CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

MARCH 2019

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #3

The Cyber Threat Landscape: Confronting Challenges to the Financial System

Adrian Nish and Saher Naumaan

The Cyber Threat Landscape: Confronting Challenges to the Financial System

Adrian Nish and Saher Naumaan

For your convenience, this document contains hyperlinked source notes indicated by this teal colored text.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Tim Maurer, Co-director of the Cyber Policy Initiative, at tmaurer@ceip.org.

Papers in this Series:

- "The Cyber Threat Landscape: Confronting Challenges to the Financial System"
  Adrian Nish and Saher Naumaan, March 2019

- "Protecting Financial Institutions Against Cyber Threats: A National Security Issue"
  Erica D. Borghard, September 2018

- "Toward a Global Norm Against Manipulating the Integrity of Financial Data"
  Tim Maurer, Ariel (Eli) Levite, and George Perkovich, March 2017

About the Authors

Adrian Nish is the head of Threat Intelligence and Response at BAE Systems' Applied Intelligence business unit. His team investigates and tracks high-end cyber threat activity for corporate and government customers around the world. Nish is a renowned expert on nation-state threats to the financial system, with firsthand experience investigating cases of complex intrusions and manipulation of payment systems. He is an associate fellow at the London-based think tank Royal United Services Institute, and holds a PhD in physics from the University of Oxford.

Saher Naumaan is a threat intelligence analyst at BAE Systems' Applied Intelligence. Her current research is on state-sponsored cyber espionage with a focus on threat groups and activity in the Middle East. Naumaan specializes in analysis covering the intersection of geopolitics and cybersecurity, and regularly speaks at events and conferences around the world. Prior to working at Applied Intelligence, she graduated from King's College London with a master's degree in intelligence and security, where she received the Barrie Paskins Award for Best MA Dissertation in war studies.

Introduction

On July 20, 2016, cyber attackers attempted to steal $150 million from the accounts of a bank in South Asia. Minutes later, the same thing happened to a bank in West Africa—attackers used the bank's own systems to send payment instructions to transfer $150 million to the attackers' chosen accounts. Counterparty banks spotted both sets of fraudulent messages and raised the alarm, ensuring that no funds were lost. However, the episode signaled a change in the threat facing financial systems today: not only could attackers conduct complex intrusions and manipulate payment systems within a single target bank, but they also could strike institutions on different continents simultaneously, while operating safely from the other side of the world. The threat of coordinated attacks against multiple parts of the financial system was no longer purely theoretical; malicious actors had demonstrated that they could do so, and the potential for systemic impacts was clear.

In the years since the July 2016 financial hacks, attackers have not made a habit of disrupting or manipulating the foundations of the financial system, and there has been no direct evidence of escalation. However, plenty of examples of continued attacks and other issues have increased the general cause for concern. Three long-term trends in particular emerge from this analysis and overall evolution of the threat landscape:

1. Attackers are increasingly building **advanced capabilities** to target **core banking** systems, particularly around payment messaging and transaction authorization. Once these tools are built, attackers will use them for as long as they remain effective. As security is tightened around certain technologies, such as SWIFT (an international financial communications network), they will look for and develop other routes to cash out.
2. Attackers are becoming more aggressive in disrupting their victims' **ability to respond**. In 2011 and 2012, attackers staged distributed denial-of-service (DDOS) attacks against U.S. banks to disrupt banking services. Though these attacks were basic and caused minimal long-term damage, the impact to the financial system was visible. Years later, the approach in the Bangladesh Bank case involved attempting to subtly hide the evidence, the equivalent of deleting security camera footage in the real world. In 2018, attackers used wiper malware across a bank's information technology systems to perform the cyber equivalent of setting the bank on fire as part of the getaway. Unfortunately, these tactics seem to work, and so attackers are likely to return to them. Where self-propagating destructive malware is used, the risk of spreading from one victim bank to others is very real.
3. Attackers continue to find ways to **collaborate**, bridging organized criminal gang activity **across multiple geographies**. Online criminal marketplaces offer tools and also services to facilitate cashing-out and money laundering. These are components of modern criminal enterprises, but the siloed nature of cyber operations and financial crime prevention make it

challenging for banks to tackle these problems. The regulatory and law enforcement communities face similar challenges, compounded by the difficulty of pursuing cross-border crime.

