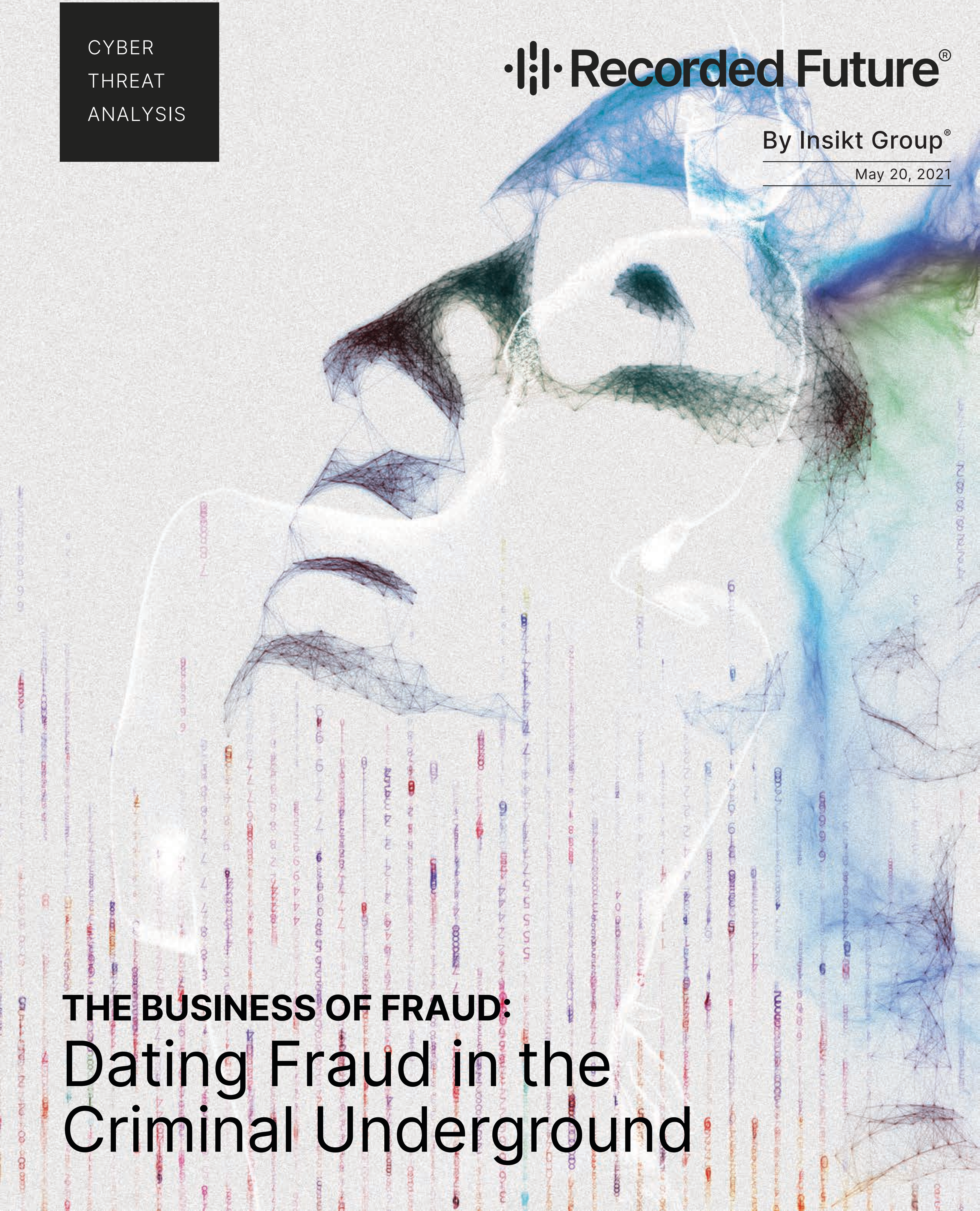
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

May 20, 2021



THE BUSINESS OF FRAUD: Dating Fraud in the Criminal Underground

Recorded Future analyzed current data from the Recorded Future® Platform, dark web, and open-source intelligence (OSINT) sources to review dating scams and the methodology and operations used by threat actors. 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".

Executive Summary

Dating fraud or dating scams are a form of social engineering in which threat actors feign romantic interest in a target to lure them into a false sense of security, allowing the threat actors to manipulate the victim into providing them with money or sensitive information or using them to channel funds. Because they are straightforward and highly effective, these scams have existed for decades, often targeting lonely individuals looking to make an emotional connection. Though appearing simple, like any other complex cybercrime operation, dating scams usually require cooperation among different threat actors, each of whom will have a specialty. Identifying targets, allocating convincing images and creating personas, and cashing out the stolen money are often all separate services offered on the underground that are combined to create a successful, persistent dating scam.

