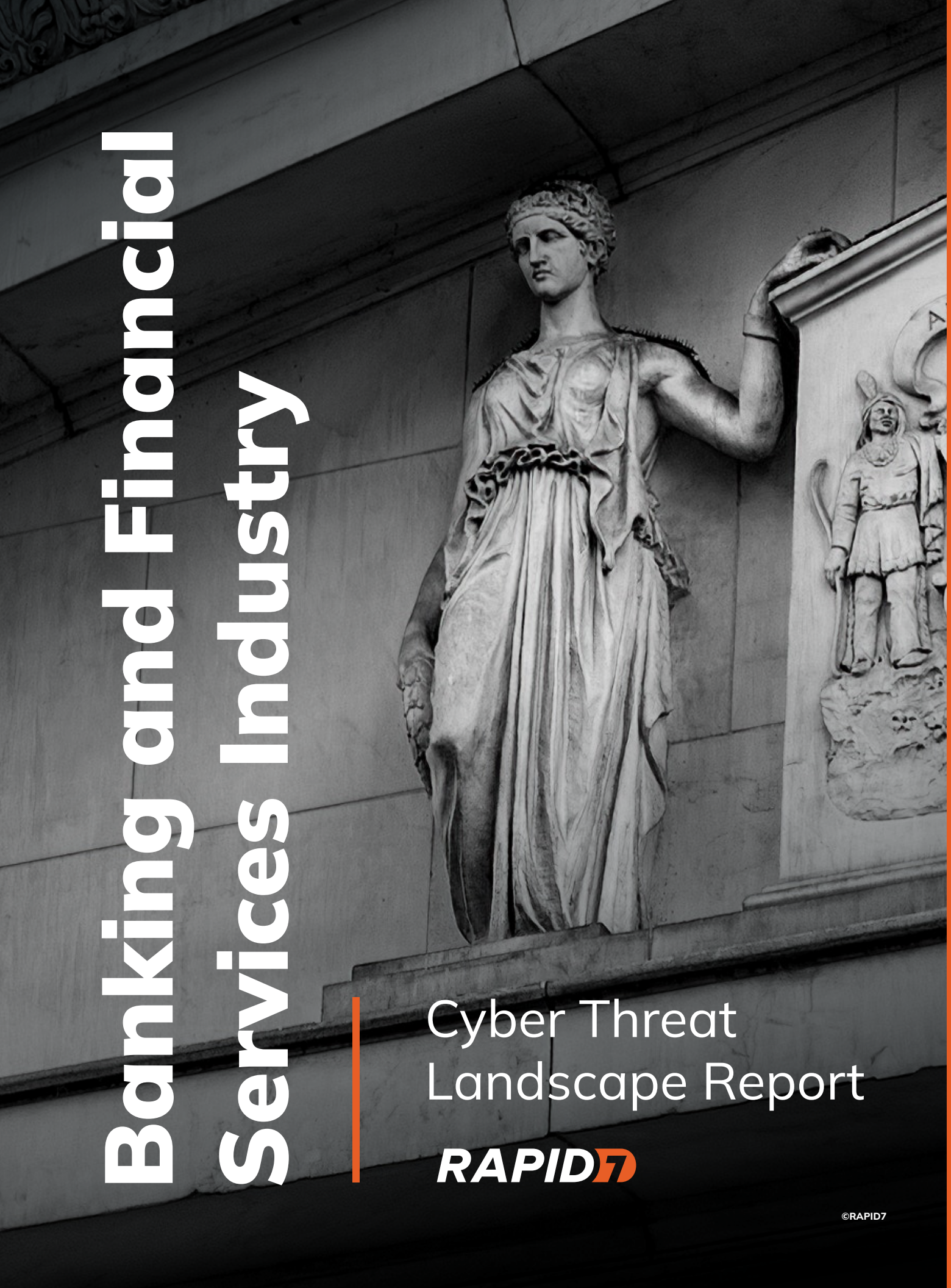

Banking and Financial Services Industry

Cyber Threat Landscape Report

RAPID7

INTRODUCTION

> **Because that's where the money is.**
>
> Infamous bank robber Willie Sutton when asked why he robbed banks.

