VISA

PAYMENT FRAUD DISRUPTION

BIANNUAL THREATS REPORT

JUNE 2021

Disclaimer:

This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it.

All Visa Payment Fraud Disruption Situational Intelligence Assessment content is provided for the intended recipient only, and on a need-to-know basis. PFD reporting and intelligence are intended solely for the internal use of the individual and organization to which they are addressed. Dissemination or redistribution of PFD products without express permission is strictly prohibited.

EXECUTIVE SUMMARY

THREATS LANDSCAPE UPDATE

- There was an overall **reduction of the fraud rate** in the card present channel, likely due to the restrictions put in place on brick-and-mortar merchants during the COVID-19 pandemic. As a result of these restrictions, there was less opportunity for fraudsters to target and monetize card present data.
- Actors operating **ransomware** campaigns continued to target organizations globally and exfiltrate sensitive data.
- Third-party service providers and **supply chain vendors** are increasingly targeted in fraud attacks.
- The past six-month period saw an increase in the targeting of payments ecosystem organizations with **DDoS attacks.**
- The closure of two **underground carding shops**, *Joker's Stash* and *ValidCC*, and numerous law enforcement operations, impacted cybercrime underground marketplaces.
- There was continued use of underground **card validation testers** despite the closure of the *Joker's Stash* carding shop.
- **Skimming** campaigns targeting **gas pumps** experienced a notable increase beginning in January 2021.
- Recent attacks utilizing **malicious insiders** represent continued interest by threat actors in targeting issuers for the purposes of **cashouts**.
- Throughout 2019 to 2021, Visa Risk identified **ATM cashout attacks** that resulted in fraud **decreased** at an average of 50% year-over-year.
- Fraud targeting **US pandemic-related government disbursement programs** persisted throughout 2020 and into 2021, and state unemployment insurance programs and US Small Business Administration Loan programs were **popular targets for fraudsters.**
- Continued **Lazarus** activity targeting the **cryptocurrency** ecosystem was identified.
- The past six months saw a continuation of **enumeration** targeting **third-party service providers.**
- New enumeration campaigns were detected targeting the **authentication stage** of transactions on eCommerce merchants.

FORECAST

- **Supply chain threats** will remain among the top payments ecosystem threats into the next six-month period.
- The **cybercrime underground, specifically carding communities and operations,** will likely experience a paradigm shift as a result of *Joker's Stash* closure.
- **Card present fraud** will likely increase in the short term as COVID-19 related restrictions are eased; however, Visa Risk anticipates the majority of fraud will continue to occur in the **card-not-present** space.
- **Ransomware** is again assessed to be one of the leading threats for the next six-month period.
- **Enumeration attacks** targeting third-party service providers will likely continue.

TABLE OF CONTENTS

THREATS TO DATA

RANSOMWARE

Ransomware remained a significant threat over the past six months. While ransomware is not a new threat, the exfiltration of data within ransomware attacks is a relatively new development. Increasingly, payment ecosystem entities are targeted with ransomware by financially motivated threat actors.

Ransomware attacks against payments ecosystem organizations persisted over the past six-month period. The use of ransomware to target the payments ecosystem was highlighted as a leading threat within the December 2020 Biannual Report, and this trend remained consistent as anticipated. Ransomware poses a threat to an organization's data and infrastructure; however, the recent trend of data exfiltration within ransomware attacks makes ransomware a significant threat to data.

Actors operating ransomware campaigns continued to target organizations across the globe and exfiltrate sensitive data in addition to encrypting data and systems on a victim's environment. This enabled the actors to extort the victims with the exfiltrated data to put pressure on the victims to pay the demanded ransom. Numerous ransomware operations also added a new pressure tactic: targeting victims with DDoS attacks after encrypting their systems. There are a handful of known threat actors leveraging DDoS attacks in their campaigns, these include the Avaddon, SunCrypt, and RagnarLocker groups.

Visa Risk identified numerous global ransomware attacks in the past six months against payment ecosystem organizations, including issuers, acquirers, and merchants. While ransomware actors are opportunistic and target any identified sensitive data, payment account data was targeted within many of these attacks.

