CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0401

The Business of Fraud: Fraud Tutorials and Courses

Recorded Future®

Recorded Future analyzed current data from the Recorded Future® Platform, dark web, and OSINT sources to review fraud tutorials and courses that facilitate threat actor campaigns. This report expands upon findings addressed in the first report of the Insikt Group's fraud series, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized". 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

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 by recruiting and training the next generation of fraudsters. Threat actors sell how-to guides and tutorials across the criminal underground on a range of cybercrime-related topics, including malware creation, mule recruitment, cashout methods, ATM bypasses, and other operations that facilitate criminal activities. These tutorials and courses cater to a wide range of cybercriminals, from cybercrime novices to more seasoned, niche-focused experts that are seeking additional guidance and knowledge, and communities and materials exist for English, Russian, and Chinese speakers.

Key Judgments

- Fraud tutorials and courses give direct instructions on how to commit fraud. These instructions are step-by-step guides for how to be a cybercriminal.
- The Carding Camp training on the forum WWH Club is well known in underground communities for enabling novice cybercriminals to undertake payment card fraud.
- Fraud Bible and the forum COOCKIE PRO provide cybercriminals step-by-step videos and printed methods on defrauding specific companies and state governments.
- GOLDIE ENROLL 5.0 course is specifically tailored to enable cybercriminals to commit online banking fraud.
- Chinese-speaking cybercriminals run their underground communities providing training to target payment processing systems and financial organizations.

Threat Analysis

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 via training tutorials and courses.

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 3 primary dark web resources — forums, shops, and marketplaces — in the report "Forums, Marketplaces, and Shops Remain Essential Venues for the Criminal Economy".

Another example of training that is focused on a variety of fraud methods is the Fraud Bible, a collection of fraud tutorials and videos organized in 80 GB of folders that offer over 200 different methods and how-to guides that target specific companies. Similarly, the forum COOCKIE PRO offers its members fraud-related educational videos that walk beginner cybercriminals through step-by-step methods of defrauding social media platforms and state governments.

While the training of the Carding Camp, Fraud Bible, and COOKIE.PRO is focused on a variety of fraud methods, there are many other courses dedicated to specific fraud areas. An example of this is the ENROLL 5.0 course, led by the threat actor "GOLDIE", an administrator of the GOLDIE ENROLL Telegram channel; the suspiria[.]ws credit cards shop; and goldie[.]cc forum, dedicated to online banking fraud.

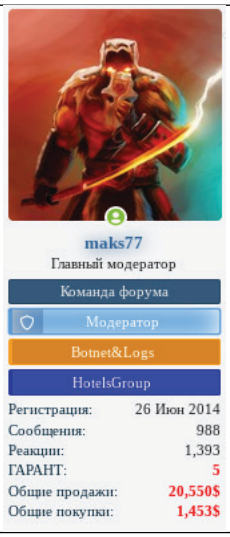
Inside the Carding Camp

Since 2015, the Russian-language underground forum WWH Club has been offering a training course on payment card fraud. WWH Club is one of the most populated low- to mid-tier Russian-speaking underground forums, and since its launch in February 2014, it has reached over 80,334 registered members, with 7,500 users who actively participate in the forum's life daily. WWH Club operates as a marketplace and discussion board focused on carding, e-commerce fraud, and money laundering, and its large member base makes it a popular cybercriminal hub in the Russian-speaking dark web.

The price of entry into the WWH Club's Carding Camp in 2021 is $900. In total, 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 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 6 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, trainees from different countries within the Commonwealth of Independent States (CIS), as well as from the Baltic states, China, and other countries, attend the course as well.

The Carding Camp training course on WWH Club is well known in underground communities for enabling novice cybercriminals to join the carding community. Carding Camp provides a full range of fraud methods. These can be general instructions on conducting fraud and scams, or company-specific schemes attempting to bypass anti-fraud mechanisms of organizations or financial institutions. The training lowers the barrier to entry for novice cybercriminals looking for methods to defraud companies and individuals.



"You came here to learn a new profession. Don't be afraid to ask questions".

"Yet, remember, you are on the forum of crooks and you either eat or become a meal yourself — do not trust anyone".