The banking sector is the single most important target for cybercriminals. Banks and financial services organizations safeguard incredibly sensitive data of users and employees alike – bank account numbers, credit card numbers, social security (or equivalent) numbers, credentials, addresses, and more. Data breaches in the industry, therefore, can lead to devastating financial losses, regulatory penalties, and incalculable damage to brand reputation.

This report exposes some of the most common attack vectors threat actors use to carry out successful cyberattacks against banking and financial services organizations, provides evidence of hackers collaborating and trading critical information that can wreak havoc on corporate networks, and offers recommendations for financial services security teams to avoid suffering such a breach or attack. Read on to learn about:

- Compromised credit cards, attacks on bank networks, banking Trojans, and other common ways threat actors target the industry
- The evolution of Tactics, Tools, and Procedures (TTPs) used to attack banks and financial services institutions
- Attacks on organizations in other industries indirectly compromising businesses in the financial industry

CONTENTS

How Do Cybercriminals Target the Financial Services Industry?

Traditionally, cybercriminals steal from banks using compromised payment card information or online banking credentials, carrying out fraudulent transactions using victims' information. Fraudsters typically purchase this data from the original attackers in underground black markets for a fraction of the face value. The prevalence of payment card fraud as a method of stealing money from banks leaves the banking sector uniquely exposed to the impact of breaches in other sectors like retail, hospitality, and ecommerce.

Banking Trojans, mostly for Windows and Android operating systems, are another traditional way for cybercriminals to defraud banks by targeting individual customers for infection. The Windows banking Trojan market has nonetheless shifted in recent years with the rise of Emotet and TrickBot, which have functioned more as multipurpose malware and downloaders for other malware than as banking Trojans. Android banking Trojans have come to dominate the mobile market due to the greater vulnerability of Android devices. Mobile banking Trojans have become an increasingly significant segment of the banking Trojan market due to the widespread adoption of mobile banking apps and the opportunities provided by infected mobile devices to bypass two-factor authentication (2FA).

A newer approach that has become more prevalent in recent years is the targeting of bank networks themselves in order to enable fraud on a scale much larger than the fraudulent use of individual payment cards or online banking credentials. The goal of these attacks is to breach bank networks and move laterally in order to gain access to systems that when compromised can enable larger-scale fraud involving SWIFT terminals or servers that support ATMs, for example. The Lazarus Group of North Korea, which engages in many different forms of cybercrime to raise revenue for the financially isolated North Korean government, was a pioneer of this more ambitious approach in its fraudulent use of compromised SWIFT access. Some of the more sophisticated Russian-speaking criminals have followed suit and targeted different internal banking systems in order to enable large-scale fraud in other ways. Breaching organizations as security-centric as banks is often difficult, so some actors have resorted to targeting bank partners, such as insurance companies, in order to move laterally into bank networks.

These attacks on bank networks should be a top consideration for network security teams at banks. Such attacks target the banks directly, rather than their customers or businesses in other sectors. They also have the potential to inflict far larger financial losses on affected banks. Network segmentation and heightened security measures for the most financially sensitive systems within those networks can reduce the risk of such attacks succeeding. Network defenders should aim to reduce opportunities for lateral movement within their networks and require more stringent authentication for those more financially sensitive systems and tools that could enable large-scale fraud in the event of a compromise.

Compromises of payment card information at merchants in other industries and of customers' online banking credentials warrant coordination between bank security and fraud detection and prevention teams. Compliance requirements for merchants, such as the Payment Card Industry Data Security Standard (PCI DSS), are a good baseline for reducing the risk of payment card breaches in other industries, but it is also important to identify breaches at merchants and stop the flow of compromised payment card data into underground black markets. The compromise of online retail banking credentials depends in part on the security posture of affected customers.

Attacks on Bank Networks

The North Korean Lazarus Group is arguably the single most formidable threat to the banking sector. The Lazarus Group has access to the more substantial and sophisticated capabilities of a government, which gives it a big advantage over common criminals. The cybercriminal enterprises operating under the auspices of the North Korean government, such as the worldwide WannaCry ransomware outbreak, have further demonstrated a high degree of audacity and ambition beyond that of common criminals. North Korean actors committing financial crimes have little or no reason to fear foreign law enforcement, given North Korea's isolation, and can thus operate with greater impunity than common criminals.