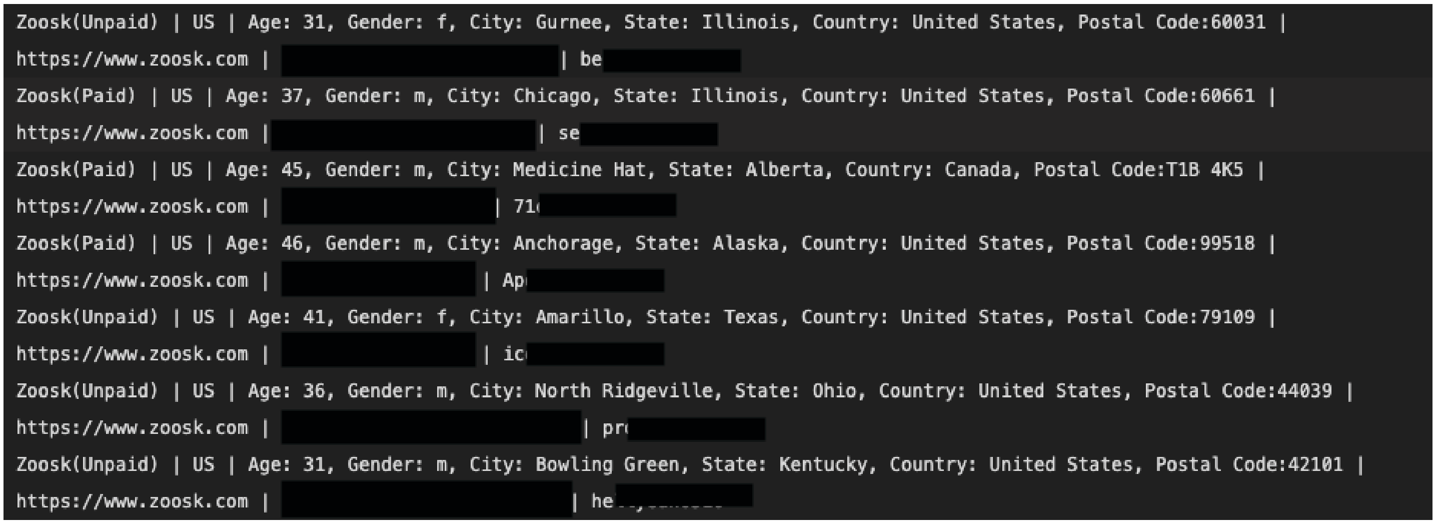
Key Judgments

- Dating scams are a niche cybercriminal ecosystem where specialized threat actors tailor their attack methods against select targets.
- The creation of subsections of dark web forums that are specifically geared toward the various stages of dating fraud — including target selection, social engineering, and cashout schemes — indicates a continued interest from threat actors to engage in these types of scams.
- The sharing of information, tools, and manuals by threat actors on dark web forums allows fraudsters to learn tips and tricks from one another and to continue to refine their techniques to successfully engage with victims. This also lowers the barrier of entry so that even novice threat actors can successfully participate in dating fraud.

Background

Dating scams are a form of fraud in which threat actors feign romantic interest in a target to lure them into a false sense of security. The term "romance scams" is also often used interchangeably by threat actors and the media; the difference between dating scams and romance scams is that romance scams typically refer to the scams that use a "spray and pray" tactic, whereas "dating scams" are more targeted when selecting their victims. The threat actors behind these scams rely heavily on social engineering and evoking an emotional response from the victims to create a false sense of trust. They use fake profiles on dating apps or social media platforms or send phishing emails directly. In the criminal underground, dating scams are specialized and, in some cases, even have their own subsection on dark web forums.

These scams often have the end goal of tricking the victims into sending money to the threat actors, sometimes through blackmail or extortion; however, in some cases, the victims are actually the recipients of funds stolen from other sources, effectively helping the threat actors to launder the funds by using them as witting or unwitting money mules. There are myriad other end goals that threat actors can have for dating scams, including the theft of the victim's personally identifiable information for account takeover or other kinds of identity theft and, less frequently, intelligence-gathering by state-sponsored groups or other threat actor groups.



```
Zoosk(Unpaid) | US | Age: 31, Gender: f, City: Gurnee, State: Illinois, Country: United States, Postal Code:60031 |
https://www.zoosk.com | [redacted] | be[redacted]
Zoosk(Paid) | US | Age: 37, Gender: m, City: Chicago, State: Illinois, Country: United States, Postal Code:60661 |
https://www.zoosk.com | [redacted] | se[redacted]
Zoosk(Paid) | US | Age: 45, Gender: m, City: Medicine Hat, State: Alberta, Country: Canada, Postal Code:T1B 4K5 |
https://www.zoosk.com | [redacted] | 71[redacted]
Zoosk(Paid) | US | Age: 46, Gender: m, City: Anchorage, State: Alaska, Country: United States, Postal Code:99518 |
https://www.zoosk.com | [redacted] | Ap[redacted]
Zoosk(Unpaid) | US | Age: 41, Gender: f, City: Amarillo, State: Texas, Country: United States, Postal Code:79109 |
https://www.zoosk.com | [redacted] | ic[redacted]
Zoosk(Unpaid) | US | Age: 36, Gender: m, City: North Ridgeville, State: Ohio, Country: United States, Postal Code:44039 |
https://www.zoosk.com | [redacted] | pr[redacted]
Zoosk(Unpaid) | US | Age: 31, Gender: m, City: Bowling Green, State: Kentucky, Country: United States, Postal Code:42101 |
https://www.zoosk.com | [redacted] | he[redacted]
```

Figure 1: Snapshot of Zoosk accounts listed on Pastebin (Source: Pastebin)

Threat Analysis

Initial Access and Setup (Pre-Scam)

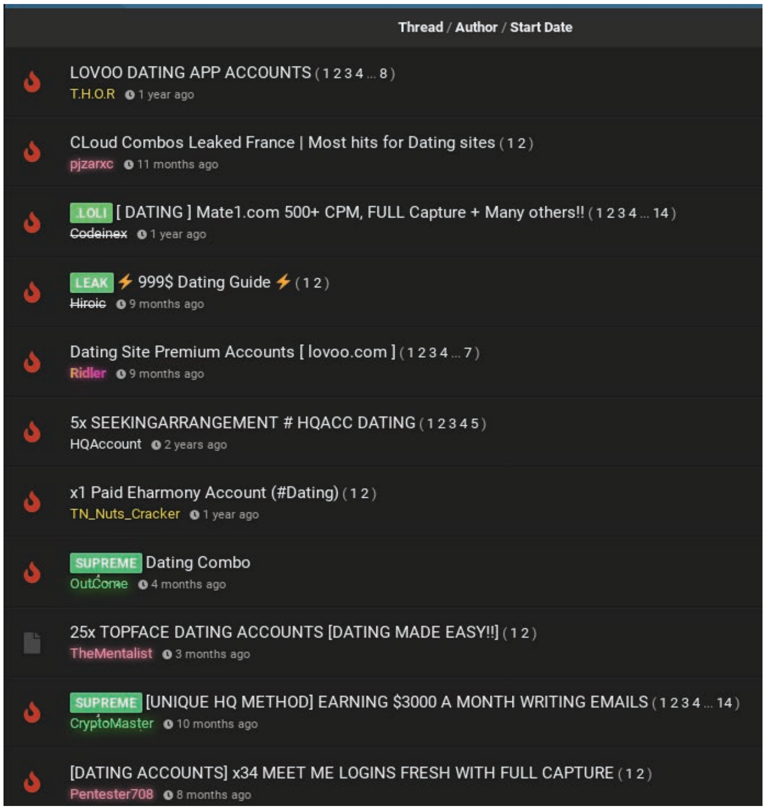
The victims of dating scams are mainly individuals who are interested in dating and romantic relationships ,making them easier targets for social engineering as threat actors do not have to work hard to build relationships online and communicate with strangers ;potential victims are willing to do it of their own accord .As face-to-face interaction has become much more limited since the start of the COVID 19-pandemic ,more people have turned to online dating to find partners.

