CYBER
THREAT
ANALYSIS

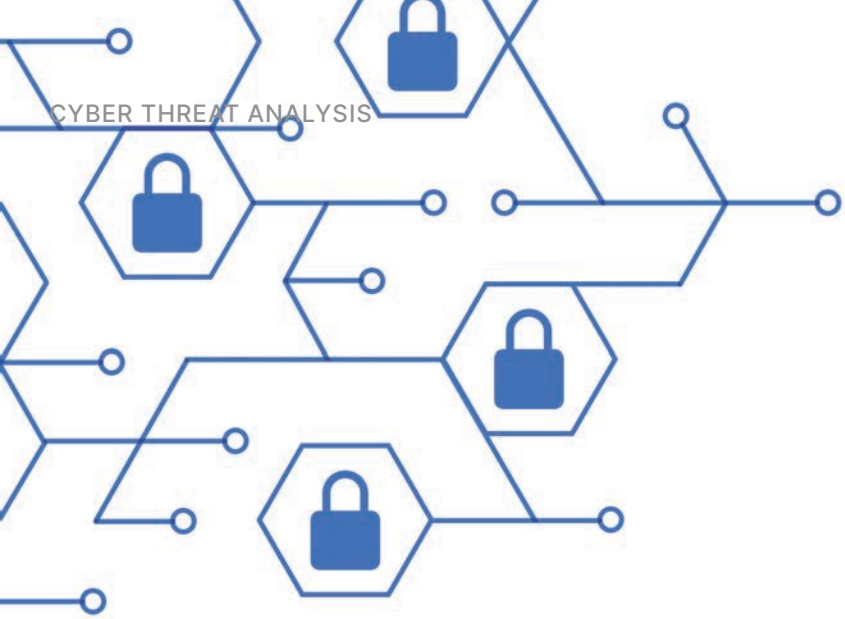
Recorded Future®

By Insikt Group®

CTA-2021-0225

THE BUSINESS OF FRAUD:

An Overview of How Cybercrime Gets Monetized



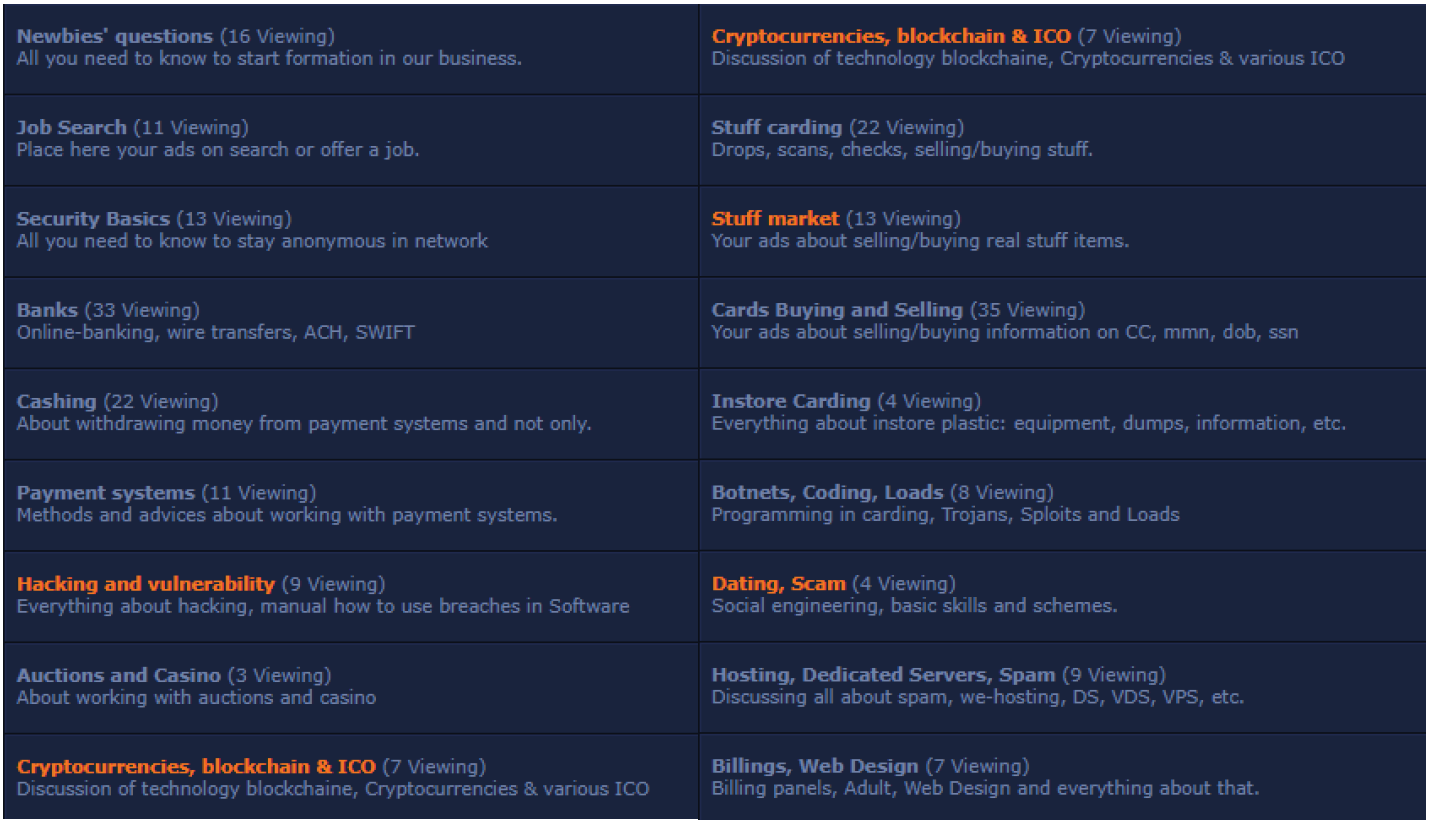
Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other OSINT sources to review 11 fraud methods and services that facilitate threat actor campaigns. In subsequent months, Recorded Future will publish in-depth reports on each method or service, the threat actors offering them, technical details where applicable, and mitigation recommendations. This report will be of most interest to anti-fraud and network defenders, security researchers, and executives charged with security and fraud risk management and mitigation.

Executive Summary

The cybercriminal fraud ecosystem is a whole and interconnected enterprise. In this report, the introduction to our series on cybercriminal fraud, Insikt Group will describe 11 types of fraud methods and services currently used by threat actors to facilitate their campaigns. For each, we provide a brief overview of some notable recent developments, list some of the top vendors of these services on the criminal underground, and provide suggested mitigations for defenders to implement. The Recorded Future Platform enables research and analysis of fraud methods available on the dark web and other sources to identify cybercriminal schemes, as well as threat actors and communities that advertise said methods.

Outline

- **Fraud tutorials and courses** provide insights into possible vulnerabilities as well as schemes and techniques used by threat actors.
- **Drops and mule** services, unlike other cybercrime services, require a physical and human presence to successfully carry out criminal operations.
- **Dating scams** involve the creation of fake profiles on dating apps or social media platforms, or direct phishing emails that target victims with the end goal of tricking the victims into sending money or facilitating fraudulent activities.
- **Online retail fraud**, including gift card fraud and refund fraud, typically entails the use of stolen information and is frequently facilitated by anti-detect and shipping services.
- **SIM swapping** is a technique used by threat actors to gain access to a victim's phone number with the end goal of using two-factor authentication (2FA) to obtain access to the victim's online accounts.
- **Money laundering services** within the dark web provide a combination of services through which threat actors can conceal the origins of their money, transfer cryptocurrency into virtual currency, have funds sent to a bank account or payment card, move funds across borders, or exchange for physical currency.
- **The role of botnets in the dissemination of malware to support fraud** continues to grow as threat actors propagate some of the most prevalent malware families targeting individuals and organizations. These malware strains are specifically designed to exfiltrate information appealing to financially motivated threat actors seeking to conduct fraud.
- **Travel and loyalty (hospitality) fraud** involves threat actors scamming users into providing personally identifiable information (PII) and financial information through fraudulent travel and hospitality services, including car rentals, hotel and flight bookings, excursions, and other vacation-related offers such as bonus points, miles, and other rewards.
- **Sales of personally identifiable information (PII) and protected health information (PHI)** are conducted by threat actors who gather victim PII stolen from compromised networks, individual infected computers, leaked databases, or phishing attacks, which is then used to facilitate a wide variety of fraud.
- **Tax return fraud**, also known as stolen identity refund fraud (SIRF), is a specific case of identity theft where a criminal files a tax return with victim information to the Internal Revenue Service or state tax agencies with the goal of stealing the victim's tax refund.
- **Bank fraud** is constantly evolving to follow current trends in the banking industry. Credit card fraud, online banking fraud, and wire transfers fraud are the main types of bank fraud.



Figures 1, 2: Main forum sections (Source: Verified Forum)

Background

Like any complex profession, fraud is a trade that requires education and cooperation to master, or, at the very least, become proficient in. Knowledge of this trade is passed down to new fraudsters from more experienced operators in criminal underground forums, some of which have been around for a quarter of a century. Popular fraud forums such as Verified, Omerta, and WWH Club provide newcomers the tutelage, professional relationships, and resources satisfying the full spectrum of needs for any fraudster. The forum Verified, arguably one the most prolific fraud-related forums predominately catering to Russian-speaking threat actors, has an extensive list of sections pertaining to specialized types of fraud, as seen below:

There are basic elements that exist for any fraud operation: the method, the target, and the cashout scheme. For example, tax return fraud requires things like W-2s stolen from a CPA (the target), filing for a tax return using tax software through an RDP connection on a victim computer (the method), and sending the money from the tax return through a series of money mules and cryptocurrency accounts to the attacker (the cashout). Dating scammers choose victims active on online dating websites (the target), build a rapport through enticing photographs, videos, and conversation to send money (the method), and then launder the funds through bank wires or virtual payments (the cashout). Though the operations are very different, the elements of fraud are the same.

Threat Analysis

1. Fraud Tutorials and Courses

Training tutorials and courses sustain the activities of various underground forums and threat actors .They nurture novice cybercriminals while providing additional supply and demand to the underground economy .Threat actors use both forums and marketplaces to advertise how-to guides and tutorials on a range of cybercrime-related topics ,including malware creation, mule recruitment ,cashout methods ,ATM bypasses ,and other methods that facilitate criminal activities .These tutorials and courses cater to a range of cybercriminals ,from cybercrime novices to more seasoned ,niche-focused experts that are seeking additional guidance and knowledge.

Established underground sellers receive new clientele represented by participants and alumni of the training, one example of which is the “Carding Camp”, a well-known course on payment card fraud organized and hosted by the forum WWH Club. Since the start of the course, thousands of Carding Camp graduates have joined the ranks of cybercriminals, multiplying the fraud and fueling the underground forums, marketplaces, and shops specializing in sales of stolen payment card data. Insikt Group previously analyzed the differences and similarities among the three primary dark web resources — forums, shops, and marketplaces — in the report “Forums, Marketplaces, and Shops Remain Essential Venues for the Criminal Economy”.

