F-Secure

CYBER THREAT LANDSCAPE FOR THE FINANCE SECTOR

July 2019

CONTENTS

EXECUTIVE SUMMARY

The finance sector is intricately woven into the daily lives of people around the world, and is at the very core of global economies. Financial entities allow citizens and organizations worldwide to manage finances, trade, and operate in different ways.

Consequently, threat actors have much to benefit from a successful cyber attack against any financial institution, and adversaries have already realized this fact – the finance industry is the most attacked sector in the EMEA region. [1]

This threat not only applies to banks, but also to exchanges, asset managers, technology providers, insurers, clearing and settlement houses, as well as supply chains to these institutions.

Both state-sponsored and criminal actors have targeted the finance sector in order to:

STEAL PERSONAL DATA

State-sponsored groups have stolen personal data in the past and used it to socially engineer individual targets, or blackmail or bribe insiders. Criminals have various ways in which they can profit from stolen personal data, such as by extorting targeted organizations, selling the data on dark web markets, committing identity fraud, or accessing customer accounts and stealing funds.

MONITOR THE FINANCIAL ACTIVITIES OF SPECIFIC CLIENTS

There is an array of motivations for governments to monitor the financial activities of certain groups and individuals. In addition, criminals may also look to track specific clients involved in significant M&A activity, in order to support insider trading schemes.

DISRUPT OR TAMPER WITH CRITICAL OPERATIONS

Politically-motivated attacks may target critical systems, such as trading computers or client portals, and sabotage them in such a way that the financial and reputational damage incurred may reach into the hundreds of millions of dollars. Highly targeted ransomware attacks are also on the rise, enabling criminals to extort larger ransoms after disrupting critical business operations.

STEAL MONEY

While North Korea is a unique case of a nation-state conducting financially-motivated attacks – many of which have been against the banking sector – the techniques used by the country's hacking units have also been adopted by organized crime groups, adding to their repertoire of ways in which to steal from banks.

Further to this, there has been a general change in the popularity of certain offensive techniques, some of which symbolize an increase in the sophistication of attacks.

These changes include the rise of:

- **DISTRACTIVE ATTACKS**
- **TARGETED RANSOMWARE ATTACKS**
- **SUPPLY CHAIN ATTACKS**
- **CRYPTOJACKING**

As such, the impacts of a breach are also constantly changing. However, costs may arise not only as a result of more damaging attacker actions, but also increasingly stringent regulators and post-breach investigations.

[1] According to NTT Security's 2019 Global Threat Intelligence Report.

INTRODUCTION

The cyber threat landscape can be extremely difficult to navigate – not only are attackers developing new techniques to evade security teams and attribution, but many security firms continue to put their own spin on the threat landscape which is, in some cases, leading to complete contradictions.

The complexity of the finance sector only exacerbates this confusion, as different niches within financial services and banking may face entirely different cyber risks. However, understanding the cyber threats relevant to specific companies and industries is an important nut to crack as it can significantly boost the efficiency of many aspects of security, from high-level exercises such as risk analysis and management, down to the implementation of new technologies and procedures.

In this report, the cyber threats to the finance sector have been broken down into three predominant categories based on attacker motivations, to help financial institutions better understand the threats that are relevant to them:

- **DATA THEFT**
Refers to attacks which set out to extract information.

- **DATA INTEGRITY AND SABOTAGE**
Refers to attacks which seek to tamper with, disrupt, or destroy critical systems.

- **DIRECT FINANCIAL THEFT**
Refers to attacks which seek to steal funds directly from the target.

Also discussed are some more generic, but still relevant, trends that are being seen in the wider threat landscape, as well as the potential impacts of a cyber attack.

DATA THEFT

State-sponsored threat actors have a range of reasons to extract different types of data from financial institutions...

Some nation-states are heavily embedded in their economies, through state-owned organizations or otherwise. As such, large international deals that are particularly relevant or impactful to these economies may naturally attract the interest of state-sponsored actors.

For example, attackers may look to help indigenous organizations position themselves more competitively against rival entities involved in a deal, by accessing the negotiation stances of those rivals via their financial advisors. However, it is not just state-sponsored actors who are interested in M&A data; cyber criminals often seek out information regarding unpublished price sensitive information (UPSI) to support insider trading schemes.

State-sponsored actors may also seek to monitor international transactions, which could be achieved by compromising various different financial entities. Visibility over this information could help to reveal illicit criminal or terrorist activities, record whether sanctions are being respected, and track specific persons of interest [1].

Relative to most other organizations, financial institutions hold particularly sensitive and valuable customer data which attracts both state-sponsored and criminal groups.