In many cases, the initial targeting of a victim occurs through dating sites or some sort of community such as social media sites. However, dating and social media sites have turned to various forms of multi-factor authentication to validate that accounts are authentic. Specifically, for dating profiles, users are given an option to verify their accounts by sending photos to the dating sites for admins to review and validate. These photos are typically taken in an unnatural pose, such as looking ahead while smiling and making a specific gesture. While having a verified profile is not necessary to sign up for dating sites, it gives users the account may interact with the sense that the person pictured on the account is who they are actually interacting with and often allows the users to let down their guard as they believe they are speaking with the person that is pictured in the photo. However, these "verification" photos can easily be manipulated by scammers looking to bypass authentication restrictions.

Dating applications have traditionally been identified by security researchers as having poor security posture, which could lead to the leakage of user data, including messages and photos in some cases, to advertisers and others. The most well-known instance of this was the 2015 breach of data at Ashley Madison, a website for those seeking extramarital affairs, which exposed 32 million user records. Other dating applications, such as MeetMindful (2021), Grindr (2021), Barcelona-based MobiFriends (2020), the South Korean dating app SPYKX[.]com, and others, have all had various data breaches, either through direct targeting by malicious actors or through vulnerabilities found in their software or improperly secured servers.

A Recorded Future query of the top dating applications in the US in 2021 yielded over 330,000 references within the last year for credential leaks associated with the apps .These references also appear on open source platforms such as Pastebin ,which showed data captured from the 2020 Zoosk data breach and included a comprehensive overview of user accounts ,such as the users 'email address and password ,age ,gender ,city ,postal code ,and whether the accounts were free or paid .If a threat actor were to use these compromised accounts ,they would have access to items such as photos and messages belonging to those individuals ,giving them the ability to pose as a real person instead of having to get photos of people or use AI-generated photos.

Furthermore, forums such as Raid Forums have a slew of advertisements specifically related to dating accounts. While the details of the accounts are not made available until after purchase, an interested threat actor could peruse the adverts until they find a post that relates to their specific scam. Notably, the dating apps were not limited to one geographic region but rather listed accounts for dating apps worldwide. Additionally, country-specific dating apps, like Lovoo, a German dating app, were listed on the forums.



Thread / Author / Start Date

LOVOO DATING APP ACCOUNTS (1 2 3 4 ... 8)
T.H.O.R 1 year ago

CLoud Combos Leaked France | Most hits for Dating sites (1 2)
pjzarxc 11 months ago

.LOLI [DATING] Mate1.com 500+ CPM, FULL Capture + Many others!! (1 2 3 4 ... 14)
~~Codeinex~~ 1 year ago

LEAK ⚡ 999$ Dating Guide ⚡ (1 2)
~~Hiroic~~ 9 months ago

Dating Site Premium Accounts [lovoo.com] (1 2 3 4 ... 7)
Ridler 9 months ago

5x SEEKINGARRANGEMENT # HQACC DATING (1 2 3 4 5)
HQAccount 2 years ago

x1 Paid Eharmony Account (#Dating) (1 2)
TN_Nuts_Cracker 1 year ago

SUPREME Dating Combo
OutCome 4 months ago

25x TOPFACE DATING ACCOUNTS [DATING MADE EASY!!] (1 2)
TheMentalist 3 months ago

SUPREME [UNIQUE HQ METHOD] EARNING $3000 A MONTH WRITING EMAILS (1 2 3 4 ... 14)
CryptoMaster 10 months ago

[DATING ACCOUNTS] x34 MEET ME LOGINS FRESH WITH FULL CAPTURE (1 2)
Pentester708 8 months ago

Figure 2: List of accounts for dating sites (Source: Raid Forums)

Dating scams do not only target those actively looking for relationships on dating sites or applications. The same tools, techniques, and procedures (TTPs) are frequently applied to targeting individuals on other forms of social media. Social media sites such as Facebook have implemented stricter protocols for new account creation to thwart bots and spammers. However, just as with dating sites, Insikt Group identified multiple ways that scammers or bots could get around these authentication protocols. For example, advertisements for captcha bypass tools were found in multiple dark web markets, such as Raid Forums and Nulled Forums. These captcha bypass tools came as a pre-configured script or could be configured for a specific targeted site. The low price point also makes it easier for low-tier or non-technical threat actors to be involved in nefarious activities.

Outside of social media sites and dating applications, spam and email campaigns have been employed by fraudsters to target victims who may be hoping for an email or SMS from a potential love interest. These campaigns are designed to send out messages to hundreds, if not thousands, of potential victims and are, thus, less tailored to the individual. Spammers specializing in dating scams provide mailing lists of targets thought to be more susceptible to this type of attack. These mailing lists are likely taken from dating sites breaches and are geographically relevant to the victims being targeted (such as the United States, Canada, and Australia). In one identified instance, a threat actor going by the moniker **Amox** was interested in purchasing email accounts from private databases acquired from dating websites and stated that they were willing to pay $1 per 1,000 accounts.