Figure 3: The CIS, Baltic States, and China, map of mentions and references (Source: Recorded Future)

Payment card fraud, or "carding", does not have to be complicated. All that the cybercriminals need are insights into how financial platforms operate, which they get from the communal knowledge of like-minded fraudsters, access to the carding material, such as stolen payment card data, and technical means to pretend to be someone else, such as a valid user or a cardholder.

Since 2015, the Russian-language underground forum WWH Club has been offering a training course on payment card fraud. The price of the course in 2021 is $900. Over 10,000 cybercriminals have taken the monthly course, which is widely advertised among underground forums. The course is taught by 10 to 15 instructors — cybercriminals with a reputation involved in financial fraud, and WWH Club forum administrators and moderators. The average group of "Carding Camp" trainees consists of 40 to 50 individuals with different levels of cybercrime experience, with most being novice fraudsters looking to improve their carding skills.

The course is six weeks long and is taught live from 6:00 PM to 9:00 PM Moscow time, Monday through Friday, using Jabber, Telegram, and Zoom group sessions. The trainees get access to the forum's closed sections, library, resources, fraudster starter pack materials, and special status on WWH Club and its partner forums. While communication inside the carding camp is in Russian, Insikt Group has observed trainees from different countries within the Commonwealth of Independent States (CIS), as well as from the Baltic states, China, and other countries.

The carding camp training on WWH Club is well known in the underground communities for enabling novice cybercriminals to join the carding community. Insikt Group analysts obtained the WWH Club carding camp materials and studied the cybercriminals' tactics, techniques, and procedures (TTPs), targets, know-how, and emerging fraud methods.

WWH Club carding camp focuses on a variety of fraud methods, and there are many other courses dedicated to specific fraud areas. One example is the "Enroll 5.0" course, led by the threat actor "susnsun", also known as "GOLDIE", who is an administrator of the GOLDIE ENROLL Telegram channel, suspiria[.]ws credit cards shop, and goldie[.]cc forum dedicated to online banking fraud. Enroll allows cybercriminals to link credit card accounts online with the ability to change cardholder's credentials to ones of their choosing. Participants of the Enroll 5.0 course receive access to the following resources:

- 30 private and public credit card shops and individual sellers
- "Probiv" services to obtain victims' PII data, most commonly including background checks and public and private records ("Probiv" is a Russian slang that generally refers to information gathering on organizations and individuals using open and closed sources and databases)
- Calling services that enable threat actors to make various changes to online bank accounts on behalf of the victims

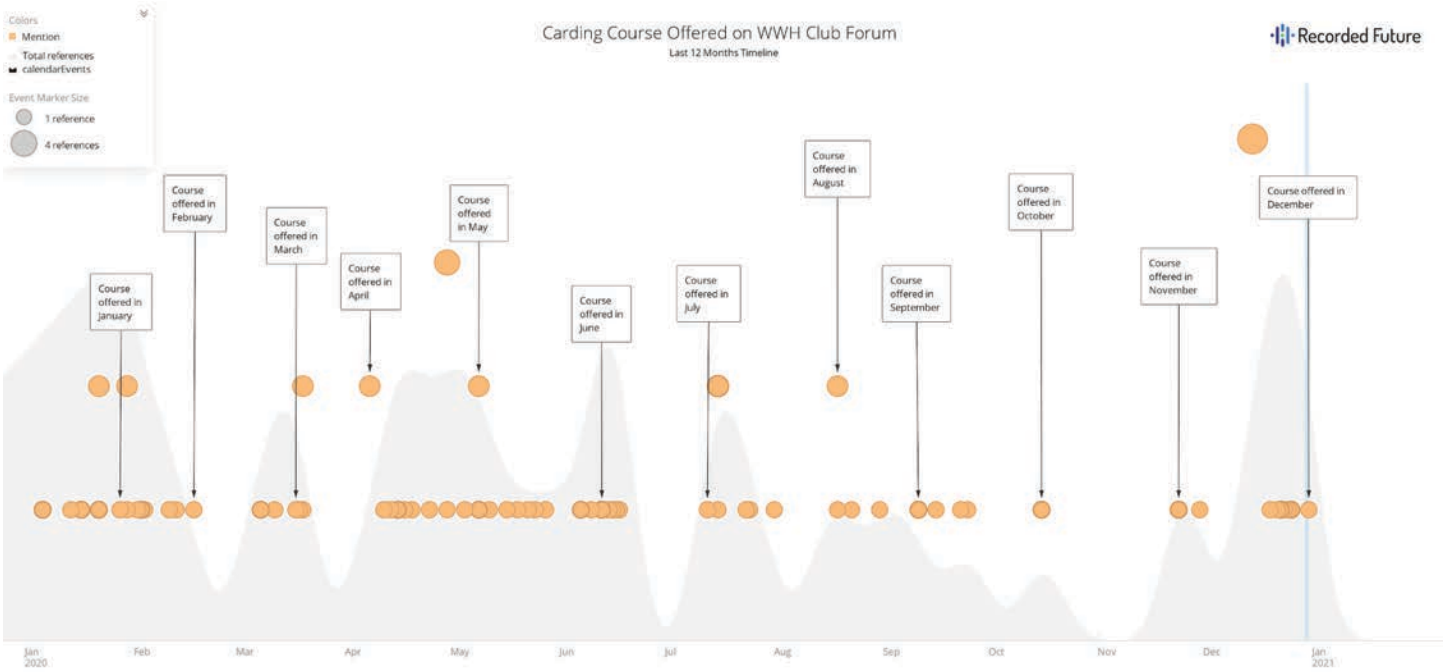


Figure 4: Timeline of the carding course offered on WWH Club, January 2020 to January 2021 (Source: Recorded Future)

Fraud tutorials and courses may not always offer the most modern tactics since threat actors are likely to exploit novel methods before sharing them with others. However, these tutorials can provide organizations with insights into possible vulnerabilities as well as schemes and techniques used by fraudsters. Equipped with this information, organizations can evaluate their policies, controls, and anti-fraud mechanisms to tailor their response against existing and emerging fraud methods.

2. Drops and Mules

After receiving the training and gathering initial fraud how-to information, cybercriminals identify drops and mules services for their operations. Some fraud tutorials and courses are specifically focused on recruiting drops and mules.

Drop services, unlike other cybercrime services, require a physical human presence to successfully carry out the carding operations. Each developed carding enterprise has a team of people who will intercept stolen packages, verify purchases, and handle the situation when a physical presence of the impersonated account owner is needed. Drop services already have teams on the ground with an established infrastructure of fake identities, IDs, warehouses, and vehicles. These teams can be used for other aspects of the operation, such as placement of banners, flyers, cold-calling, recruiting others, and cashing out at banks and ATMs.

Another form of a drop is the money mule. The FBI defines a money mule as a person who transfers illegally acquired money on behalf of or at the direction of another person. They are used as intermediary recipients of stolen funds, cash out stolen payment cards at ATMs, or use their accounts to launder funds between various accounts. Money mules who have accounts with a history of legitimate transactions or those with a good credit history are often prized because transactions involving their accounts are less likely to be flagged.

Cracked Forum, Club2CRD Forum, Verified Forum, and WWH Club Forum are the most notable criminal forums advertising drops and mules services. The drops and mules ecosystem starts with a recruitment process that allows cybercriminals to involve local personas in their criminal enterprise.

Recruitment Process

Threat actors have been known to create fake companies or use hacked accounts of legitimate companies, posting job vacancies on popular job search engines such as Indeed, ZipRecruiter, and Monster advertising what appear to be legitimate jobs for job seekers. Once the threat actor has hired the applicant, the individual is given access to a web panel where they can fulfill their weekly duties and requests. Thus the individual is sometimes knowingly and sometimes unknowingly carrying out the nefarious activities of the threat actor. This factor is significant in running the drop, so when drops are discussed on forums they are always identified as "witting" or "unwitting" drops. Witting drops are typically recruited through word of mouth. Each type has its own advantages and disadvantages.

Bank Mules Examples

- December 2020: A member of Club2CRD Forum posted an advertisement requesting UK drop services for well-known banks in the region, including Lloyds, Halifax, Barclays, RBS Santander, and Natwest.
- November 2020: A Mexican threat actor on Boveda Forum sought a bank mule for Banorte, one of the largest banking and financial services companies in Mexico.
- April 2019: A forum member identified themselves as a Canadian money mule advertising their services and looking to establish long-term relationships within well-established networks.

Shipment Drops Examples

- December 2020: A Turkish threat actor on Darbeturk Forum posted an advertisement looking for someone to drop stolen cargo and remove the shipping label off of a package.
- October 2020: A threat actor on Boveda Forum advertised looking for drop services in Argentina, leaving their Telegram information for those interested in doing business.

3. Dating Scams

While the more popular perception of the end goal of dating scams is to convince the victims to send money to the threat actors, there have been instances of threat actors sending victims money and using them as money mules and shipping drops. Dating scams involve the creation of fake profiles on dating apps or social media platforms, as well as direct phishing emails that target victims with the end goal of tricking the victims into sending money to the threat actors or providing the threat actor with other fraud-related assistance. The actors behind these dating scams rely heavily on social engineering and evoking an emotional response from the victims to create a false sense of trust. Furthermore, there are a myriad other end goals that threat actors can have from dating scams, including the theft of the victim's personally identifiable information, identity theft, and, less frequently, intelligence-gathering.

In the criminal underground, running dating scams is a specialty, and, in some cases, will even have its own subsection on fraudster forums. Like other complex cybercrime operations, dating scams usually require cooperation among threat actors, each of whom will have a specialty: identifying targets, allocating convincing images or creating personas, and cashing out the stolen money are all separate services offered on the underground that are combined to carry out successful, persistent dating scams.