This assessment reviews the current cyber threat to the financial system, using real-world examples from financially motivated attackers, and provides lessons to help improve sector-wide resilience and security.

The Current Situation

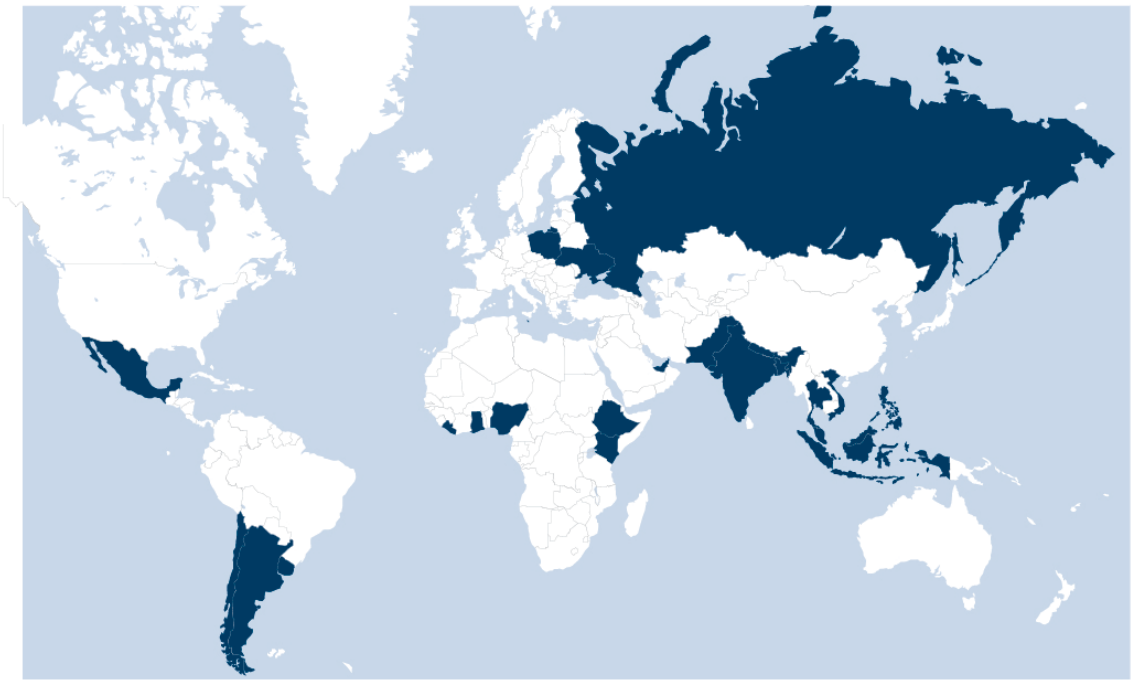
In the past decade, the capability and motivation of threats to the financial sector have transformed from small-scale opportunistic crimes to efforts to compromise entire networks and payment systems. Most of the earlier attacks took advantage of low-hanging fruit, such as weak defenses and existing vulnerabilities, and did not require many resources. As hacking tools became more readily available and the services providing them became commercialized, teams of financial attackers formed and developed their own kits, and some offered their services for hire. Today, targeted intrusions have become the norm. Security vendors have raised awareness of the threat by publicizing information about high-end campaigns, but this publicity has also spread the knowledge of how to build advanced tools and operate covertly. Proliferation-through-publication has given everyone, from the hobby hacker up to nation-state agencies, more information to develop and conduct their attacks.