"Care for your safety? Do not work in the Commonwealth of Independent States (CIS)".

— "mans77", aka "maks77", course instructor, WWH Club forum chief moderator

Figure 1: Inside the Carding Camp, words of wisdom from one of the course instructors (Source: WWH Club)

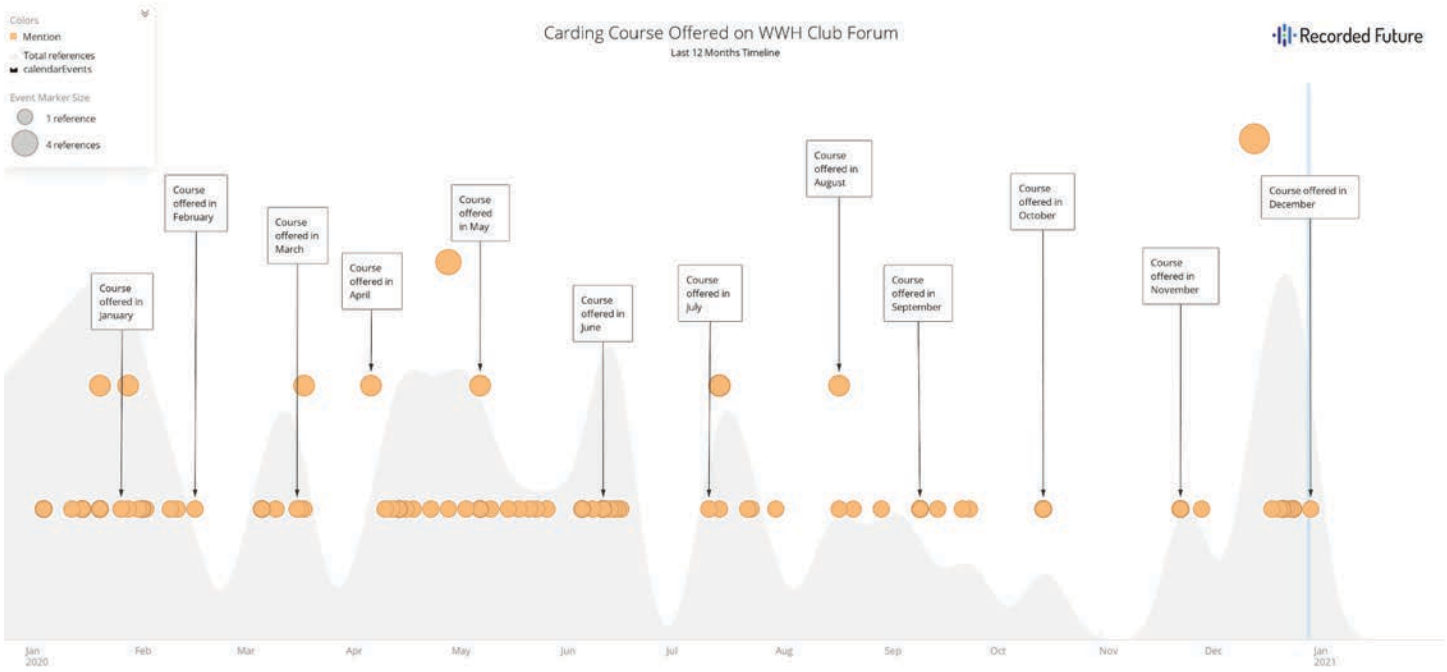


Figure 2: Timeline of the carding course offered on WWH Club, January 2020 to January 2021 (Source: Recorded Future)

Carding Camp's curriculum consists of the following training sessions:

1. Safety and Security
2. Anonymity and Virtual Machine Setup
3. Drops and Money Mules
4. Intermediaries and Mail-forwarders
5. Anti-Detect Tools
6. Linken Sphere (video lesson)
7. Carding in the US, UK, and the EU
8. Carding Banks
9. Carding Merchants
10. Gift Card Fraud
11. Enroll
12. PayPal (video lesson)
13. Account brute-forcing
14. eBay
15. Carding with Android
16. Pickup
17. Anti-Fraud Evasion
18. Social Engineering
19. Hotels Fraud
20. Airfare Fraud

Training sessions ,including both chat conversations and video lessons ,are recorded for trainees 'convenience .Instructors offer exercises ,assign homework ,and end every lecture with a question-and-answer discussion.