Vast swathes of personal information are often covertly collected by governments, who are looking to create databases that can be used to support future campaigns, whatever they may be. For example, financial data such as bank statements would allow state actors to identify individuals that may be particularly susceptible to bribes. Alternatively, secret or embarrassing customer expenditures may present opportunities for blackmail. Such techniques are common among many intelligence agencies, who seek to establish multiple channels for acquiring information.

In addition, in-depth knowledge of customers' spending habits may also be used to craft phishing messages that have a higher probability of success. This use of stolen personal data from financial institutions is not unique to state-sponsored groups, and is also a methodology that has been deployed by criminals.

For example:

CUSTOMERS IN THEIR OVERDRAFT MAY BE MORE PRONE TO CLICKING ON A LINK THAT PURPORTEDLY ALLOWS THEM TO CLAIM BACK FUNDS.

ELDERLY CUSTOMERS, WHO ARE GENERALLY MORE SUSCEPTIBLE TO ONLINE SCAMS, MAY BE ENTICED BY DOCUMENTS ABOUT THE CANCELLATION OF ACCESS TO THEIR PERSONAL PENSIONS.

WEALTHY CUSTOMERS MAY BE FOOLED BY THE OFFERING OF A SPECIAL INTEREST RATE THAT IS DESIGNED ONLY FOR PEOPLE THAT HAVE ACCUMULATED A HIGH AMOUNT OF FUNDS IN THEIR ACCOUNTS.

Stolen personal data may include details that would allow criminals to steal funds from customer accounts. Alternatively, threat actors may choose to sell this data on the dark web; credit card details can fetch up to $100 each, and login information for online payment services such as PayPal can fetch up to $200.

Finally, and whilst not unique to the finance sector, there have been many cases of criminals threatening to publish stolen data from financial institutions unless a ransom is paid.

[1] A person of interest is an expression used to describe any individual of significant interest to law enforcement or government intelligence. Typically, this may include ultra-high-net-worth individuals, foreign officials and key decision-makers, and political dissidents and opponents.

DATA INTEGRITY AND SABOTAGE

Sabotage refers to the disruption or destruction of systems, and is one of the most popular methods of extortion by cyber criminals. Ransomware is commonly used for such purposes, although distributed "denial-of-service" (DDoS) attacks are also prevalent in this space.

Ransomware attacks have traditionally been generically sprayed across as many users as possible, making them fairly simple to defend against. However, the rise of highly targeted techniques in order to distribute ransomware has escalated this risk – see the "Generic Trends – Targeted Ransomware" section for more information.

From a state-sponsored perspective, the risk of a cyber attack intended to sabotage financial systems is more complex, as it depends on the geopolitical relations between a country and its rivals. Typically, destructive state-sponsored cyber attacks against financial institutions have only occurred where relations between two governments are extremely strained.

Two prominent examples are:

1. RUSSIA VS. UKRAINE

The ongoing conflict between Russia and Ukraine, triggered by Russia's annexation of Crimea in early 2014, has created the ideal testing ground for the Kremlin to hone its cyber warfare strategy. Over the last four years, Russian hackers have targeted various entities within Ukraine's critical national infrastructure, including banks, where files were deleted and systems were rendered permanently unusable after being wiped.

2. NORTH KOREA VS. SOUTH KOREA

In March 2013 – one month after North Korea's third nuclear weapon test, and when tensions between the North and South were considered by many to be at an all-time high – North Korea launched a coordinated cyber attack against organizations in the South.
The attack, dubbed Dark Seoul, permanently destroyed tens of thousands of computers across several banks and broadcasters.

In addition, there have been indications that state-sponsored cyber attacks against foreign financial systems may extend beyond sabotage. Russian spies have previously been tasked with understanding how to cause a major economic crash through the manipulation of "trading robots". The primary concept was, if you could compromise trading systems and dump huge volumes of stock onto the market, the consequent drop in market prices would trigger a chain reaction whereby applications all over the world also sell stock in that market, causing a major crash.

