Cyber Crime in the Payments Industry

A Threat Research Paper from Anomali Labs

Executive Summary

The Payments industry remains a lucrative target for financially-motivated actors. Payment systems, the network of infrastructure that it relies on and the organizations that own or protect them are all at risk of being viewed for potential vectors of attack. In 2018, we have observed a shift in the types of attacks that are likely associated with an evolving technological landscape and consumer trends. There were some startling new methods of attack. One included a globally orchestrated ATM cash-out scheme totaling losses of $13 million. In another attack, the Magecart Group's digital skimming operations remained undetected on insecure webforms, stealing bulks of sensitive payment information. According to multiple security experts, both of these methods are forecasted to be replicated by other criminal groups. SWIFT-related attacks continue to be popular in very targeted and high-value fraud attempts. We observed a marked shift towards the targeting of more higher value targets and merchants. Technological trends such as the adoption of EMV (Europay, Mastercard, and Visa) in the United States have likely pushed criminals to adapt their techniques to more creatively steal digital payment card data as opposed to compromising brick-and-mortar retail shops.

Key Takeaways

- Since EMV adoption, criminals shift targeting efforts from brick-and-mortar retailers to Card Not Present (CNP) merchants.
- The global orchestration of ATM attacks and digital payments skimming on insecure webforms emerged as two new attack methods in 2018.
- Attackers increasingly exploited third-party agents such as payment processors and payment service providers in 2018.

What is the Payments Industry?

The Payments industry ecosystem encompasses all global consumer and business payment service providers. It includes purchases of goods and services using cash, cheque, debit or credit cards, and more. The four dominant industry players: Visa Inc, MasterCard, American Express and Discover Financial, command nearly three quarters of the payments industry market capitalizations. Similar to other industries the ecosystem is made up of a number of companies and suppliers as depicted by Figure 1 below.

Figure 1: Notable organizations within the payments industry sector

Trends in the Payments Industry

Understanding how the industry is evolving can help to highlight some ways in which adversaries will act. If an industry trend places limits on what was previously lucrative or leads to a new soft target, opportunistic criminals are likely to change tactics.

Overview

One of the changes to the payments industry relates to the methods in which consumers are choosing to make payments. Use of card transactions has increased over the last several years, while cash and cheque payments have declined.[1] The prevalence of E-commerce (online merchants or retailers) and emergence of M-commerce (mobile payments) has helped to accelerate this growth. For example, research from 2016 found that 74% of people in Britain were mobile payment users.[2] Chip and PIN, and EMV adoption has been a further evolution to the card industry. Since 2014, Europe has conducted widespread adoption of EMV technology. Despite the trends in Europe, there was a delay in EMV and contactless card adoption in the United States. Apple Pay helped to initiate greater contactless payment adoption in the U.S., with merchants choosing to upgrade their terminals to allow for this payment option.[3] Figure 2 represents a number of financial technologies (FinTech) that have been disrupting the payments sector. The proliferation of smartphones has meant that "mobile payment services such as Apple Pay, Android Pay, and Samsung Pay are predicted to grow rapidly."[4] "It's predicted that by 2025, 75% of all

Figure 2: Categories of FinTech Disruptive Technologies

1 https://www.bis.org/cpmi/publ/d105_uk.pdf
2 http://www.valuewalk.com/wp-content/uploads/2017/05/Payments-Industry-SLIDE-DECK-05.12.2017.pdf
3 https://www.thepaypers.com/expert-opinion/payment-trends-in-the-us-the-emv-migration-and-the-future-of-mobile-payments/771640
4 https://gomedici.com/overview-of-the-payments-industry/

transactions will be made without cash."[5]

Consequently, the introduction of disruptive technologies has widened the attack surface for criminals seeking new opportunities to profit. Disruptive technologies often enter the market with designs lacking adequate controls. This ultimately exposes consumers to security and privacy risks. Wearable technologies and the Internet of Things (IoT) are examples of an environment in which attackers have taken advantage of default security mechanisms and complacency from the consumer. Large-scale fraud is facilitated by the prevalence of personal data that criminals can exploit. These insecure technologies, combined with organisations failing to practice basic cyber hygiene, help facilitate criminal groups' desire to compromise networks and steal privileged data for subsequent sale on underground forums and marketplaces.

