Banking & Financial Services

Cyber Threat Landscape Report

April 2019

www.intsights.com

Table of Contents

Executive Summary

The financial services sector faces a constant stream of cyberattacks levied by threat actors seeking to infiltrate corporate defense networks. These cybercriminals are after the substantial financial assets each bank or financial institution is responsible for, but data leaks can also provide them with customer information, records, and credentials that allow them to diversify their attacks and spread security teams thin. Cyber fraud has also created a whole new set of challenges, as this activity often takes place on external channels, like retail sites and social media channels. Distributed denial of service (DDoS) attacks disrupt web traffic, rendering banks and financial service institutions incapable of fulfilling the services they provided to their customers.

In this report, IntSights provides a comprehensive overview of the current cyber threat landscape in the financial services and banking sector based on key threat data collected in the IntSights Enterprise Threat Intelligence & Mitigation Platform. We took a random sample of some of our financial services customers and analyzed the threats targeting these organizations to find noteworthy trends, patterns, outliers, and developments. Threat researchers analyzed the most significant action in attack types, attack vectors, and regional trends facing these organizations, and offer commentary on best practices to defend against the latest trends and attack vectors.

Banks and financial services organizations were targeted in 25.7 percent of all malware attacks last year, more than any of the other 27 industries we tracked.

Summary of key findings from this report:

- **BANKS GET HIT WITH 25.7 PERCENT OF ALL MALWARE ATTACKS:**
Banks and financial services organizations were targeted in 25.7 percent of all malware attacks last year, more than any of the other 27 industries we tracked.

- **212 PERCENT INCREASE IN STOLEN CREDIT CARD DATA:**
In 2019 Q1, we saw a 212 percent year-over-year increase in instances of compromised credit cards.

- **129 PERCENT INCREASE IN CREDENTIAL LEAKS:**
We saw a 129 percent year-over-year increase in credential leaks as a result of the Collection #1 leak (more on Collection #1 later).

- **102 PERCENT INCREASE IN MALICIOUS APPS:**
We observed a 102 percent year-over-year increase in malicious applications, including fraudulent mobile banking apps.

- **ALTENEN GETS SHUT DOWN:**
Hacker hub Altenen.com was taken down in May 2018 after Israeli authorities arrested the site's manager. It was estimated that Altenen had facilitated fraud for over 20,000 credit cards and $31 million in money laundering. This large-scale shutdown left cybercriminals scrambling for several months until a new site, Altenen.nz, emerged.

- **SS7 FLAWS EXPOSED:**
For the first time, cybercriminals publicly exposed flaws in SS7, a protocol used by telecommunication companies to coordinate SMS routing, to intercept messages that authorize payments from accounts.

- **ORGANIZATIONS IN DEVELOPING COUNTRIES AT RISK:**
Financial organizations based in developing countries – namely in Latin America, Africa, and South Asia – were attacked more frequently because many lack the external-facing security systems that are common in more developed regions of the world.

By the Numbers

Two significant external events helped to shape the financial services industry cyber threat landscape over the past year: The shutdown of the ubiquitous cybercriminal forum Altenen, and the largest leaked credential collection published in history. More so than any other factors these two events impacted financial organizations and cybercriminals alike.

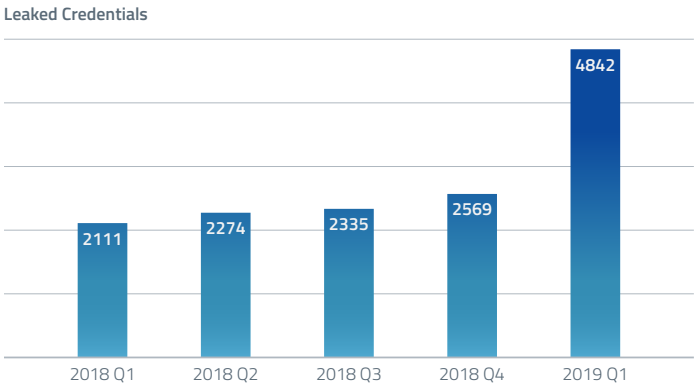
Here are the key annual findings we identified:

129% year-over-year increase in leaked credentials

January 2019 marked the biggest global data leaks in history. Known as "Collections #1-5", in homage to the relatively innocuous file names containing the data in question, these leakages exposed roughly 2.2 billion records of login credentials and personal information worldwide.