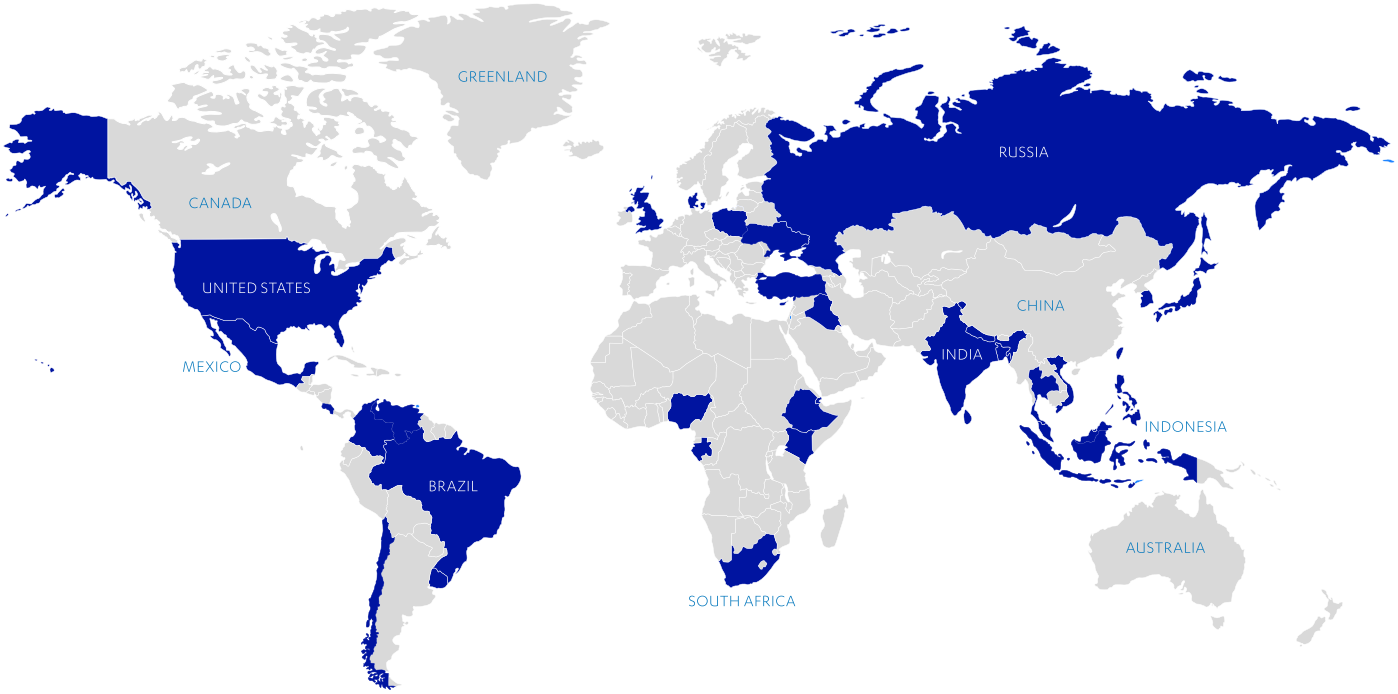
While such an attack has not yet been conducted, its impact on a financial institution, as well as the wider economy, may be inferred by the following two cases:

The theory behind this attack against trading systems was based on the US "flash crash" in 2010, when a trader dumped huge volumes of stock on the US market and triggered a domino effect. The US market was devalued by $1 trillion in 15 minutes, but quickly recovered.

In August 2012, a computer-based trading error caused US financial services firm Knight Capital to lose around $450 million. A cyber attack against trading systems could mimic the effects of this computer error.

DIRECT FINANCIAL THEFT

Cyber criminals often target many different industries to steal funds by manipulating or compromising finance departments. However, banks represent unique targets from which adversaries can steal tens of millions of dollars in a single attack.



Publicly known countries targeted by financially-motivated attacks from North Korea.

Cyber criminals are not the only threat in this space – North Korea's attacks against banks around the world have been well-documented for over three years now, and the techniques used by the country's hackers have also been adopted by criminals. These methodologies are as follows:

SWIFT ATTACKS

Attackers compromise a bank's SWIFT payment operators, steal their credentials, and subsequently send fraudulent transfer requests via the SWIFT messaging system.

When confirmation messages of these transactions are sent back to the compromised bank, the attacker's malware intercepts and deletes them, thus removing evidence that the transactions occurred.

The illicitly transferred funds get withdrawn from the attackers' accounts by money mules, and the cash is then laundered.

PAYMENT SWITCH APPLICATION COMPROMISE

Payment switch applications manage the communications between different entities, enabling the transfer of data between "issuing" and "acquiring" banks. When a customer goes to withdraw funds from an ATM, a request gets sent to the customer's bank. The payment switch application handles this request, conducts a number of checks, for example whether the customer has the required funds in their account, and sends a confirmation – or rejection – message.

Attackers are compromising these payment switch applications, so that ATM requests made by the attackers' cards are intercepted by the malware. The malware then automatically authorises these requests, regardless of their legitimacy, and the ATM releases unlimited cash for the money mules.

These are not the only techniques that attackers are using to steal money from banks. For example, "ATM jackpotting" is when an attacker physically penetrates an ATM and directly installs malware onto the system. They can then remotely instruct the ATM to dispense cash when a money mule is there.

Traditionally, ATM jackpotting has occurred in developing regions such as South America, although in 2018 there was an emergence of these attacks in the US, suggesting a possible proliferation of this technique.

