



FINANCIAL SERVICES THREAT LANDSCAPE REPORT: THE DARK WEB PERSPECTIVE

JULY 2018

TABLE OF CONTENTS

- 3 INTRODUCTION
- 4 THE GOLDEN AGE OF [CYBER] BANK ROBBERIES
- 5 GLOBAL TRENDS IN ATTACK STRATEGIES
- 7 GLOBAL TRENDS BY THE NUMBERS
- 13 THE TOP THREAT ACTORS TARGETING FINANCIAL INSTITUTIONS
- 17 THE DARK WEB: TURNING A THREAT INTO INTELLIGENCE
- 18 PREDICTIONS FOR 2019
- 19 CONCLUSION & RECOMMENDATIONS FOR FINANCIAL SERVICES ORGANIZATIONS



INTRODUCTION

There's no question that the threat landscape is constantly shifting for financial services companies. Throughout 2017 and the first half of 2018, we've seen a continued increase in attacks that directly target financial organizations, which comes as no surprise. However, increased access to user and account data has enabled cybercriminals to run large-scale fraud attacks and more successful phishing campaigns. These account-centric attacks can be very hard for financial organizations to spot and don't just cause financial losses. They can be incredibly damaging to brand reputation and lead to huge fines. Pre-discovery of these attacks through hacker methods, tools and other indicators is critical for banking and financial services organizations to protect customers, reduce fraud costs and maintain their brand reputation.

Additionally, new laws and regulations have focused financial organizations on maintaining compliance and protecting against direct threats. Therefore, they'll concentrate their attention on vulnerability management, risk assessment and new corporate defense systems that protect against already-known cyber attacks. As a result, they neglect indirect threats that target their customers and don't spend time proactively discovering new threats, attack strategies and actors that target the financial services industry.

The reason that cybercrime and APT groups are continuing to find success attacking banks and financial organizations is because they can perform reconnaissance on their targets using the surface, deep and dark web to greatly increase their attack success rate. Once attackers understand what they are up against in terms of technologies, cyber security defense systems and business process, they can more effectively plan their attack and be successful in nearly half of the ones they launch.

All cyber attacks start with a motivation, which is important to understand in order to properly protect your organization and your customers. Cybercrime groups, scammers and even state sponsored APT groups have two key motivations for attacking a financial institution:

1. **Financial:** High payoffs and the relatively low risk of detection are inspiring criminals to "go online". It is way less likely to get caught hacking a bank than physically robbing a bank.
2. **Cyber Warfare / Cyber Terrorism:** This is considered an act of war. When a state sponsored APT group attacks a bank or other financial services company, it creates fear and financial damage – just like a terrorist attack.

Some groups break up or are caught by law enforcement, but the high profits and the ability to develop and use very sophisticated TTP's (Tools, Techniques and Procedures) ensures a never-ending supply of hackers, groups and motivation to attack financial companies. Cybercriminals are constantly evolving their TTPs much faster than banks can keep up, creating a continuous battle and race to close gaps.

Financial organizations need to expand their view of the threat landscape to ensure they're not just focused on protecting their corporate assets, but also on identifying new threats, protecting their customers and stopping malicious activity before it causes damage. In this report, we'll provide a comprehensive overview of the current threat landscape for financial services and banking organizations based on research conducted by the IntSights Threat Research team and key threat data collected by the IntSights platform. We hope this report helps you understand the important threats and trends that your organization faces so that you can make smarter cybersecurity decisions for the year ahead.



THE GOLDEN AGE OF [CYBER] BANK ROBBERIES

The mid 1800's to the early 1900's could be considered "The Golden Age" of bank robberies. Outlaws like Jesse James, Bonnie and Clyde, and John Dillinger became notorious for their robberies, taking advantage of poor security technology and weak legislation to pull off big heists. However, as new technology became available, like security cameras, silent alarm systems, and timed locks for vaults, banks were able to better defend themselves and deter criminals from targeting them.

Today, banks and financial services organizations are faced with a similar "Golden Age" of cybercrime.

From the start of 2017 through the first half of 2018, cybercrime groups have generated billions of dollars worth of profit and have caused gross losses of more than \$1 trillion to the markets because of their attacks, according to the World Economic Forum¹. Over the past year, we have seen a surge in attempts to attack banks across both existing and new vectors, including targeting major bank transfer platforms (such as SWIFT), phishing emails and phishing websites to steal credentials (targeting both customers and employees), mobile malware and fake mobile applications, ATM scamming methods, ATM and PoS (Point of Sale) attacks, DDoS campaigns and attacks against e-banking interfaces.

Most of these attacks are executed on a daily basis against banks around the globe, but can be divided into 2 general types based on the motivation:

1. **Financial:** cybercrime groups driven by the opportunity to gain financial profits.
2. **Political:** usually conducted by state sponsored APT groups, whose motivation is not always clear or known, but typically driven by political reasons, gaining moral advantage, or just to damage a country's financial stability.


TOP 3 NOTABLE CYBER HEIST INCIDENTS OF 2017 – 2018 (BY TOTAL AMOUNT STOLEN)



\$4.4M
NIC Asia Bank
Nepal
November 2017



\$60M
Far Eastern Bank
Taiwan
October 2017



\$100M
Post-Soviet Bank
Russia
February 2017

TOP 3 NOTABLE DATA BREACH INCIDENTS OF 2017 – 2018 (BY TOTAL RECORDS LEAKED)



90k
BMO and Simplii
Canada
May 2018



143M
Equifax
USA
September 2017



100k
FAFSA: IRS
USA
April 2017



GLOBAL TRENDS IN ATTACK STRATEGIES

MOBILE BANKING AS AN ATTACK VECTOR

From 2H 2016 to 2H 2017, we saw a 24% increase in banking trojan infections from mobile applications, such as the Android/Marcher malware, that took advantage of auto-install vulnerabilities in the Android platform. It victimized millions of Google Play users by impersonating legitimate apps for video players, Flash players, games and system utilities. We have also seen mobile banking trojans delivered as fake updates or through targeted email or SMS phishing. But the most sophisticated so far has been the Android/LokiBot malware, which takes all the functions of Android/Marcher and adds crypto-ransomware capabilities, among other malicious activities. This malware can encrypt files and lock devices, send phony notifications to trick users to open their online banking apps, and even allow the attacker to impersonate the victim's IP address for use in other fraudulent activities. Android/LokiBot has targeted more than 100 financial institutions around the world. By our estimate, LokiBot has generated close to \$2 million in revenue from kit sales on the dark web.