Cyber Crime

Worldwide ATM Cash-Out Attacks

In early August 2018, India-based Cosmos Bank's e-system was targeted in a malware attack that infected its ATM switch server, which was attributed to a suspected spearphishing email originating from the North Korean APT known as Lazarus Group.[6] In an astonishing worldwide event, within a 24-hour period, 450 cloned cards (non-EMV) were used in 28 countries to withdraw over $11.5 million. Initial reports pointed to Cosmos Bank having been afflicted by multiple malware infections; however, it was later revealed that the attackers had used a spoofed ATM Point-of-Sale (POS) switch to compromise the connection between the Central and Core Banking System. The malicious switch is believed to have been responsible for facilitating the fake transactions and unauthorized ATM withdrawals. The withdrawals totalled over 14,000 fraudulent transactions: close to 2,849 in domestic RUPAY transactions and 12,000 international Visa transactions. The switch enabled the attackers to send fake "Transaction Reply Messages" (TRE) [that enabled] withdrawals and [disabled] fraud detection measures.[7]

Several days before the Cosmos Bank attack, the FBI released a warning on a global fraud scheme called "ATM Cash-out" that posed an imminent threat to financial institutions.[8] The new highly orchestrated attack against Cosmos bank is believed to have potentially paved the way for similar attacks in the future.

EMV Adoption

The adoption of EMV globally is pushing criminals to think of new ways to make a profit. According to Visa, EMV is a standard for credit cards and payment processing that leverages an embedded chip to enable cryptographic transactions and facilitate secure storage. This cryptographic capability allows for validating transactions in a way that is nearly impossible to counterfeit with current technology. Despite this fact, adoption of this standard has not removed the possibility of credit card fraud. Instead, criminals have shifted their tactics to circumvent the latest security enhancements.

Since EMV adoption among merchants in the North American market has matured, Visa Threat Intelligence started to see an observable shift in the victim types from predominantly brick-and-mortar retailers to online, e-commerce, or Card Not Present (CNP) merchants. This shift started in late 2016 and continues to present day (YTD 2018), with only about 20% of breaches involving brick-and-mortar locations.

As payment data increasingly contains dynamic elements and is less valuable to criminals, like with EMV chip-based or Point-to-Point encrypted transactions, the prospect of criminals making money from larger merchants diminishes. This results in fewer breaches at larger merchants and more frequent breaches at smaller, likely less-protected merchants. In 2018 alone, Visa Threat Intelligence observed over half of all reported breaches worldwide (60%) involve smaller merchants.

CNP merchants are attracting cybercriminals more than ever before around the globe, accounting for more than half of all payment card breaches. However, even in light of the lower number of breaches involving brick-and-mortar locations, the source of the majority of stolen card data continues to be high volume brick-and-mortar merchants. Merchants with

5 https://gomedici.com/overview-of-the-payments-industry/
6 https://www.zdnet.com/article/how-hackers-managed-to-steal-13-5-million-in-cosmos-bank-heist/
7 https://www.securonix.com/web/wp-content/uploads/2018/08/Securonix-Threat-Research-Cosmos-Bank-Report.pdf
8 https://www.enisa.europa.eu/publications/info-notes/atm-cash-out-attacks

a higher volume of payment card transactions attract more attention from cybercriminals; however, in most cases, it requires much more skill to gain unauthorized access and remain undetected.

Attackers Select High Value Targets

Criminals are increasingly focusing on those victims that yield a higher return on investment (ROI). This is likely a reflection of past successes of reported cyber attacks and the heightened security among large retailers and other merchants. Level 1 merchants transact 6 million or more payment cards per year, where Level 2 merchants transact more than 1 million but less than 6 million per year. The graph on the right produced by Visa Threat Intelligence, shows that in 2017 and in the first half of 2018, more breaches have occurred at Level 1 Merchants.