After obtaining and processing the collections, IntSights threat researchers naturally saw a big spike in leaked credentials during this time period. The instances of credential leaks in Q1 2019 nearly doubled those of any of the previous four quarters dating back to Q1 2018.

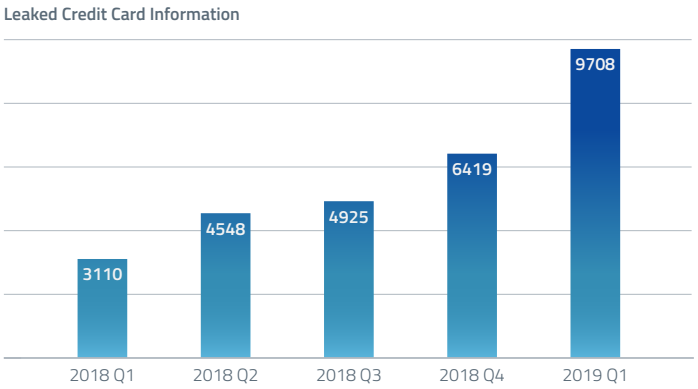
IntSights saw a huge spike in leaked credentials after Collections #1-5 published 2.2 billion records.



212% increase in leaked credit cards

IntSights observed 9708 instances of compromised credit card data in 2019 Q1, marking a 212 percent increase year-over-year. The number of leaked credit cards continued to rise steadily throughout 2018 – despite a relative plateau through Q2 and Q3 – before skyrocketing in early 2019.

Cybercriminals use these compromised credit card numbers to primarily make small purchases, as this practice does not often attract unwanted attention. However, these small purchases can generate nearly ten times more "free money" than what the card is worth on the black market.
Since credit card companies will typically reimburse customers who have been victimized by fraudulent credit card usage, cybercriminals find stealing card numbers to be a relatively safe and simple way to generate profits. The risks are small and the potential gains are significant.

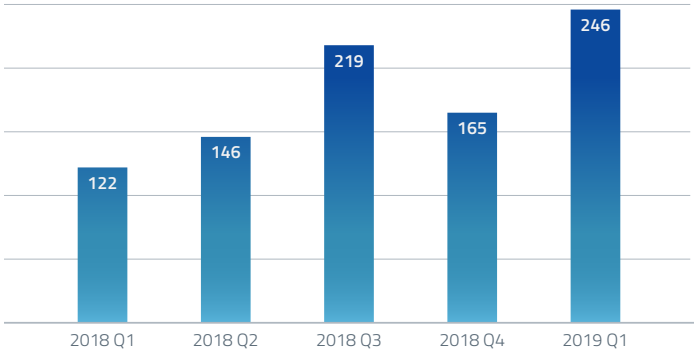


102% year-over-year increase in malicious applications

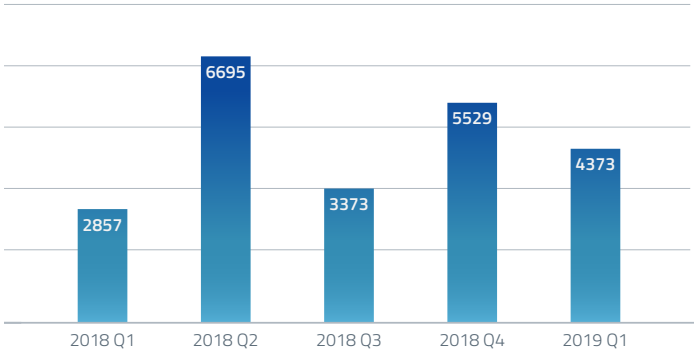
IntSights observed steady growth in the frequency of malicious applications since early 2018. This includes fake mobile banking apps that mimic major blue-chip banking apps, which have proven to be remarkably successful endeavors for hackers, as more than 1 in 3 consumers are fooled by fraudulent mobile apps.

While we observed a brief dip in the number of malicious applications in 2018 Q4, it appeared to only be a temporary lull, as 2019 Q1 brought more activity in this area than ever. As consumers grow more and more comfortable with mobile banking, the risk of malicious applications grows in parallel.