Another growing trend is fake mobile banking applications. With this method, threat actors develop fake mobile applications to steal account credentials and login details from users who unknowingly download the app. Additionally, they will typically infect their victims with malware, usually for harvesting credential and personal information. Bank account logins are one of the top digital goods being sold in [Dark Web black markets](#), so not only do cybercriminals steal login credentials to commit fraud, they can also sell the credentials in black markets to generate further profits.

EXTORTION ATTACKS IN THE NEW AGE OF DATA PRIVACY LAWS

In early 2018, we started to see several attempts to extort banks and financial services, like what happened to [CIBC and Bank of Montreal in Canada](#). In this attack, a threat actor contacted the bank and asked for a fee of \$1M to not publish personal details that they managed to steal. Extortion attacks like this are becoming more and more threatening to financial institutions given new privacy laws across the globe, which are being strictly enforced and can result in huge fines. These fines and brand reputation damage can be way more costly than downtime or lost data. Therefore, organizations are willing to pay more to not have a breach disclosed to the public, rather than pay to regain access to their data.

THREAT ACTORS MOVING TO PRIVATE, PEER-TO-PEER CHANNELS

Dark web black markets are still the main channel for trading bank accounts credentials, credit cards and payment services accounts. However, we have recently seen many black markets vendors move their activities to social media and [private messaging platforms](#) (such as: Facebook groups, Telegram channels and ICQ). This can make it increasingly difficult for security teams and threat hunters to monitor for instances of leaked account information or fraud attempts.

**WANT TO READ
MORE ABOUT
THE CIBC
AND BANK OF
MONTREAL
BREACH?**

**[DOWNLOAD OUR
SUMMARY AND
TIMELINE REPORT]**

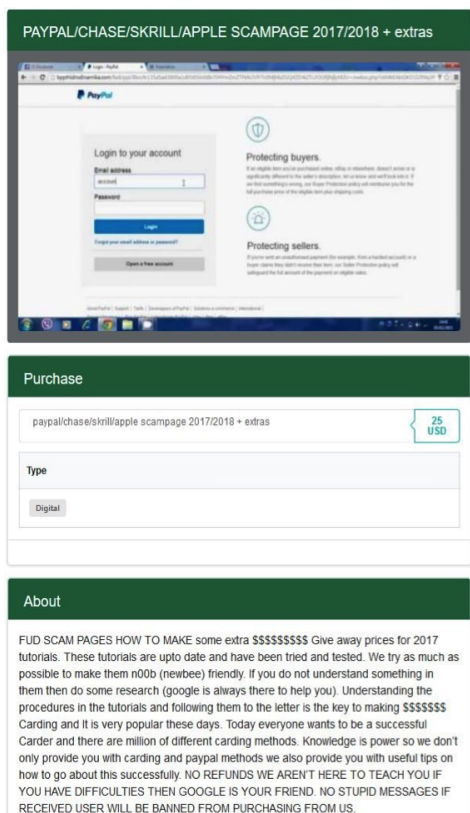
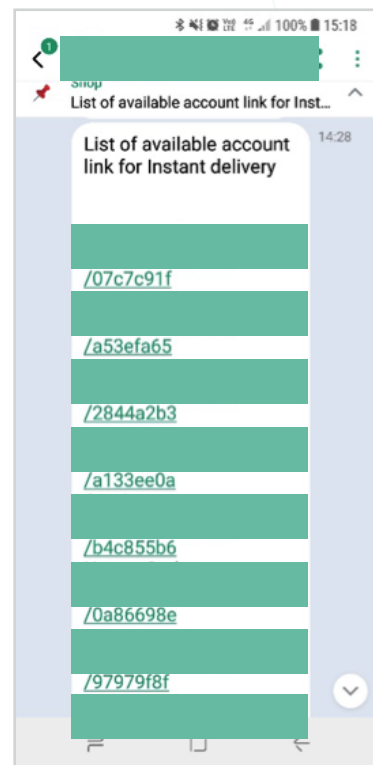


PHISHING-AS-A-SERVICE (AKA PHISHING KITS) LOWERING THE “HACKER BARRIER TO ENTRY”

In recent years, the commodification of dark web services is a well-known trend. High-skilled and technically-proficient hackers offer services and stolen data to novice hackers. This trend certainly did not skip phishing attacks. In the past, phishing attacks were almost entirely dependent on a hacker’s ability to build a site, write the malware programs and launch the campaign. Today, many of the components of a successful phishing attack can be purchased online through these “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. Phishing Kits 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.

Figure 1: Threat Actor Offering Accounts for Sale via ICQ



These kits have significantly lowered the “hacker barrier to entry”, enabling novice hackers to easily run successful phishing attacks on their own. In addition, it’s enabled phishing sites to be developed and launched at a rapid pace. Some sites can be in the air for only a few hours before going down or changing domains. This trend is similar to how new malware is developed. As defense measures and IOC sharing track and identify malware faster and faster through their hash, the malware needs to constantly create new iterations of itself to circumvent these defenses. Phishing Kits have enabled the same rapid change for phishing sites.