Content is arguably the most important element of any dating scam. Fraudsters need to constantly collect images and videos of new, real individuals (often women in their teens or 20s) to appear believable to the victims and require a component of human infrastructure to conduct their operations. Creating

Figures 5, 6: Shipping drops banner ads (Source: WWH Club Forum)

[Translation of top image: DON'T WORRY BE HAPPY
RESHIPPING
ONLY QUALITY DROPS IN THE USA FOR STUFF]

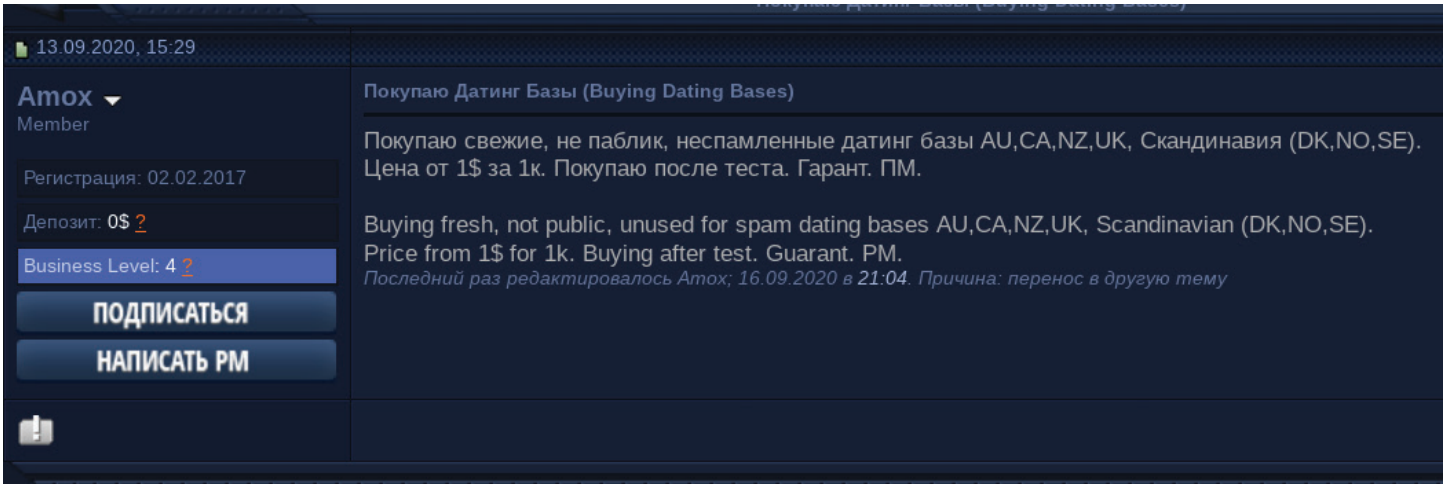


Figure 7: Amox's advertisement (Source: Exploit Forum)

female personas that appear authentic and believable requires things like having multiple pictures of the same individual that include friends or family, or that show the individual in various locations or clothing. This allows the persona to employ social engineering techniques and extend an email conversation with their target using these multiple images.

For example, "samsung110", a member of the forum Verified, posted that they are searching for just that: images and videos of women between the ages of 28 to 33 years old, including those with the ability to produce new photos or videos on demand. This latter request suggests that the threat actor providing the content will have a direct or indirect relationship with the woman they're using as bait, who could possibly be an accomplice.

Spammers specializing in dating scams provide specified mailing lists of targets thought to be more susceptible to this type of attack — the type of individual who may be hoping for an email from the person of their dreams. These mailing lists are geographically relevant to the victims being targeted (such as the United States, Canada, and Australia), and are likely sourced from leaked or fraudulent online dating databases. One such threat actor named "Amox" was looking to purchase email accounts from private databases acquired from dating websites paying one dollar per 1,000 accounts.

Lastly, there is the cashout service operated by fraudsters specializing in dating fraud drop accounts. These threat actors create bank accounts with unique names likely matching that of the persona who instigated the conversation through phishing attempts by email, social media, or online dating platforms. Threat actors like "edmon", who will create accounts under the name of your choice, will accept transfers via services like wire transfers, Western Union, and MoneyGram. They will then forward the money that same day to the client's WebMoney purse, Bitcoin wallet, or a payment card of a Russian or Nigerian bank.

4. Online Retail Fraud

Multiple e-commerce, social media, and financial organizations around the world are targeted by cybercriminals attempting to bypass or disable their security mechanisms, in some cases by using tools that imitate the activities of legitimate users. Threat actors who have obtained compromised payment cards will then attempt to access the funds on those cards. If the payment card information was obtained from a compromised online merchant, for example by using a sniffer, that information will contain everything needed to attempt online retail fraud. This includes basics like the card number, the victim's name, address, and security code. Although most major online retailers have implemented various methods of anti-fraud mitigation, such as using cookies and fingerprinting of browsers, threat actors have come up with means to circumvent many of those methods.

Every web browser has a unique fingerprint known to legitimate websites. E-commerce companies and banks often use this type of fingerprinting to block transactions from browsers that have previously been recognized as insecure or involved in fraudulent activity. The practice by cybercriminals of using various virtual machines, proxies, and VPN servers is not that effective since the anti-fraud systems have capabilities to identify suspicious IP addresses and virtual machines. As a result, cybercriminals have developed anti-detection software, such as Linken Sphere, AntiDetect, Multilogin, Che Browser, and FraudFox. These anti-detection software services allow threat actors to change all web browser configurations dynamically and generate an unlimited number of new ones, imitating the activities of legitimate users.

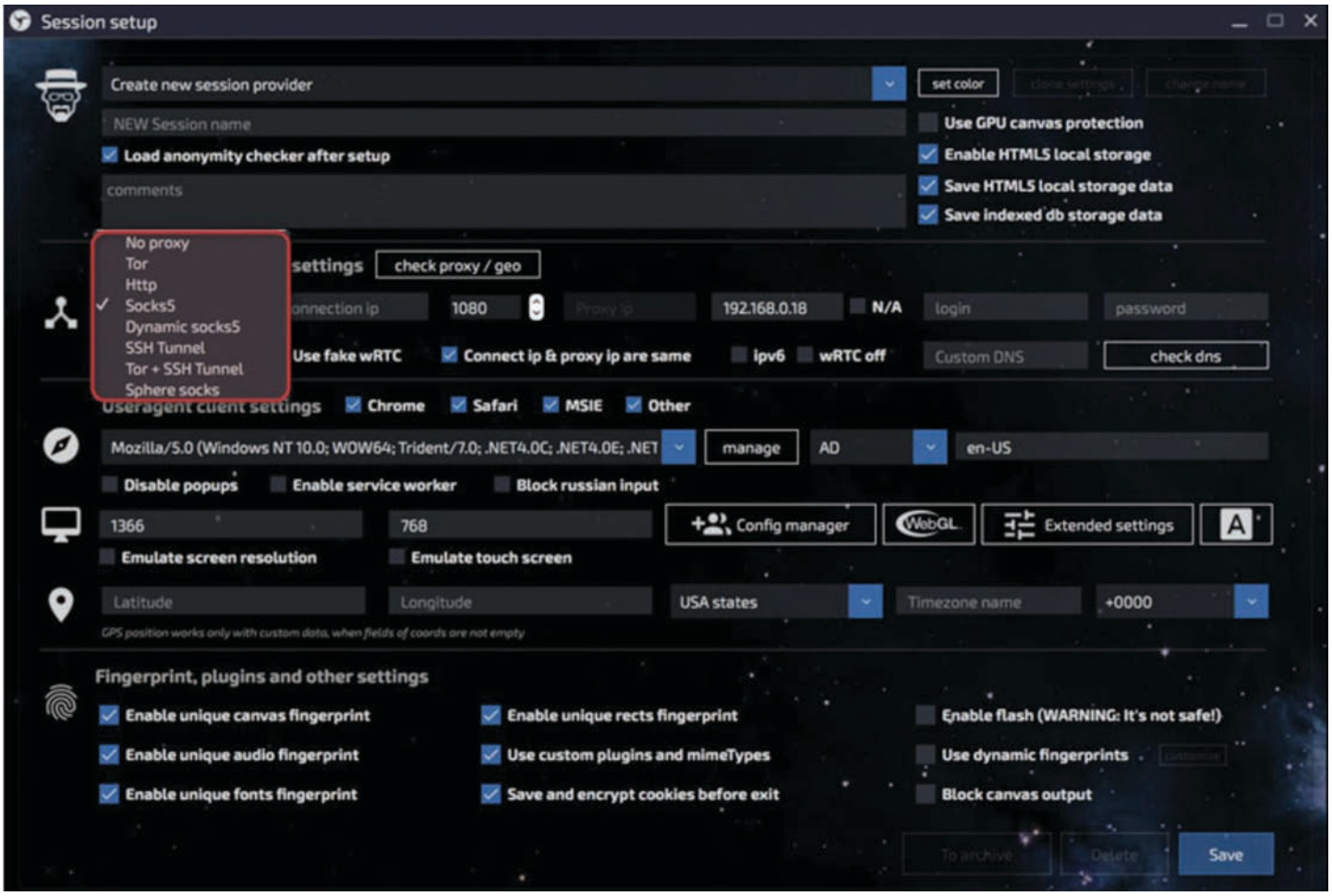


Figure 8: Linken Sphere session setup interface allows users to select an appropriate connection through various protocols

- **Linken Sphere** is a Chromium-based web browser that allows cybercriminals to bypass anti-fraud systems of various organizations by imitating real user behavior. The product was launched in July 2017 and quickly obtained high recognition on the dark web due to its substantial functionality, affordability, high-quality technical support, and advertisements across major underground forums. Linken Sphere was first introduced on the Russian-speaking forums Exploit, Club2CRD, and WWH-Club on July 4, 2017, by the threat actor "nevertheless", an administrator of the Tenebris Team forum, the official forum of Linken Sphere. (See our in-depth technical analysis of Linken Sphere.)
- **AntiDetect** is an anti-detection browser for creating browsers with different configurations. The configuration is a collection of Javascript files copied by a special method from real browsers. The most popular versions of AntiDetect are 7.7 and 8. According to the developers, AntiDetect v.7.7 is tailored both for professionals and beginners, whereas version 8 is created exclusively for professionals. AntiDetect has been known on the dark web since at least 2013 and was created by the threat actor "bite.catcher".
- **Multilogin** is a tool created by an Estonia-based team and positions itself as legitimate software (Multilogin Software Ltd). The developers state that its primary technical features are unique fingerprints and the ability to work with multiple accounts at a time. The developers created their own anti-detection browsers called "Mimic" based on Chromium and "Stealthfox" based on Mozilla Firefox browsers. According to the Multilogin owners, creating a browsing profile in Multilogin creates a completely separated virtual browsing environment. Cookies, local storage, and other cache files become completely isolated and cannot leak between profiles. Instead of trying to prevent websites from reading the computer's fingerprint, Multilogin allows reading it but replaces original fingerprints with different ones.
- **Che Browser** is a desktop application that substitutes the browser and hardware fingerprints of user PCs. According to a developer's statement, the tool is needed to create and successfully manage multiple accounts on

various websites such as Facebook, Bing, Yahoo, Google, or online gambling services. It is used by partners of CPA networks, cappers, SMM managers, and internet trolls who create and use accounts on an industrial scale from the same PC. The tool allows selecting the desired user profile and connection parameters. Then cybercriminals can use Google Chrome with the already spoofed browser and hardware fingerprints to defraud websites they visit. Each browser profile is unique because it is taken from a real PC, and each browser profile is given to only one person. The browser has been actively advertised across multiple dark web forums since at least April 2019 by a threat actor with the usernames "CheBrowser", "Che_Browser", and "gcc".