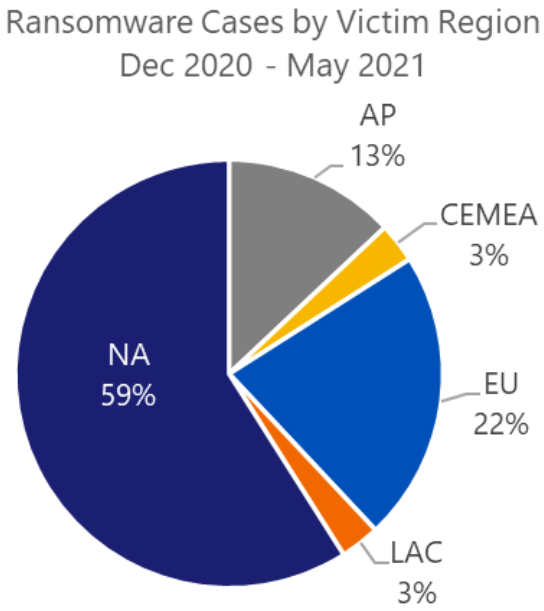

Figure 1: Ransomware Cases by Victim Region

With the increase in ransomware attacks against nearly every industry vertical, efforts to combat ransomware also increased. In a notable disruptive development, several members of the Egregor ransomware operation

were arrested. The individuals allegedly provided intrusion capabilities and financial and logistical support to the Egregor Ransomware-as-a-Service (RaaS) operation. Authorities were able to monitor the flow of bitcoin transactions conducted by the suspects, and consequently tied numerous attacks to the arrested individuals. It is also believed the individuals were involved in the now defunct Maze Ransomware group.

Ransomware operations are generally conducted via a ransomware-as-a-service (RaaS) model in which numerous vetted affiliates conduct the ransomware operations. This results in varying tactics across ransomware variants and even within the different campaigns conducted by the same variant. However, attacks will often involve numerous stages within the kill chain that include initial intrusion through exploited vulnerabilities, network reconnaissance, credential and sensitive data theft, lateral movement, and eventual deployment of the ransomware variant itself.

The tools and malware used within each stage of the kill chain varies significantly across campaigns and ransomware variants. Some of the early stage malware includes, Mimkatz, Cobalt Strike, Trickbot, Dridex, among many others.

CYBERCRIME UNDERGROUND UPDATES

The past six-month period saw numerous significant developments within the cybercrime underground. Fraudsters remain immensely active within the myriad cybercrime communities and continue to share tactics, techniques and procedures for conducting fraud and cyber threat campaigns.

CARDING SHOP JOKER'S STASH' CLOSES OPERATION

Paramount among the recent cybercrime underground developments was the closure of the leading carding shop, *Joker's Stash*. *Joker's Stash* and its operators were responsible for buying and selling compromised payment account data from nearly every large level 1 and 2 merchant compromise. The majority of this data was obtained from the compromise of the targeted merchant's point-of-sale (POS) system and resulted in track 1 and track 2 payment account data exposure. Visa Risk reported extensively on many of the POS malware variants used across these attacks.

On 15 January 2021, a post was identified on a popular cybercrime underground forum in which the *Joker's Stash* administrator claimed that the operators of the shop were retiring. Indeed, the *Joker's Stash* operators claimed that "Joker goes on a well-deserved retirement. Joker's Stash is closing." and assured readers that "WE WILL NEVER EVER OPEN AGAIN! Do NOT trust possible future imposters!". The announcement by the administrator followed the seizure of four domains belonging to the *Joker's Stash* operation in December 2020. Subsequent to the operation, the seized domains displayed a banner informing visitors that "This Site Has Been Seized" followed by images of the FBI and Interpol seals.

The closure of *Joker's Stash* marks a significant development in the underground community as *Joker's Stash* was reportedly responsible for posting over 35 million compromised card present payment accounts and 8 million card not present payment accounts in the past year alone. Despite the closure, PFD assesses that the peddling of compromised payment accounts will persist as a popular fraud tactic. There will likely be competition within the underground community to fill the void left by *Joker's Stash* closure. Visa is closely monitoring the situation and will remain vigilant in identifying any emerging carding shops that may be the successor to *Joker's Stash*.

VALIDCC CARDING SHOP SEIZED BY LAW ENFORCEMENT

In addition to the closure of *Joker's Stash*, another popular cybercrime underground carding shop, known as *ValidCC,* disclosed they were the target of a successful law enforcement operation which led to the termination of the carding shop. A representative for *ValidCC* made this announcement on 28 January 2021 and stated that the law enforcement operation resulted in the seizure of *ValidCC's* infrastructure, such as servers and database. Consequently, the *ValidCC* operators were unable to access the compromised payment account data contained within the seized database and effectively lost access to the carding shop.

ValidCC was among the leading cybercrime underground carding shops that deal in compromised card not present payment account data. The shop had thousands of users and the operators of the shop were involved in both the campaigns to compromise the payment account data through eSkimming, as well as the sale of the compromised data. Nearly 700 eSkimming attacks were attributed to ValidCC, and the threat actors behind the shop also targeted third party service providers across Europe, Asia Pacific, North America, and Latin America and the Caribbean.

CONTINUED USE OF VALIDATION TESTERS

Validation testers are used by threat actors to check that a previously compromised payment account is valid and will receive approval responses when the actor attempts to use the account for fraud. Threat actors often purchase a compromised payment account from an underground carding shop and subsequently check that payment account on one of these validation tester services. For example, an actor was previously able to purchase a payment account from *Joker's Stash* and then check the validity of that same payment account by using a tester service that was embedded on the *Joker's Stash* website.