Malicious Application



Assets Offered on Black Market



High fluctuation in financial assets offered on the black market

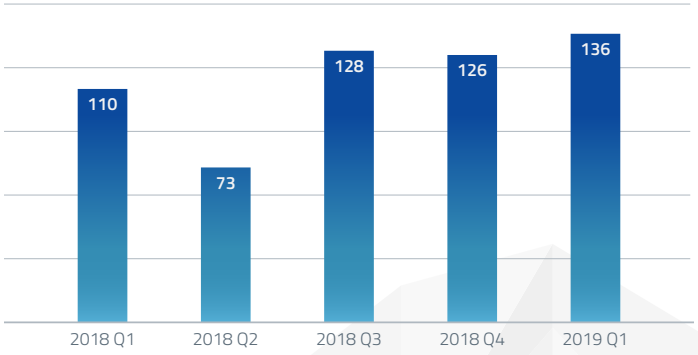
Financial assets are hot commodities on the black market. These can include credit card numbers, bank account numbers, or any other references to a company's name being listed on web forums and black markets. IntSights observed a fluctuating trajectory in this area over the past year.

After an initial period of decline in 2018 Q3 during the fallout of Altenen's shutdown, activity jumped back up in Q4. This likely had to do with Altenen.nz becoming more established, though its usership to date pales in comparison to its predecessor. As threat actors reacted to the takedown and began using other forums, our team had to track which new channels they moved to and update our collection sources accordingly. Still, the data shows a clear resurgence in assets available for purchase in black markets, indicating that the heights reached in 2018 Q2 may not have been an anomaly.

23% increase in leaked documents

The frequency of leaked documents observed has remained relatively stable over the past year, with some marginal growth. After a significant drop in 2018 Q2, there was a big increase in Q3. In 2019 Q1, the total number grew again, though far more modestly this time, to reach its highest point yet. While credit card and bank account details are by far the most common financial assets shared online, cybercriminals also look for sensitive documentsand personally identifiable information (PII) as well. Your security team needs to monitor hacker forums and other dark web sources for potential attacks planned against your organization.

Leaked Documents



Most Common Attack Types

Cybercriminals have a constantly expanding arsenal of TTPs used to exploit banking and financial services organizations. Hacking tools enable faster campaigns, social media and mobile devices give threat actors new ways to target customers, and data leaks from thousands of external sources are costing banks millions of dollars each year in fraud costs. New attack vectors emerge constantly, leaving organizations scrambling to cover any newfound weaknesses or attack strategies.

The following are some of the most common types of attacks leveraged against financial institutions over the past year.

Vulnerabilities in SS7

In February 2019, United Kingdom-based Metro Bank became the first publicly reported victim of a new attack vector: The codes sent through text messages to customers to verify transactions. Cybercriminals were able to exploit flaws in SS7 – a protocol used by telecommunication companies to coordinate how they route SMS around the world – to intercept messages that authorize payments from accounts. This scheme enabled the attackers to empty some of the customers' bank accounts. However, the bank reported only a small number of its customers were affected by this attack.

This was not the first instance of an SS7 exploitation. In 2017, German newspaper The Suddutsche Zeitung reported that hackers had exploited SS7 to steal money out of bank accounts in Germany. However, Metro Bank was the first bank to be publicly identified as a victim of this kind of attack.

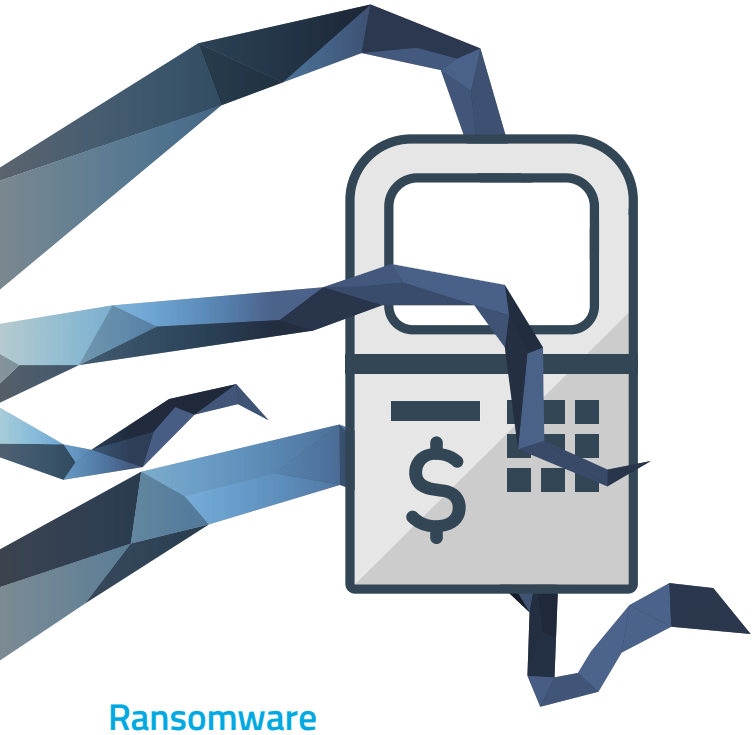
Cybercriminals exploited flaws in SS7 to intercept messages that authorize payments from banks accounts.