But as the dark web goes, there’s a caveat in these Phishing Kits. Many of the hackers that create these tools leave a backdoor in them. This backdoor gives them access to the data that the novice hacker gathered in his phishing attack, thus taking a “cut” out of the novice hacker’s effort, if not robbing him from all the information he obtained.

Figure 2: Phishing Kit Offered for Sale in a Black Market



GLOBAL TRENDS BY THE NUMBERS

METHODOLOGY:

For this section, our methodology is based on data collected by the IntSights intelligence platform. As part of our monitoring and threat intelligence process, we collect data on attack indications, leaked credentials, leaked credit cards and the creation of fake social network profiles, among other threat types as well. For this report, we analyzed data collected on the top 50 banks and financial services organizations in the US and Europe.

Attack indications can be considered a generic term. For this threat landscape report, we focused on 2 key attack indications, which we consider to be the three most relevant attack indications to financial institutions:

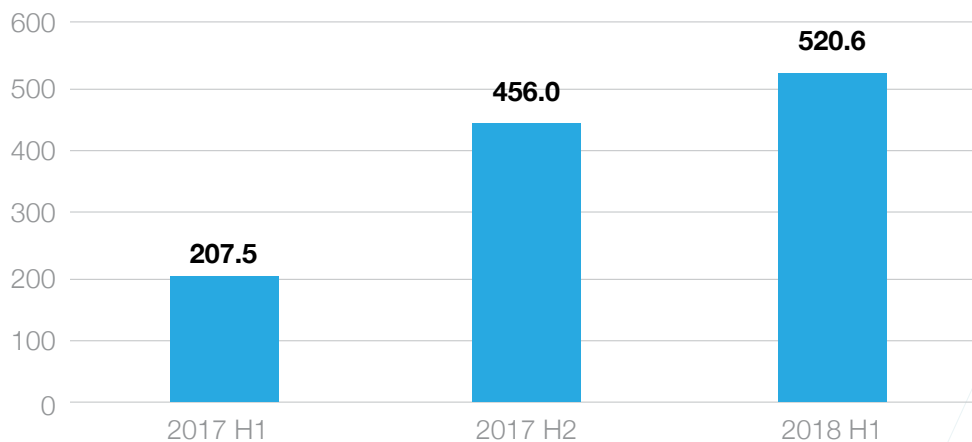
1. Company or customer data is offered for sale in a black market
2. Phishing email target list was found

IntSights monitors cybercriminal activity from thousands of sources across the clear, deep and dark web to help organizations anticipate cyber attacks. Over the past year and half, we've seen the following trends based on alerts and threat types we've identified against financial services organizations.

151% INCREASE IN ATTACK INDICATIONS

Based on our analysis of attack indications, financial organizations are the most-attacked industry. From H1 2017 to H1 2018, we saw a moderate rise in indications to attack financial organizations. In H1 2017, we saw an average of 207 attack indications per US bank. In H1 2018, that figure rose to 520. The indications include dark web chatter mentioning the company, the appearance of company assets (IP Ranges, Domains, Emails, and employee data) in target lists or campaigns, and malware or malware code targeting these companies. This year-over-year increase in attack indications comes as no surprise, as financial companies were, are, and will continue to be targets for threat actors.

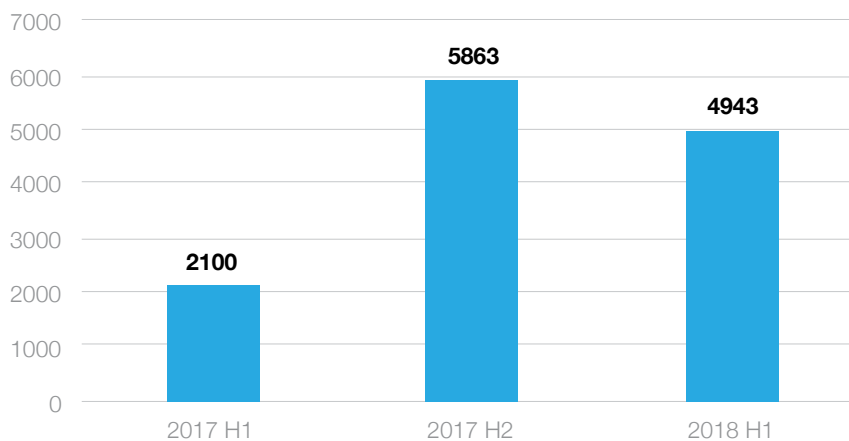
Average Attack Indications Per US Bank



135% INCREASE IN BANK DATA OFFERED FOR SALE IN BLACK MARKETS

Financial information, bank account logins, IP addresses, domain names and other financial records are considered valuable details that can be used for many types of attacks. Based on our data of leaked banking information, we saw a 135% year-over-year increase in financial data being sold on dark web black markets. For the first six months of 2018, we've seen an average of 98.9 incidents of data leakage per bank. That translates to 3.8 incidents per week per bank.

Bank Data Offered for Sale in a Black Market



Traditionally, the top products sold on dark web black markets were drugs, prescription medicines, stolen credit cards, personal information, and carding “cash-out” tutorials. But during the last two to three years, the IntSights research team has seen a growing trend of trading bank accounts logins. Black markets are full of vendors that offer “high balance bank accounts logins” at major banks within the USA, Europe and Asia.

