion of Ukraine by Russia in February 2022.


Accounts available for international wire transfer, Hongkong, **Thailand**, **Singapore**, European and **USA** accounts available.
No online access available.
Can receive funds from any country.
payment, No time wasting messages plz only serious and long term individual/organization required.

Post 1 of 1 by Dbluebird on Jan 31 2022, 07:53

Figure 5: Wire transferring services to popular offshore banking destinations (Source: Recorded Future)

We identified the forum user "kith" on the now-defunct Raid Forums posting information on offshore banking, specifically recommendations on choosing a bank, optimal countries, and other best practices. As is common across forums, these sources serve as a means of sharing intelligence as much as selling compromised data, as such sharing builds commonality and trust and strengthens the community. Although opening or wiring funds to offshore accounts were not specifically referenced by institutional names, we identified threat actors advertising said services, specifically on messaging platforms, to countries that are popular destinations for international bank accounts, such as Hong Kong and Singapore.

These services are often customizable, and threat actors are willing to work with customers on specific requests, including, we believe, the ability to use wire transferring services to wire funds to an offshore bank.

Accounting Fraud

Accounting fraud is the deliberate alteration of a company's financial records so as to hide profits, cover up losses, or otherwise obfuscate the actual financial condition of a company. In today's digital world, accounting fraud is also expanded to include threat actors changing account information to facilitate funds transfers and payments to accounts under their control. For cybercriminals, our investigations did not identify specific threat actors stating their services in committing accounting fraud. Rather, we identified hacking services, insider threats, and exposures to networks that would facilitate a threat actor in gaining access to a company's financial records with the intent of manipulating documentation.

Over the last year, we identified threat actors advertising their hacking services on a range of dark web forums. These services cover an array of capabilities, including changing records, upgrading credit ratings, and customizable services per requests. Many of these advertisements occurred on compromised payment card-related forums such as Card Villa and Carding Mafia, but forums such as Hack This Site and XSS Forum also listed postings for these services. Many of these services were also described as customizable, highlighting that a hacker is willing to discuss with a client their specific requests, needs, and expectations.

In addition to these hacking services, we also reported on over 90 separate incidents of threat actors advertising and selling various types of network accesses, such as Citrix, remote desktop protocol (RDP), web shell, and others, into compromised systems over the last year. Often these forms of access are associated with malware and ransomware infections, but a motivated threat actor could also use these access methods to gain permissions into a company's accounting department and acquire financial documents and other sensitive corporate records that can be altered or changed. In April 2022, the threat actor "mavro5220" listed for purchase access to a Canada-based bank. If this access is coupled with a vulnerability that permits a threat actor to change account numbers (for example, this listing from "Brady" in December 2021 purporting to be able to change account numbers), a threat actor could change account numbers and other sensitive information so as to reroute funds to accounts under the control of a threat actor.

Not all network intrusions are destructive; rather, a motivated threat actor could target a company with malware that results in them lingering within a network for as long as they remain undetected. By remaining undetected, a threat actor could siphon off accounting records and proprietary financial data that could be used to reroute funds and data into accounts controlled by threat actors. As previously reported by Insikt Group, threat actors are continuing to use different aspects within social engineering to gain access into a victim's network, specifically phishing or business email compromise (BEC). These types of attacks are most often successful against small-to-medium sized enterprises that may lack detection mechanisms or security training of employees to detect said attacks. Based on Insikt Group findings, we have identified threat actors mostly deploying remote access tools and remote access trojans (RATs) when looking to conduct more intrusive and espionage-related activities. Over the last year, our data sets showed the following remote access tools and RATs being used by threat actors with phishing events: KONNI, PlugX, REMCOS RAT, Cobalt Strike, and Revenge RAT.

Last, insider threats, from unintentional insiders who unknowingly download malware to malicious insiders who deliberately breach protocols to acquire privileged information, also pose a means to conduct accounting fraud. In June 2021, employees at the South African bank Postbank stole the bank's master key in plain, unencrypted text (permitted the key's holder to access and manipulate account balances) from its data center, resulting in at least 25,000 fraudulent transactions. In addition, an insider may be recruited by a more advanced threat group to gain access to accounting-related systems and documents. FIN7, an advanced, financially motivated threat group, has attempted to spread its malicious activities by recruiting professionals under the guise of an authentic IT company as well as mailing infected USB drives that contained GRIFFON malware.

Outlook

The 4 types of fraudulent activities that facilitate bank fraud covered in this report showcase the overlaps between how different types of fraud are using similar methods and require similar data to facilitate activities. As a majority of bank-related fraud involves compromised payment data and accounts, compromised PII data and bypass methods (among others) are used in accounting, loan, checking, and wire transfer fraud types in addition to other forms of fraud. These types of fraud are being actively sought after and advertised across the entirety of the dark web criminal ecosystem, with threat actors continuing to incorporate instant, encrypted messaging platforms into their methods for advertising, discussing, seeking, and selling services and products.

As highlighted in Recorded Future's 2020 series on the automation and customization of the dark web, the threat actors highlighted in this report (as well as the many others) are continuing to customize their services, host automated shops and marketplaces with easy-to-use interfaces, and update their attack vectors to defeat security measures. We believe that threat actors will continue to incorporate automation and customization into their business model so as to attract customers and make profits. As the demand for these services show no signs of dissipating, we recommend working with Recorded Future so as to receive timely updates and notifications of events or listings that may affect your brand. Once an alert is received, we recommend triaging it for severity and working with us to identify solutions and steps to be taken in the future to harden your security measures.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.