The simplified concept of carding ,explained by the Carding Camp instructors ,has 4 components:

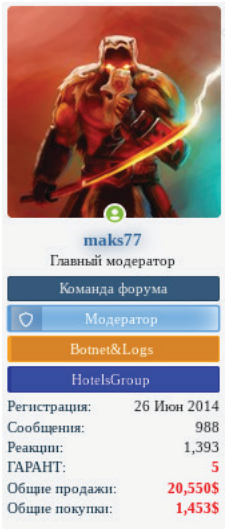
1. Find a store.
2. Get carding material (such as stolen payment card data).
3. Card that store to the max.
4. Profit.

"Carding is about networking with experienced comrades. You have to bond with others, as well as help and motivate each other".

"Carding is not just stealing, it is analyzing the data. Despite the result, you have to record the process. With this knowledge, you will become a better carder".

— "Пейн", course instructor, WWH Club forum moderator and arbitrator

Figure 3: Inside the Carding Camp, more words of wisdom from one of the course instructors (Source: WWH Club)



"Your task is to mimic a real user. Every little detail counts: get a proxy, as close to the cardholder's ZIP code as possible, start from a search engine, browse to an online store, warm it up by spending time to check various related products. If you are about to card a laptop, pretend to be a grandma looking for a present for her grandson. Don't act as a carder and you won't look like one."

— "mans77", aka "maks77", course instructor, WWH Club forum chief moderator

Figure 4: Inside the Carding Camp, words of wisdom from one of the course instructors (Source: WWH Club)

Throughout the Carding Camp course, some terms specific to frauding were referenced:

- "Karton" — payment card data
- "Dumps" — data encoded on the magnetic stripe on the back of a payment card, necessary to manufacture a cloned card (Track 2 and sometimes Track 1 data); used for in-store shopping
- "Fullz" — full info on cardholders (includes personal cardholder's info, like mother's maiden name, Social Security number, address, date of birth); used for online shopping
- "CVV" (Cards) — card data obtained from an on-line transaction using something like a sniffer (typically includes both payment card information like card number, ZIP code, and security number, and the account holder's information like name and address)
- "Kidala" — a ripper, meaning an individual who rips off others criminals
- "Deer" — a member who breaches forum rules or a n00b asking ridiculous questions
- "Zaliv" — bank transfer of funds from a compromised account
- "Obnal" — cashout (withdrawal of funds from an ATM or other similar device)

By the end of the Carding Camp's 6 weeks of training, the new cohort of cybercriminals knows where to find the necessary tools and materials to conduct payment card fraud. Some of the trainees form smaller groups to join forces and share experiences of what works and does not work for them in carding.

Although the contents of the Carding Camp may not always offer the latest tactics, since course instructors are likely to exploit novel methods before sharing them with the Carding Camp's audience, the materials and curriculum provide an insight into possible vulnerabilities as well as schemes and techniques used by fraudsters.

GOLDIE ENROLL

WWH Club Carding Camp focuses on a variety of fraud methods, but there are also 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. The process called "enroll" allows cybercriminals to link credit cards to online accounts with the ability to change cardholder's credentials. 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 a victim's PII, 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 using social engineering via telephone

The threat actor also advertises compromised bank accounts on their Telegram channel and offers direct access to themselves via@ susnsun) Telegram ,(Goldiecarding@jubber[.] ru) Jabber ,(or forum private messaging ,which leads to the forum's administrator's account .Additionally ,GOLDIE ENROLL underground criminal community has a private chat for its members.

Upon completion ,the participants of the ENROLL 5.0 course are invited to become part of the criminal enterprise and sell compromised accounts via the GOLDIE ENROLL Telegram channel.

The threat actor behind the moniker GOLDIE ENROLL is part" MEDELLIN ,"a major fraud network operated by Sergey Pokatsky ,a high-profile cybercriminal likely residing in Tomsk, Russia who also advertises educational materials and conducts webinars on fraud-related topics.

