SWIFT Institute

SWIFT Institute Working Paper No. 2016-004

Forces Shaping the Cyber Threat Landscape for Financial Institutions

William A. Carter

Publication Date: October 2, 2017

The views and opinions expressed in this paper are those of the authors. SWIFT and the SWIFT Institute have not made any editorial review of this paper, therefore the views and opinions do not necessarily reflect those of either SWIFT or the SWIFT Institute.

Contents

I. Executive Summary

Financial institutions have long been the leading targets for cybercrime, but the tools and tactics used are changing. New technologies are increasingly incorporated into financial networks and the broader internet, transforming the attack surface that adversaries can exploit. The incentives for attackers are also shifting, forcing banks to face more numerous and sophisticated adversaries. And as cyber awareness grows in the financial sector and firms continue to invest billions in new defenses, attackers are changing their approaches to stay one step ahead.

Consumer bank and credit card fraud remains the number one form of cybercrime affecting financial institutions, but the tactics and targets are changing. Fraudsters are increasingly targeting mobile devices and business customers, while traditional credit card fraud and PoS attacks remain a leading form of consumer fraud, but are losing dominance.

Digitization is also transforming the geography of cybercrime by bringing billions of users in developing markets online, providing criminals with new targets with limited cybersecurity awareness and low defenses. Developing markets in Asia are the primary targets now, but as millions of customers are brought online in Latin America and Africa, criminal communities are flourishing in these regions.

As fraud prevention and retail security have improved and the value of stolen credit card data and bank credentials has declined, attackers have stepped up large-scale coordinated attacks on financial institutions' core networks, going for a few very large payouts instead of lots of small ones. Extortion is the number one concern for financial institutions, as internet of things (IoT) botnets and mass distribution of sophisticated crypto-ransomware threaten to take banks offline. "Don't click the link" campaigns have helped to make traditional phishing attacks less effective, so attackers are increasingly using pretexting and watering-hole attacks to gain access to bank networks.

Once inside, attackers are combining multiple cash-out strategies to extract millions of dollars of profits from their victims over the course of months. Instead of dealing with a single Distributed Denial of Service (DDoS) attack or ransomware attack, financial institutions find themselves grappling with multi-layer DDoS attacks that provide a smokescreen for criminals to conduct thousands of fraudulent transactions and steal customer data, covering their tracks by utilizing ransomware.

The adversaries defenders must be prepared to face are also changing. Increased geopolitical tensions between the existing cyber powers could lead to increases in espionage and disruptive attacks on financial institutions, and for the first time nation state actors have been observed engaging in financially motivated cybercrime. With more than 30 new countries investing in developing offensive cyber capabilities, the nation state threat landscape is poised to expand dramatically.

At the same time, the proliferation of easy-to-use malware and contract hacker services on the black market has opened up sophisticated attacks to a wide range of adversaries. What were once exclusively nation state capabilities are now available to organized crime groups that work with governments, and even to generic cybercriminals through open-source malware libraries. Automation allows criminals to leverage these resources to launch attacks cheaply at scale, making their lives easier and defenders' lives more difficult. The most sophisticated groups are exploiting the connections between financial institutions, breaching small banks to rob large ones and taking advantage of international borders and lack of capacity in developing markets to evade capture.

As attackers become more sophisticated and more targeted, defenders will need to devise new ways to protect the whole financial system down to its smallest links, not just their own networks. The financial system is global and it is integrated, and defenders need to become more global and better integrated to keep up. Small and medium financial institutions, particularly in emerging markets, serve as easy entry points to the global financial system. The industry's leaders will need to strengthen their smaller partners and help build cyber awareness and capacity in emerging markets to stay ahead of attackers who are sophisticated and savvy enough to exploit the weakest links in the system.