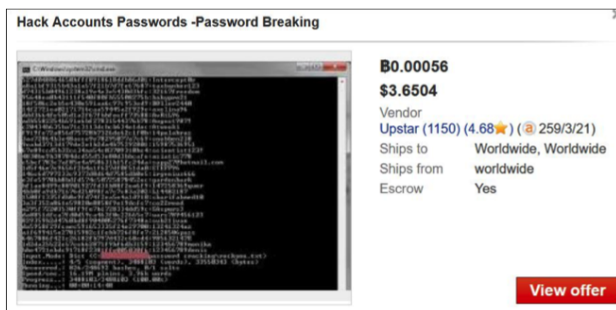


Figure 3: Bank Account Credentials for Sale in a Dark Web Black Market

The cost for a single bank account login with “fullz” (full name, date of birth and full address) is about \$20. Some vendors will sell accounts in groups, for example, 1,000 fresh bank accounts logins can be sold for \$5,000 (or \$5 per account). To distribute account information, hackers will usually use the following channels:

- ✓ Dark web black markets
- ✓ Social networks, such as Facebook, Ren Ren (The Chinese version of Facebook), and VK (The Russian version of Facebook)
- ✓ Chat platforms, such as Telegram, ICQ, Jabber, The Chinese “QQ” and many others

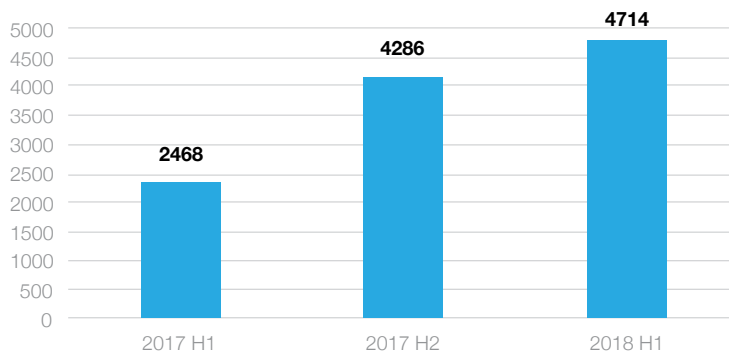


91% INCREASE IN CORPORATE EMAIL ADDRESSES FOUND ON PHISHING TARGET LISTS

Phishing emails are a common and simple attack for hackers of all abilities to perform (as we discussed in Section 3). During the last 18 months, we've seen a 91% increase in financial company employees that are targeted for phishing. In H1 2018, we detected 94.3 phishing target list incidents per bank, which translates to 3.6 target list incidents identified per week per bank.

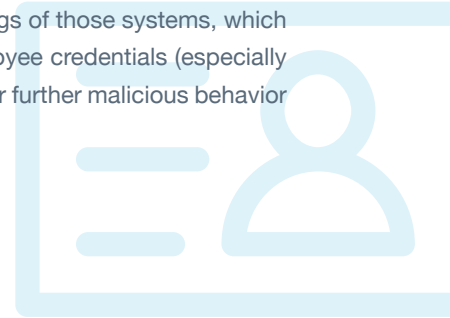


Corporate Emails Found in Phishing Target List

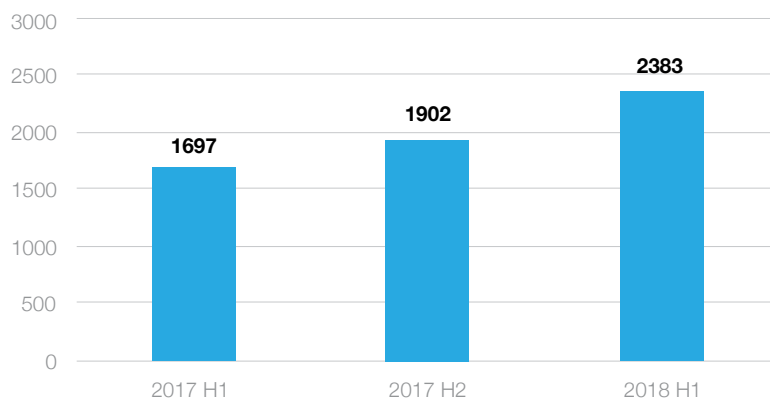


40% INCREASE IN CORPORATE CREDENTIAL LEAKAGE

Whether it's employees or customers, credential leakages are on the rise. Attackers love credentials to financial systems because it makes for easy data theft and fraud. From H1 2017 to H1 2018, we've seen about 40% growth in leaked employee credentials for financial organizations. Leaked credentials enable a whole lot more than simple theft. Gaining access to customer-facing or corporate systems can help hackers understand the inner-workings of those systems, which can be used to facilitate a bigger and wider breach of data or money. Gaining access to employee credentials (especially those of senior management or IT staff) can compromise a trove of data that can later be used for further malicious behavior and schemes.



Leaked Employee Credentials



149% INCREASE IN STOLEN CREDIT CARD INFORMATION

One of the trends we saw over the course of the last year was the commodification of black market trade and services. Access to credit card and account data has made it easy to commit fraud, and companies are typically on the hook to pay for these costs. In 2017, consumers reported \$905 million in total fraud losses². This trend has built a hierarchical system in which higher-skilled hackers sell data to more novice hackers, which has lowered the “hacker barrier to entry” (discussed in Section 3). This has caused a surge in credit card information for sale across black markets.

Over the past 18 months, we have observed a 149% increase in credit card information being sold on black markets. Credit card prices range from single dollars for simple debit cards, to hundreds of dollars for high-end platinum cards. The most common use for these illegally-obtained card numbers is purchasing goods. Whether online or in physical stores, small purchases of tens of dollars don’t attract unwanted attention, but can generate nearly ten times more “free money” than what the card is worth on a black market. This trend is expected to keep rising, as this is the most simple and safe way to reap profits with minimal to no risk. Credit card fraud is essentially a victimless crime, as credit card companies will usually reimburse any customer or retailer who has been hit with such fraud. Therefore, credit card companies are the ones who are primarily interested in stopping these fraud attacks.