Despite the closure of *Joker's Stash,* validation testers experienced consistent use over the past six month period. This trend indicates that threat actors within the cybercrime underground remain interested in obtaining compromised payment account data to conduct fraud. Visa Risk continues to monitor for and detect new validation services that appear on the cybercrime underground.

FRAUDSTERS TARGETING FRAUDSTERS

As discussed in detail within this report, the eSkimming threat landscape experienced a development whereby threat actors targeted the eSkimming malware deployed by other threat actors to effectively steal the payment account data from the first threat actors. In addition to this incident of threat actors targeting other threat actors, in March 2021, a cybercrime underground carding shop, *Swarmshop,* was targeted by users of the illicit website. According to researchers, *Swarmshop* is a mid-sized carding website that has been in operation since at least April 2019. The shop has around 12,000 active users.

In this attack, the threat actors obtained a *Swarmshop* database that included extensive information on the website's administrators and users, including approximately 12,000 user names/nicknames, hashed passwords, account history, and contact details. While additional cybercrime underground operations were targeted by cybercriminals, the *Swarmshop* incident was unique in that bank account details and payment account numbers were also obtained as part of the compromise.

In total, approximately 600,000 payment account numbers and associated data such as expiration date, cardholder name, and CVV2, were obtained in the compromise. Additionally, 69,592 US Social Security and Canadian Social Insurance numbers, and 498 online banking credentials for various global institutions were acquired. The data was posted by the threat actors to another cybercrime underground forum and was easily accessible for users of this forum.

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a scam in which a fraudster impersonates high-level executives or a trusted party through social engineering or computer intrusion techniques to convince employees to conduct unauthorized transfers of funds or release sensitive information.

There was a 69% increase in reported Business Email Compromise scams from 2019-2020, according to an FBI report released this past quarter. Total reported cybercrime losses now exceed $4.1 billion, with BEC scams accounting for $1.8 billion of the losses.

BEC schemes have evolved over the years. Fraudsters used to spoof email accounts of chief executive officers or chief financial officers and request wire payments. Malicious actors then began to compromise personal and vendor email accounts and send fraudulent messages from these legitimate accounts, making the scams much more difficult to detect. The scams continued to evolve to include requests for W-2 tax information, gift cards, and personal data.

According to the FBI, BEC actors have increased their use of tech support and romance scams over the past year. In Tech Support scams, fraudsters impersonate IT professionals and offer to help targets resolve issues such as a compromised bank account or virus on a computer. In romance scams, the fraudsters often try to exploit users of online dating apps and trick users into sending money.

The recent increase in BEC scams has been fueled in part by the COVID-19 pandemic. Cybercriminals have exploited government stimulus packages, financial aid programs, unemployment insurance, and small business loans to lure victims into making fraudulent payments or sharing sensitive information in these scams.

GAS PUMP SKIMMING

Skimming campaigns targeting gas pumps experienced a notable increase beginning in January 2021. In these attacks, threat actors place a removable device on the point-of-sale at gas pumps to harvest the magstripe track data from payment accounts that are used at the targeted pumps. Gas pump skimming is certainly not a new threat. **However, throughout the course of the pandemic, Automated Fuel Dispenser (AFD) skimming campaigns experienced a decline in frequency.**

The recent lifting of Covid-19 related restrictions led to increased travel and in-person activities, which in turn increased the frequency at which consumers visited gas pumps. Throughout the COVID-19 pandemic, MCC 5542 (Gas Pumps) experienced a steady decrease in payment volume. Beginning in March 2021, however, the volume increased by an average of 20% as compared to the previous monthly averages. Thus, the payment volume at gas pumps re-emerged as an attractive target for threat actors. Notably, there was also an increase in reports of skimming devices placed on the point-of-sale terminals that were located inside of the gas stations.

Many automated fuel dispenser (AFD) merchants implemented secure acceptance technologies both in-store and at the pump due to the April 2021 EMV liability shift for AFD merchants. While this resulted in more secure payments at gas pumps, many AFD merchants have not fully integrated EMV acceptance due to a myriad of reasons. However, the liability shift has now passed and the percentage of stations with EMV acceptance continues to increase.

NOTABLE CYBER THREAT ACTOR: TA505

TA505 continued to distribute its proprietary Get2 Loader during January 2021, updating and introducing new techniques in their spam campaigns. In February 2021, TA505 named 10 new, predominantly North America-based victims to their "Clop Leaks" data leak site.