- **FraudFox** is a tool aimed at spoofing browser fingerprints based on a modified Mozilla Firefox web browser. According to the developers, FraudFox is a Windows 7 Enterprise-based virtual machine, which is compatible with VMWare Workstation, VMWare Fusion, and VirtualBox. Users can move and copy it from one location to another, storing it online or on a USB. The browser provides regular updates and 48-hour technical support service. FraudFox does not allow users to save a specific set of fingerprint parameters to match each online account and ensure consistency with every login and is not intended to work with multiple accounts.

Fraud with stolen user web browser fingerprints, session cookies, and other system data from compromised host machines is quite popular among cybercriminals. There are a number of dark web shops that offer these types of data for sale that can be used by cybercriminals to bypass anti-fraud solutions of various organizations.

One of the primary platforms on the dark web for the sales of compromised user system data has been Genesis Store, created in 2018 by the threat actor "GenesisStore". Genesis Store sells packages of compromised account credentials and associated user data designed to allow threat actors to not only obtain the needed credentials but also to bypass anti-fraud solutions by effectively masquerading as the legitimate user since they are accessing the platform from what is, essentially, a copy of the victim's machine. Victim data is sold in a single package referred to as a "bot", which includes account credentials, IP address, browser fingerprint (system information), and cookies. After purchasing a bot, the victim data can be imported into a browser plugin called Genesis Security, allowing the attacker to perform an online identity takeover of the victim to perform attacks such as account takeover or card-not-present fraud. The price for each bot varies depending on the number of account credentials, types of accounts, and geographical location of the victim.

Notable Threat Actors

- DeaNox: A member of Cracked forum, observed advertising techniques via ebook to engage in fraud against Amazon. According to the actor, this method bypasses Alexa Voice Service (AVS) and allows access to alleged algorithms.
- TheWizard: A member of Versus Market, advertising a how-to on how to card Amazon and eBay using a mobile device or cell phone.
- Andrij2142: A member of BHF, previously advertising a Russian refunding service for use on non-Russian online stores, such as Amazon, Victoria's Secret, and Bloomingdale's.
- Pod: A member of Demon Forums, advertises an international refunding service, including clothing, food, and electronics with $10,000-or-more limits on purchases. Pod also manages a Telegram channel to communicate with prospective customers.
- Deceive: A member of Cracked Forum and administrator of The Refund Bar, a relatively new refunding service active since October 2019. According to their Telegram channel, The Refund Bar is the "most vouched service on Cracked Forums".

5. SIM Swapping

SIM swapping fraud, also known as SIM card hijacking, is a technique used by threat actors to gain access to a victim's phone number with the end goal of using two-factor authentication (2FA) to obtain access to the victim's online accounts, including banking, social media, cryptocurrency, and other personal or corporate accounts. SIM swapping is one of the easiest ways to bypass the 2FA mechanism. If a subscriber loses their phone, the carrier can replace the old SIM with all of their contact information and their original phone number. The primary steps to perform a successful SIM swapping attack, which usually involves an insider, are as follows:

- Cybercriminals identify the phone number of the victim and their personally identifiable information (PII) (using social engineering, phishing, or insider information)
- Cybercriminals call the mobile carrier to report the loss of the phone to block the SIM card.
- Mobile carriers transfer the phone number to the controlled SIM card. In this case, the attackers can use the SIM on a separate mobile device and still maintain access to the victim's contact list, can make and receive phone calls, and send short message service (SMS) messages. As a result, cybercriminals gain access to most 2FA methods used by financial organizations, by intercepting SMS verification codes.

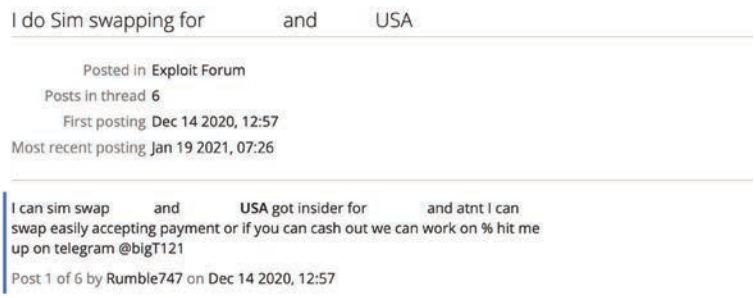


Figure 9: SIM swapping advertisements on the dark web (Source: Recorded Future)

The following cybercriminals are some of the most active in SIM swapping fraud:

- "novaking", a member of the forum Club2CRD, Omerta, Carding Mafia, and Envoy, offers SIM swapping services against US and Italian mobile carriers to bypass SMS 2FA and to get access to the victims' bank and cryptocurrency accounts with subsequent cashing out of the stolen funds. The threat actor stated that their profit share for this service is 70%.
- "Panther", a member of the low-tier Russian-language Dublikat forum, offers SMS interception, recovery, and blocking services. According to the threat actor, they can target various organizations, but the service is primarily used to target banks and payment systems. The price is determined individually, as per the customer's request.

We conducted an analysis of dark web sources for threat actors advertising SIM-swapping guides and how-to methods. Advertisements for these guides and methods occurred on both dark web marketplaces and forums, with the majority of these being advertised on dark web marketplaces. The Canadian HeadQuarters Marketplace (Canadian HQ) contains the most SIM swapping-related listings, with at least 12 threat actors advertising such services. Below are the most active threat actors Recorded Future found to be offering unique SIM swapping-related methods and how-to guides, that have received positive feedback, and are experienced marketplace vendors:

- "cashoutallday", a member of Canadian HQ, first advertised a how-to method for SIM swapping any carrier in September 2020, and has continued to update the advertisement. Our data indicates that cashoutallday has offered SIM swapping-related methods since at least July 2020. The listing is currently priced at $99 CAD.
- "exotickush4", a member of Canadian HQ, is advertising a how-to method for SIM swapping any phone number, specifically for cashout services. The listing is currently priced at $25 CAD.
- "RussianMob13", a member of the Canadian HQ, is advertising a how-to method for SIM swapping that permits SMS takeover. The method is described as being tested (and confirmed to be working) in November 2020 and is priced at $80 CAD.

Another type of fraud against mobile carriers is SMS interception attack, which is a different attack vector based on targeting the global telephony protocol Signaling System 7. Some threat actors perform or actively look for SMS interception services; however, SMS interception requires technical proficiency from a hacker and is usually performed by threat actors who operate botnets, web injects, or other malware to compromise high-value targets.

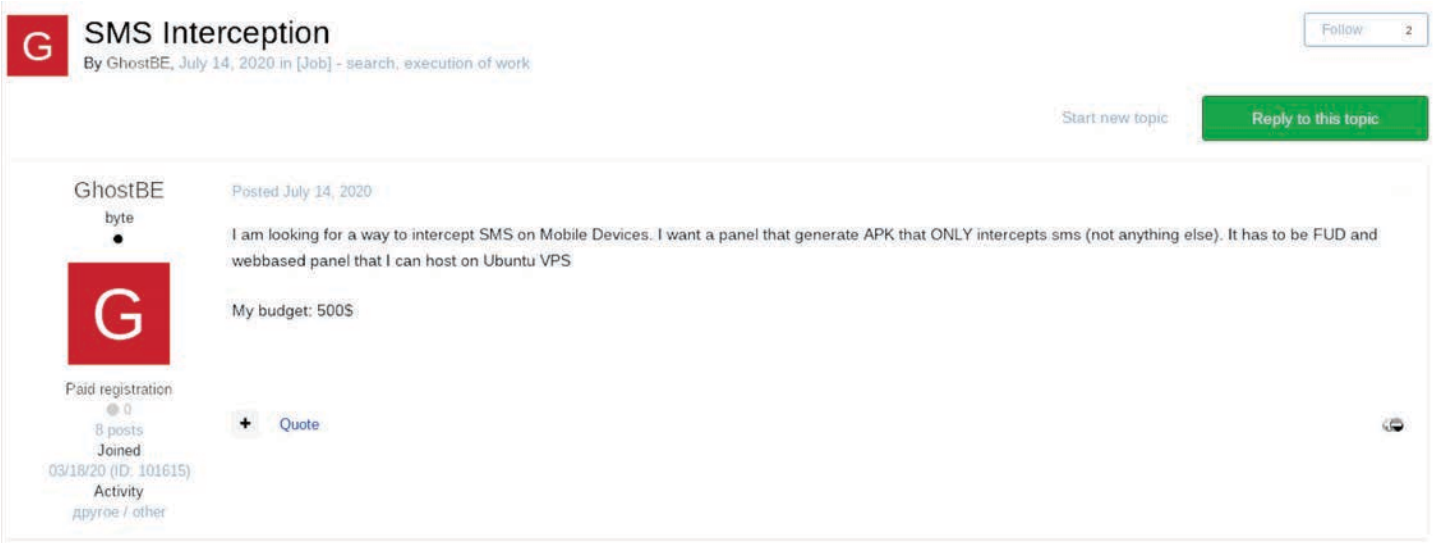


Figure 10: Requests of SIM interception service on the dark web (Source: Exploit Forum)

6. Money Laundering Services

Money laundering services within the dark web facilitate a combination of activities through which threat actors can conceal the origins of their money ,transfer cryptocurrency into virtual currency ,have funds sent to a bank account or payment cards ,or exchange to physical cash .Many of these services are linked to the use of cryptocurrency .Of these ,Bitcoin is likely to continue to be the most widely used cryptocurrency in the monetization of laundering operations.

The ability to turn a cyberattack into usable currency is the most important aspect of cybercrime .To facilitate this ,money laundering services are a mainstay of any prominent dark web forum involved in hacking or fraud ,both of which would be familiar to the vast majority of ransomware operators and affiliates .Advertisements for money laundering services ,tools ,or procedures are often located within sections of an underground source specifically devoted to ads or discussions surrounding fraud topics as a whole ,including other popular offerings related to counterfeit documents or crypto mining.

Essential aspects of dark web money laundering include the ability to mix and exchange cryptocurrency ,transfers to and from virtual currency bank accounts ,and the delivery of physical fiat currency .It is highly likely that at least some members of more prominent cyber threat activity within open-source reporting over the past year ,such as ransomware cartels ,have accounts on underground forums and may also be using some of the vetted laundering services advertised there .At a minimum, cyber threat entities who receive their ransom payments in Bitcoin require some level of Bitcoin mixing to keep their personal BTC addresses unknown .Advanced threat actors would likely do more than just this ,and ,after mixing their BTC ,would have a variety of options to choose from provided by these laundering services.

Alternative forms of laundering money continue to remain readily available for criminal actors across the dark web regardless of their proficiency level in navigating underground sources. For example ,virtual currencies such as Qiwi have historically remained of interest to cybercriminals operating within Russia, particularly on underground marketplaces that specialize in the sale of narcotics .Converting stolen funds into alternative virtual currencies continues to remain a viable alternative for laundering despite efforts in countries such as Russia to outright ban cash deposits on anonymous electronic wallets.