Fraud Bible

The Fraud Bible is a collection of multiple fraud tutorials and videos that takes up 80 GB and consists of over 200 different methods and how-to guides on conducting fraudulent activities. Some of the methods are general in nature, while others target specific companies. Fraud Bible is positioned as a one-stop-shop providing practical instructions, offered at an affordable price, that lower the barrier of entry for beginner cybercriminals looking to engage in various forms of fraud.

The Fraud Bible is a massive collection of all things fraud. Obtaining a copy of this collection on the dark web allows novice threat actors to kick-start a career in cybercrime — anyone equipped with the Fraud Bible's how-to guides can begin researching how to target hundreds of companies of various sizes and industries. Although it does not present sophisticated attack tips, it provides more than sufficient resources for beginner cybercriminals to enter the fraud scene and find information about operational security, social engineering, and places to buy stolen data to pursue fraudulent activities.

The availability of Fraud Bible tutorials will likely increase the number of threat actors attempting to commit crimes against the businesses included within it. The tutorials within the Fraud Bible are mainly based on a trial-and-error method when cybercriminals attempt to defraud specific organizations, walking through what eventually worked for them. Some of the schemes are scam-based, teaching an aspiring fraudster to become a con artist as opposed to a savvy hacker. However, even these methods provide bits and pieces of information necessary for defrauding a specific target, including otherwise hard to find details such as target site login information, the checkout process of a particular organization, or a Bank Identification Number (BIN) that worked in that scheme.

COOCKIE PRO

Threat actors also use social media platforms for their criminal needs. A new YouTube channel, COOCKIE PRO, hosts fraud-related educational videos and is advertised on the forum COOCKIE PRO, a Russian-language forum launched around June 2018 that specializes in the sale and advertising of compromised user logs, malware, and tutorials. The listed stealer logs are harvested from victims infected with different infostealers. The forum provides tools for optimizing victim data, such as a Netscape-to-JSON cookie converter. The forum offers original private Linken Sphere anti-detection browser configurations with session cookies, which work as a combination of fingerprints emulating real devices. According to forum advertisements, all configurations have been stolen from real user devices and are regularly updated. Unique configurations are sold to a single buyer only, for varying prices:

- Unfiltered configurations: $2 each
- Configurations filtered by operating systems and web browsers: $3 each
- Minimal configurations package: $5
- User logs with session cookies are subject to negotiation.

As an example, one of the COOCKIE PRO videos provides step-by-step instructions for filing for Pandemic Unemployment Assistance (PUA) in a particular US state. The video shows the process of obtaining the victim's personally identifiable information, logging in on behalf of the victim, collecting relief funds offered by the state, and cashing out these funds. The general flood of fraudulent unemployment requests that has overwhelmed government workers in many states is also enabled by the low barrier to entry for cybercriminals who can purchase stolen accounts or cheap tutorials and methods on how they can conduct similar fraud.

In our report "Unemployment Fraud in the Criminal Underground", we analyzed the current threat landscape of unemployment fraud in the United States within closed sources and underground reporting. Tutorials hosted on COOCKIE PRO have made unemployment fraud more accessible to threat actors operating within underground sources in recent months, preying on COVID-19 pandemic unemployment relief funds.