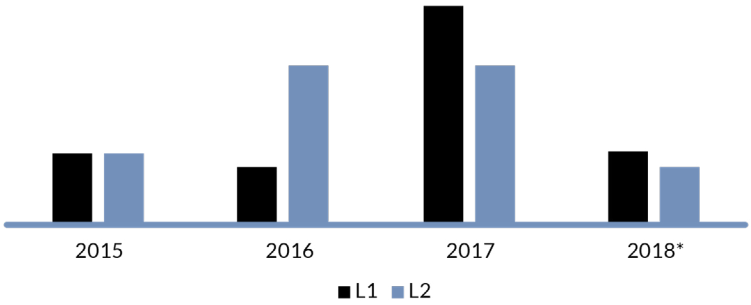

Figure 3: Level 1 and 2 Merchant Breaches

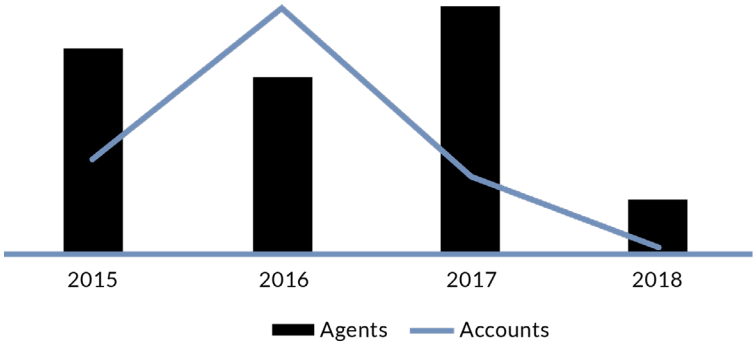

Figure 4: Involvement of Third-Party Agents

This type of behavior is exemplified in the Society for Worldwide Interbank Financial Telecommunication (SWIFT) banking network cyber attacks that have been reported over the past three years beginning in 2015. One of the most notable events took place in February 2016 where $81 million was stolen from the Bangladeshi Central Bank by abusing the SWIFT messaging system.[9] After the success of the Bangladesh Bank cyber heist, similar targeting was reported in 2016 against financial institutions such as Tien Phong Bank (Vietnam), Banco del Austro (Ecuador), Sonali Bank (Bangladesh), and an unnamed Ukrainian Bank.[10] More recently, the August 2018 Cosmos Bank hack included fraudulent SWIFT transactions close to $2 million being sent to a bank in Hong Kong.

Third-Party Agents and Trusted Partnerships are a Company's Weakness

Beginning in 2017, Visa Threat Intelligence started observing a substantial increase in targeting and breach activity involving third-party Agents such as payment processors and payment service providers. The type of attacks at payment processors commonly involve network intrusions, data theft, and manipulation of ATM withdrawal limits resulting in fraudulent withdrawal of cash by highly organized criminal organizations. In the first half of 2018, we have noticed a slight decline in the number of breaches involving processors and service providers, but it remains a major area of concern going forward.[11]

Threat Actors and Groups

The below section highlights some of the more prominent malicious actors and groups known to have targeted the payment sector:

Advanced Persistent Threat (APT)

An advanced persistent threat (APT) describes a type of cyberattack that is highly sophisticated, prolonged, and targeted, which tend to be aligned with particular nation-states, and exhibit behaviors aligned with the strategic needs of that country's government.

9 https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
10 https://www.six-group.com/interbank-clearing/dam/downloads/de/events/2017/sbof/5-Cyber-Fraud-e.pdf
11 Visa

Group Name	Description
Lazarus/Chollima/APT38	Lazarus group has been attributed to a number of high profile attacks. This group is believed to originate from North Korea, and is financially-motivated actor group. The group uses custom malware.
Anunak/Carbanak/FIN7	This financially-motivated group has been involved in numerous attacks against the financial and retail sectors. FIN7 campaigns have used malware to infect organizations for the purpose of locating Point-of-Sale systems. They will then steal payment card information which gets sold in underground forums.
Sofacy/APT28	Russian attributed APT28 has been related to planned attacks against financial institutions in the past. It remains unclear why the attacks were planned, but it is likely to support the policies and strategic vision of the Russian State. It is possible that the group may have been responding to international sanctions.