Protecting financial networks not only requires financial institutions to improve the security of their own systems, but to change the security balance of the entire internet environment. Cyber threats to financial institutions increasingly come from insecure low-cost mobile and IoT devices outside their own networks. This requires new approaches to defense, including developing new authentication and monitoring technologies for bank networks, and supporting the development of security solutions for these new devices outside the banks' own networks. Improving cybercrime education and awareness for new internet users in the developing world and supporting efforts to build law enforcement capacity to combat cybercrime around the world is also critical.

Many financial institutions recognize the growing risks of cybercrime and are investing in their cyber defenses, but as changes in the attack surface, attacker incentives, and defenses evolve, so will the threats. Understanding the forces that shape the threat landscape is essential for financial institutions to get ahead and stay ahead of their adversaries in cyberspace.

II. Introduction

Financial institutions have long been the leading targets for cybercrime. Banks are where the money is, and the industry provides the most profitable avenue for hackers to monetize their skills. Early intrusions by script kiddies and hacktivists were mostly motivated by a desire to build a reputation in the hacker community, but were relatively unsophisticated and did little damage. By 2000, however, cybercriminals were starting to see the potential of computer intrusions, and since then have become more organized, technically skilled, inventive, and brazen. A brazen attack on Bangladesh Bank in 2016 attempted to steal $1 billion in a single stroke.[1]

Financial institutions have taken notice. Cybersecurity is consistently ranked as one of the top risks to financial institutions in surveys,[2] reflecting the accelerating pace of high-profile attacks over the last few years. The financial industry experienced more data breaches than any other industry in 2016,[3] and data breaches cost financial institutions an estimated $245 per stolen record (including indirect costs), well above the average of $141.[4]

Defenses continue to evolve, but attackers seem to stay ahead. Financial services is the fastest-growing and largest market for cybersecurity products and services. Information security spending by global financial institutions grew 67% from 2013-2016,[5] and in the U.S. alone, financial sector cybersecurity spending is expected to total $68 billion cumulatively from 2016-2020.[6] There are signs that this investment is having an impact. According to some surveys, cybersecurity incidents in the financial sector have remained relatively constant over the last three years, but the types of incidents have evolved.[7]

[1] Kim Zetter. “That’s Insane, $81M Bangladesh Bank Heist? Here’s What We Know.” *Wired*, May 17, 2016. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

[2] “Cybersecurity is the most prevalent IT risk for banks.” KPMG, September 6, 2016. https://home.kpmg.com/bh/en/home/insights/2016/09/cyber-security-most-prevalent-it-risk-fs.htmlb ; Joseph E. Silva. “Top 10 Issues Facing Financial Institutions in 2017.” *The National Law Review,* March 6, 2017. http://www.natlawreview.com/article/top-10-issues-facing-financial-institutions-2017 ; “Top 10 operational risks for 2017.” *Risk.net*, January 23, 2017. http://www.risk.net/risk-management/operational-risk/2480528/top-10-operational-risks-for-2017 ; “2017 Risk Practices Survey.” Bank Director, 2017. http://www.bankdirector.com/files/7714/8941/6245/2017_Risk_Practices_Survey.pdf

[3] Verizon. “2017 Data Breach Investigations Report: 10th Edition.” http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[4] Ponemon Institute LLC. “2017 Cost of Data Breach Study.” June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

[5] Pricewaterhouse Coopers. “Global State of Information Security Survey: 2017.” http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html

[6] Homeland Security Research. “U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020.” May 2016. http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/

[7] Pricewaterhouse Coopers. “Global State of Information Security Survey: 2017.” http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html

Consumer fraud has been around for decades, and remains the top form of financial crime. Cyber theft of credit card data has been around since the dot com era in the early 2000s.[8] Banking Trojans have been prolific at least since Zeus was discovered in 2006.[9] But new threats have also emerged in recent years. In 2012 and 2013, disruptive attacks by nation states took center stage with the Operation Ababil[10] DDoS attacks on U.S. banks by Iran and the DarkSeoul[11] attacks on South Korean banks by North Korea. More recently, highly skilled organized crime groups like Carbanak, Corkow, Dridex, Cobalt and Buhtrap that specialize in targeted cyber attacks on financial institutions have gained notoriety after stealing billions of dollars from bank networks.[12]

In order to gain insight into the current forces transforming the threat landscape for banks and the impact of new defenses on attacks, we reviewed data on financial cybercrime activity, as well as some of the high-profile attacks on the financial sector in the last few years. We also conducted interviews with bank executives, regulators, law enforcement officials, and cybercrime and cybersecurity experts from around the world.