These email spam campaigns have also seen success when their victims are over the age of 50 and looking for a connection. Threat actors leverage their emotional vulnerability to take advantage of them. When a deeper psychological connection is established or another common interest is identified, the threat actors are then able to manipulate the victim into taking actions like sending them money or giving out personally identifiable information.

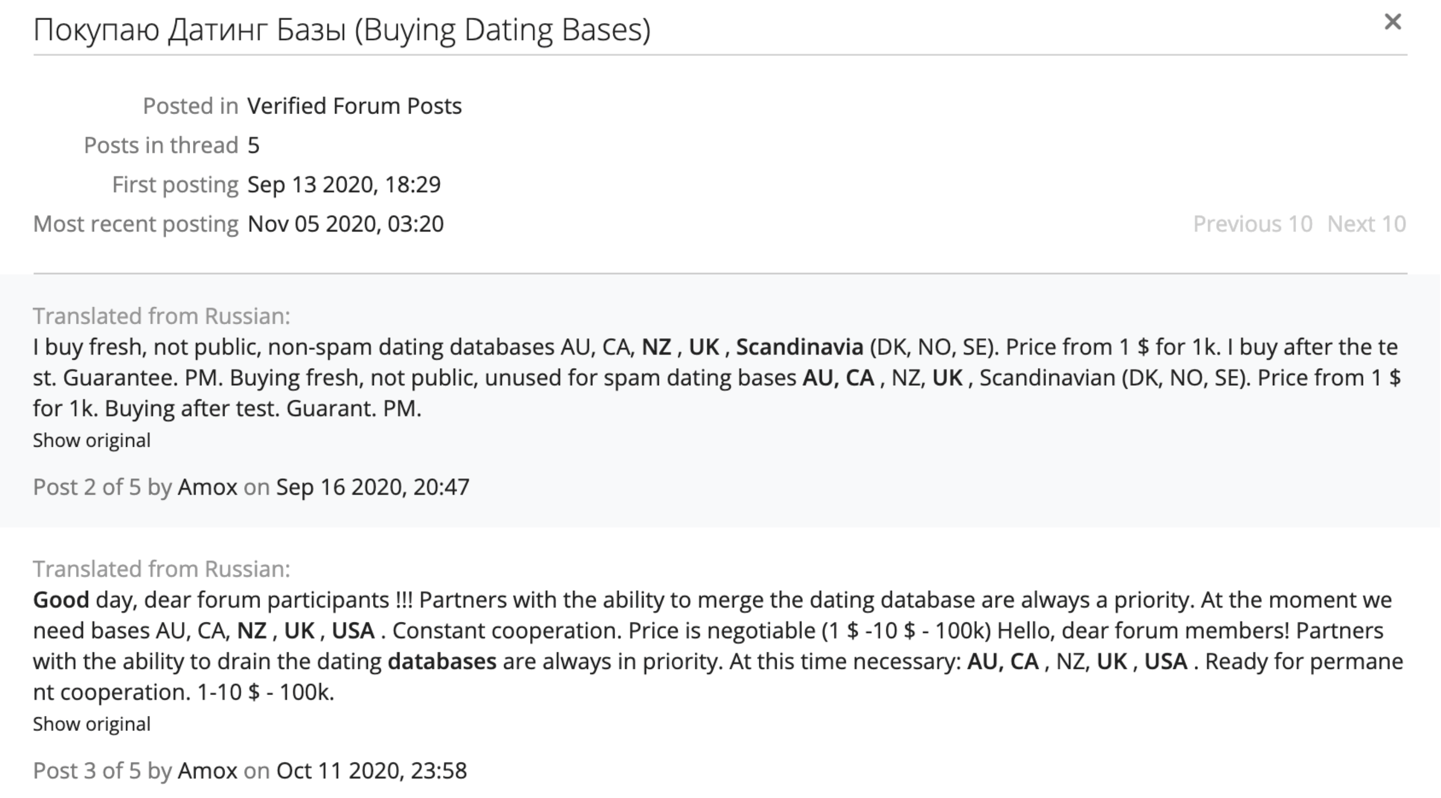
For example, **msmtp**, a member of the high-tier forum Verified advertised a dating fraud service focused on spamming and social engineering launched in June 2018. According to the threat actor, they specialize in “dating replies”, which entails sending mass emails using their own and their customers’ databases to solicit responses and engaging targeted individuals in dating and romantic communications to commit fraud. msmtp registered on the forum in December 2015, and as of April 2021 holds a $1,000 deposit and has received mostly positive feedback and reviews from other members of Verified, indicating that their service is likely thriving.

The threat actor stated that their customers can receive dating replies to email addresses of their choice or msmtp could receive the dating replies via their own email addresses. If their customers chose to go with msmtp’s emails addresses, the threat actor guarantees that they use databases dumped from major dating sites and similar paid platforms which they claim to update weekly.

msmtp’s dating fraud service price list:

- $0.50 for English-language replies from the US, Canada, Australia, the UK, and Europe
- $1.00 for replies from Italy
- $1.50 for German-language replies from Germany, Austria, Switzerland, and the Netherlands

msmtp calls their service “dating replies” because they only charge customers for an actual reply from a targeted individual. This scheme starts from msmtp sending spam en masse, using various databases, including those collected from breached dating sites. Then customers receive replies directly to the emails of their choice or msmtp’s emails, which the threat actor passes on to the customer according to the abovementioned price list. The initial spam campaign message is aimed at a broad audience interested in online dating. For example, the following text is the threat actor’s suggested email template for beginning the dating fraud conversation:



Покупаю Датинг Базы (Buying Dating Bases)

Posted in Verified Forum Posts
Posts in thread 5
First posting Sep 13 2020, 18:29
Most recent posting Nov 05 2020, 03:20