Organized Crime

A large proportion of attacks on payment systems or financial institutions are opportunistic in nature and perpetrated by cybercriminals. Organized cybercriminal groups pose a significant risk to these organizations as these groups use skilled technicians and coordinated efforts when applying their knowledge and resources to achieve their financially-motivated goals.

Group Name	Description
Dridex Group/Indirik Spider/TA505	The Dridex group operates “Dridex” one of the most prolific banking trojans from 2015. The Dridex malware has experienced multiple updates over the years. The groups campaigns have also been associated with the Necurs botnet, RockLoader, and Locky.
Magecart Group	Magecart is threat group that specializes in skimming credit card details from unsecured online payment forms.
Cobalt Gang	This group has been reported on for conducting “logical attacks” against ATMs. They are best known for a technique called “touchless jackpotting”, which is where an infection causes the ATM to empty its contents.
GCMAN Group	This threat group infects financial institutions with the goal of transferring money to digital currency.
RTM	This group has been active since at least 2015. It targets customers remotely banking in Russia and the surrounding region.
FIN5, FIN8, FIN6, FIN10	The groups that fall under the FIN categories have largely targeted Point-of-Sale (POS) systems to steal sensitive information.

Hacktivism

Hacktivists tend to exhibit low-level skills and target organizations using nuisance attacks e.g. DoS, DDoS or web defacements in an opportunistic manner such as poorly-protected web servers or individual web pages to achieve a political and social objective or gain notoriety for their malicious actions. According to Zone-H, there were 235 threat actors or groups who conducted 674 defacements against bank-related organizations located in 46 different countries between January 1, 2018 to December 4, 2018.[12] Nonetheless, we have seen a marked decrease in 2018 for the number of attacks attributed to hacktivist groups against the payments industry.

The below table identifies hacktivist groups that have impacted the financial sector throughout the year.

Source	Actor/Group	Description
Zone-H	Ayyıldız Tim	A nationalistic team that originate from Turkey. They were active during 2018 in a campaign against Donald Trump due to the U.S. putting pressure on the Turkish economy. They have defaced a number of sites that are financial-based, but this does not appear to be targeted as they have defaced numerous sites in multiple industries with generic messages. The threat to the financial sector and/or payments is likely to be when it is deemed to be in defence of Turkey. Otherwise they will target easily exploitable web applications and servers.
Zone-H	EXI2T CYBER TEAM	An Indonesian team, made up of a number of actors. There are flag colors in some of the defacements, but the messaging is mostly generic security-related. This is likely to be opportunistic defacements.
Zone-H	99Syndicate	The defacements that belong to this team are also generic in nature. The language appears to be in Indonesian. Not targeted. They also appear to behave like pentesters.
Zone-H	Team PCE	“Pakistan Zindabad” is a slogan that expresses victory and patriotism in Pakistan. The actors that seem to operate under Team PCE typically deface with this slogan. They appear to have targeted lots of Indian websites, which have been reported in the news. This team appears to provide messaging that is both generic and sometimes political in nature.
Zone-H	Network Ghost Security	Opportunistic and generic
Zone-H	Typical Idiot Security	This team defaces a lot of sites, and are opportunistic. They have defaced 3,756 sites since December 2017. They behave like pentesters and do not appear to be targeting any industry in particular.
OSINT	Anonymous Greece, Anonymous Kurdistan, Greek BlackHat Community	These groups collectively targeted Turkish banks during a campaign this year.[13] They allegedly leaked sensitive information.