In this paper we examine these forces and their implications for the threat landscape of the future. In section III we discuss the threat landscape for financial institutions' customers, and how new developments in fraud detection and prevention are changing the nature of bank fraud. In section IV, we delve into the new tactics that organized criminal groups are using in targeted attacks on financial institutions' own networks.

III. Consumer fraud: New defenses and mobile banking are transforming the landscape

Financial institutions are not only improving defenses on their own networks. They are also providing new and more effective protections for their customers, employing new tools like multi-factor authentication and chip cards to cut down on consumer credential theft, and introducing machine learning to enhance fraud prevention.

a) New defenses are transforming consumer fraud and carding

[8] "The Past, Present and Future of Credit Card Security." *The One Brief*, retrieved June 12, 2017. http://www.theonebrief.com/the-past-present-and-future-of-credit-card-security/

[9] TrendMicro. "A Brief History of Notable Banking Trojans." *TrendMicro Blog*, August 31, 2015. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

[10] Roland Dobbins. "Breaking the Bank: An Analysis of the 2012-2014 'Operation Ababil' Financial Industry DDoS Campaign." Proceedings of the APNIC 36 conference, February 2014. https://conference.apnic.net/data/37/breakingthebank.pdf

[11] Jonathan A.P. Marpaung and HoonJae Lee. "Dark Seoul Cyber Attack: Could it be worse?" Proceedings of CISAK 2013 Conference, May 12, 2013. http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf

[12] Group-IB. "The evolution of targeted attacks on financial institutions." June 2017. http://bibf.com/cybersecurity/wp-content/uploads/2017/06/Evolution-of-Targeted-Attacks-on-Financial-institutions-NGN.pdf

For criminals, targeting a bank's customers is often cheaper and easier than targeting the banks themselves. Most banks see their customers as the weakest link in their IT security.[13] Consumer credential theft and card skimming remains the most costly form of cybercrime for financial institutions,[14] but new defenses are pushing attackers in different directions. In recent years, large-scale attacks on point-of-sale (PoS) systems have been a major headache for banks whose security has focused on their internal systems and traditional online banking portals. PoS attacks became so prevalent that the underground market has become flooded with credit-card information, sending prices plummeting and forcing carders to compete over customers through rewards programs, product guarantees, and 24/7 customer service.

Banks have also adapted their defenses, implementing new fraud prevention measures and improving their ability to block compromised cards quickly. The adoption of chip cards in the U.S. and improvements in retailers' security practices have made carding more difficult, even as it has become less profitable. The combination of lower profit margins and better security has caused a shift in the market. PoS malware development in the U.S. declined by nearly 90% in 2016,[15] and carding activity has shifted almost entirely to card-not-present fraud. Not all consumers have benefitted equally from this shift, however. The Chinese underground, for example, has grown its carding offerings dramatically, and PoS and ATM skimmers and stolen credit card data have become top offerings.[16]

b) *As consumer bank fraud becomes harder, business customers are being targeted*

One way that fraudsters are replacing lost income from consumer financial fraud is by targeting businesses. The most prevalent form of financial fraud targeting businesses is business email compromise (BCE), in which fraudsters send fake emails to employees pretending to be the boss and ordering them to make large transfers from the companies' bank accounts. The practice has become so prevalent that the FBI instituted a public awareness campaign in the U.S., issuing a series of public service announcements to let companies know about the risk. More than $5 billion has been stolen through BCE attacks, and losses have grown exponentially from January 2015 – December 2016.[17]