Translated from Russian:
I buy fresh, not public, non-spam dating databases AU, CA, **NZ** , **UK** , **Scandinavia** (DK, NO, SE). Price from 1 $ for 1k. I buy after the test. Guarantee. PM. Buying fresh, not public, unused for spam dating bases **AU, CA** , NZ, **UK** , Scandinavian (DK, NO, SE). Price from 1 $ for 1k. Buying after test. Guarant. PM.
Show original

Post 2 of 5 by Amox on Sep 16 2020, 20:47

Translated from Russian:
Good day, dear forum participants !!! Partners with the ability to merge the dating database are always a priority. At the moment we need bases AU, CA, **NZ** , **UK** , **USA** . Constant cooperation. Price is negotiable (1 $ -10 $ - 100k) Hello, dear forum members! Partners with the ability to drain the dating **databases** are always in priority. At this time necessary: **AU, CA** , NZ, **UK** , **USA** . Ready for permanent cooperation. 1-10 $ - 100k.
Show original

Post 3 of 5 by Amox on Oct 11 2020, 23:58

Figure 3: Screenshot of Amox advertising email accounts from dating websites (Source: Recorded Future)

"Hello, I'm a good lady who is looking for a good gentleman. If you are interested, respond to my email. Thank you!"

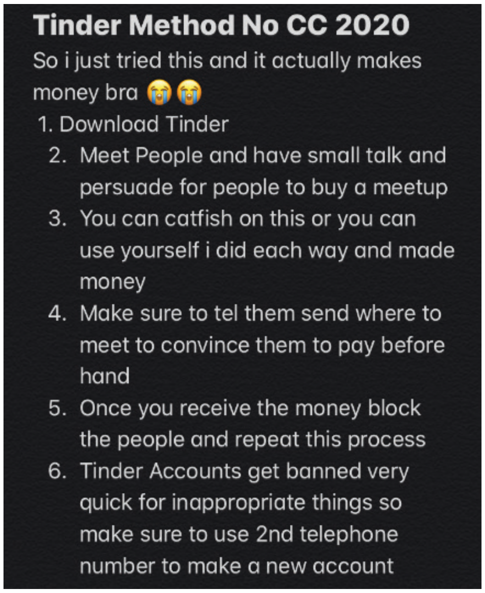
The email is drafted in the language of the targeted individual and may contain additional details, such as the fictitious sender's age, country, and city.

According to the threat actor, they take a minimum of $500 for an order but charge only for replies that suggest the targeted individual's interest in dating.

Finding and Engaging Victims (Mid-Scam)

Once the threat actors successfully register for a site and go through the validation screening ,they can use the sites to scout for victims .On social media sites ,this can be done by joining dating-focused groups and targeting individuals through there. Alternatively ,on dating apps ,the individuals can look for those who may be perceived as being vulnerable ,such as people who may not be aware of the types of security risks involved with the apps .The targeting of victims ,and subsequent conversations, rely heavily on social engineering techniques to make the threat actor appear genuine and to form a connection with the victim.

Many dark web sources offer social engineering guides specifically for dating sites ,such as the Fraud Bible ,an 80 GB collection of fraud tutorials and videos organized in folders that offer over 200 different methods and how-to guides that target specific companies .Some of the methods are general ,while others target specific companies ,such as Tinder.