Leaked Credit Card Information

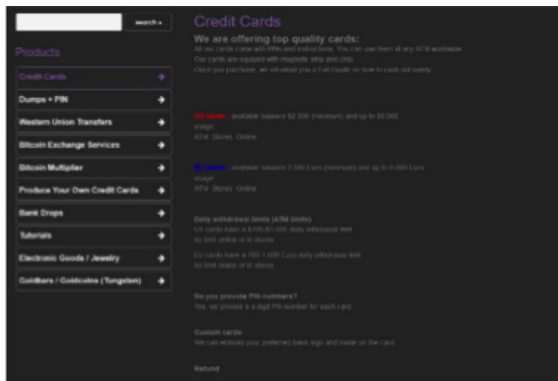
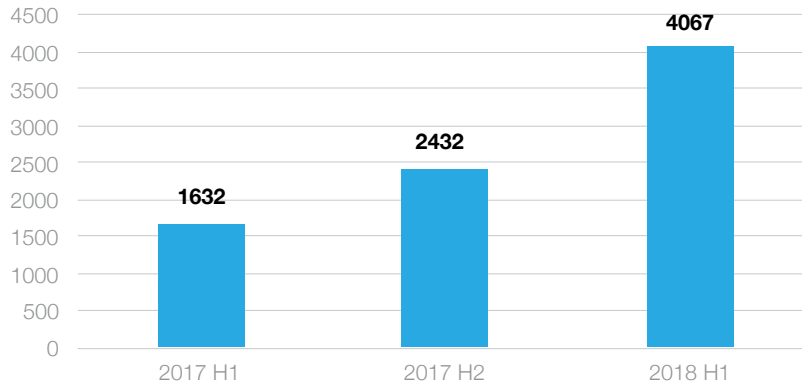


Figure 4: Credit Cards and Payment Service Account Offered for Sale in a Dark Web Black Market

Stolen credit card information (including credit card number, expiration date, CCV, full card owner name and other personal details) and payment service accounts (like PayPal) have always been considered a top-selling product on dark web black markets. However, due to the commoditization of credit card info on black markets, a full slate of credit card details can be sold at just a few dollars. Just like in any free market, vendors have started selling larger volumes of credit cards to maintain competitive pricing with sufficient profit margins.



In 2018, we've typically seen single fresh credit card information for sale starting around \$20 for cards with a relatively low balance amount (e.g. \$100). For cards with higher balances (e.g. \$10,000) hackers can get up to \$1,000 per card. Each card comes with the full details about the card owner (full name, full address, email, CVV, PIN and expiration date). Another option is buy a dump of cards, CVV, expiration dates and pins. A dump of 100 cards usually costs about \$150 - \$500 depending on the dump quality.

Payment service accounts are usually sold anywhere from a few dollars to up to \$50. Just like with bank account details, credit card and payment service accounts are usually distributed by hackers via the following channels:

- ✓ Dark web black markets
- ✓ Social networks, such as Facebook, Ren Ren (The Chinese version of Facebook), and VK (The Russian version of Facebook)
- ✓ Chat platforms, such as Telegram, ICQ, Jabber, The Chinese "QQ" and many others

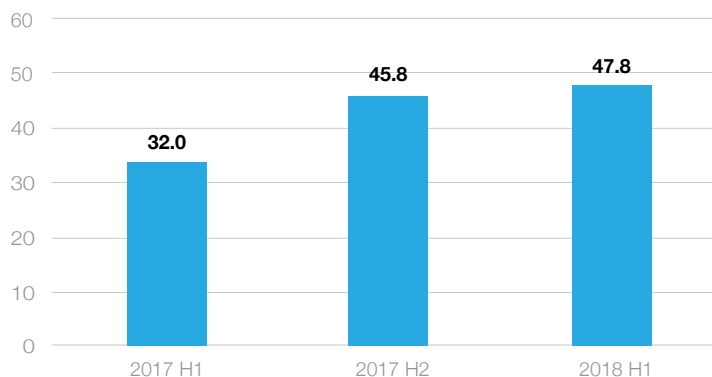
49% RISE IN FAKE SOCIAL MEDIA ACCOUNTS

Social media has become a popular tool for hackers because many users assume profiles and pages are legitimate. Fake social media profiles, apps, and accounts can be used in a variety of malicious ways. A fake profile can lure users to phishing sites or downloading fake apps. It can pose as customer service and ask for confidential information. It can spread false information to misdirect the public, manipulate stock price or influence the public to buy or sell. Additionally, it can also be used to harvest personal data and enrich other personal data that the attacker might hold.

We saw a moderate rise from 2017 to 2018 in fake social media accounts for financial organizations. In H1 2017, we saw an average of 32 fake profiles per US bank. That figure rose to 47.8 in H1 2018, which translates to nearly two new fake profiles created per bank each week.

Social media has become the new "town square", and as such, we believe we will continue to see this tactic used by cybercriminals to dupe unknowing users with poor technical skills.

Average Faked Profiles Created per US Bank



MOBILE BANKING AS AN ATTACK VECTOR

As we discussed in Section 3, fake mobile banking apps that mimic major blue-chip banking apps are having resounding success for hackers. In fact, more than 1 in 3 consumers are fooled by fraudulent mobile apps. As more banking activities move to mobile, users have a greater risk of being tricked by cybercriminals and falling victim to mobile banking theft.

According to a survey from Avast, 58% of mobile banking application users identified the official mobile banking app as fraudulent, while 36% mistook the fake interface for the real one. These findings highlight the level of sophistication and accuracy applied by cybercriminals to create trusted and high-quality copies, which are designed to spy on users, collect their bank login details and steal their money.