For example ,money laundering services operated by the threat actor-" B "-offer features such as the transfer of Bitcoin into virtual currencies popular in the Commonwealth of Independent States) CIS (such as PerfectMoney and WebMoney .For Russian citizens ,money can be directly deposited into" payment cards")likely referring to prepaid cards- .(B -further claims they can deposit or send physical cash to locations throughout the world. -B -continues to operate as an active member of Verified Forum.

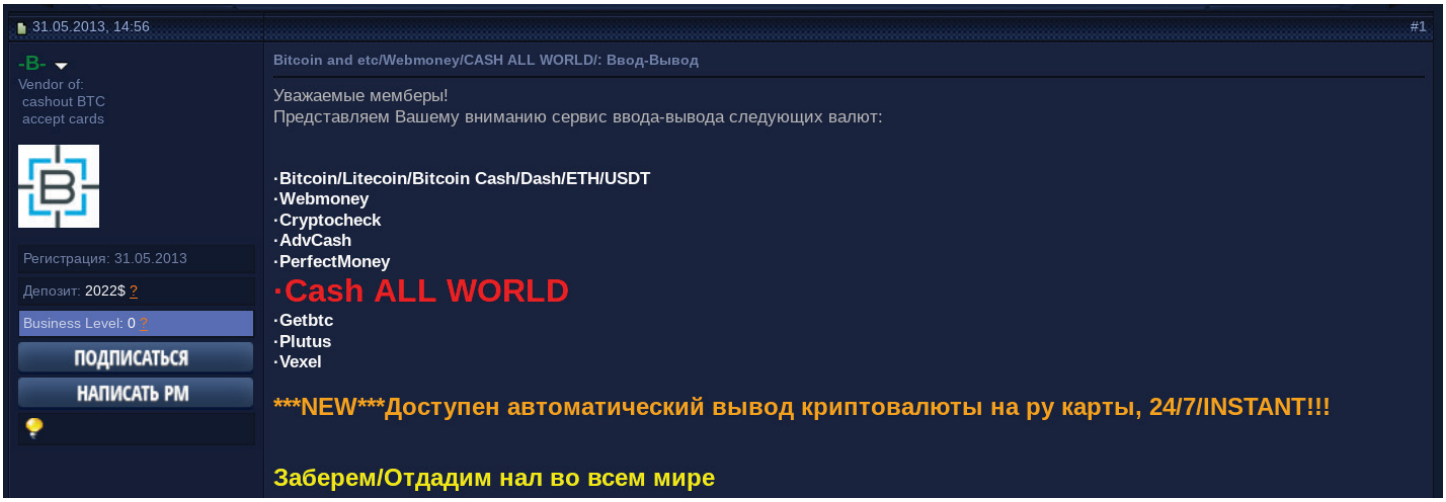


Figure 11: Money laundering services operated by the threat actor -B- (Source: Verified Forum)

[Translation: Bitcoin and etc/Webmoney/CASH ALL WORLD: Buy or Sell
Dear members!
We would like to bring to your attention the service of buying and selling the following currencies:
- Bitcoin/Litecoin/Bitcoin Cash/Dash/ETH/USDT
- Webmoney
- Cryptocheck
- PerfectMoney
- Cash ALL WORLD
- Getbtc
- Plutus
- Vexel
****NEW*** Available - automated transfer of cryptocurrencies into RU cards, 24/7/INSTANT!!!*
We will pick up/Drop off cash all over the world]

Figure 12: Ad banner on the forum Verified with Oneteam operations in New York, USA (Source: Verified Forum)

[Translation: ANY TYPE OF OPERATION WITH Bitcoin AND CASH USA/NEW YORK]

- "Oneteam", also known as Seva, is a prolific money launderer on the Verified Forum and other forums. They have operated since 2009 and have over 1,000 positive reviews. One of the features they advertise is the ability to conduct all sorts of money laundering operations in New York, USA.

While other cryptocurrencies such as Monero offer additional security features and more stringent security measures that enable its users to more easily circumvent law enforcement officials, threat actors rely heavily on the capability of victims potentially with little background on the subject of cryptocurrencies to be able to transfer funds. Separate cryptocurrency mixing services will almost certainly continue to be used by criminal entities to assist in obfuscating their trail, which is still only considered to be pseudo-anonymous.

Cryptocurrency users are advised to protect their earnings by using cold storage such as a USB drive, physical Bitcoin, or a paper or hardware wallet. While this does not guarantee 100% security, disciplined storage practices definitively decrease any potential risk of losing one's cryptocurrency.

7. The Role of Botnets in Dissemination of Malware to Support Fraud

In a report published by the International Data Corporation (IDC), researchers predict that "by 2025 there will be 55.7 billion connected devices worldwide, 75% of which will be connected to an IoT platform." Cybercriminals, as well as nation-state actors, have continued to demonstrate the flexibility and dynamic aspect of a botnet operation by leveraging routers and other equipment to perform unconventional tasks such as rendering devices inoperable or using them to disseminate malware strains specifically designed to support financially motivated fraud activity. Criminals used Emotet to download third-party banking malware such as Trickbot, IcedID, and Gootkit, which support the continued spread of their botnet via a number of modules. Operators of info-stealer trojans, business email compromise (BEC) groups, and ransomware gangs are some of the customers of these botnets. Additionally, tutorials for the development and support of botnets specifically designed to execute malware with functions specifically repurposed to conduct fraudulent activity like keylogging remained plentiful within the criminal underground throughout 2020.

Outside of basic tutorials or methods for the development of a botnet with limited features, more prolific strains of malware commonly associated with malicious botnet activity remained the most popular strains impacting all industry verticals by the end of the year.

Emotet is an advanced trojan primarily spread via phishing email attachments or links that, once clicked, launch the payload. The malware then attempts to proliferate within a network by brute-forcing user credentials and writing to shared drives. Throughout Q1 2020, Emotet was the subject of media headlines after it was observed developing new methods of dissemination via Wi-Fi networks, targeting major government entities around the world, and causing a denial of service across entire networks. Microsoft reported on an Emotet infection that worked as a denial-of-services attack when an employee was targeted with a phishing email. The compromised machine was then used to distribute Emotet across the entire network, causing infected PCs to overheat, stop working, and reboot because of system errors.

Emotet is difficult to combat because of its "worm-like" features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Despite recent law enforcement efforts to combat the Emotet botnet, Emotet and Trickbot were suspected to have been operated for a time by different threat actor groups. However, Trickbot's operators have used Emotet as a dropper/loader for their own malware variant. The hosts are being distributed to brokers and used as initial access vectors for corporate network compromise and potential distribution of ransomware variants, including the Ryuk ransomware variant. Two malware strains that have continued to be observed working in tandem via the operators of Emotet in 2020 include Trickbot and Qakbot, with the latter suspected of having replaced Trickbot for a time given the shift in payloads being deployed onto victim systems for the purposes of stealing banking information to the appeal of criminals conducting fraud.

Considered to be the successor to the infamous Dyre banking trojan, the TrickBot banking trojan leverages multiple attack vectors, including redirection attacks and web injects, to attempt to steal information from financial institutions and initiate fraudulent wire transfers. The primary methods used by threat actors to distribute banking web injects continue to be phishing and exploit kits, and the most popular injects often offer customized options catered to cybercriminals attempting to target a specific company. Additionally, the administrative panels of these web injects sometimes promote features such as the inclusion of plugins to connect with botnet infrastructure.

Often historically deployed by the botnet affiliated with Emotet activity, Trickbot is a sophisticated malware variant, offering a number of evasion techniques, different methods of spreading, and a large number of capabilities to generate revenue. One of the primary functions of Trickbot (similar to other banking trojans) is to lift credentials and other sensitive login-related data appealing to financially motivated actors using methods such as web injects and a keylogging function. As database breaches and login credentials with passwords have become widely marketed by threat actors, keylogging as a standalone attack vector to harvest credentials through the deployment of botnets has become less relevant. Information of interest to the actors includes usernames, passwords, personal identification numbers, and possibly answers to security questions. The role of the malware acting as a loader to download additional payloads of malware cannot be overstated.

Actors continue to generate profit from the development or sale of malware strains that incorporate keylogger functionality to steal information of interest, particularly on low-tier forums that likely attract a broader audience. Trickbot has previously been co-opted to distribute ransomware and other banking trojans, using the botnet formed by a large number of infections. Despite the United States Cyber Command and the security industry's attempted disruptions of the TrickBot botnet, the controllers associated with the malware have continued to remain resilient.

First observed in mid-2014, TA542 is an alleged Russian-speaking threat entity most commonly known for its development and continued support of the Emotet botnet to target victims worldwide. The group characteristically conducts consistent campaigns over the course of several months at a time before ceasing operations to redevelop modules for Emotet use in future campaigns. TA542 has used Emotet to download third-party banking malware such as Trickbot and Qakbot to launch widespread email campaigns on an international scale, and load TA542's modules for spamming, credential stealing, email harvesting, and spreading on local networks.

TA542 has become one of the most prolific threat actors in the overall cyber threat landscape, leveraging Emotet to orchestrate high-volume, international email campaigns that distribute hundreds of thousands or even millions of messages per day.

8. Travel and Loyalty (Hospitality) Fraud

Hospitality fraud is the use of travel-related services and rewards to defraud legitimate users of funds or rewards points. This type of fraud involves threat actors scamming users into providing personally identifiable information (PII) and financial information through fraudulent travel and hospitality services, including car rentals, hotel and flight bookings, excursions, and other vacation-related deals. Once PII and financial data have been harvested, threat actors use this data to conduct identity theft, use it in social engineering attacks, or monetize it by listing it for purchase on open sources (including social media) and the dark web. Likewise, hospitality fraud includes threat actors reselling compromised rewards points such as frequent flyer miles, or using them to book highly discounted travel for both witting and unwitting customers.

From a cyber perspective, threat actors use an array of different methods to facilitate hospitality fraud: conducting phishing and spamming campaigns to acquire PII, purchasing flight tickets with stolen payment cards, creating replicas of travel agency websites, social media advertisement spoofing campaigns, and use of automated and customized malicious tools (brute-forcing and credential stuffing) to access user accounts. Threat actors list hospitality fraud services, customized tools, and compromised account data on both low- to high-tier forums, as well as on dark web markets and independently run shops, including SlilPP Market and Exploit Forum. As a rule, threat actors leave reviews for the fake travel agencies on the forums where they share their experience and photos from travel destinations as proof. That increases the reputation of the fake travel agencies and encourages other cybercriminals to use these services.