A number of these victims publicly disclosed breaches related to the exploitation of multiple vulnerabilities present in a large US software company's file sharing service. TA505 has previously contacted executives, partners, and customers of their victims; however, in the case of these newly named victims, the Clop ransomware does not appear to have been deployed. The adversary has more recently focused on big game hunting operations and the deployment of Get2 Loader and SDbot; FlawedGrace activity has been observed less frequently, though it appears the adversary continues to maintain their full toolset despite its reduced use of some tools.

PANDEMIC-RELATED GOVERNMENT DISBURSEMENT FRAUD

Fraud targeting US pandemic-related government disbursement programs persisted throughout 2020 and into 2021, and state unemployment insurance programs and US Small Business Administration Loan programs continued to be popular targets for fraudsters.

In December 2020, the US Internal Revenue Service announced that a second round of stimulus fund disbursements and Congress later authorized an extension of the Pandemic Unemployment Assistance (PUA) program, supplying additional federal unemployment insurance benefits to be added to state unemployment claims through early September 2021. Additionally, US$284B was allotted for a second round of the SBA Paycheck Protection Program (PPP2) along with a US$20M injection into the SBA's Economic Injury Disaster Loan Program (EDIL) to assist small businesses.

In December 2020, threat actor discussions focusing on strategies used to target pandemic-related stimulus programs were identified. Fraudsters were keeping updated on changes to states' application systems and processes, including the implementation by states of identification verification services, which proved a hindrance for some fraudsters in their criminal efforts. Some underground discussions specifically detailed which states implemented identity verification checks and tactics, techniques and procedures (TTPs) to circumvent or defeat verification checks. Nevertheless, it does appear that states' implementation of additional identification verification measures created a level of meaningful obstacles for fraudsters.

64% of claims in Maryland from Jan – Feb 2021 were flagged as potentially fraudulent by the state.

In 2020 and 2021, numerous cases of pandemic-related disbursement fraud targeting funds distributed by the state of Maryland were investigated.

February 2021, a phishing scheme targeting business owners in an attempt to steal the personal and business information needed to apply for a U.S. Small Business Administration (SBA) loan was identified. Fraudsters used an email phishing scam posing as an executive from an SBA participating financial institution and send unsuspecting business owners an email with an invitation to register for the new round of PPP funds. Subsequently, in March, the US Department of Justice issued a warning regarding fake unemployment benefit websites created by fraudsters to harvest personally identifiable information (PII) of unsuspecting victims, whereby victims are lured through phishing and smishing (text message) links from fraudsters posing as the state workforce agency (SWA).

CARD PRESENT THREATS

The Covid-19 pandemic had a fundamental impact on the payments ecosystem, with a particular impact on brick-and-mortar merchants. Restrictions put in place around the globe on in-person gatherings, travel, and hospitality services reduced the payment volume within the card present channel. As a result, many of the threats throughout the past six months targeted the card-not-present, eCommerce channel, as discussed throughout this report. However, as more of the population becomes vaccinated, restrictions are increasingly lifted around brick-and-mortar commerce and threat actors are increasingly targeting the card present channel. While the threat to eCommerce remains higher than that to brick-and-mortar commerce and will likely remain so due to increased secure acceptance technology, threat actors have conducted notable campaigns against the card present channel in the past six months.

DEVELOPMENTS IN ESKIMMING

eCommerce continues to experience significant increases in payment volume and, as a result, threat actors continue to target eCommerce merchants with eSkimming malware to capitalize on the amount of payment data that flows through the eCommerce channel.

While the increase in eCommerce and threat actor targeting of this channel is not a new development, the COVID-19 pandemic accelerated the shift to eCommerce, both from a legitimate payment volume and threat actor targeting perspective, and this trend persisted over the past six month period. In fact, approximately 70% of at-risk payment accounts over this period were comprised of card-not-present data, as compared to 30% for card present data.

Visa Risk reported on numerous new and novel techniques that threat actors employed over this period to target eCommerce merchants and customer's payment account data entered into checkout forms on the merchant websites. The most notable of these developments are as follows:

WEB SHELLS

Beginning in 2020, threat actors increasingly utilized web shells to facilitate eSkimming attacks against eCommerce merchants. Web shells are tools used by threat actors to establish and maintain access to compromised servers, deploy additional malicious files/payloads, facilitate lateral movement within a victims' network, and remotely execute commands. Actors employ numerous methods to deploy web shells, but often use application plugins and PHP code. In many of the identified eSkimming attacks, the web shells were used to

establish a command and control (C2) infrastructure, which was used in the targeting of payment accounts. Throughout 2020, at least 45 eSkimming attacks using web shells were identified, and this trend persisted into 2021 and appears to be increasing. Thus, the use of web shells is assessed to be a new common tactic employed by eSkimming threat actors.