The Lazarus Group's attacks on the banking sector have been more complex than those of common criminals. They aimed to achieve more ambitious goals by enabling very large fraudulent transactions via the SWIFT interbank payment network. These attacks came to light with the 2016 breach of the Bank of Bangladesh and have often targeted banks in developing countries, such as Vietnam and Ecuador since then. These attacks involved lateral movement within the compromised networks of these banks to SWIFT accesses, which the actors compromised and manipulated in order to send huge fraudulent transfers. The Lazarus Group later expanded its horizons to ATM fraud in its FASTCash operation, which targeted the servers inside bank networks, which when compromised enabled fraudulent ATM withdrawals.

Some of the more sophisticated criminals in Russia and other former Soviet republics have adopted similar strategies for enabling largescale fraud, albeit by targeting banking systems other than SWIFT. For example, the group MoneyTaker targeted the Automated Workstation Client of the Central Bank of Russia (AWS CBR), another interbank payment system like SWIFT within Russia, in a similar manner. MoneyTaker also targeted card processing systems within banks to enable fraudulent transactions on cards that the attackers controlled by changing or removing their withdrawal and overdraft limits.

These attacks depend on lateral movement within compromised networks but could begin at any number of points around a bank's network perimeter. For example, Rapid7 coverage of a trusted and prestigious forum for vetted Russian-speaking criminals revealed a threat actor selling a web shell with administrator privileges on the network of an unidentified US mobile and online bank for $10,000.

ATM malware is a significant threat to banks and does not necessarily require access to internal bank networks to install it locally on targeted machines. Rapid7 coverage of underground criminal forums revealed a threat actor offering source code for unidentified ATM malware targeting Wincor, Diebold, and NCR machines for $10,000.

The dominance of North Korean and more sophisticated Russian-speaking criminals in this market does not exclude the risk of attacks by other actors that do not fit this profile. For example, Rapid7 coverage of underground criminal forums revealed an English-speaking threat actor selling remote code execution vulnerabilities in four subdomains belonging to the Brazilian bank Bradesco for a total of $2,000 or $500 each.

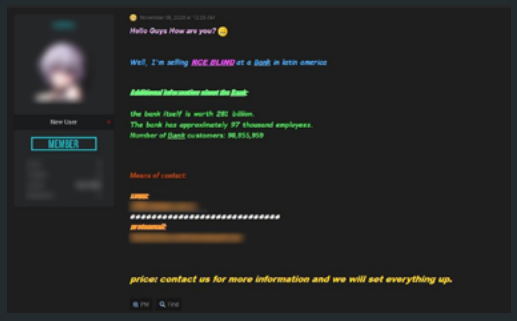

FIGURE 1

Web shell with admin privileges on a US bank network for sale on a prestigious Russian cybercrime forum

FIGURE 2

Source code for an unknown ATM malware for sale in a cybercrime forum

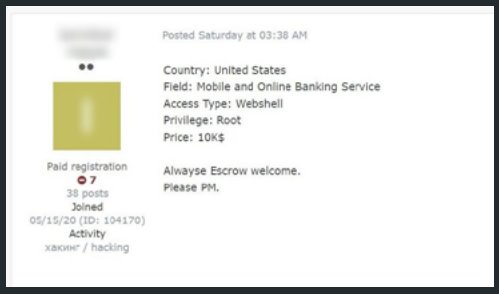

FIGURE 3

A threat actor offers remote code execution vulnerabilities for domains belonging to a Brazilian bank

Attacks on Other Businesses that Affect Banks

Banks can and should strive to increase customer security awareness and give customers incentives to improve their security hygiene.

Banks are uniquely exposed to secondhand risk and fraud resulting from compromises of payment card information at merchants in other industries, particularly retail, hospitality, and ecommerce. A significant proportion of fraud against retail banks issuing credit cards therefore results from incidents on networks and systems beyond a bank's direct control. PCI DSS may help to reduce this secondhand risk, but many payment card attacks against compliant merchants succeed nonetheless. Fraud investigators at banks can help to stop the flow of compromised payment card information into underground black markets by identifying and notifying breached merchants. This practice has enabled the discovery of many payment card breaches at merchants in other industries, which, in turn, shed light on the tactics, techniques, and procedures (TTP) of attackers targeting payment card data.