GENERIC TRENDS

DISTRACTIVE ATTACKS

Ransomware and DDoS attacks are now being used to divert the attention of security teams away from more sinister activity. In other words, while security teams are responding to these disruptive attacks, attackers are covertly active elsewhere in the victim's network.

Another method of distraction involves deliberately alerting security controls, for example, through the use of known malware samples. Security teams respond to this threat under the impression that it has been dealt with successfully, leaving them more likely to remain ignorant of more sophisticated and evasive malware that has been installed elsewhere.

TARGETED RANSOMWARE

While ransomware has been commonplace for several years now, targeted ransomware attacks are on the rise. The way in which strains such as SamSam, Ryuk, LockerGoga, and others, have spread is symbolic of this trend.

The footprint of a targeted attack is significantly smaller in comparison to an outbreak or spam campaign. Targeted attacks allow attackers to hit specific systems, including critical infrastructure, thus can extract more money from a single victim than opportunistic campaigns.

SUPPLY CHAIN ATTACKS

Supply chain attacks seek to breach targets by compromising associated third parties and using them as an attack vector. As many highly targeted industries continue to invest in and improve their security postures, compromising those industries through their supply chain is an effective way to evade many security controls.

Due to the high levels of security investment in the finance sector, attackers are increasingly looking to compromise financial entities via their supply chains.

CRYPTOJACKING

Cryptojacking is the unauthorized use of a computer in order to mine cryptocurrency. Mining can leverage local and cloud processing power, and significantly compromises computer performance.

Cryptojacking grew in 2018 to become one of the most popular methods of revenue generation among criminals, as it is extremely profitable and provides longer infections that give consistent income at lower risk for attackers.

While cryptojacking does not involve any theft or tampering of information, such attacks may incur significant opportunity costs due to the deterioration of system performance and the consequent drop in productivity. For example, were criminals to infect customer-facing servers, trading systems, or other critical systems, costs could quickly escalate.

TRICKLE-DOWN EFFECT

Since 2017, there has been a continued uptick in the capabilities of cyber criminals. Not only are criminals increasingly developing their own malware, but the speed with which they are re-weaponizing exploits and mechanisms developed by state actors is growing.

Further to this, many of these actors are offering their customizable strains or services-for-hire on dark web markets, exemplified by large increases in "cybercrime-as-a-service" offerings.

This has created a "trickle-down" effect, whereby advanced hacking capabilities are being made available to less able criminals. Partly as a result of this, the security industry is reporting a general rise in the adoption of more modern TTPs by attackers. This includes the use of unique malware families, in-memory techniques, and anti-analysis characteristics.

IMPACTS OF A BREACH

DIRECT FINANCIAL LOSS

As discussed, many cyber criminal groups, as well as North Korea, target banks to steal money. Further to this, ransomware demands ranging from a few thousand up to over one million dollars have been paid by victims, in order to restore critical business functions and data.

NETWORK DOWNTIME AND LOST PRODUCTIVITY

In 2018, UK-based TSB Bank suffered a week-long service disruption, the cost of which totaled nearly £200m. While this was not caused by a cyber attack, a destructive attack may incur similar costs.

The costs of the IT failure included, among other things, £115.8m on customer redress, remediation resource and fraud costs, and £30.7m on additional resource and advisory costs "to support the remediation of systems and operating defects". TSB also waived £29.9m worth of avoidable customer fees and charges.

REPUTATION AND COMPETITIVENESS

Customers may lose trust in the organization's ability to maintain confidentiality of data, and consequently move to a competitor.

REGULATIONS AND FINES

Authorities across the globe are becoming decreasingly tolerant of data breaches, through the introduction of more stringent regulations, post-breach investigations, and fines. For example, the average fine issued by the UK's Information Commissioner's Office to companies around the world doubled in the last year alone. In addition, post-breach interaction with regulatory bodies and affected parties averaged $1.76 million in the US in 2018, up from $1.56 million in 2017 and $1.10 million in 2016 – these include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services, and regulatory interventions.

M&A DEAL SIZE

Were the negotiation stance of a financial advisor and its client to be accessed by a rival in an ongoing deal, the financial advisor's ability to obtain the optimal outcome for their client would be severely hindered.

OTHER COSTS

Common costs associated with a breach may also include:

- **BREACH CONTAINMENT AND REMEDIATION, WHICH CAN COST OVER $1 MILLION IN EXTRA FEES IF COMPLETED LATER RATHER THAN EARLIER**
- **DAMAGE CONTROL OR RECOVERY**
- **NEWLY REQUIRED SPENDING ON SECURITY HARDWARE, SOFTWARE, AND SERVICES**
- **DATA RECOVERY EXPENSES**
- **INCREMENTAL HIRING**

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats. Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.


F-Secure