Currently, the cyber threat from malicious actors looms large over the financial sector (see figure 1). Examples of recent successful attacks include the April 2018 attack against Mexico's domestic interbank payment network SPEI, in which $15 million was stolen from multiple financial institutions, and the May 2018 attack on Banco de Chile, which lost $10 million through international payment transfers. The Banco de Chile attackers also created a smokescreen for their activity by deploying wiper malware that destroyed several thousand systems on the bank's network and left banking operations unavailable for several days. In late 2018, there were further attacks—Cosmos Bank in India, Bank Islami in Pakistan, and Redbanc in Chile all suffered similar intrusions and impacts on their business operations. In February 2019, attackers compromised the payments systems of a Maltese bank and attempted to transfer €13 million from it.

The pattern of targeted institutions shows that this is mostly a problem for central and commercial banks in developing nations. Financial organizations in Latin America, Asia, and Africa have less mature cybersecurity than their counterparts in wealthier parts of the world, and attackers know this. Attacking a big Western bank with advanced security and intelligence teams is likely to end in

exposure and unwanted attention from law enforcement. A stolen $1 million from a victim with poor security is worth just as much as $1 million from a top-tier investment bank, a beneficial risk-versus-reward situation that is evident to potential criminals.

FIGURE 1
Geolocations of Payment System Attacks, 2016–2018



However, Western financial institutions are vulnerable in their own ways, though many of the problems and incidents that they have experienced have been of their own making. In April 2018, Britain's TSB suffered a computer system meltdown as the bank attempted to migrate customer records to a new system. The issue took over a month to resolve and was estimated to have cost the bank $300 million. Two months later, Visa cardholders in Europe experienced service disruptions following a hardware failure that left them unable to carry out chip-and-PIN transactions for a few hours. Given the declining use of cash by many consumers, this system failure significantly disrupted transactions for many individuals and businesses. Legacy infrastructure is not just a problem for the financial industry; incidents with failing systems and botched upgrades have similarly disrupted transport sector firms as well as telecommunications companies. However, downtime that impacts people's access to bank accounts and other funds has caught the eye of policymakers, and as a result the regulators are looking more closely at the sector's cyber resilience.

Analysis of Key Challenges

Banks have always been prime targets for attackers, and they have always understood the need for security to protect assets such as cash and customer information. In response attackers have taken advantage of technological enablers (connectivity, complexity) and have developed new tools and techniques (capabilities) to conduct their attacks. These three key factors, and their importance to the threat landscape, present critical challenges for the sector in the battle to combat the threat.

Connectivity

The rise of the internet has brought a huge increase in connectivity for financial institutions. Faster information flows can improve the sector's efficiency but also create new channels that can serve as vectors for attack. A typical bank will have a large number of systems that are connected to the internet in order to allow it to fulfill business functions, and yet its systems also serve internal users who are checking email, browsing websites, and accessing other online services. This vital connectivity can make financial institutions vulnerable to cyber attacks.

Globalization has also connected more financial institutions through the SWIFT network. The economic development benefits of access to correspondent banking are significant, not least because that access enables businesses to trade with suppliers and customers in other countries using common currency, such as U.S. dollars. However, such a system is attractive to criminals, as money can be moved from fraud perpetrated in one jurisdiction to another. Strong recommended controls exist to prevent fraudulent activity, both in terms of cybersecurity around payment system interfaces and anti–money laundering regulations, but the adoption of best practices has not spread as fast across the globe as connectivity itself, leading to opportunities where the system's weaker members can be exploited.

Complexity

The increasing connectivity that has been seen over recent decades has led to an increase in complexity of networks and system interfaces, which in turn has dramatically increased the challenge of network defense. For example, greater requirements for logging activity creates a need for improved storage and monitoring. Organizations then must consider how to respond to incidents, which may require a variety of tools and skill sets to conduct analysis. Top-tier banks spend hundreds of millions of dollars every year to secure and safeguard their systems. Smaller financial institutions, however, may suffer from a form of "cyber poverty," where they lack the resources to maintain the same level of confidence in their security. This gap between leaders and the broader community expands each year, raising the potential that a successful attack on weaker members could have systemic risk implications for all.