The emphasis of payment card fraud has shifted in recent years, away from in-person fraud and toward online fraud. This shift began with the 2015 introduction of EMV chips into payment cards in the US, which is the single largest market for cyber fraudsters. These chips are an obstacle to the successful cloning of compromised cards and have thus been a deterrent to in-person fraud operations. Covid-19 has pushed the fraud market even further in this direction, with consumers making a dramatic shift to ecommerce purchases and home deliveries.

These changes have thus favored online fraud and have accordingly altered the TTPs and targeting of payment card attacks. Ecommerce and the websites of brick-and-mortar businesses have become equally or perhaps even more important targets than in-person point-of-sale (PoS) systems, as their compromise enables the collection of card verification values (CVVs) and other data points needed for online fraud. PoS malware was once at the forefront of payment card breaches, but digital payment card skimmers have begun to supplant them as the tip of the spear in this market.

Digital payment card skimmers are the virtual counterpart of the hardware skimmers that criminals install on ATM readers and other payment card terminals in order to collect their data. Attackers install this malware, often in the form of JavaScript or some other script, on merchants' compromised websites and use it to collect the payment card details that customers input when making purchases. The Magecart skimmer was a pioneer in this field when it first began to grow. Magecart and its variants have remained leaders in this market niche since then. Its users have been responsible for some of the most noteworthy online card breaches, such as those at Ticketmaster, Newegg, and British Airways.

Ecommerce websites are also a source of stored payment card data. Rapid7 researchers found a threat actor selling a database from a March 2020 breach of the ecommerce website Joom with 573,911 account records. Those account records included stored payment card information. The actor's asking price for the database was $1,500.

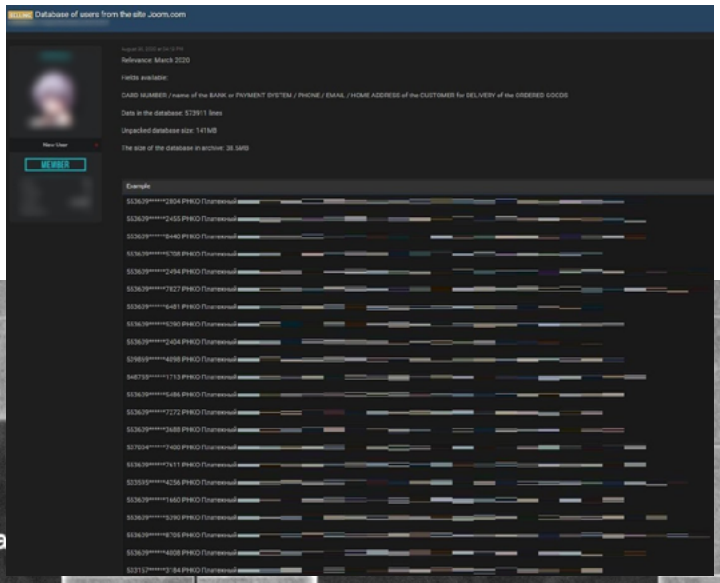

FIGURE 4

Database from an ecommerce website breach in early 2020 for sale

The shift toward online fraud has also fueled interest in defeating card issuers' heightened anti-fraud measures for online payments. For example, Rapid7 coverage of underground markets revealed a fraudster selling purported knowledge of a way to bypass Visa VBV 3D Secure for $21. That XML-based protocol aims to add another layer of security for online card payments. Similarly, we found a threat actor selling a Python script and an associated video and guide to bypass VBV 3D for $200.

Rapid7 coverage of underground criminal communities has nonetheless indicated that some fraudsters still seek to circumvent EMV chips, rather than simply shifting to online fraud. Rapid7 researchers discovered a criminal threat actor offering software that supposedly enables fraudsters to clone cards and bypass chip and PIN authentication measures for in-person fraud.