BCE is particularly difficult for financial institutions because it is extremely difficult for them to prevent. From the bank's perspective, the transaction is being submitted through the proper channels by a legitimate and authorized employee of the customer business. While the bank can try to flag transactions to suspicious accounts or that deviate from the usual behavior patterns of the business, it is difficult to prevent all fraud. Some banks are attempting to

[13] Kaspersky Lab. "New Technologies, New Cyberthreats: Analyzing the State of IT Security in Financial Sector." 2017. https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf?aliId=372190581

[14] Kaspersky Lab. "New Technologies, New Cyberthreats: Analyzing the State of IT Security in Financial Sector." 2017. https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf?aliId=372190581

[15] SonicWall. "2017 Annual Threat Report." https://www.sonicwall.com/docs/2017-sonicwall-annual-threat-report-white-paper-24934.pdf

[16] Lion Gu. "Prototype Nation: The Chinese Criminal Underground in 2015." TrendMicro, 2017. https://documents.trendmicro.com/assets/wp/wp-prototype-nation.pdf

[17] Federal Bureau of Investigation. "Public Service Announcement: Business Email Comrpomise Email Account Compromise: The 5 Billion Dollar Scam." May 4, 2017. https://www.ic3.gov/media/2017/170504.aspx

combat the practice by educating their customers about the risk and requiring multiple executives to authenticate transactions, but losses continue to grow.

c) *Mobile malware is becoming a leading means of consumer bank fraud*

Another form of fraud that is replacing traditional carding and PoS attacks is mobile banking fraud. Consumers increasingly conduct their banking through their mobile devices, connecting millions of new devices to bank networks, and a growing share of financial transactions are conducted using mobile payment systems and digital currencies. Almost half of banking customers around the world use mobile banking, and 42% of banks expect mobile banking to become their main form of customer interaction in the next three years.[18]

For criminals who target consumer bank accounts, this provides a new avenue of attack. Mobile malware and account fraud has exploded around the world. One study from Kaspersky lab found that mobile malware attacks more than tripled in 2016, led by mobile banking Trojans.[19] McAfee data shows that the number of mobile malware samples on file nearly quadrupled from Q1 2015 – Q4 2016.[20]

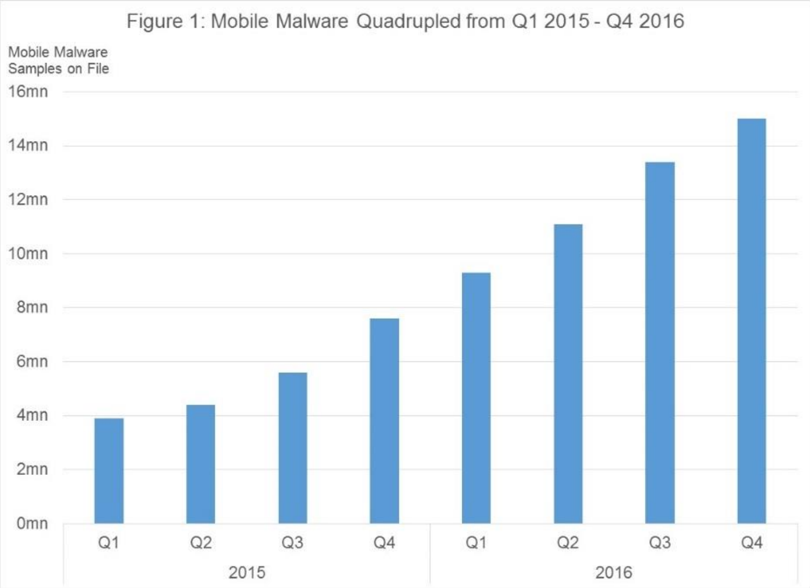
Figure 1: Mobile Malware Quadrupled from Q1 2015 - Q4 2016

[21]