12 zone-h.org
13 https://medium.com/@anonopsgr/anonymous-greece-turkish-banks-and-erdogans-private-army-hacked-71ad8dff7ece

OSINT	Anonymos Catalonia	This team targeted the Bank of Spain in August 2018 with a DDoS, causing the site to become inaccessible.[14] The attack was part of #OpCatalonia.
OSINT	Anonymos	During June 2018 #OpIcarus targeted banks.[15]

Strategic Outlook

Given the continual growth of innovative and disruptive technologies being introduced in the payment sector, we expect threat actors — particularly financially-motivated groups — to evolve their tactics in order to exploit weaknesses in these technologies and their implementation while employing tried-and-true tactics such as social engineering to compromise payment systems. We assess with moderate confidence that well-orchestrated ATM cashout schemes and fraudulent SWIFT-based payment scams will continue to be more commonly used by cybercriminals.

The below represents our 2019 attack predictions for the payment sector:

- Increased attacks against online point-of-sale (e-commerce merchants), third-party Agents, ATMs, and gas pumps
- There will be a re-emergence of older fraud schemes such as fraudulent card applications and physical compromise of Point-of-Sale systems (skimming/shimming)
- Attackers will go where the market forces them. Attacking online sales with keyloggers during payment card entry is the new battleground allowing threat actors to avoid dealing with EMV transactions.
- The fluctuating international geopolitical environment will continue to draw large-scale attacks from heavily-sanctioned nations. For the most part, this will probably impact cryptocurrency exchanges.
- Hacktivists are likely to continue to pose a nuisance threat to the payments industry as they conduct annual campaigns.
- Hacktivist groups backed by a national requirement however, are likely to act as and when the context arises.

Recommendations

We encourage all organizations and more specifically institutions with retail payment systems, review the mitigation recommendations outlined in the joint Technical Alert (TA18-275A) released by the U.S. Government in early October 2018[16]. The report covers a list of key recommendations, we advise organizations follow to better protect and defend their business and customers from cyberattacks. The following represents the topical areas detailed in the report:

- Require chip and personal identification number cryptogram validation,
- Isolation of payment system infrastructure,
- Logical segregation of operating environments,
- Employ encryption of data in transit,
- Monitor for anomalous behavior as part of a layered security strategy.

Build a Cyber Threat Intelligence Program

One of the biggest challenges facing retailers, merchants and payment processors is detecting cyber threats as early as possible and taking action to defeat attacks. Threat Intelligence provides insight into malicious actors targeting your sector, geography, community, etc. Organizations are turning to Threat Intelligence to understand their adversaries, learn how to detect when they are being targeted, and combat threats efficiently.

Anomali provides a powerful Threat Platform that integrates threat intelligence from myriad sources,

14 https://www.hackread.com/ddos-attack-anonymous-catalonia-cripples-bank-of-spain-website/
15 https://blogs.akamai.com/sitr/2018/06/operation-opicarus2018.html
16 https://www.us-cert.gov/ncas/alerts/TA18-275A

including public and private providers and premium third party research organizations. Organizations can quickly access intelligence from any source via the Anomali APP Store, a marketplace for threat intelligence. This store includes retail-specific threat feeds, including Visa Threat Intelligence, a suite of intelligence "derived from Visa investigations and forensic reports covering breaches in the global payments ecosystem." Anomali operationalizes intelligence, automating the detection of serious threats targeting the network. Learn more at www.anomali.com.

Join an Information Sharing and Analysis Centers (ISACs)

The dynamic nature of the threat landscape requires businesses to share information about the latest business and security risks to stay ahead of latest business and security risks impacting their organization and industry. By joining a sector-specific Information Sharing and Analysis Center (ISAC), Information Sharing and Analysis Organization (ISAO), or sharing community, businesses of all sizes obtain a wider view of the threat landscape enabling them to build stronger protection, detection, and response capabilities.

Anomali encourages all organizations interested in joining or wanting to build a trusted community using our technology to visit our ISAC webpage. For businesses operating in or supporting the financial and retail sectors, we recommend considering membership in the Financial Services Information Sharing and Analysis Center (FS-ISAC) and Retail ISAC (R-CISC).