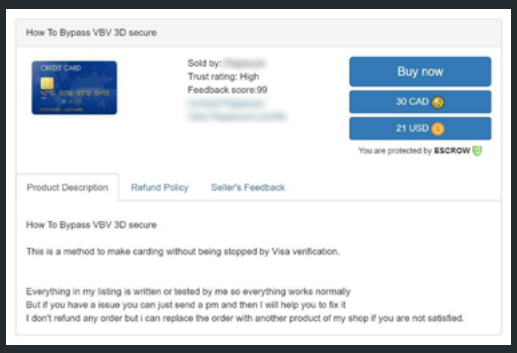

FIGURE 5

Fraudster auctioning off the information necessary to crack Visa's card payment security protocol

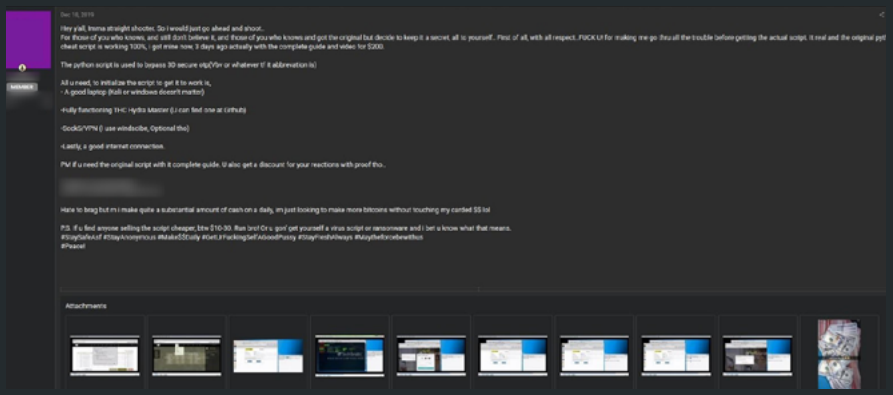

FIGURE 6

Python script for sale with an accompanying guide to bypass a Visa security protocol

Incidents at insurance companies, another sector of the broader financial services industry, are another source of secondhand risks to banks. The Russian-speaking Cobalt gang has targeted insurance companies in order to move laterally from them into bank networks. The goal of this targeting of insurance companies is to exploit the business relationships, network connections, and email communications between insurance companies and banks in order to gain access to the latter.

Technology companies that support banks are another source of third-party risk for banks. Breaches of those companies can indirectly enable attacks on banks themselves. For example, Rapid7 coverage of underground criminal forums revealed a threat actor selling access to a variety of data from a breach of a banking software company for $5,000. The compromised data included: credentials for mail servers, VPNs, and database servers; email correspondence; and information on the company's employees and customers.

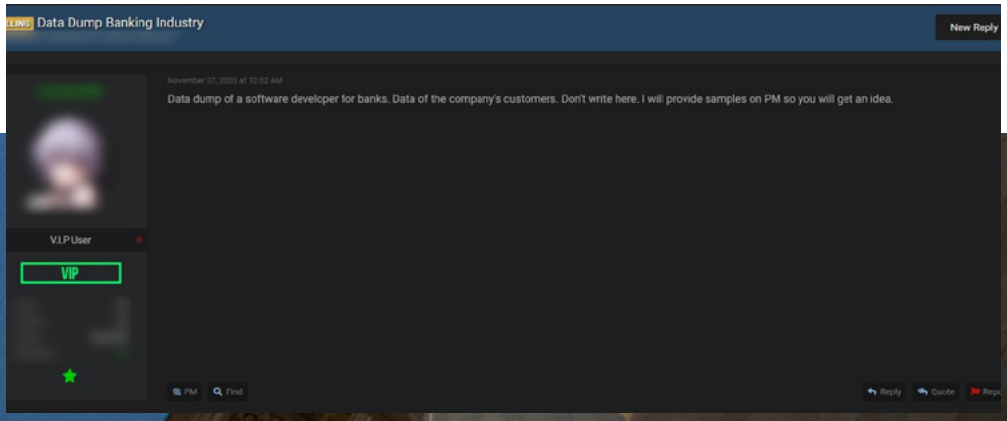

FIGURE 7

A threat actor offering access to different types of data from a breach of a banking software company

Banking Trojans

Banking Trojans are one of the most common and typical types of criminal malware and are responsible for a large share of attacks on banks, albeit indirectly via their customers. The core function of a banking Trojan is to compromise online banking credentials used on compromised devices and to use that unauthorized access for fraud, either by the attackers themselves or third-party buyers in underground black markets. Banking Trojans may nonetheless have many other functions. Indeed, two of the most prolific Windows banking Trojans in recent years, Emotet and TrickBot, have expanded their functionality to the point that the compromise of online banking credentials is arguably no longer their core function. Among their many other features, Emotet and TrickBot can serve as downloaders for other types of criminal malware, particularly ransomware. Attackers may deploy ransomware after they have collected online banking credentials or whatever other information they can monetize.