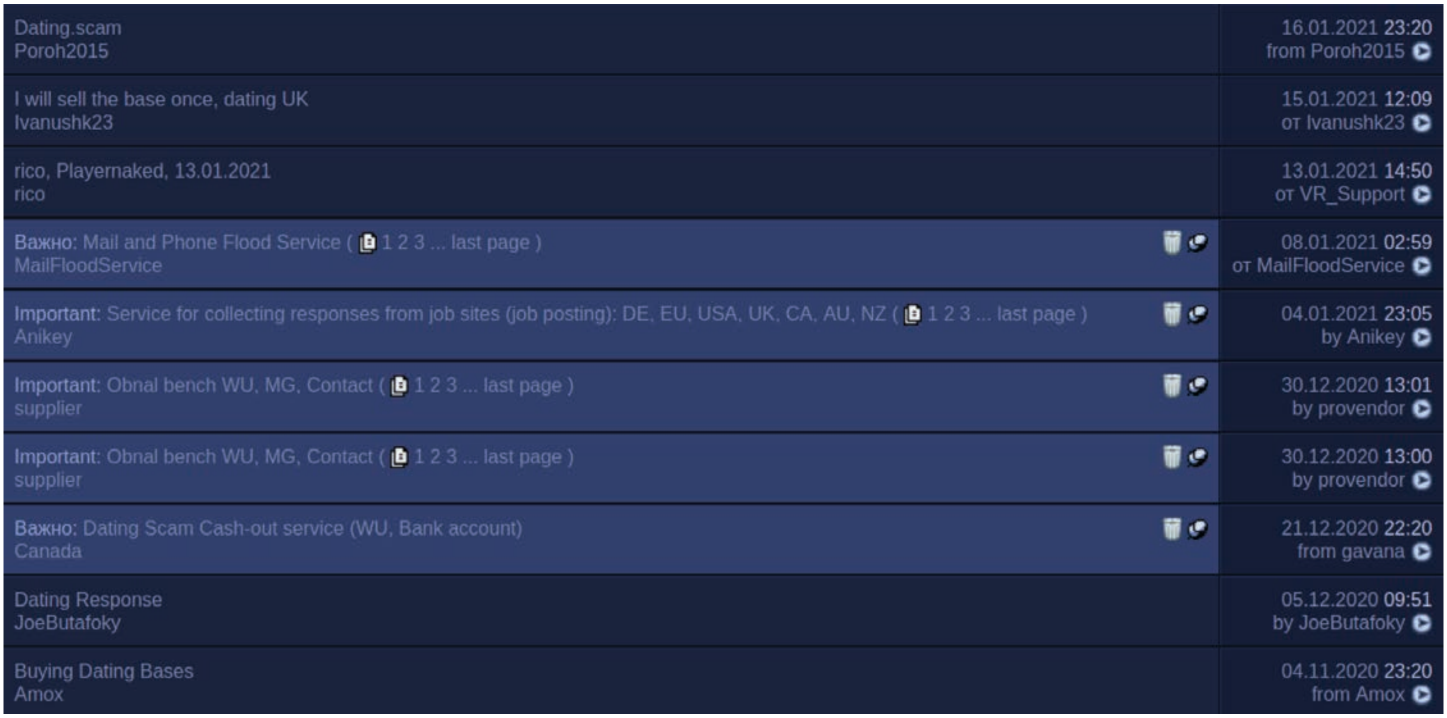


Tinder Method No CC 2020

So i just tried this and it actually makes money bra 😭😭

1. Download Tinder
2. Meet People and have small talk and persuade for people to buy a meetup
3. You can catfish on this or you can use yourself i did each way and made money
4. Make sure to tel them send where to meet to convince them to pay before hand
5. Once you receive the money block the people and repeat this process
6. Tinder Accounts get banned very quick for inappropriate things so make sure to use 2nd telephone number to make a new account

Figure 4: Tinder tutorial showing sample methodology (Source: Fraud Bible)



Dating.scam Poroh2015	16.01.2021 23:20 from Poroh2015
I will sell the base once, dating UK Ivanushk23	15.01.2021 12:09 от Ivanushk23
rico, Playernaked, 13.01.2021 rico	13.01.2021 14:50 от VR_Support
Важно: Mail and Phone Flood Service (1 2 3 ... last page) MailFloodService	08.01.2021 02:59 от MailFloodService
Important: Service for collecting responses from job sites (job posting): DE, EU, USA, UK, CA, AU, NZ (1 2 3 ... last page) Anikey	04.01.2021 23:05 by Anikey
Important: Obnal bench WU, MG, Contact (1 2 3 ... last page) supplier	30.12.2020 13:01 by provendor
Important: Obnal bench WU, MG, Contact (1 2 3 ... last page) supplier	30.12.2020 13:00 by provendor
Важно: Dating Scam Cash-out service (WU, Bank account) Canada	21.12.2020 22:20 from gavana
Dating Response JoeButafoky	05.12.2020 09:51 by JoeButafoky
Buying Dating Bases Amox	04.11.2020 23:20 from Amox

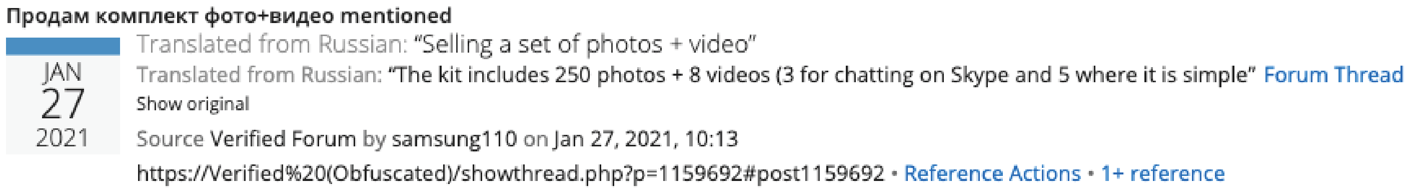
Figure 5: Verified forum subsections in the dating scam section (Source: Verified Forum)

Although the Fraud Bible method in Figure 4 does not use sophisticated attack techniques, it shows beginner cybercriminals one way to enter the dating fraud scene, pursue specific targets, and use social engineering to defraud the members of one dating site.

Verified Forum, a high-tier Russian-language forum specializing in carding and other fraudulent activities is another example of how dark web threat actors focus on dating scams. The forum contains an entire subsection that is dedicated to topics related to dating scams, such as discussions of threat actor's personal experiences running a dating scam service, fraudsters offering packaged photos sets of individuals, and various services such as call schemes and cashout services, among others, which can be seen in the figure below.

The social engineering guides identified on Verified detail how threat actors can frame themselves as caring, loving, and generous to gain the victim's trust. Techniques to appear more realistic are also outlined. For example, accounts that have a significant online footprint are more likely to put a victim at ease since the individual has a presence outside of the dating app. By having a fake network of friends and a presence on other social media sites or applications, the victim is less inclined to think that the person they are speaking to is fake. In one example, a victim stated that she had trusted the scammer because the individual had other social media sites, a LinkedIn account, a bank account, and a Zillow account, among others, appearing legitimate.

Convincing content is arguably the most important element of any dating scam, and in the social engineering phase, there are other ways in which the threat actor can purchase items to make themselves appear more legitimate. Fraudsters need to constantly collect images and videos of new, real individuals (often women in their teens or twenties) to appear believable to the victims and require a component of human infrastructure to conduct their operations. Creating personas that appear authentic and believable enough to form a deep enough relationship to effectively scam a victim 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. Samsung110, a member of the forum Verified, was searching for just that: images and videos of women, with or without identification documents. The threat actor was also looking to partner with a threat actor who had photoshop skills who could alter photos, such as swapping faces with bodies of unrelated individuals or who could produce new photos and videos on demand.