Another common use for a fake mobile banking application is to serve as a convenient platform to infect users with types of malware. We are seeing a steady increase in the number of malicious applications for Android devices, which can bypass security checks on popular Android app stores (including Google Play) to make their way onto consumers' phones. Additionally, other applications (like gaming apps) can contain banking trojans that steal user credentials. Android users should be cautious when downloading any application and ensure they have a strong antivirus for Android installed to detect and protect from money-grabbing malware.

While financial companies have continued to invest in tools and processes to protect themselves, their large customer bases make them very attractive targets for cybercriminals. Fake mobile applications can be effective because they can be developed and deployed outside of any bank systems, making them difficult to identify and monitor for.



THE TOP THREAT ACTORS TARGETING FINANCIAL INSTITUTIONS

CYBERCRIME GROUPS

Cybercrime groups can have a range of motives, attack a wide variety of targets and are characterized by varying capabilities, TTP's (Tools, Techniques & Procedures), modus operandi and more. When attacking the financial sector, these groups focus on fraud, burglarizing ATMs, executing transactions through the SWIFT systems and penetrating intranets of financial organizations through the use of banking malware.

The most dominant groups in the financial sector are: MoneyTaker, Carbanak and Cobalt. You can find an overview of each group below.

MONEY TAKER

Country	Russia
Threat Level	High
Level of Sophistication	High, the group is known for their self-developed attacking tools, customization of public tools for their needs, tools for erasing footprints, and malware that will run even after rebooting.
Countries of Operation	Worldwide
Typical Targets	Banks, financial services companies, supply chain (companies providing services and/or technology to financial companies)
Attacking Tools	<ul style="list-style-type: none"> • MoneyTaker – for altering the details of accounts that are about to receive a money transfer • Metasploit and powershell – for hacking, gaining control and stealing authorizations • Screenshotter / Keyloggers – for recording keystrokes and screenshots • LogMeIn Hamachi, UltraVNC, Plink and NirCmd – for gaining remote control and executing orders. The latter tool also enables deleting values and keys from the registry, establishes communications with a VPN, alters files, alters computer definitions, etc. • ASLRSideChannelAttack – for stealing highly classified authorizations • Mimikatz – for stealing identification details (usernames and passwords) • PsExec – for running processes locally through RDP/SMB/RPC protocols • Banking Trojans – Citadel and Kronos
Attributed Campaigns	More than 20 successful attacks on banks, financial institutions and law firms in the USA, UK, and Russia.



CARBANAK

Also Known as	Annaunak, Anunak, Carbon Spider, FIN7, Navigator, TelePort Crew, Calcium
Country	Russia
Threat Level	High
Level of Sophistication	High, the group is considered to have a sub-state capability. The types of malware that the group uses provide a wide range of possibilities, including threat of authorizations, disabling AV tools, threat of credit cards details and personal information, seizing control over R&D and more.
Countries of Operation	USA, Germany, Eastern Europe, Ukraine, China, Malaysia, Kuwait and West Africa
Typical Targets	Banks, financial services companies and e-commerce / retail corporations
Attacking Tools	<ul style="list-style-type: none"> • Carbanak – self-developed backdoor • Designated malware, such as Zeus • Backdoor of the Anunak group signed by a Comodo SSL certification • VBScript and PowerShell script files • Metasploit, PsExec, Mimikatz, FreeRDP, NCat, NPing • NetScan, Backdoor Batel • MBR Eraser – for erasing footprints • Soft Perfect Network Scanner – for Lan Scans • SSHD backdoor – for stealing passwords and gaining remote access • Ammy admin remote administration tool and team viewer – for gaining remote access • Andromeda – botnet for lateral infection • Bateleur – for stealing financial information
Attributed Campaigns	<ul style="list-style-type: none"> • More than 300 successful attacks on banks, financial institutions and retailers • Attack on Oracle systems and the company support portal



COBALT

Also Known as	MetaStrike
Country	Russia
Threat Level	High
Level of Sophistication	High, sub-state capabilities, including detection and exploitation of vulnerabilities, and ongoing updating of the systems and targets they attack.
Countries of Operations	Europe, Russia, Ukraine, Thailand and Taiwan
Typical Targets	Banks
Attacking Tools	<ul style="list-style-type: none"> • Buhtrap worm • Cobalt strike and Metasploit • Mimikatz • LightManager tool for enabling remote access to computers • Team viewer • Guide – legitimate document creation software that enables hackers to install and load their main module • SDelete – tool for irretrievable file deletions
Attributed Campaigns	<ul style="list-style-type: none"> • Theft of \$9.7 M from the Russian MetakinvestBank • ATM's theft of \$2.18 M from Taiwan banks • SWIFT attack on Russian banks • More than 200 other attacks on banks in Europe, Thailand, Turkey and Taiwan

WHAT DRIVES NATION-STATE APT GROUPS

We know that hackers hack for a variety of reasons. Some hack for financial profit or for information that is worth money. Some hack to satisfy their egos or gain peer recognition. Some hack alone, and some hack in groups. But many hackers, or more accurately “hacktivists,” join groups like Anonymous in order to demonstrate their dissatisfaction with powerful organizations, such as corporations and governments who fail to share their world views. These hackers don’t consider themselves to be bad actors. They see their activity in a positive light, viewing themselves as contributors to a greater body of knowledge, and often hacking without a clear vision of the second-order effects of their actions.

However, another category of hacker supports nation-state strategy by operating in the cyber domain. These hackers are difficult to categorize, since they may be directly employed by an arm of a national government or may be from an organized crime entity employed by a national government. Think of recent hacks like JP Morgan Chase, which was attributed to an undefined group in Russia. Understanding the motivation of hackers and the organizations whom they are associated with is essential to understanding their tactics. Knowing one’s enemy is a fundamental concept in kinetic warfare and is equally important, albeit more difficult, in the cyber environment.