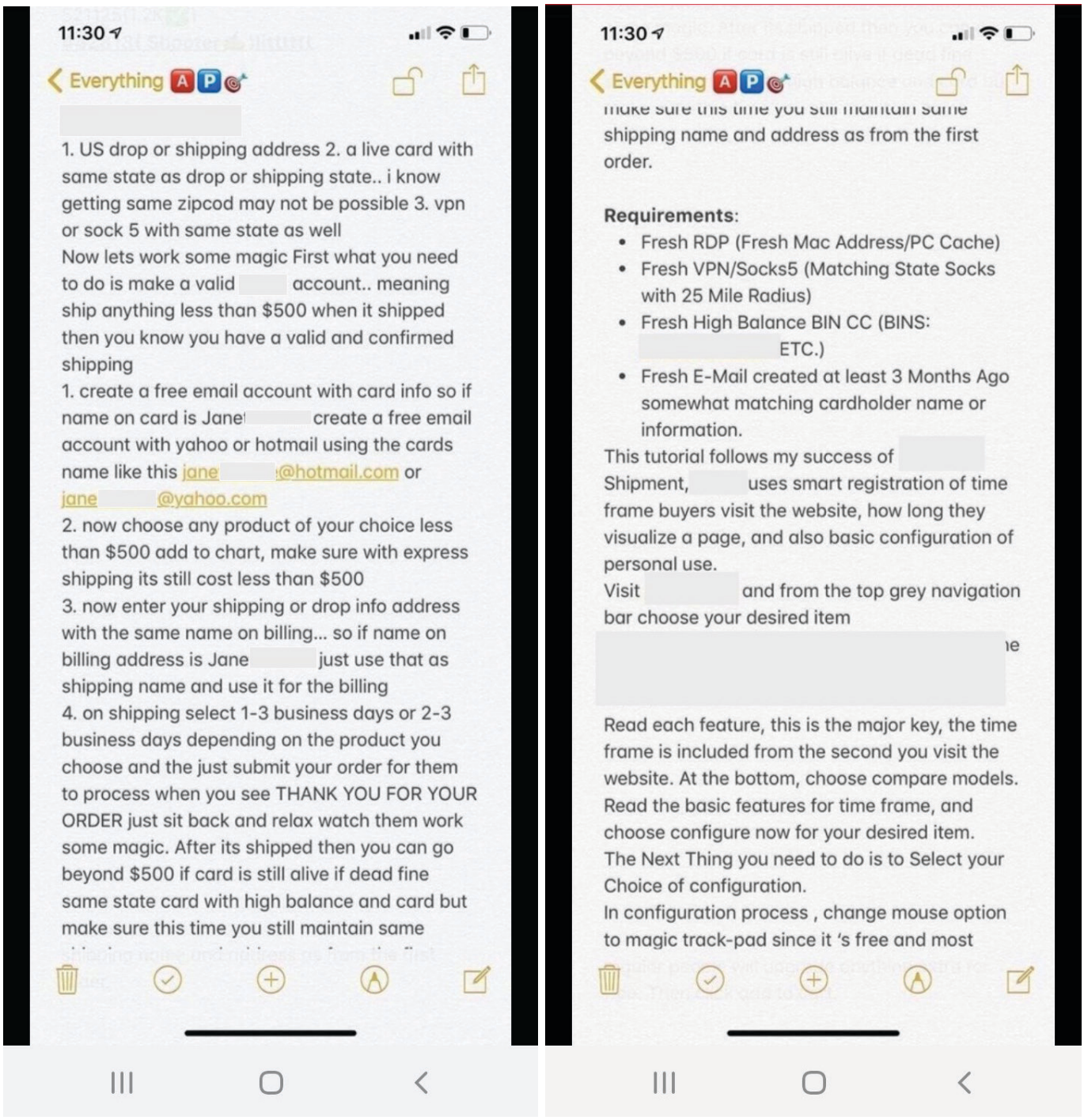


Figure 5: Sample tutorial (Source: Fraud Bible)

Chinese-Language Fraud Tutorials

Carding tutorials ,how-to guides ,recruitments ,and general intelligence sharing has been well-established across dark web forums ,markets ,and shops that are administered by and cater to English -and Russian-language speakers for many years .But these types of criminal activities are not reserved just for the aforementioned speakers .As a result of the interconnectedness of the internet coupled with mobile apps and websites becoming the norm for purchases and transactions ,cybercriminals who speak other languages have opened their own dark web markets, forums ,and shops that cater to language-specific users as well as those who are familiar with regional e-commerce ,bank ,or financial-related institutional brands they wish to target .One such language is Mandarin Chinese ,hereafter referred to as Chinese.

An examination of our source collections over the last year for threat actors using dark web sources in Chinese identified the following themes:

- Threat actors are listing advertisements and posting in Chinese on well-established dark web forums and shops that specialize in listing compromised financial data and services, including VClub, Club2CRD, PRTship | Carders, Carding Mafia, ProCrd, WWH Club, and Card Villa.
- These sources, and others, feature the following types of financial-related listings and discussions: advertisements for compromised payment cards, news events (specifically the closing of Joker's Stash in Chinese), requests (looking for partners and services), and comments, promotional postings offering free data to increase reputation, and sharing intelligence on operational security practices and needs (software and tools) to harvest payment data.
- The 2 most popular Chinese-focused sources were Exchange Market and FreeCity Market, with 33 and 24 references, respectfully, for listings related to tutorials, how-to guides, and hacking-related listings targeting payment data systems and institutions.