Mobile banking Trojans have become an increasingly important segment of the banking Trojan market for two reasons. The widespread adoption of mobile banking apps makes mobile devices an equally or even more important target for attackers that seek to compromise online banking credentials. Furthermore, most 2FA for online banking logins relies on mobile devices, via either SMS or authentication apps. Compromising mobile devices with banking Trojans can thus facilitate attacks on online banking credentials by enabling 2FA bypasses. SMS intercept functionality is typical of mobile banking Trojans, and some now have the ability to collect 2FA codes from authentication apps. Most mobile banking Trojans are for Android rather than iOS, given the greater vulnerability of the former.

Criminals that target retail bank accounts often sell the data that they have compromised to third parties in underground criminal forums and black markets, rather than monetize it themselves. This data often sells for a fraction of its face value. Rapid7 researchers found a Russian-speaking criminal selling a database of bank account details for 20,400 US bank customers. The database included account numbers, names, mailing addresses, email addresses, phone numbers, and IP address. The actor began auctioning this database at a price of $10,000, with a “buy now” price of $20,000.

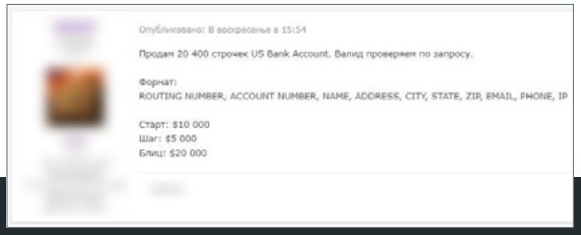

FIGURE 8

A Russian threat actor offers a database of over 20,000 US bank accounts for sale

CONCLUSION AND RECOMMENDATIONS

Attacks on bank networks themselves are the most significant threat to the banking and financial services sector because they target the banks directly and can cause the greatest financial losses via fraud. The North Korean and Russian actors that dominate this market niche are among the most sophisticated criminals worldwide and operate with relative impunity. Lateral movement within bank networks to the most financially sensitive systems that can enable large-scale fraud, such as SWIFT terminals, ATM servers, and card processing systems, is integral to the success of these attacks. Network security teams at banks can improve defenses for these most financially sensitive systems by using network segmentation to impede lateral movement into them and requiring more rigorous authentication to access them.

Fraud with individual compromised payment cards may involve much smaller transactions but nonetheless adds up to significant amounts in aggregate. The breaches at merchants in other industries that enable this fraud may be beyond the direct control of banks, aside from their ability to impose security compliance requirements on merchants. Bank fraud detection and prevention teams can at least identify breaches at those merchants and thereby stop the flow of compromised data. Future compliance requirements and breach investigations should also take into consideration the growing trend away from in-person PoS compromises and toward online compromises and fraud.

The compromise of online banking credentials on customers' devices via banking Trojans also remains partially beyond the control of banks, aside from their application security efforts and their ability to impose security hygiene on users, such as password complexity and 2FA. 2FA, in particular, is an important defense for online banking credentials, and the proliferation of mobile banking Trojans that can bypass it poses a significant threat. The use of authentication apps is more secure than SMS, but even that method is vulnerable to at least some mobile banking Trojans that target those apps.

External threat intelligence and digital risk protection solutions can give security teams an advantage over hackers and fraudsters. Proactive identification and validation of threats targeting your specific organization enables your security teams to prevent devastating cyber attacks by neutralizing them at the source. They also help your security organization cull through all the noise of numerous IOC feeds, by alerting you of specific, credible threats to your organization. Rapid7 equips customers like you with the tools and intelligence you need to take down threats as they emerge and protect your organization and brand reputation. Learn more about how our threat intelligence solution can empower your security teams fight the bad guys and defend your organization.

POWER TO THE PROTECTORS

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/