It is valuable to explore nation-state, and nation-state-sponsored APTs, because they generally have deep resources and their collective motivations run across the spectrum. Because nation-state APTs are funded extremely well relative to small groups and individuals, they can be particularly formidable adversaries for other countries and for commercial industries, regardless of vertical. In short, nefarious nation-state-sponsored cyber activity can have devastating effects on a country’s national security and its economy. All nation-state groups are not created equal, and like individual hackers, each has a different motivation and level of cyber capability. As we look at the cyber terrain from a global perspective, we see several countries that surface in the media most often: China, North Korea, Russia, Iran and the US.

LAZARUS GROUP

Also Known As	DarkSeoul, Silent Chollima, Hastati Group, Bureau 121, Unit 121, NewRomanic Cyber Army Team, Hidden Cobra
Related Sub-Groups	Bluenoorf, Andariel
Country	North Korea
Threat Level	High
Level of Sophistication	High, the group has powerful capabilities, independently developed tools, leverages commercial tools, sophisticated modus operandi, capabilities evading cyber defense systems, three-tiered attack servers and encrypted communications.
Countries of Operation	Worldwide
Typical Targets	<ul style="list-style-type: none"> • Banks, financial organizations and governments
Attacking tools	<ul style="list-style-type: none"> • Banswift – Malware used to steal information • Solarbot – botnet used to steal personal details from online forms • Ratankba / QuickRide – tool for collecting information from a computer, it also can download and upload executable files • Enigma Protector – tool used to protect executable files • SilverLight – tool used to exploit vulnerabilities in Flash • Recon – scanning tool used to identify systems of interest
Attributed Campaigns	<ul style="list-style-type: none"> • The attack on Sony Pictures • WannaCry ransomware attack on multiple organizations around the world • Theft of \$12 M from Banco del Austro in Ecuador • Theft of \$1 M from Tien Phong Bank in Vietnam – SWIFT attack • Theft of \$81 M from the Central Bank of Bangladesh • Theft of \$60 M from FEIB Bank in Taiwan • Theft of \$5 M from various banks in Nepal



THE DARK WEB: TURNING A THREAT INTO INTELLIGENCE

When you think about the different types of cyber threats, what are the ones that immediately spring to mind? Most people will think along the lines of ransomware, phishing, distributed denial-of-service (DDoS) and malware.

These kinds of attacks are significant, and obviously deserve your attention when it comes to security. However, they are also a very specific type of TTP used by cybercrime groups to attack an organization directly. However, this focus on stopping direct attacks typically blights an organization's view of the cyber threat landscape. As we've outlined in this report, cybercriminals continue to find ways around corporate defense systems and have begun circumventing these defenses using social media, mobile application stores and phishing schemes. These tactics leverage an organization's brand and credibility to trick users and run scams. While this is not a direct attack against a corporate system, these attacks can be incredibly damaging and costly.

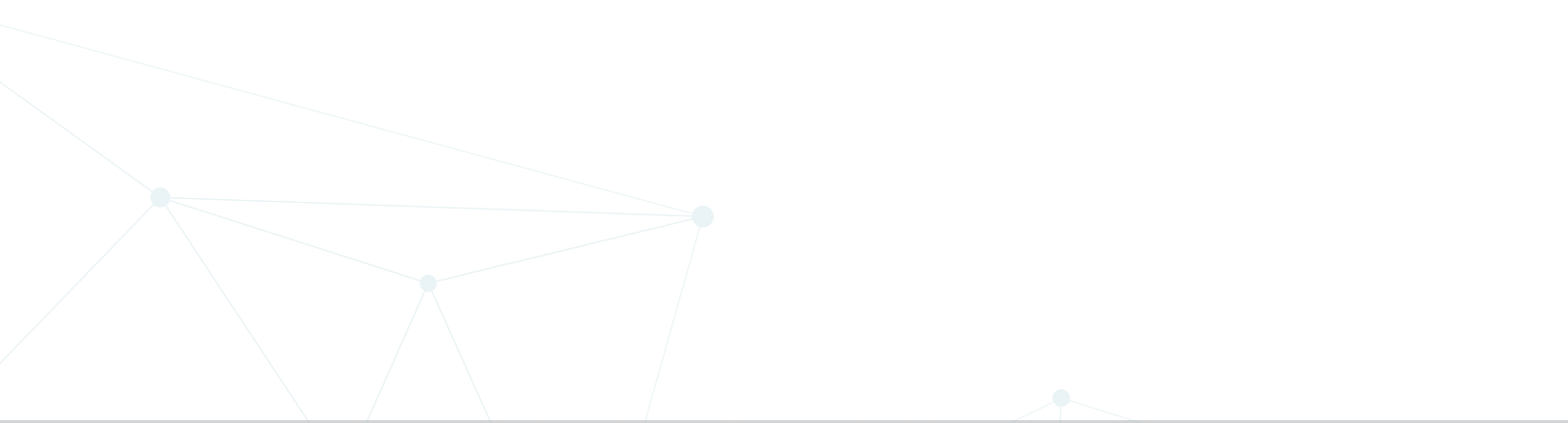
As a result, financial services organizations need to expand their view of the threat landscape to not just protect against direct attacks, but protect their customers and prevent successful fraud.

TURNING DARK WEB ACTIVITY INTO THREAT INTELLIGENCE

The dark web is a comfort zone for illegal activities, such as buying and selling drugs, weapons, PII and corporate information. As personal and corporate data becomes increasingly lucrative, cybercriminals are shifting more focus to these "digital goods" because the risks are much lower compared to dealing and delivering guns or drugs. When data is stolen, criminals turn to the dark web and black markets to make a profit from "digital goods", like compromised employee login credentials, stolen data, source code, stolen credit cards and other information about the organization and its customers.