Capabilities

Attackers have improved in terms of capabilities. The prototypical modern criminal gang is a cyber crime gang. Although the resulting fall-off in bank robberies and other armed crime, with its corresponding decrease in physical violence, is to be welcomed, the potential for large-scale losses through cyber attacks continues to increase. These risks have grown as tools and information about bank systems have become more available to anyone who can pay for them. A manual on automated teller machine (ATM) security might be available for a small fraction of a bitcoin on hidden internet markets. Likewise, malware that can steal credit card information from the memory of point-of-sale systems, or provide remote access to systems behind enterprise firewalls and proxies, are available for a price online.

Cyber criminal gangs are more than isolated groups and individuals operating from the shadows. Some of these groups operate like businesses and actually are established as overt companies in order to secure the services of code developers that can build financial access tools, hosting services for launching attacks, and of course banking facilities to help with money laundering. They have a division of labor, with individuals specializing in particular areas, thus improving their productivity and overall proficiency.

The situation would be challenging enough for network defenders if criminals were the only figures of concern. Financial institutions also have to contend with adversarial nation-state groups. State actors have a disproportionate effect on the threat landscape, as they have the resources to invest in offensive cyber tools and techniques. Such capabilities raise the risk of misuse and the threat that these tools and techniques will leak into the public domain. Although nation-states may originally have developed their offensive capabilities for military conflict or espionage, these tools can be repurposed to attack financial systems—as was seen in the February 2016 Bangladesh Bank attack. Offensive cyber capabilities and knowledge are inherently leakier than traditional weapons, and cases such as the EternalBlue exploit, which enabled the May 2017 WannaCry worldwide ransomware attack, show how this can play out.

Looking Back to See Forward

As important as it is to recognize today's challenges, it is also vital to examine how the landscape may change to prepare for future threats. It is difficult to predict the future in a domain as dynamic as cybersecurity, but an overview of the evolution of attacks against the financial system over recent decades points to the following trends.

Attacks Against Credit Cards (Late 1990s Onwards)

Since the last 1990s, one staple tactic of cyber criminals is the theft of credit card numbers. Often the attackers will use the stolen cards to buy goods online, or they will sell or trade the cards in underground markets, which include major dumps of card data on "carding sites." Although improvements in the Payment Card Industry Data Security Standard (PCI-DSS) have mitigated older attack techniques (such as directly stealing unencrypted card numbers from insecure databases), criminals have found other approaches. The industry had a wake-up call in 2014, when Target and Home Depot fell victim to intrusions and interception of card numbers from their point-of-sales systems. Yet the breaches continue as the techniques evolve. One of the major cases in 2018 was British Airways' loss of customer payment data, captured through malicious code injected into the company's website. The code exploit allowed the attackers to intercept card numbers in plaintext as they were being entered. The card details were then discovered being sold on internet marketplaces, likely for a significant profit to the criminals. This history of attacks on payment card data shows the challenge of securing systems against innovative, motivated adversaries.

Attacks Against Online Banking Users (Mid-2000s Onwards)

When online banking became widespread in the mid-2000s, banking Trojans emerged as a tool for stealing funds from users. Simple versions would steal online banking passwords, which the criminals could later use to access accounts. As defenses advanced, so too did the malware. More capable variants would inject additional code into users' browsers, modifying the browsers to replace beneficiary details on bank transfers with the criminals' own account numbers. ZeuS and SpyEye, two popular banking Trojans from 2006 onward, were used to steal tens of millions of dollars from bank accounts globally. The malware authors were innovative not just with their tools, but also in creating business models around "malware-as-a-service." Shylock was another milestone, using techniques from multiple previous banking Trojans to create an advanced capability. Known as "hijack" by the authors, the malware forwarded live banking sessions to the attackers, who would use them to conduct bank transfers to money mule associates. As in the case of credit card data theft, the use of banking Trojans has not gone away, though it is less of a threat than it once was. Some of the criminal groups who used banking Trojans are still active, but have realized that there is greater profit to be made by attacking banks directly, rather than their customers.