Продам комплект фото+видео mentioned

JAN
27
2021

Translated from Russian: "Selling a set of photos + video"

Translated from Russian: "The kit includes 250 photos + 8 videos (3 for chatting on Skype and 5 where it is simple" Forum Thread

Show original

Source Verified Forum by samsung110 on Jan 27, 2021, 10:13

https://Verified%20(Obfuscated)/showthread.php?p=1159692#post1159692 • Reference Actions • 1+ reference

Figure 6: samsung110 advertisement of photo packages (Source: Recorded Future)

Samsung110 was also selling images and videos of women between the ages of 26 and 33 years old. In April 2021, the threat actor was selling a package with 250 photos and 8 videos, 3 of which samsung110 suggested using for video chat communications, such as Skype. Additionally, some of the threat actor's reviews and posts suggest that in addition to providing content, samsung110 is also involved in dating fraud directly, both running campaigns to defraud individuals and facilitating other cybercriminals' dating fraud operations. Specifically:

- In October 2020, samsung110 was looking for a photoshop designer capable of altering photos, such as swapping faces with bodies of unrelated individuals.
- In March 2020, samsung110 was looking to buy photos and videos of women with or without identification documents.
- In December 2019, samsung110 left a positive review for "Slavenin", a vendor of dating fraud cashout service on the Verified forum.
- In July 2019, samsung110 left a positive review for "approved_calls", a vendor of calling service on Verified forum known for its social engineering calls to commit various forms of fraud, including dating fraud.
- In April 2018, samsung110 was also engaged in dating fraud targeting gay individuals.

Furthermore, targeting isn't just limited to photo packages. Fraudsters also employ call services to engage their victims, which can be tailored according to the persona employed by the threat actor. A live phone conversation with a male or female caller adds significant legitimacy and can persuade the victim into further action.

approved_calls, a member of the high-tier forums Maza and Verified, has advertised a calling service catering to various fraud-related operations since September 2015. According to the threat actor, they currently employ phone operators that speak any language, with male and female voices. approved_calls is offering their services for the following fraud-related activities:

- recruitment of drops and mules (such as social engineering individuals)
- carding — payment card fraud (such as calling banks and pretending to be a legitimate cardholder)
- spoofing calls (to portray themselves as someone they are not)
- reshipment fraud (such as confirming orders and deliveries)
- dating fraud (scamming and social engineering users of dating sites)
- drafting correspondence (for dating fraud and fake recruitment purposes)
- receiving calls to a specific number (dating fraud only)
- calling to render target's phone lines inoperable/busy (advertised as "phoning DDoS")
- follow-up calls (to support and reinforce spamming campaigns)

According to approved_calls, their prices vary from $5 to $15 per phone conversation, with $5 per call for bulk orders or calls to mules and drops; $8 to $10 per call to businesses (such as online stores); and $15 per call for dating fraud. The threat actor noted that they use phone numbers with the same country codes as the call recipients. The service accepts payments in Bitcoin, WebMoney, and Qiwi and is open for business 24/7, but approved_calls' service does not extend to the Commonwealth of Independent States (CIS) and they will not make calls in Russian.

Cashing Out

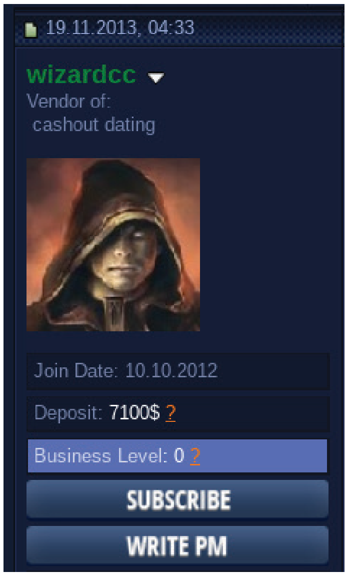
Dating scam fraudsters are generally financially motivated: Their end goal may be to have the victim willingly send a sum to the threat actor, to extort the victim, or to use them as a money mule. For this reason, many threat actors offer cash-out services on the dark web to help these fraudsters get their funds.

Slavenin, a member of the high-tier forum Verified, is one threat actor advertising a cashout and money laundering service. According to the threat actor, they have operated the service since February 2019 and specialize in dating fraud cashout. Slavenin claims to provide their customers with fund transfers using bank accounts, MoneyGram, Westen Union, Contact, RIA Money Transfer, Unistream, and KoronaPay money transfers. According to the threat actor, their commission is a follows:

- 16% for less than $5,000
- 15% for $5,000 to $10,000
- 12% for over $10,000
- 11% for money transfer companies
- 4,000 Russian rubles (approximately $55) is the minimum commission

Slavenin claims that they can make transfers to any bank, WebMoney, or Bitcoin wallets within 24 hours. The service operates per Moscow time zone with Sunday as a day off.

Another such individual, wizardcc, advertised cashout services that could be used with numerous financial institutions. The threat actor has been on the forum since December 2012 and has hundreds of positive exchanges and reviews for their cashout services, which focus on dating fraud cashouts and which the threat actor has operated since November 2013.



19.11.2013, 04:33

wizardcc

Vendor of:
cashout dating

Join Date: 10.10.2012

Deposit: 7100$?

Business Level: 0 ?

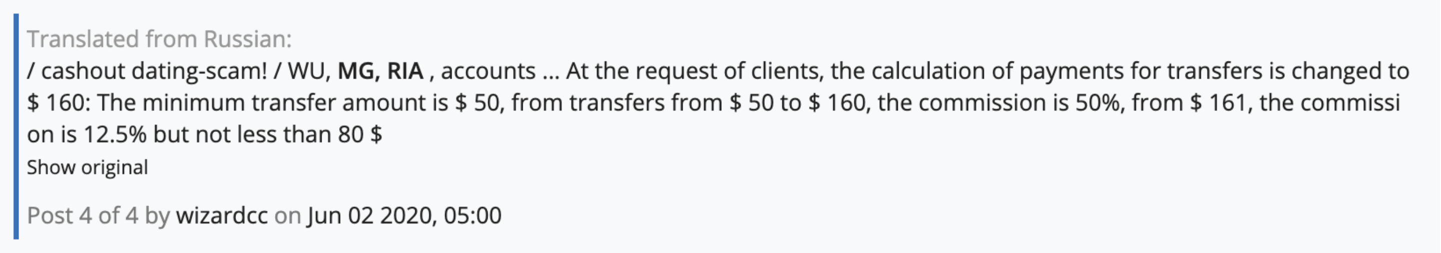
Figure 7: wizardcc's profile on Verified Forum (Source: Verified Forum, Recorded Future)

The threat actor claims to provide their customers with fund transfers in Russia using Western Union, Ria Money Transfer, WorldRemit, Contact, Unistream, Azimo, KoronaPay, and Coinstar. Additionally, wizardcc stated that they can receive fund transfers in US dollars or euros from individuals to bank accounts that they control, which likely belong to individuals hired as money mules. According to wizardcc, they do not accept money transfers from Baltic states, Russia, or other countries of the Commonwealth of Independent States (CIS). The threat actor is operating a Jabber bot that can receive orders 24/7.

wizardcc's commission is 12.5% with an $80 USD per-transfer minimum. The threat actor claims that they can transfer to any bank account in Russian rubles, WebMoney, Qiwi, Yandex Money, AlfaBank click, or Bitcoin wallets within 24 hours.