Malware

Banks and financial services organizations were the targets of 25.7 percent of all malware attacks last year, more than any other industry. Trojan viruses are among the more common types of malware attacks. Some of the most well-known banking Trojans used in 2018 were Adload, ATRPAS and Emotet.

- Adload is a tool that opens a backdoor on the targeted system, where it downloads and installs programs to gather information. This information, which includes the username and computer name, is sent to the attackers' server.
- ATRPAS is a Trojan targeting Windows that steals information from affected computers and sends it to the attackers' server.
- Emotet is a modular banking Trojan that is primarily used as a downloader or dropper of other banking Trojans.

In addition to Trojan attacks, IntSights observed large-scale malware attacks leveraged against multiple organizations. In September 2018, a Russian hacking group executed an attack campaign against financial institutions in Russia and Belarus using a malicious code disseminated in CHM (Microsoft Compiled HTML Help). The attack was carried out through the dissemination of spear-phishing emails in Russian, with a malicious malware in the attachment file. The spear-phishing emails were sent from addresses belonging to different Russian financial institutions.



Ransomware

You don't need a gun and a mask to hold up a bank anymore. Cybercriminals use ransomware to effectively hold banks hostage until they pay up. Attackers are, in essence, executing a denial of service that can cost banks millions of dollars each day the attack continues. A bank cannot fully function under a ransomware attack, since most of its key data is typically locked.

On February 13, 2019, CI Banco, a Mexican bank, suffered a ransomware attack that infected an employee's computer with the intent to spread laterally through the network. The bank had to shut down all operations to contain the threat, disconnecting from the Interbank Electronic Payment System (SPEI) and stopping its online operations and ATMs. However, the bank said no money or data was stolen during this attack. A week earlier, a similar ransomware attack targeted another Mexican financial institution named Afore Invercap.

You don't need a gun and a mask to hold up a bank anymore.

ATM Attacks

ATM Malware: Since the start of 2018, more than 20 ATM malware families have hit banks around the globe. FASTCash and ATMJackPot are two of the malware applications that caused the greatest damage in 2018 through 2019. The notorious hacking group Lazarus has used FASTCash in dozens of ATM hacks. The attackers inject a malicious executable into the switch application server of the ATM network. FASTCash allows attackers to transmit fake messages that approve fraudulent withdrawal requests.

ATM Card Skimmers: Organized cybercriminal groups install payment card skimmers on ATMs around the world, with new stories emerging daily about perpetrators being arrested. For this technique, attackers put a small device on the ATM's card swipe mechanism. When customers swipe their cards through the skimmer, the device captures the card information, including the card number, expiration date, and full name. These attackers also place an undetectable camera on the ATM to record the PIN number the customer is entering. The groups that install the skimmers later use the information stolen to make fraudulent charges.

Mobile Banking Attacks

Mobile banking attacks can be sorted into two primary categories:

1. Fake banking apps
2. Banking Trojans

Most financial institutions build mobile applications to give customers access to their assets remotely. While such apps might appear to be secure on the surface, they are, in truth, vulnerable to sophisticated cyberattacks because they lack the security features necessary to protect users. MazarBot, BankBot, LokiBot and Anubis are some of the most known examples of banking Trojans.

Anubis: This malware was found on Google Play. It is designed to steal banking credentials, locking personal files on Android devices, and locking users' screens to prevent them from accessing their devices. Anubis is targeting more than 370 banking applications around the world.