Attacks Against Bank Payment and Core Banking Systems (2014 Onwards)

To be profitable, attacks against credit cards and retail banking users rely on the criminals being able to scale up their campaign. But instead of stealing small amounts from many individuals, another approach is to hack the bank itself and make a single large heist. In recent years, several groups have become proficient at doing exactly that. Such attacks require planning and preparation, social

engineering to select a target, malware to remotely control systems within a bank's network, the skills move around and avoid detection, knowledge of how to use or manipulate bank payment systems, accounts to receive the stolen funds, and someone to pick up the stolen money. Much of this is standard network intrusion technique—exactly what cyber spies do on a daily basis—and the practice has been documented extensively by the security community in blogs over recent years. However, attacker knowledge of payment and core banking systems has improved. In the 2016 Bangladesh Bank heist, the attackers not only used the local SWIFT payment interfaces but conducted a "hot patch" of the live system in order to bypass certain security features. The attackers not only recognized the need to do this (by understanding the security controls) and identified how to do it (by reverse-engineering the SWIFT software), but actually carried it out in a real attack (by building custom malware): all factors that made this attack an unprecedented escalation in the threat.

However, it is more challenging to get money out of the financial system than it is to hack individual banks; this is where most attacks fail. International transfers still require clearing before funds can be withdrawn, a twenty-four- to forty-eight-hour window that provides sufficient time in most cases for the transfers to be stopped following a heist. As the industry moves to faster payments, this time window and safety net will be removed—but for now, the attackers are looking to other means of cashing-out. One method of note is targeting payment card authorizations for ATMs within issuing banks' networks. This relies on the attacker stealing card numbers from core banking systems, creating cloned debit cards, and providing these to a string of associates to withdraw funds from ATMs around the world. When the authorization requests come back to the bank's systems, the attackers use malware to intercept and approve the fraudulent requests. Millions can be stolen in a matter of hours through coordinated schemes run across multiple countries. This happened to India's CosmosBank in August 2018, as well as in multiple other unpublicized cases recently.

Although the prospect of funds being transferred from the legitimate to the criminal economy is concerning, and the banking community should be taking this risk seriously, it is important to recognize the broader risks that come from attackers gaining knowledge of core banking systems and ways to access and manipulate these systems in the future. The threat actors conducting attacks for financial gain could be motivated to simply disrupt or otherwise cripple the financial system; they have built up capabilities that may be used for this purpose. The use of ransomware and wiper malware in cyber heists, designed to impede victim response, indicates that threat actors are not averse to causing availability impacts to conduct their attacks.

Attacks Against Interbank Networks (2018 Onwards)

Attacks on financial institutions throughout 2018 have shown multiple examples of what the next evolution in attacks could look like, and how such attacks are likely to harm financial stability. In

April 2018, Mexican authorities detected fraudulent activity on the SPEI system, the country's local intrabank payment network. This was part of a coordinated series of cyber attacks, estimated to have netted around $15 million. SPEI is similar to SWIFT in that it allows payment messages to be sent between member banks. However, it is unlike SWIFT in that it is a real-time gross settlement (RTGS) system, where funds can be withdrawn immediately or on the same day following a transfer (equivalent to Fedwire in the United States or CHAPS in the United Kingdom). As mentioned earlier, this speed is attractive to profit-driven actors, which makes RTGS systems and other interbank networks (such as those that connect ATMs) a point of significant interest to present-day attackers. In recent months, Pakistan and Chile have experienced similar incidents, with the latter's Redbanc network publicly confirming an intrusion in January 2019. The motive for these attacks is undoubtedly financial gain, but an attacker may also choose to disrupt operations as part of the getaway. Doing so on an interbank network would cause widespread outages across multiple banks, which could leave a vital part of a country's financial system offline for days—with significant impact on individuals and loss of trust in the system.