Figure 13: Advertisement of a fake travel agency on the forum WWH Club by PoshTravel (Source: WWH Club forum)
[Translation: POSH TRAVEL
OUR PRICES AND SERVICES
HOTELS 20-40% OF ACTUAL PRICE
AIR 40-60% OF ACTUAL PRICE
DEPOSITS 20-40% OF ACTUAL PRICE
TOURS 50% OF ACTUAL PRICE
HELICOPTERS 40% OF ACTUAL PRICE
YACHT RENTAL 40% OF ACTUAL PRICE
@POSHTRAVELINFO]

Notable Threat Actors

- "Serggik00" is a member of multiple Russian-language forums who advertises a dark web "travel agency" that provides cybercriminals with travel services such as travel and hospitality services, including hotel bookings, car rentals, and excursions.
- "PoshTravel" is a member of multiple Russian-language forums who is involved in travel and hospitality fraud, as well as in the sales of the compromised PII and money laundering.
- "Roman77714" is a threat actor who regularly sells multiple airline accounts with balances and bonus miles as well as gift cards. The threat actor is one of the primary sellers on multiple Russian-language forums such as DarkMarket, Dark Money, and WWH Club.

9. Sales of Personally Identifiable Information (PII) and Protected Health Information (PHI)

While personally identifiable information and protected health information are in some cases sold by actors who also sell compromised banking information and credit card information and often on the same forums and marketplaces, PII and PHI sales can pose a more dynamic threat to victims. Compromised PII can allow threat actors to compromise financial accounts, take out loans and lines of credit in the victim's name, compromise accounts for other online services, and in the case of PHI, fraudulently obtain prescriptions and defraud insurance companies. And while payment cards are relatively easy to replace and victims of credit card fraud are typically not held liable by their providers, the theft of PII and PHI is much more pernicious and invasive. It is much harder — in some cases impossible — to change the information contained in PII and PHI. Likewise, the fraud committed using stolen PII and PHI can take much longer to mitigate, sometimes leaving the victim with serious or permanent consequences.

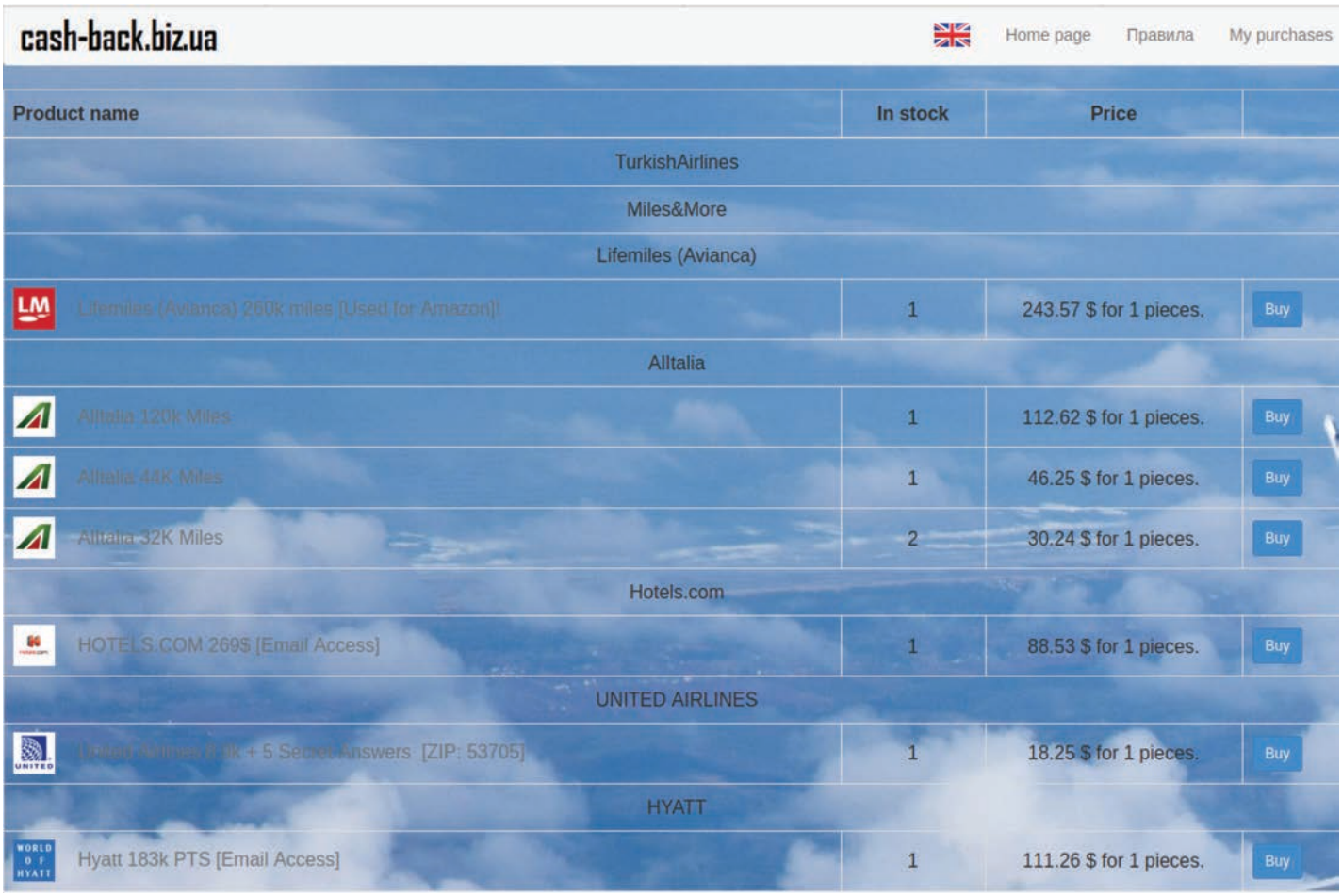


Figure 14: cash-back[.]biz.ua shop selling multiple compromised airline and hotel accounts (Source: cash-back[.]biz.ua)

Sale of PII

The sale of personally identifiable information (PII) involves the trafficking of data that could be used to identify a person, such as their full name, date of birth, Social Security numbers, email addresses, passports, and other identifiers.

While most of the sales of PII are automated and customers can access webshops such as SSN.BAR to purchase as much PII as they need, there are multiple actors who advertise direct sales of stolen PII data sets on forums. For example, on June 4, 2020, "stooper", a member of multiple underground communities, advertised on Exploit forum an auction for an allegedly newly compromised database that consisted of 4 million PII records. The database fields included IP address, first name, last name, email, address, city, state, ZIP code, Social Security number, driver's license, date of birth, phone number, account number, employer, and monthly income. On that same day, "sportsmen177", a member of multiple underground communities, advertised the same PII database for sale. The actor claimed that the database contained 800,000 records harvested in March 2020. Sportsmen177 further alleged the full database contained over 250 million records collected between 2019 and 2020. A subset of 4 million records was composed of full PII, including the Social Security number and date of birth fields.

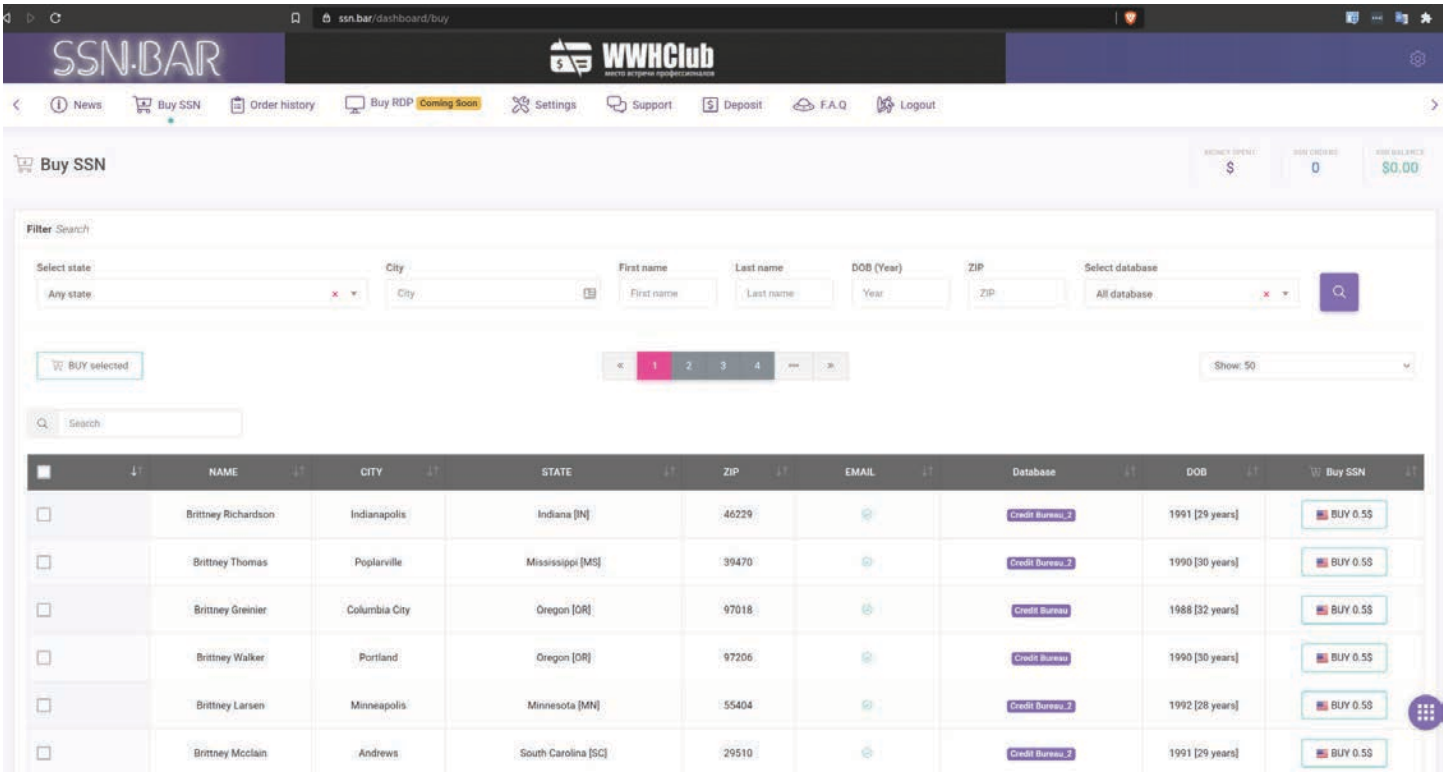


Figure 15: SSN.BAR PII shop (Source: SSN.BAR)

Sale of PHI

The sale of protected health information (PHI) involves the trafficking of personally identifiable information like medical treatment history, test results, and medical insurance information.

- Threat actors are using mid-to-high-tier forums such as Raid Forums, Exploit Forum, and XSS Forum to advertise stolen PII and PHI-related data.

SQL injection (MITRE T1190) and Valid Accounts (MITRE T1078) are the primary attack vectors used by threat actors to conduct attacks to steal PHI.

In one of the most recent events, in December 2020, "Avanter", a member of the mid-tier Raid Forums, was identified sharing a US Department of Labor Occupational Safety and Health Administration (osha[.]gov) database that consisted of the full names and physical addresses, the place of hospitalization, and a description of incidents and injuries for American soldiers.