Gustuff Banking Trojan: Gustuff was first introduced on a well known Russian cybercrime forum in April 2018 and has since become very popular. This Trojan is capable of phishing credentials and automate bank transactions for over 100 banking apps, such as J.P.Morgan, Bank of America and Wells Fargo. As of April 2019, financial institutions in Australia were under siege by an ongoing malicious mobile malware campaign called "ChristinaMorrow." Attackers are sending the Gustuff banking Trojan via SMS messages to groups of victims. This campaign actively steals banking credentials, phone numbers, and files from the victims' mobile devices. Since the malware is sent as a message that contains a payload-downloading URL sent from one of the group's contacts, people often don't hesitate clicking it. Most of the targets in this campaign work in the financial sector in Australia. The attackers gather the needed data from infected devices, which in turn allow them to pass through two-factor authentication, log in to corporate networks, and propagate the malware even further.

Fake Banking Apps: Google Play unknowingly harbors many fake apps posing as legitimate apps offered by real banks. The legitimate appearance makes it extremely difficult for customers to differentiate between real and fake apps. Users are lured to download these fake apps that steal their bank account and credit card information.

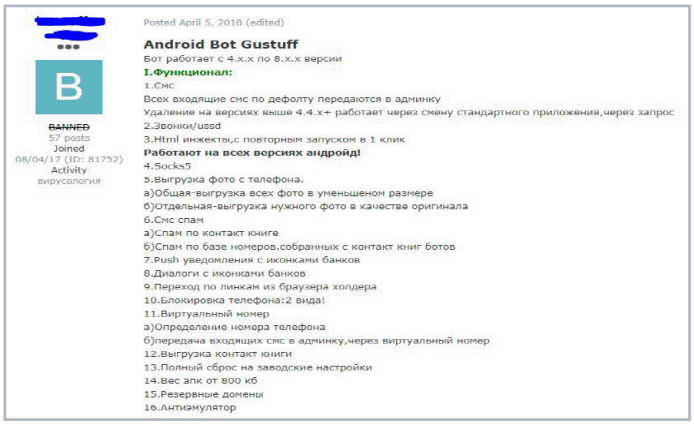


Figure 1: The Gustuff Banking Trojan is offered for sale for the first time on a Russian dark web cybercrime hub.

Figure 2: A real example of a malicious app impersonating a well-known bank.

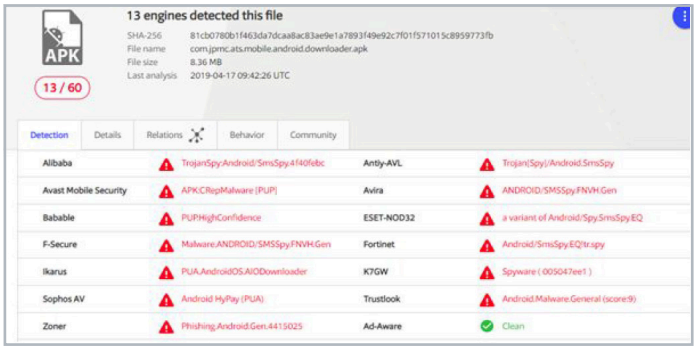
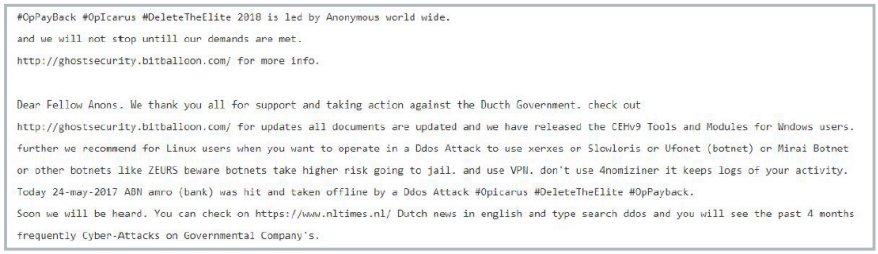


Figure 3: After uploading the app to Virustotal, it was confirmed to be malicious.

Distributed Denial of Service (DDoS)

A DDoS attack involves attacking a bank's network, website, email systems, servers, data transfer and more. According to Verisign, the most-targeted sector in 2018 Q1 was financial services, with 57 percent of its mitigation activity occurring for this industry. Our observations reinforce this, as the finance sector also appears the most on DDoS target lists found on the dark web. In April 2018, the UK's National Crime Agency named DDoS as the leading threat against businesses.