Because the dark web doesn't constitute a direct attack on an organization, like ransomware or phishing, many companies do not consider the dark web as part of their security strategy or digital attack surface. However, you have an opportunity to use this dark web activity to identify early indications of attacks against your customers, your employees and your corporate systems.

Leveraging dark web threat intelligence can help you widen your view of the threat landscape and ensure you are identifying and mitigating attacks before they cause financial or reputational damage.



PREDICTIONS FOR 2019

Based on the data and activity we've tracked over the past 18 months, here is how we expect the financial services threat landscape to continue changing, and which tactics cybercriminals will use to exploit systems, employees and customers.



Infiltrating Large Supply Chains Through Small Vendors

By infiltrating vendor software or SaaS products that are used in larger technology supply chains, criminals can compromise many enterprises simultaneously. Even large, established technology solutions used by financial companies could become susceptible to breaches.



Attacking 3rd Party Software Tools

As more developers rely on 'plug and play' software kits and open source, they are more likely to become the target of attacks. And because 3rd party software is used in so many different applications, breaches would be hard to patch quickly without service disruptions.



Increase in Cyber-Attack-as-a-Service

Why bother to plan and execute a cyber-attack on your own? Hackers for hire and Cyber-Attacks-as-a-Service have become very affordable, enabling any lowly cybercriminal to launch attacks against banks and financial firms. For anywhere from a few hundred dollars to few thousand dollars, you can run a massive DDoS or phishing attacks with limited knowledge of how they work.



Extortion Attacks Will Become the New Ransomware

One of the most significant landmarks of 2018 is privacy laws and the awareness for user privacy. Given the large fines for GDPR laws and massive data breach incidents in the US that drew attention from the Senate, we believe attackers will try to leverage a company's fear of similar incidents. Regulation fines and brand reputation damage can be way more costly than downtime or lost data. Therefore, organizations are willing to pay more to not have a breach disclosed to the public, rather than pay to regain access to their data. Hackers will leverage this fear as a tactic to get more money.



Black Markets Vendors Moving to Social Media and Private Chat Rooms

As we've previously noted, many black market vendors are moving their business operations to social media platforms (such as Facebook closed groups) and encrypted chat rooms (such as Telegram, ICQ and Jabber). We expect this trend to continue over the next year as it provides black market vendors with better privacy and secrecy. By doing so, it will be harder for law enforcement agencies to track and monitor their activities.



CONCLUSION & RECOMMENDATIONS FOR FINANCIAL SERVICES ORGANIZATIONS

While the threat of a cyberattack is something that every enterprise needs to consider, banks and financial organizations are especially at risk due to the sensitive and financial information they store. The good news is that there are effective early detection and mitigation steps that can be taken to reduce successful attacks against your organization and your customers. Here are our top five considerations for the financial sector today.

1. Use Threat Intelligence to Take a Proactive Approach to your Security Program

Attacks over the past few years provide an excellent example of why organizations should take a proactive approach to enterprise cybersecurity, rather than a reactionary one. Businesses that conduct active threat hunting and collect cyber threat intelligence can prevent cyber attacks before they are even executed. By monitoring common hacker activity across the clear, deep and dark web, you can identify key attack indications early, and shift your focus from reactive response to proactive mitigation.

2. Evaluate Risks – Not Just Compliance – as a Way to Increase Security

In regulated industries like financial services, it's easy to assume that if all government-mandated regulations are met, the enterprise is secure. However, meeting compliance never means you're completely secure. 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 compliance, can help increase an organization's security levels and ensure you're working on stopping threats, not meeting compliance standards.

3. Leverage Automation Tools to Sift Through the Noise

Data has proliferated at such an incredible pace that automation is necessary for security teams to identify actual threats. If your team is spending much of their time manually scanning messages or data for threats, they're losing valuable time that could be spent addressing threats, proactively patching the most urgent vulnerabilities, and prioritizing other security actions. Implementing automation software that allows your employees to focus on acting, instead of searching for where they need to act, can help security teams filter through the massive amounts of data to identify and respond to relevant threats.

4. Track Threats Specific to Your Organization

Many cyberattacks could be prevented if it was clear that a specific threat or vulnerability could be used against the organization. By monitoring and tracking specific threat types and threat actors, we can be better prepared for and defend against cyber threats.

5. Never Underestimate the Power of Cyber Security Training

Employees are always a weak link in the cybersecurity chain. 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. Make sure you have a practical and effective security awareness and training program in place.

ADDITIONAL SOURCES

1. <https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/>
2. <https://www.experian.com/blogs/ask-experian/identity-theft-statistics/#s2>





ABOUT THE RESEARCHER: ITAY KOZUCH

Itay Kozuch is the Director of Threat Research at IntSights. He is a cybersecurity expert with over a decade of experience managing cyber-security and threat research. Prior to IntSights, Itay served as a Manager and Head of Cyber Technologies at KPMG. He previously led cyber projects and served as a CISO for major companies in Europe, West Africa and Central America.

ABOUT INTSIGHTS

IntSights is redefining cyber security with the industry's first and only enterprise threat management platform that transforms tailored threat intelligence into automated security operations. Our ground-breaking data-mining algorithms and unique machine learning capabilities continuously monitor an enterprise's external digital profile across the surface, deep and dark web, categorize and analyze tens of thousands of threats, and automate the risk remediation lifecycle — streamlining workflows, maximizing resources and securing business operations. This has made IntSights' one of the fastest growing cyber security companies in the world. IntSights has offices in Tel Aviv, Amsterdam, New York and Dallas and is backed by Gililot Capital Partners, Blumberg Capital, Tola Capital, Blackstone and Wipro Ventures.

To learn more, visit www.intsights.com.