Threat actors can also open bank accounts with unique names, matching that of the persona who instigated the conversation through phishing attempts via email, social media, or online dating platforms. The opening of accounts can be done by the threat actors themselves through tutorials, or they can engage with other threat actors who specialize in bank fraud. Wire transfers, Western Union, and MoneyGram are some of the popular options used by threat actors to create accounts under the name of the fraudster's choice. From there, the threat actors who specialize in bank fraud can accept the stolen funds through the accounts and then forward the money to the fraudsters via their choice of WebMoney purse, Bitcoin wallet, or other payment methods.

While dating scams are typically a function of financially motivated operations, they can sometimes lead to other types of fraud or even nation-state operations. In other scenarios, the threat actor encourages the victim to download a separate app, which can then be used to deploy spyware or leak other information. In one scheme identified by Interpol in January 2021, fraudsters engaged with victims via dating apps and had conversations to build their trust. After establishing rapport, the threat actor purported to give their victims financial advice and encouraged them to download an app to "join" an investment scheme or a financial venture. Once the victim transferred funds to the app, their financial information was compromised and they were locked out of the "investment" app. In another scheme, Israeli soldiers were tricked into installing malware and spyware into their phones by Hamas operatives who posed as women in their teens and twenties. The malware-infected apps allowed the threat actors to exfiltrate photos, messages, contacts, and the geolocation of targeted soldiers giving Hamas operatives vital information on their adversary's location, operations, and structure. A similar information exfiltration attempt was identified in 2017, when the Iranian state-sponsored advanced persistent



Translated from Russian:
/ cashout dating-scam! / WU, **MG, RIA** , accounts ... At the request of clients, the calculation of payments for transfers is changed to $ 160: The minimum transfer amount is $ 50, from transfers from $ 50 to $ 160, the commission is 50%, from $ 161, the commissi on is 12.5% but not less than 80 $

Show original

Post 4 of 4 by wizardcc on Jun 02 2020, 05:00

Figure 8: wizardcc's advertisement of cashout services (Source: Recorded Future)

threat group (APT), tracked as OilRig, used a persona of a woman, named "Mia Ash," to target employees of corporations such as Deloitte in order to compromise systems and steal sensitive or proprietary information.

"Sextortion" scams are a particularly odious form of dating fraud in which individuals are convinced to send suggestive photos or are engaged in sexual activities while unknowingly being recorded. The victims are typically lured into what they believe is a quasi-sexual relationship with the threat actors posing as a romantic interest and are then convinced or coerced into providing media of a sexual nature. The threat actor then uses these photos or videos to pressure the victim into sending them money or goods in exchange for the photo or video not being released publicly. Sextortion scams are typically financially motivated, but they can also be used as blackmail to manipulate the victim into doing something against their will, such as engaging in other illegal activities. Sextortion schemes have impacted a wide range of the population, including youths, military servicemen and women, and the elderly.

Outlook and Mitigations

Dating scams have been around for decades due to their predation on universal human emotions. However, as people become more aware of these types of scams, the fraudsters behind the dating scams have developed and employed new measures to ensure that they appear authentic to the victim. The social engineering aspect is also key to ensuring the success of a dating scam, as these threat actors often prey on individuals who seek connections online or through dating apps. Victims of dating fraud are often middle-aged and may not be aware of the enhanced techniques threat actors used to fool their targets. In a 2020 report, AARP — the American Association of Retired Persons, a US-based interest group that focuses on issues affecting Americans over 50 years old — stated that dating scams were the costliest scam to people ages 60 and older. Additionally, these dating scams have seen an increase during the COVID-19 pandemic, as fraudsters prey upon people being cooped up in their homes and away from loved ones. Mitigation steps that individuals can employ include the following:

- Limit the amount of personally identifiable information on forums, social media, or dating apps. Do not accept connection requests from people who you don't know, do not reuse passwords across multiple sites, and do not download applications that have not been verified or vetted on Google Play or on the Apple App Store.
- Keep communications within the respective application as much as possible and be wary of links sent or the match wanting to move the conversation to an alternative platform.
- Research the individual that you are speaking with to see whether their images or data have appeared elsewhere, such as on other social media sites or in the news, or if they are using a generic image that has appeared in association with multiple identities. However, just because they may have an online presence does not necessarily mean that they are a legitimate individual.
- Be wary of the individual asking you for items such as financial information or compromising photos that could be later used to extort the victim.
- Be cautious if the person seems too "perfect" or if they profess their love too quickly.
- Never send money to anyone that you have only communicated with online or by phone. Additionally, never accept large sums of money from someone that you have only communicated with online.

Mitigation strategies to thwart dating scams extend beyond the user to the company's developers and security teams. Developers can aid this by performing penetration tests of the application, participating in bug bounty programs for the application and remediating identified vulnerabilities, securing data-in-transit, and minimizing the storage of sensitive data. Security teams can help to decrease the risk of fraudsters being active on their applications by enhancing protocols such as multi-factor authentication, having a repository of photos that have been known to be associated with spam or bot accounts, and using those as a check to identify whether new accounts are attempting to repurpose those photos, and ensuring that databases are properly secured to prevent data leaks.

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.