What Comes Next? A Proposal for Change

A recent joint report from BAE Systems and SWIFT looked at likely financial system targets for attackers in the coming years. It examined how cyber criminals would likely move to targeting markets and market participants. They might choose to attack foreign exchange markets, trade finance, securities and other areas, looking to make large gains in single intrusions or use persistent access to play the market over longer periods. However, just as criminals have not stopped targeting credit cards, it is unlikely that they will give up on other, still-useful approaches. All of the techniques mentioned in this paper will likely remain a threat in the years to come. Reflecting on the key challenges outlined earlier, certain steps can be taken to improve the situation going forward:

- With greater **connectivity** comes greater interdependence. To mitigate the increased risk of greater connectivity, institutions will need to embrace **collaboration**. Technological innovations may provide some level of improved collaboration; areas such as machine-readable intelligence are promising. However, there is also a need for leadership in building trust through engagement, both across teams within organizations and between organizations themselves. The financial industry has made great strides in engagement already, and many communities have emerged to share intelligence and security best practices. Such initiatives should be encouraged and expanded.

- As technology advances, **complexity** will continue to increase. This will make the job of network defense even harder in the years to come. Organizations must make a point of **simplifying security**. At a management level, this practice should entail greater transparency around what security is and is not in place, as well as the risks around specific gaps. At a

technical level, these efforts should mean that technology is secure by default, taking the burden off individuals to configure or maintain it.

- In response to **attacker capabilities**, the financial community needs to be proactive. Law enforcement, banks, and other members of the community must work together to identify the most serious threat groups and **disrupt or deter** them from attacking the financial system. This requires a shift in mindset from traditional compliance-based approaches, but a more proactive approach is vital to future network defense and should be regarded as being as important as bolstering defenses through security solutions. Policymakers should follow the trends in financial crime and learn more about how criminals are gaining greater knowledge about sensitive parts of the system each year. In the same way that techniques proliferated from high-end espionage campaigns into criminal attacks, the knowledge of how to attack and manipulate the financial system could flow in the other direction in times of conflict. Shutting down criminal activity today might help mitigate attacks from other malevolent actors in future.

Conclusion

In summary, the cyber threat to the financial system shows no signs of diminishing. If anything, recent cases demonstrate the opposite: more groups are determined to find more ways of stealing from and exploiting banks and their customers. Targeted network intrusions against banks were rare just a few years ago, but now they are happening on a weekly basis. Although these attacks have mainly impacted organizations in Asia, Africa, and Latin America, the attackers are increasing their experience and capabilities. Well-defended major banks cannot be complacent in thinking this is someone else's problem. These cases provide network defense lessons for everyone.

As discussed in the introduction, in one 2016 case, two banks were compromised and robbed on two continents simultaneously. Such coordinated heists in separate parts of the world would be much more difficult in the physical domain, but in cyberspace it is a matter of having a computer, the internet, and elite hacker skills. As access to tools and skillsets has grown, so has the threat to banks, the financial system, and the economies that rely on them. Furthermore, the growing interdependence, crossing institutions and geographies, increases the systemic risk and likelihood of significant disruption from either intentional attacks or unintended consequences.

The good news: To conduct a successful attack against the financial system requires defeating many layers of defense. So far, in most cases, the bad guys have not been able to pull off successful end-to-end attacks at will. Defenses are, to a degree, working, if only for now. The bad news: In an

increasingly connected world beset by increasing competition, confrontation, and conflict, financial organizations have many potential threats on the horizon. There is a general trend toward increased sophistication in attacks against the financial sector, and adversaries are developing capabilities that may well be used for disruptive attacks in future. However, through collaboration, clear articulation of the risks, and bold action to combat the threat actors, the financial sector can directly address the challenge of securing its networks and members in the face of targeted attacks.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org