Mobile banking Trojans are a rapidly growing threat, and are evolving quickly. The first major mobile banking Trojan, GM bot, was discovered in 2014.[22] Since its release, mobile

[18] Kaspersky Lab. "New Technologies, New Cyberthreats: Analyzing the State of IT Security in Financial Sector." 2017. https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf?aliId=372190581

[19] Kaspersky Lab. "Mobile Malware Evolution 2016." February 27, 2017. https://press.kaspersky.com/files/2017/02/Mobile_report_with-Interpol_2016_27-Feb-20172.pdf

[20] McAfee Labs. "Threats Report: April 2017." April 2017. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

[21] McAfee Labs. "Threats Report: April 2017." April 2017. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

[22] Check Point and Europol. "Banking Trojans: From Stone Age to Space Era." March 21, 2017. https://www.europol.europa.eu/publications-documents/banking-trojans-stone-age-to-space

banking Trojans have become a popular form of attack, and are increasingly adopting new features and being incorporated into other mobile malware campaigns like ransomware attacks.[23] One advantage that mobile banking Trojans have over traditional banking Trojans is that they can be configured to intercept software tokens and SMS verification codes used in multi-factor authentication, defeating one of the most popular tools used by banks to combat consumer credential theft.[24]

d) ICT4Crime: Financial inclusion is creating new threats in the developing world

The digitization and mobilization of financial networks has also helped to transform the geography of cybercrime, with billions of new customers conducting financial transactions online in emerging markets. The strategy of building out communications infrastructure in order to enable development in the third world (information and communications technology for development or ICT4D) has brought hundreds of millions of people into the global economy and global financial system. But it has also created a new generation of internet users with limited cybersecurity awareness or access to security products and services, and new technology users looking for upward mobility and access to wealth. ICT4D is also ICT4C – ICT for crime.

Mobile phones have become the keystone of ICT4D strategies,[25] and for many in the developing world, mobile phones have become their primary point of access to the internet, and to their bank. As the chart below shows, smartphone users in developing countries are significantly more likely to use mobile banking services than in developed nations. While the average rate of mobile banking penetration in developed nations in this study is just 34%, the average for developing countries is 58%.[26] The same is true of mobile payments. Africa is now the largest center of mobile money transfers in the world, with 14% of all Africans receiving money through their mobile devices.[27]

Mobile malware is also more prevalent in the developing world. More than 10% of mobile devices in the developing world are infected with malware,[28] and the top 10 countries for mobile malware infections are in the developing world, with countries in the former USSR

[23] Check Point and Europol. "Banking Trojans: From Stone Age to Space Era." March 21, 2017. https://www.europol.europa.eu/publications-documents/banking-trojans-stone-age-to-space

[24] Candid Wueest. "Internet Security Threat Report: Financial Threats Review 2017." Symantec Corporation, May 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

[25] Richard Heeks. "The ICT4D 2.0 Manifesto: Where Next for ICTs and International Development?" Institute for Development Policy and Management, 2009. http://www.oecd.org/ict/4d/43602651.pdf

[26] Statista. "Usage of Mobile Banking Apps Worldwide in 2014, by Country." https://www.statista.com/statistics/468943/usage-of-mobile-banking-apps-worldwide-by-country/

[27] Symantec and the African Union Commission. "Cyber Crime & Cyber Security: Trends in Africa." Global Forum for Cybersecurity Expertise Initiative, November 2016. https://www.symantec.com/theme/cyber-security-trends-africa

[28] McAfee Labs. "Threats Report: April 2017." April 2017. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

leading in infections from mobile banking Trojans.[29] Asia has the highest rates of online and mobile banking in the world, and the most rapid growth of banking Trojan activity.[30]