We cannot definitively ascertain whether the listings above were posted by native Chinese speakers ,but it is becoming a more common tactic for threat actors to use Chinese as an obfuscation technique) many appear to use freely available online translators ,(or to specifically target Chinese speakers with the intent of connecting with like-minded criminals or identifying other Chinese speakers in other countries to facilitate fraudulent activities.

Figure 6: Listing by dxddla for CVV tutorials and software. The description reads: "This resource includes (Xingtianle's newest tutorial + integrated systems, Napoleon tutorial, North American Chinese team J3 tutorial, CC international CPA [internal course]) total 27.57G. System: Import with VM virtual machine, internal software tools, cvv data shop, all are complete and you control the whole tutorial, size is 18+G" (Source: FreeCity Market)

Regarding listings posted on Exchange and FreeCity markets, we identified the most listings on Exchange but believe that FreeCity will continue to be an attractive source for threat actors, as the market also caters to English and Korean speakers. An example of a carding tutorial listings on FreeCity Market was posted by the vendor "dxddla" in February 2021 under the title "CVV Tutorials The Most Complete Fee-based Course + System (All Tutorials with Software Systems for CVV use) Automatic Shipping":

The CVV tutorial listings, per the above description, includes the following 7 file names (translated from Chinese to English):

- New Integrated System.tgz
- Napoleon Tutorial.mp3
- North America Chinese Team J3 Tutorial.zip
- cvv Advanced Toolkit.rar
- CC International CPA [Internal Course].zip
- 2,3,4,5 class.7z
- 1. Course Catalogue and Summary.7z

Similar listings for tutorials, how-to guides, and general knowledge are also actively advertised on Exchange Market. The following table outlines a sample of 5 threat actors who listed the aforementioned carding product types in 2020 (products are currently available for automatic buying):

Threat Actor	Intelligence
"75066"	In May 2020, the threat actor authored a sales thread for the latest set of training materials for the carding industry in 2020. For $200, a buyer will receive materials that include different targeting methods (point-of-sale, compromised CVV, etc.), how-to methods, as well as operation and embezzlement techniques. A buyer will receive a Telegram handle, after purchase, from the operator of 75066 for direct communication.
"342919"	In May 2020, the threat actor posted an advertisement for interested users to join their carding team as a member ($400) or to become an apprentice ($200) for learning purposes. Regarding apprenticeship, the threat actor stated they would provide one-on-one guidance, consulting services for carding, and tutorial methods. Regarding team partnership, a member will collaborate with other members to develop tools and share in profits. Based on similar language use and techniques (will share a Telegram channel with buyers), this threat actor may be operated by or shares a relationship with the above-mentioned moniker 75066.
"499135"	In June 2020, the threat actor advertised online teaching courses for carding methods. For $700, a buyer would receive 2 one-on-one meetings (within 30 days) on tools, operating procedures, methods, and operational security for targeting an entity for carding.
"578518"	In July 2020, the threat actor posted an advertisement for tutorials, tools, and services on using payment card and CVV data titled "Great Value! The Most Complete (Tutorial Internal Software Tools Virtual Machine) Properties" (Figure 11). Specifics included: 7 tutorials (using CVV data, needed software, anti-fraud techniques), 2 toolkits, BINs (valid and for practice), and general TTPs.
"569674"	In August 2020, the threat actor advertised for $10 a carding tutorial that includes where to purchase compromised CVVs (websites) and how to test them after purchase. The tutorial also contains how-to videos on the following: setting up your workstation (VPN and SOCKS5 implementation), incorporating fingerprint disguise software (Chameleon, MU, and Lincoln Sphere), and monetizing compromised CVVs online.

Figure 7: Sample of CVV tutorial advertised by 578518 (Source: Exchange Market)

Outlook

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.

Fraud tutorials and courses may not always offer the most innovative 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.

Recorded Future recommends 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.