The most common tactics used by threat actors to deploy these web shells include:

a) Vulnerabilities in unsecured administrative infrastructure

This primarily included accesses that were not password protected, unsecured credentials, or weak, easy to guess passwords that were easily cracked by threat actors.

b) eCommerce-related application/website plugins

Threat actors often injected the malicious code or exploited vulnerabilities in plugins or other applications that were integrated into a merchant's eCommerce environment.

c) Outdated/unpatched eCommerce platforms

Merchants running outdated or unpatched eCommerce platforms were often targeted with eSkimming attacks that exploited vulnerabilities in the platforms.

NEW ESKIMMING TACTICS EMPLOYED BY THREAT ACTORS

Targeting vulnerabilities in popular eCommerce platforms remained an attractive and effective method employed by threat actors to target card not present payment account data. For example, the end-of-life for Magento version 1, which effectively ended support for one of the leading eCommerce platforms, occurred in June 2020. Visa Risk consequently reported on the risks of running this, or any other unsupported, outdated platform. Threat actors were quick to exploit these vulnerabilities and there were numerous attacks against merchants running Magento version 1 after the platform reached its end-of-life.

This trend persisted into the first six months of 2021. In one such attack, threat actors again exploited the Magento 1 vulnerabilities to inject malicious eSkimming code onto a merchant's website, and a second eSkimmer was then injected on top of the first. As researchers noted, this in of itself is not unique, however the second eSkimmer targeted the fake payment page created by the first eSkimmer; effectively stealing the payment data from the threat actors who deployed the first eSkimmer.

The actors responsible for the second eSkimmer deliberately scanned for eCommerce sites that were already infected with eSkimmers exploiting Magento Version 1, and would then inject their own script to steal the data from the first threat actors. This attack highlights threat actor's continued innovation in the eSkimming threat landscape, but also further exemplifies the dangers of running outdated and unpatched software, such as Magento Version 1, on an eCommerce environment.

Threat actors further innovated by using techniques such as publicly available jpeg files to exfiltrate payment account data from an infected merchant website. In March 2021, researchers detected this new eSkimming variant which infects the Magento PHP source code to steal customer data and store it encoded in an image hosted on the victim's own website. In previous eSkimming attacks, attackers sent data hidden in image files and stored stolen data in files on the victim's server, however, this variant uniquely combines the two techniques. The attacker can then retrieve the stolen data while disguising the action as an innocuous image request.

Additionally, an eSkimming campaign utilized the popular, privacy-focused chat application Telegram to operate as a command and control (C2) within eSkimming attacks. Telegram was previously utilized by threat actors in eSkimming campaigns, and the recent activity confirms that the tactic is still being used. The use of Telegram enables the threat actors to easily access the C2 infrastructure and exfiltrate data using numerous types of internet connected devices, facilitates persistence and avoids detection as Telegram is often allowed by enterprise anti-virus solutions, and provides for anonymity as little personally identifiable information (PII) is required to use Telegram. As such, Telegram offers an attractive solution for C2 infrastructure for eSkimming threat actors.

ENUMERATION

CONTINUATION OF ENUMERATION TARGETING THIRD-PARTY SERVICE PROVIDERS

Visa Risk identified the recurrence of a previously identified trend whereby threat actors conduct enumeration activity on eCommerce merchant sites using third-party service providers. Enumeration is the scalable and programmatic automated testing of common payment fields via eCommerce transactions to effectively guess the full payment account number, CVV2, and/or expiration date. In this campaign, the actors target various merchant verticals and specifically exploit third-party platforms/services to target the merchants that utilize the platform/service.

In February and March 2021, a new enumeration campaign targeting flower shops/florist merchants was identified. In this campaign, the merchants shared a common third-party service provider that supplied web design and other digital marketing services. The enumeration activity impacted 33 flower shop/florist merchants and involved over 2,500 enumerated transactions per merchant. Threat actors primarily targeted US issuers in this campaign, but the incident impacted issuers globally.

In a previously reported campaign, threat actors targeted at least 4 merchant verticals, in multiple global regions. The attack began in early August and persisted through November 2020.

This recent enumeration activity reaffirms the continuation of the trend whereby threat actors carrying out enumeration attacks are increasingly targeting merchant service providers. The targeting of service providers is a tactic identified in other threat vectors, such as eSkimming, and enables the actors to target numerous entities by exploiting the use of a common third-party. It is assessed that the service provider enumeration attacks are attributable to the same actors/group(s), given the commonalities in tactics, techniques and procedures (TTPs).

ENUMERATION TARGETING AUTHENTICATION STAGE

In March 2021, Visa Risk identified an enumeration campaign targeting the authentication stage of transactions on eCommerce merchants. This is a notable development in enumeration tactics, as most enumeration prior to this campaign was conducted in the authorization stream.