Avanter shared the database with forum members through a file sharing service and stated that the database was stolen from the National Health Organization and contained 50,000 records.

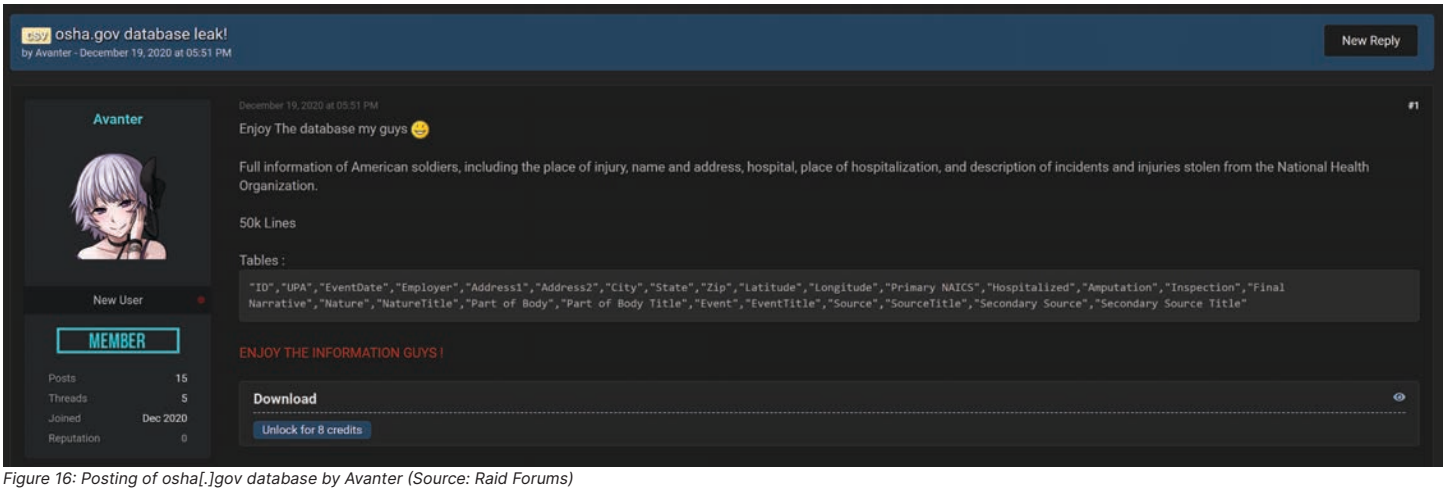


Figure 16: Posting of osha[.]gov database by Avanter (Source: Raid Forums)

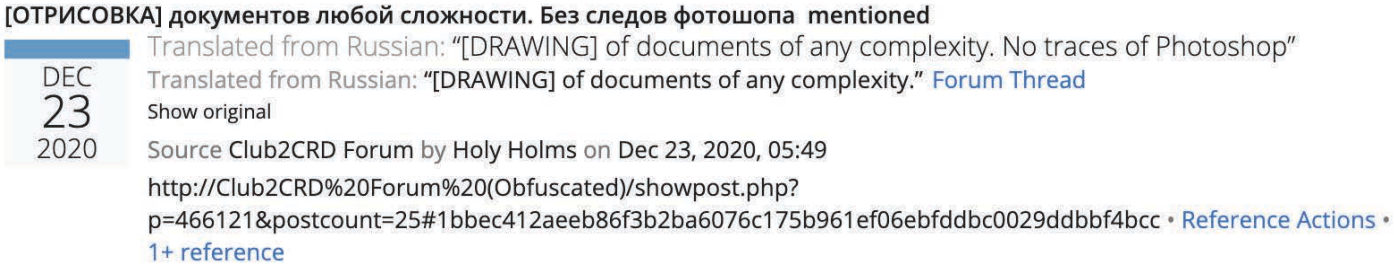


Figure 17: Holy Holms offering to produce forged documents on the forum Club2CRD (Source: Recorded Future)

Sale of Forged Identification Documents

ID forgery is an integral part of the carding process (that is, payment card fraud), around which a cohort of specialized cybercriminals on various underground forums and marketplaces has emerged.

Cybercriminals use counterfeit IDs mostly for carding, as merchants sometimes require buyers to present an ID when conducting a purchase. Some banks and similar financial institutions also require electronic copies of IDs for identity verification. This is particularly true of e-banks, which rely heavily on digital documents and images as part of their KYC ("know your customer") practices. The Russian-language slang for the production of counterfeit documents is "otrisovka" (отрисовка), whose literal translation is "drawing" or "painting". Figure 17 below shows an example of a search result for "otrisovka" on the Recorded Future Platform, in which the threat actor "Holy Holms" is offering to produce counterfeit documents on the forum Club2CRD.

Fake IDs will also continue to present an issue for law enforcement agencies globally, be it at a local level due to the use of fake IDs to circumvent drinking age laws, or globally, as we have seen with the use of fake documents by terrorists in both Europe (Paris and Brussels attacks) and the US (six of the 19 9/11 hijackers reportedly used fake passports).

The Use of Voter Rolls as a Source of PII

There is likely an ongoing interest in election infrastructure, namely voter databases, from criminal threat actors looking to use PII and other data obtained from these systems to commit financially motivated fraud and other crimes.

Over the past four years and as recently as January 2021, we have identified the sale and distribution of alleged voter registration databases from over 30 different states on criminal markets and forums. At this time, many of these advertisements are for records from previous years, likely exfiltrated from publicly available or requested data, and are regularly recycled as "new" or "up to date" and often advertised by threat actors — falsely — as leaked data.

These voter databases are featured regularly on criminal forums, namely for use in fraud efforts, as the PII within these databases is highly valuable for social engineering and spearphishing attacks. In terms of election interference, this publicly available information can be (and has been) used to specifically target individuals of specific political affiliation, age, or locality.

These instances likely originate from publicly available information either through the official public records from a government entity (available online or by request through the Freedom of Information Act) or from scraped data from an affiliated data broker website.

10. Tax Return Fraud

Tax return fraud ,also known as stolen identity refund fraud)SIRF ,(is a specific case of identity theft where a criminal files a tax return with victim information to federal or state tax agencies with the goal of stealing the victim's tax refund .The success of these schemes relies on criminals 'filing of the tax return before the legitimate filers do .In the underground economy ,tax refund fraud frequently requires collaboration between multiple threat actors with different specialties ,such as collecting credit reports and tax forms in bulk ,gaining access to online tax preparation software to submit the tax return ,and recruiting money mules to receive and send the stolen tax refunds .Other attackers may target tax preparation firms directly ,as gaining access to these networks will provide both the victim PII and the tax software needed for SIRF .While most forms of tax fraud are seasonal ,reaching a peak in the months before filing and extension deadlines ,some threat actors have been known to file amended tax returns of compromised accounts even years after the victims had already filed including fictitious losses and requesting additional refunds without the victim ever knowing.

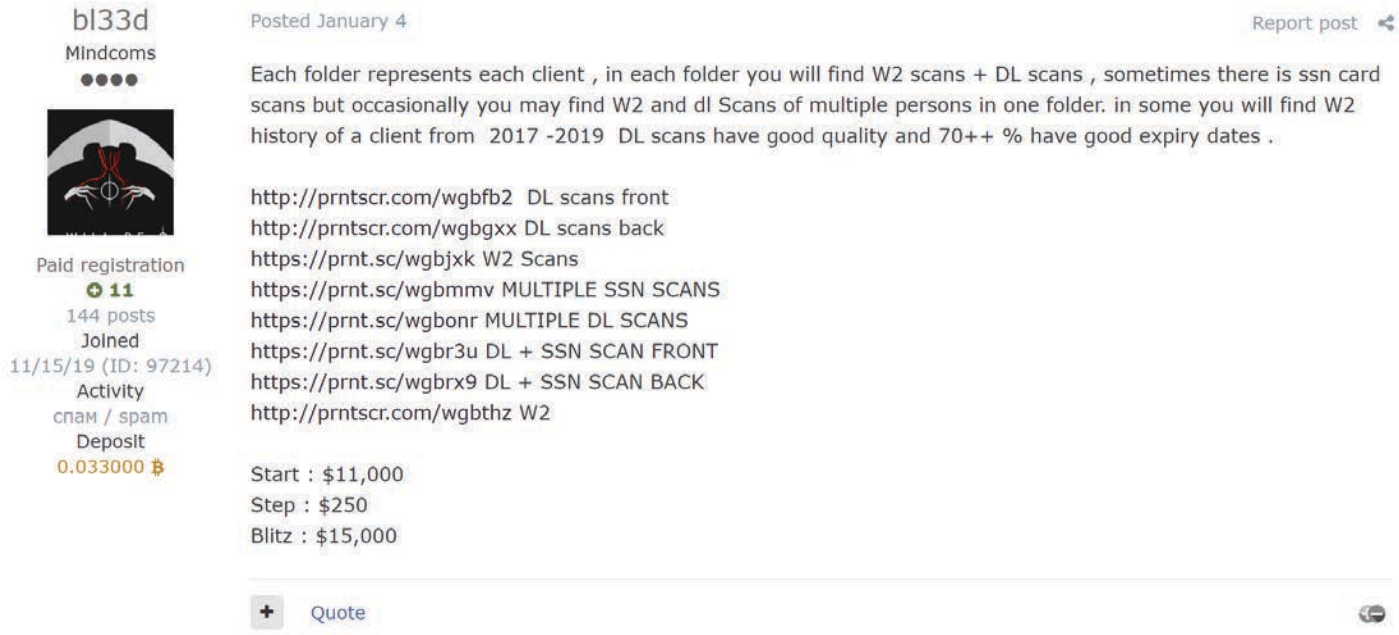


Figure 18: bl33d's advertisement (Source: Exploit Forum)

One example of the sale of such data happened on January 6, 2021, when "bl33d", a member of the top-tier forum Exploit, was seen auctioning off US taxpayer personally identifiable information for 1,500 individuals, which included W-2 forms, driver's licenses, and SSN scans from 2017 to 2019. bl33d provided screenshots that indicate the data was possibly obtained from a CPA in California, making it likely to be used to claim fraudulent tax returns in that state.

In addition to the sale of the PII and tax forms needed to conduct SIRF ,underground communities have multiple members who purchase access to the individual PCs and networks of CPA firms running tax software ,as well as provide money laundering services for the fraudulent tax returns .One such threat actor is" iqservicc ,"who ,each year ,buys RDP access to PCs running recent ,popular tax software such as ProSeries ,Turbotax ,Drake, Ultratax ,Lacarte ,ATX ,Taxwise ,TAXSLAYER PRO ,CrossLink, and ProTaxPro .This allows an attacker to fraudulently file taxes on legitimately purchased and registered tax software through IP addresses that would not appear suspicious) as opposed to VPNs ,proxies ,or geographically distant IPs .(Such a combination greatly increases the chance of processing a successful tax refund through the IRS.