#OpPayBack #OpIcarus #DeleteTheElite 2018 is led by Anonymous world wide.
and we will not stop untill our demands are met.
http://ghostsecurity.bitballoon.com/ for more info.

Dear Fellow Anons. We thank you all for support and taking action against the Ducth Government. check out
http://ghostsecurity.bitballoon.com/ for updates all documents are updated and we have released the CEHv9 Tools and Modules for Windows users.
further we recommend for Linux users when you want to operate in a Ddos Attack to use xerxes or Slowloris or Ufonet (botnet) or Mirai Botnet
or other botnets like ZEURS beware botnets take higher risk going to jail. and use VPN. don't use 4nomiziner it keeps logs of your activity.
Today 24-may-2017 ABN amro (bank) was hit and taken offline by a Ddos Attack #Opicarus #DeleteTheElite #OpPayback.
Soon we will be heard. You can check on https://www.nltimes.nl/ Dutch news in english and type search ddos and you will see the past 4 months
frequently Cyber-Attacks on Governmental Company's.

Figure 4: An example of Anonymous' OpIcarus, an operation designed to take down websites associated with the global financial system through DDoS attacks.

Insider Threats

In some cases, attacks come from within an organization's own network. An example is Qin Qisheng, a former manager in Huaxia Bank's technology development centre in Beijing, who spotted a loophole in the bank's operating system that allowed him to withdraw more than $1 million from the bank's ATM. Qin inserted a few scripts in the banking system that allowed him to test the loophole without triggering an alert. Between November 2016 and January 2018, Qin made 1358 cash withdrawals.

Phishing-as-a-Service (Phishing Kits)

Phishing kits are software packages that streamline the process of copying a site design and uploading it to another web server as a phishing site. They come with simple instructions on how to use them to duplicate a site and upload it to a web server. After the copied site is up, the hacker starts sending phishing emails to target users, attempting to trick them into visiting the site. Phishing kits have increased the quantity and velocity of phishing attacks around the world by lowering the hacker barrier to entry, enabling novices to run campaigns with limited technical knowledge. While this is not a new development or trend, phishing attacks still remain one of the most common methods cybercriminals use to target organizations.

Examples of DDoS attacks on banks:

- May 2018: Dutch banks ABN Amro and Rabobank were the victims of DDoS attacks that left their online banking services unavailable for an extended period of time.
- August 2018: A DDoS attack targeted the website of Spain's central bank, Banco de España.
- November 2018: Russian bank Sberbank reported it registered 62 DDoS attacks in 2018, with 25 of them considered to be high-intensity.

Figure 5: A poster is looking to recruit specific banks' employees on a Russian dark web forum.

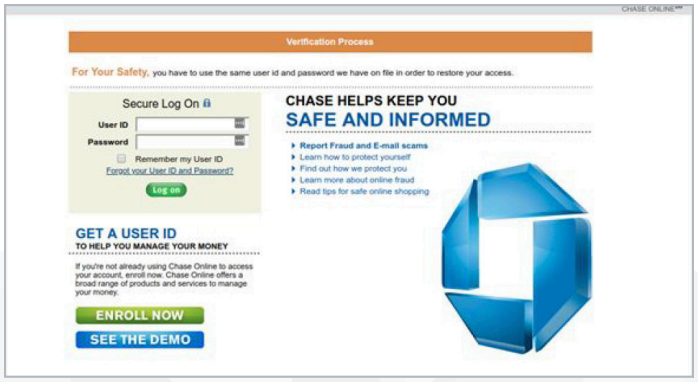


Figure 6: A verified phishing website using a bank's branding to lure in unwitting customers.

Regional Trends

In recent years, threat actors have most frequently targeted banks and financial institutions in developing regions of the world. Our research shows that financial organizations based in Latin America, Africa, and South Asia – primarily India and Pakistan – are particularly susceptible to attacks because many of them lack the same comprehensive security systems that are common at large corporations based in more developed countries throughout North America, Western Europe, and parts of Asia, like Singapore and Japan. With fewer barriers, cybercriminals are able to exploit organizations in developing nations with far greater ease. However, this doesn't mean organizations in developed countries are impervious to cyberattacks.