In the authentication enumeration attacks, fraudsters identify a merchant that does not have adequate security controls, such as CAPTCHA, on their website. This enables the fraudsters to automate authentication attempts on targeted ISO BINs and iterate through the PAN values for that ISO BIN. Visa Risk assesses that the actors are monitoring for a "challenge screen" during the checkout process, which provides sufficient evidence that the PAN is valid. The challenge is generally provided by the issuer via an iframe onto the merchant website.

Therefore, if the actors are indeed automating this attack, it is likely they are monitoring the network traffic on the website for indication that this iframe and associated challenge screen are requested.

The merchants targeted in these attacks did not have adequate security controls, such as CAPTCHA, which rendered the authentication service as implemented by the merchants vulnerable to these attacks.

THREATS TO INFRASTRUCTURE

SUPPLY CHAIN THREATS

Ransomware attacks and data breaches of supply chain vendors increased over the past period and sufficient protection of third-party service providers and supply chain vendors is increasingly critical. In December 2020, security researchers reported on an eSkimming campaign targeting some of the leading eCommerce hosting providers and platforms. The skimmer utilized in this campaign harvests payment account data by injecting a malicious checkout page during the checkout process on eCommerce merchant websites that utilize the service provider solutions. Third-party services have included marketing services, reservation facilitation, online and mobile order facilitation, and content management systems (CMS) for eCommerce websites.

The targeting of third-party service providers is also a tactic that was recently identified within payment account enumeration campaigns, and the recent attacks against the service provider SolarWinds further exemplifies threat actor interest in and success with the targeting of supply chains.

In January 2021, a large US software company disclosed that multiple vulnerabilities in its file-sharing service was exploited by malicious actors. The service is a technology that enterprises worldwide have used to transfer large files. As a result, the malicious actors were able to steal data from the service's customers and subsequently used the stolen data as leverage in extortion attempts. Specifically, the actors threatened to publish the data if victims did not pay a ransom. As usual in recent extortion attempts, the threat actors selectively leaked a sample of data to pressure victims into paying up. The campaign was attributed to cybercrime actors affiliated with the notorious eCrime group known as GRACEFUL SPIDER (aka Clop ransomware team). According to reports, the actors stole data from dozens of companies and government organizations.

The impact of ransomware and network intrusion incidents on supply chain entities, such as the Solar Winds events, illustrates the increasing difficulty of protecting against these threats, as organizations must now also consider not only the security of their network and operations but also the security of their supply chain and vendors.

INSIDER THREATS

In early 2021, issuing banks were increasingly targeted with cashout attacks in which threat actors conducted fraudulent point-of-sale (POS) transactions and ATM withdrawals. **To carry out these attacks, the actors enlisted the assistance of malicious employees that had privileged access at the targeted issuer.** The employees used their privileges to effectively increase the limits on a select number of payment accounts, which were subsequently used for fraudulent cross-border POS and ATM transactions.

The majority of the fraudulent transaction activity occurred within the POS channel, which is a departure from previous insider cashout attacks in which ATMs were predominantly targeted. In addition to this most recent malicious insider attack, Visa Risk previously identified similar insider threat ATM cashout attacks conducted in 2017 and 2020.

The recent attacks utilizing malicious insiders represents continued interest by threat actors in targeting issuers for the purposes of cashouts, targeting both the ATM and POS channels to conduct the fraudulent transactions.

ATM CASHOUTS

ATM cashout attacks are historically one of the top threats within the payments ecosystem. In these attacks, threat actors typically target an issuing bank with malware to either increase limits on issued payment accounts or affect the transaction message from the issuer's payment switch application to approve fraudulent ATM withdrawals. ATM cashouts are potentially immensely profitable as exemplified by the most prolific and successful of the ATM cashout groups, the North Korean-backed FASTCash. Additional advanced persistent threat groups conducting ATM cashout attacks include Silence and Cobalt, both of which carried out numerous successful attacks with diverging TTPs.

Beginning in 2019, **the frequency of ATM cashout attacks significantly declined**. Indeed, throughout 2019 to 2021, identified ATM cashout attacks that resulted in fraud **decreased year-over-year**.

FIN7 POS malware is generally delivered via phishing campaigns sometimes accompanied by social engineering phone calls. Malicious attachments deploy a variant of the Carbanak malware combined with other tools aimed at stealing payment card data from the victim's POS system.

LAW ENFORCEMENT UPDATE

There were notable and impactful law enforcement actions against eCrime groups and operations in the first few months of 2021. Three prominent malware operations— Emotet, Netwalker, and Egregor—were disrupted by authorities.

MAJOR INTERNATIONAL DEBIT FRAUD RING HALTED

Following an 18-month multiagency international investigation, US and European authorities arrested 105 suspects in major payment card fraud enforcement operation in the US and Western Europe from October 2020 through February 2021. In April 2019, US Law Enforcement identified an international organized crime group perpetrating large-scale debit card fraud against North American and European issuers, which involved cross-border transactions at collusive merchants.