Lastly ,but debatably of most importance ,is the cashout method ,used by threat actors such as" Асад) "Asad (who specialize in laundering funds stolen from tax refunds through ACH or wire transfers to accounts under their control .This type of service would be used by actors such as iqservicc ,who submits tax refunds through compromised computers running tax software with victim PII obtained from actors such as bl33d. Асад likely uses a series of money mules ,transferring funds from one to another before finally delivering the funds to an account controlled by their client ,the threat actor who initiated the fraudulent refund.

11. Bank Fraud

Fraud in the cybercriminal sphere is perhaps most closely associated with bank fraud ,which refers to the use of primarily 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 the countries and on the jurisdictions ,the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft .For this reason ,bank fraud is largely considered a white-collar crime.

While there are historically many types of bank fraud ,such as accounting fraud ,bill discounting fraud ,check kiting ,forgery, fraudulent loans ,payment card fraud ,phishing ,or wire transfer fraud ,the techniques primarily used by cybercriminals today are credit card fraud ,online banking fraud ,and wire transfer fraud.

Credit Card Fraud

Credit card fraud is an inclusive term for fraud committed using a payment card ,such as a credit card ,prepaid card ,or debit card .The purpose may be to obtain goods or services or to transfer funds to another account that is controlled by a criminal.

Credit card fraud can be authorized ,where the genuine customer unwittingly makes a payment to another account which is controlled by a criminal ,or unauthorized ,where the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party. Unauthorized transactions happen in two different ways" :card present "and" card not present."

These types of fraud are facilitated by a multitude of cybercriminals and online webshops that sell credit card data and personally identifiable information) PII .(We will cover the most prolific threat actors and criminal persistent threat) CPT(groups in the report focused on bank fraud.

Online Banking Fraud

Online banking fraud is a type of fraud that involves access to an online banking account .Threat actors use multiple ways to access online banking services ,such as using stolen identity)identity theft (to open new accounts) application fraud (or obtaining valid credentials to existing accounts) account takeover (with the help of phishing ,credential reuse ,or malware.

Application Fraud

Application fraud takes place when a person uses stolen or fake documents to open an account in another person's name. Criminals can steal information directly from victims using malware, buy necessary information from shops that sell PII, or obtain fake documents such as utility bills and bank statements from threat actors who specialize in creating the fakes. All of this can be used to build up a personal profile that can seem legitimate enough to conduct banking transactions, such as opening accounts or even obtaining credit or loans. These accounts can also serve as a waypoint to accept stolen funds from other compromised accounts. In this case, threat actors frequently distinguish between intrabank and interbank transfers when discussing the movement of funds between compromised and created accounts. In some cases, threat actors will "age" the accounts by conducting smaller, legitimate transactions such as depositing funds or moving funds between different accounts they control, all designed to make the accounts seem more legitimate and less likely to raise suspicion when involved in actual criminal transactions. Sometimes the threat actors will even take out small lines of credit and pay them off faithfully in order to then take out a larger loan than they intend to default on.

Figure 19: Instore carding section (Source: Verified Forum)

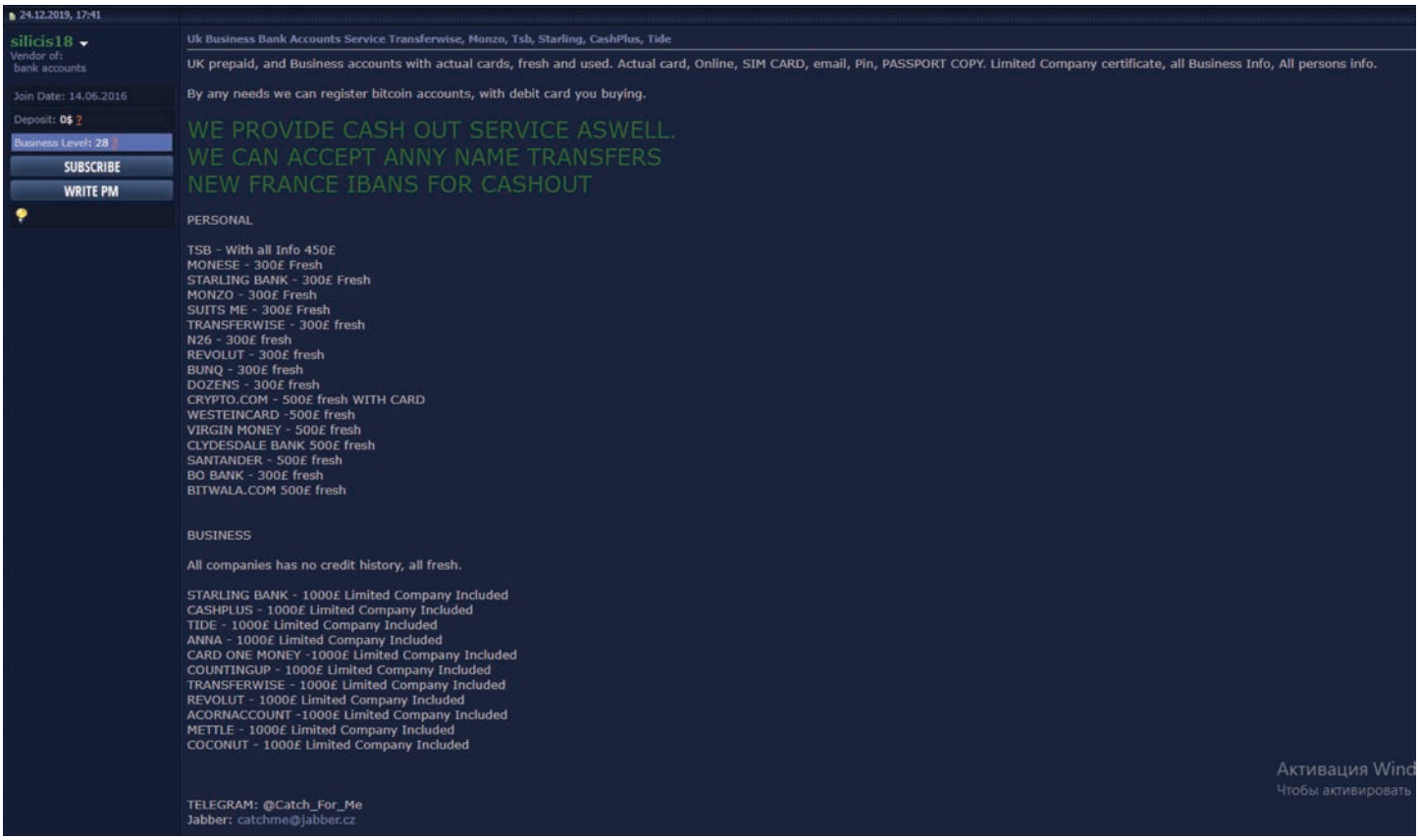


Figure 20: Silicis18 advertisement (Source: Verified Forum)

Another angle cybercriminals use to obtain access to online banking is by hiring money mules, who typically receive a commission for the service or provide assistance because they believe they have a trusting or romantic relationship with the individual who is asking for help moving money. Criminals then use such accounts to receive cash stolen from compromised accounts, usually obtained by some form of account takeover.

One example that can be found on Verified Forum is an advertisement posted by "silicis18", a member of multiple underground communities, where they offer a wide variety of ready-to-go bank accounts for money laundering purposes, as seen in Figure 20 below.

Account takeover

In account takeovers, fraudsters will attempt to assume control of a customer's account (credit cards, online banking). To do this, criminals use parts of the victim's identity such as a compromised email address to gain access to financial accounts. Monitoring the email allows the threat actor to intercept communication about the account to keep the victim blind to any notifications from the financial institution about fraudulent activity. Thus the victims are often the first to detect account takeover activity but only after they discover questionable withdrawals or charges on monthly statements they did not authorize.

Among some of the most common methods by which a threat actor will commit an account takeover are brute-force attacks, phishing, and malware. Other methods include "dumpster diving" to find personal information in discarded mail, and the outright purchase of lists of "fullz", a slang term for full packages of identifying information sold on the criminal underground.

One example of an automated PII shop selling fullz is Card2Life ,a platform where their customers can purchase compromised login credentials to different banks in the US based on their value.

76916	BEYOND CHECKING=56910.20$/ BEYOND SAVINGS=20006.69$	410.00$
58808	CONVENIENCE CHECKING=58808.31$	370.00$
406962	Checking=359231/Checking=5100/Checking=11410/Checking=31221	500.00$
15135	Checking=1979/Savings=12156	180.00$
14952	SIMPLE SAVINGS=14952.24$	180.00$
45458	BEYOND CHECKING=45395.18$/ BEYOND CHECKING=63.07$	340.00$
208652	CONVENIENCE CHECKING=16066$/ 60 PLUS CHECKING=165432.25$/STANDARD SAVINGS STMT=3713.74$/ SIMPLE SAVINGS=23441.97$	500.00$

Figure 21: Card2Life PII selection panel (Source: Card2Life)

Another process cybercriminals use to boost their efficiency is called "enroll". Threat actors add online access to existing credit cards, thus expanding their control over the compromised account. Online access allows for changing of contact information and billing addresses associated with the credit card, making it easy to bypass the address verification system (AVS) that validates billing information during the payment process online.

Wire Transfers Fraud

Wire transfer networks such as the international SWIFT interbank fund transfer system are tempting targets because once a transfer is made, it is difficult or impossible to reverse. While not the only form of wire fraud, since these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace, making them an especially tempting target for threat actors focusing on wire transfer fraud.

This type of fraud is the most sophisticated because the threat actor needs access to the banking operator or cashier's computer, which will allow them to perform the unauthorized transactions. One of the biggest attempts to steal money using SWIFT fund transfers was the Bangladesh Bank robbery, a theft that took place in February 2016. 35 fraudulent instructions were issued by hackers via the SWIFT network to illegally transfer close to $1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh. Five of the 35 fraudulent instructions were successful, transferring $101 million, with $20 million traced to Sri Lanka and $81 million to the Philippines. Most of the money transferred to the Philippines went to four personal accounts, held by single individuals, and not to companies or corporations.

Outlook and Conclusions

Fraud services will likely grow and mature in 2021 and beyond, as more people around the world shift to remote work and online shopping. Fraud is a lucrative criminal enterprise that draws other cybercriminals and has the potential to further evolve with the use of automation. As has been consistent through 2020, we expect that fraud methods and services will continue and expand in scope and size threatening a diverse set of industry verticals.

We recommend that organizations conduct the following general measures to defend against fraud methods and services detailed in this report:

- Use threat intelligence gathered from dark web sources to inform your security team's awareness of active criminal threats.
- Conduct security awareness training for employees to help them recognize and report suspicious activities.
- Protect accounts by using multi-factor authentication.
- In place of SMS 2FA, use authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator for additional security.
- Keep systems and software up to date.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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