According to the SWIFT ISAC report issued in April 2019, the banks that suffered the most from cyberattacks involving the SWIFT system were located in countries with a very high risk rating on the Basel AML Country Corruption List. The report also states that in the past 15 months, most of the cyberattacks against financial institutions were in Africa, Latin America, and Central and Southeast Asia. In addition, the targets in all attacks were smaller banks in terms of their volume of international transactions per day.

Latin America

We found numerous successful cyberattacks against Latin American banking and financial services organizations in 2018 and the early part of 2019. There were a wide variety of attack vectors, along with a corresponding wide range of motivations. Organizations in Mexico and Chile were hit particularly hard. Banco de Chile suffered a $10 million theft as a result of a malware attack in May of last year. The attackers used a destructive software as a cover for a fraudulent SWIFT transfer, and a KillMBR wiper tool against the bank's workstations and servers.

Mexico's central bank, Banco de México, suffered an attack in December 2018 in the form of $15 million fraudulent cash withdrawals from five institutions linked to the bank's electronic payment system, SPEI. The attackers used a vulnerability in third-party software connected to SPEI to access the system. Banco de Mexico claimed that neither the SPEI infrastructure nor the client's money were affected. This incident occurred only five months after Bancomext, the state-owned trade bank, blocked attempts to steal $110 million through a compromise in the network that enabled the attackers access to the global SWIFT interbank system.

Financial organizations in developing countries are particularly susceptible to cyberattacks because they lack the comprehensive security systems that are common in more developed areas.

Hackers also attacked the Mexican insurance firm AXA, causing problems to the SPEI interbank payment system. However, AXA reported that clients' information and money were not affected in this attack.

In addition, Hackers infiltrated Chile's ATM interbank network, Redbanc, in December 2018, but it was not discovered until the following month. The attackers gained access to the network after tricking a Redbanc employee into downloading a malicious program during a fake job interview over Skype. The employee was asked to download a software program to submit his application form. Redbanc claimed this attack had no impact on its operations.

Africa

We saw cybercriminal activity in several African countries last year. Western African financial institutions were attacked in a wave of cyberattacks, including organizations in Congo, Ghana, Ivory Coast, Cameroon and Equatorial Guinea. Kenya lost an estimated $297.9 million to fraud and cyberattacks in 2018, with banks being among the top victims. The Central Bank of Kenya expects cyberattacks against financial institutions in the country to increase in both sophistication and frequency. One of Kenya's top banks lost about $1.9 million in a recent cyberattack. The data on Kenya's financial sector shows that fewer than 10 of the 47 banks operating in the country have sufficient security systems.

South African banks have also been prime targets for cyberattacks in recent years. According to the South African Banking Risk Information Centre (SABRIC), the country has the third-highest number of cybercrime victims in the world. From January to August 2018, SABRIC reported that cyber and digital banking crimes resulted in losses of over $13 million, where mobile banking losses increased by 100%. Online banking scams were responsible for more than $6 million in losses, which was the biggest loss in this period.

South Asia

India, Pakistan, and other countries in South Asia are rapidly adopting new technology to catch up with more developed economic powerhouses like Western Europe and the United States. However, in many cases, cybersecurity efforts have lagged behind advances in business operations, leaving organizations in this region to guard expansive attack surfaces without the necessary defense resources.

The most significant example of an attack in South Asia came in October 2018, when more than 150,000 Pakistani credit card numbers were offered for sale on Joker's Stash, a marketplace for stolen credit cards. Pakistan's Federal Investigation Agency declared that almost all banks in the country were affected.

There were two other large-scale cyberattacks against South Asian organizations in the same month. Pakistan's Bank Islami suffered a cyber attack on its international payment card network, as the attackers stole 2.6 million Pakistani Rupees ($19,500) from customers' accounts. The Indian subsidiary of the State Bank of Mauritius was robbed of $14 million through compromised IT systems as hackers used fraudulent SWIFT messages to steal the money. However, the bank was able to recover $10 million.

Another example is the Cosmos Bank in India, the second biggest cooperative bank in India, which lost $13.5 million in August 2018 through unauthorized interbank transactions.

Kenya lost an estimated $297.9 million to fraud and cyberattacks in 2018.