To conduct the scam, the suspects created shell companies and opened accounts for these companies at various US-based financial institutions. Transfers were made into the shell company accounts from locations in Europe, which initiated credit and debit cards to be issued for the accounts. Criminals then monetized the maximum credited amount on the cards at collusive merchants, mostly in Spain. After monetizing the stolen funds, the suspects abandoned the shell company accounts and transferred the monetized funds into bank accounts owned by other members of the crime group in an attempt to launder the funds.

ARREST OF ENUMERATION ATTACK HACKER IN SPAIN

Authorities in Madrid have arrested the prime suspect in the November 2019 network intrusion and significant enumeration attack against a large online merchant operating in Spain. In this attack, a popular media-based merchant in Spain experienced a high-volume enumeration attack in which the threat actors used the registration process for new accounts on the merchant to enumerate payment accounts. The majority of the attack targeted payment accounts issued by Spanish financial institutions. Subsequent to this attack in Spain, the actors attempted another enumeration attack against the same merchants' U.S. website. The actors also targeted the same payment accounts from the Spanish financial institutions in this U.S.-based attack.

FIN7 ARRESTS: CASE UPDATES

In the past six months, two high-ranking members of the notorious hacking group, FIN7, were sentenced to federal prison by the US Department of Justice, and two other FIN7 members currently in custody await continuation of their cases.

FIN7 is a financially-motivated group that often targets merchant point-of-sale (POS) systems to harvest track 1 and track 2 payment account data and subsequently sell the compromised data in the cybercrime underground. The group is estimated to employ more than 70 individuals organized into separate units responsible for malware development, phishing campaigns, and network intrusions. Estimates suggest the group generates US$50M per month through its illicit activities and is ultimately responsible for billions of dollars in damage to US companies and individual victims. FIN7 favors targets in the hospitality, restaurant, and gaming industries and has victims across the US, having allegedly stolen over 20 million payment cards from more than 3,600 businesses since 2015.

Figure 2 depicts business locations that were compromised and had customer payment card data stolen.

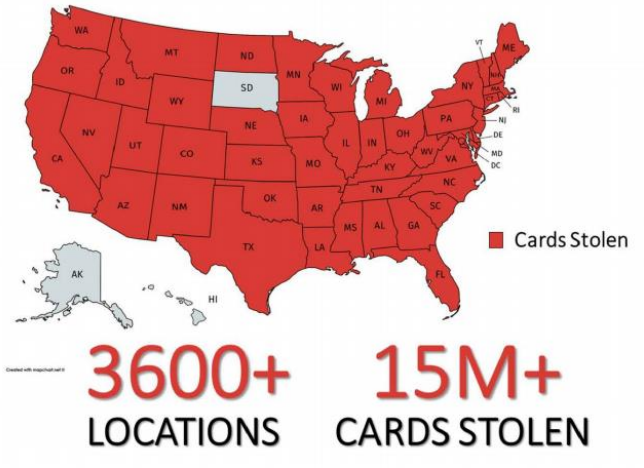

Figure 2: FIN7 U.S. Nationwide Impact
(Image Source: US Department of Justice)

FIN7 POS malware is generally delivered via phishing campaigns sometimes accompanied by social engineering phone calls. Malicious attachments deploy a variant of the Carbanak malware combined with other tools aimed at stealing payment card data from the victim's POS system.

Fedir Hladyn, a FIN7 Systems Administrator, pleaded guilty to 1 count of Conspiracy to Commit Wire Fraud and 1 count of Conspiracy to Commit Computer Hacking, and was sentenced on 16 April, 2021 to 10 years in prison and US$2.5M in restitution. In his plea agreement, he admitted his responsibilities included coordinating activities among separate business units, supervising hackers, maintaining FIN7's servers, and aggregating stolen payment card data, among other tasks.

Andrii Kolpakov, a FIN7 pen-tester, pleaded guilty in November 2020 to 1 count of Conspiracy to Commit Wire Fraud and 1 count of Conspiracy to Commit Computer Hacking, was sentenced on 25 June, 2021 to 7 years in prison and US$2.5M in restitution.

The trial of Denys Iarmak, another FIN7 pen-tester, indicted on 1 count of Conspiracy to Commit Wire Fraud, 14 counts of Wire Fraud, and 1 count of Conspiracy to Commit Computer Hacking, is scheduled to continue on 12 September 2022.

Dmytro Federov, a FIN7 pen-tester, also indicted on 1 count of Conspiracy to Commit Wire Fraud, 14 counts of Wire Fraud, and 1 count of Conspiracy to Commit Computer Hacking, awaits continuation of his case.

The US Department of Justice continues to coordinate with government and law enforcement agencies internationally to pursue cybercriminals impacting business and consumers through malware, ransomware, hacking, and other fraud schemes.