Extending Control into the External Threat Environment

It's no secret that cybercriminals use the dark web as a safe space to operate discreetly and without regulation. The barriers are significantly lesser than operating on the open web, and there is more to gain by stealing digital goods – compromised employee login credentials, corporate data, source code, credit cards, and other corporate assets – than by dealing traditional black market goods like firearms and drugs.

Traditional cybersecurity strategies focus on stopping direct attacks, like ransomware, phishing, DDoS, and malware attacks. Because cybercriminals primarily dwell and operate on the dark web, corporate cybersecurity teams must extend their defense outward to collect and analyze external threat intelligence.

Threat actors are using tactics like social media impersonation, malicious mobile applications, and phishing schemes to circumvent corporate networks and leverage organizations' brands to trick users and run scams. While these are not direct attacks against a corporate system, they can be incredibly damaging and costly. This is why organizations need to be operating in the external threat environment, seeking out threats before they manifest into attacks.

Intelligence gathering is another vital piece of the puzzle. Think of it like a military defense operation: You need to know how and where the enemy will strike, so you deploy special units to gather intelligence on your opponents. In cybersecurity terms, threat actors are constantly looking for weaknesses and ways to circumvent corporate defense systems. Knowing how they will attack and when they plan to do so is crucial to thwart an attack at the start of the cyber kill chain. The sooner you are aware of a threat, the sooner you can take steps to mitigate your risk and neutralize the threat.

In today's increasingly digitized world, financial services organizations need to expand their view of the threat landscape to not just protect against direct attacks, but protect their customers and prevent successful fraud.

The sooner you are aware of a threat, the sooner you can take steps to mitigate your risk and neutralize the threat.

Recommendations for More Effective Cyber Threat Defense

Banks and financial organizations are particularly at risk of suffering cyberattacks, perpetual fraud, brand impersonation, and customer targeting due to the sensitive information they guard. But this doesn't mean the entire industry is resigned to falling victim to these attacks. Looking externally to identify threats at their source can keep your organization one step ahead of cybercriminals looking to penetrate your defenses, commit fraud and scam your customers.Here are our top five considerations for the financial sector to navigate today's dynamic landscape:

1. Infuse External Intelligence Into Your Cybersecurity Operations

Given the rapidly-evolving nature of cyber threats, organizations need to be more proactive in their cybersecurity approach. Businesses that actively hunt for threats and collect external threat intelligence can identify and dismantle attacks before they are even executed. By monitoring hacker activity across the open, deep and dark web, you can identify key attack indications early, and shift your focus from reactive response to proactive mitigation.

2. Compliance With Government Mandates Does Not Ensure Security

In highly regulated industries, like financial services, it would be natural to assume that meeting all government-mandated regulations would ensure secure enterprise networks. But there are cybersecurity threats that have nothing to do with ISO certifications, SSAE certifications, or any other compliance-related protocol. Focusing on risk, instead of simply on being compliant, can help increase an organization's security preparedness and actively engage threats before they manifest into attacks.

3. Operationalize Monitoring and Mitigation to Respond More Quickly

Implementing automation that allows your employees to mitigate threats quickly can help security teams identify and respond to relevant threats. Timeliness is a crucial component of an effective response.

4. Focus on Threats That Relate Specifically to Your Organization

There are millions of IOCs for your security team to sift through, but you need to know how a threat might be targeting your company. Leveraging your digital footprint can help you bring context and prioritization to new threats so you can focus on the real issues threatening your organization.

5. Never Underestimate the Power of Cybersecurity Training

Employees are always a weak link in the cybersecurity chain, particularly those in customer service or support. These individuals are focused on creating a positive customer experience, not on looking for suspicious behavior of potential threat actors. By training your entire organization to be aware of common hacker tactics, you can significantly strengthen one of the most common and successful attack vectors for cybercriminals, employee social engineering. Make sure you have a practical and effective security awareness and training program in place.

About the Author

Hadar Rosenberg
is a Threat Intelligence Research Analyst at IntSights, focused on finding new threat actors, learning their tactics and understanding key trends in the threat landscape. She lived in China for 5 years and speaks fluent Chinese. Hadar researches criminal activity across the dark web to uncover key intelligence from unique sources. She believes the Asian cyber ecosystem is still mostly unknown and finds it very interesting to explore this secret underworld.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the open, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Singapore, Tokyo, New York, Dallas, and Tel Aviv.
To learn more, visit: **https://www.intsights.com.**