COORDINATED LAW ENFORCEMENT TAKEDOWN OF EMOTET INFRASTRUCTURE

In January 2021, authorities seized the botnet infrastructure supporting the *Emotet* malware and cybercrime service. The seizure came as the result of a collaborative effort between law enforcement agencies in a number of countries worldwide.

Emotet, which began in 2014 as a banking trojan, evolved into a loader service that was used to establish access that would then distribute additional malware, such as Trickbot. *Emotet* was distributed via a fully automated process using an infected Word document attached to an email. While the phishing lures changed over the years, the basic delivery of *Emotet* remained consistent: either an attachment to an email or download via a malicious link in the email text. Once opened, the victim would be prompted to enable macros, which would deploy the malware. *Emotet* proved a particularly tricky adversary as the malware was designed to change its code each time it was initiated, making it difficult for antivirus programs to detect the initial download. Moreover, *Emotet* was provided as a service to cybercriminals and was involved in and facilitated threat campaigns of various types and across numerous industry verticals.

The disruption of *Emotet*'s infrastructure was a long-term operation by numerous national and international law enforcement and investigative agencies, listed in the graphic below. The botnet infrastructure consisted of hundreds of servers located across the globe. Through a coordinated strategy, law enforcement gained control of the infrastructure, initiated an internal takeover, and sent infected devices a module that automatically uninstalled the malware on 25 April 2021. In addition to the infrastructure takedown, Ukrainian police arrested two suspects charged with involvement in the maintenance of the Emotet infrastructure. If found guilty, the suspects face up to 12 years in prison.

THREATS LANDSCAPE FORECAST

- Supply chain threats will remain among the top payments ecosystem threats into the next six-month period. The payments ecosystem was inundated with supply chain attacks in the previous period whereby threat actors utilized supply chains to facilitate eSkimming, ransomware campaigns, and enumeration attacks. **Supply chain attacks** are vastly popular outside of the payments ecosystem as well, as exemplified by the recent Solar Winds attack. Supply chains prove an attractive target for threat actors as the successful compromise of a third-party can enable the actor to gain access to all of the organizations that utilize the product or service provided by that third-party. Thus, the actor must only compromise one environment to effectively compromise all of the organizations that utilize that environment. Given the effectiveness of previous supply chain attacks within the payments ecosystem, supply chains are expected to remain an immensely attractive target for threat actors.

- The **cybercrime underground will likely experience a paradigm shift** as a result of *Joker's Stash* closure. *Joker's Stash* was the leading carding shop for most of its approximately seven year operation with an estimated profit of hundreds of millions of US dollars. The shop was responsible for selling the payment account data obtained from some of the largest merchant breaches within the past decade, and had a superb reputation within the cybercrime underground. As such, the closure of *Joker's Stash* has left a significant void within the cybercrime underground that will likely be attractive to enterprising cybercriminals. However, given the increase in secure acceptance technology, card present data is now less attractive to cybercriminals and **it is assessed that the next premier operation will likely involve card-not-present data obtained through eSkimming, enumeration or other tactics.**

  Card present fraud will likely increase in the short term as COVID-19 related restrictions are eased and eventually lifted. Visa Risk identified indications of this trend in the gas pump skimming activity, as well as an increase in the number of card present investigations conducted by Visa Risk over the previous period. The pandemic and its consequent restrictions expedited a shift in payment volume from card present to card-not-present. The fraud inevitably followed this shift and largely targeted the eCommerce channel throughout the course of the pandemic. However, the gradual return of card present fraud was anticipated as the pandemic entered its final stages. Visa Risk expects that while fraudsters will increasingly target card present environments as payment volume increases for brick-and-mortar merchants, fraudsters will likely continue to focus operations on card not present environments.

- **Ransomware** is assessed to be one of the leading threats for the next six-month period. As anticipated in the previous biannual report, ransomware was a top threat trend and garnered attention and participation from threat actors of every caliber, ranging from some of the most sophisticated threat actors to low-level criminals. The payments ecosystem also remained an attractive target for ransomware actors and this trend will persist into the next six months. Visa Risk is actively monitoring ransomware campaigns and developing capabilities to identify payments ecosystem victims earlier in the infection chain to prevent the eventual ransomware deployment.

- While **government disbursement** programs remain open, it is expected that threat actors will continue their attempts to perpetrate fraud against these programs until fraudsters identify that controls are in place to mitigate the most prevalent general fraud tactics.

- **Enumeration attacks** targeting third-party service providers will likely continue as fraudsters identify new vulnerabilities in other service provider verticals. Additionally, the overall number of enumerated PANs is likely to continue its moderate increasing trend as threat actors continue to evolve strategies and develop new TTPs in attempted enumeration attacks.