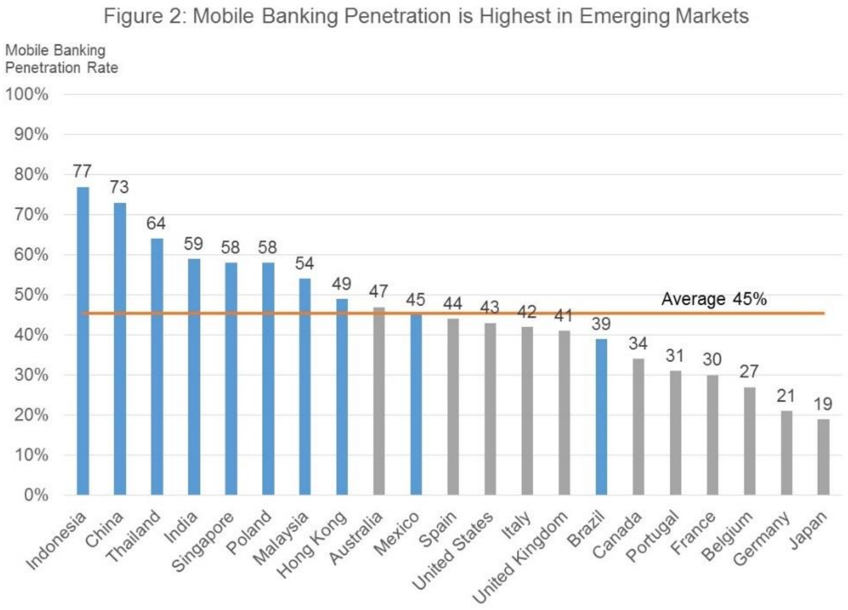

Figure 2: Mobile Banking Penetration is Highest in Emerging Markets

[31]

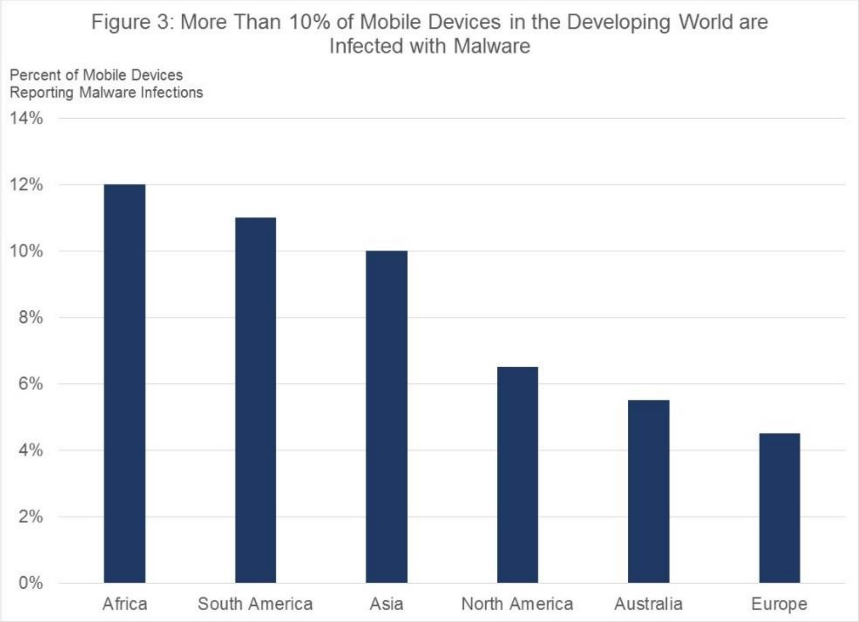

Figure 3: More Than 10% of Mobile Devices in the Developing World are Infected with Malware

[32]

[29] Kaspersky Lab. "Mobile Malware Evolution 2016." February 27, 2017. https://press.kaspersky.com/files/2017/02/Mobile_report_with-Interpol_2016_27-Feb-20172.pdf

[30] Candid Wueest. "Internet Security Threat Report: Financial Threats Review 2017." Symantec Corporation, May 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

[31] "Usage of mobile banking apps worldwide in 2014, by country." Statista, 2017. https://www.statista.com/statistics/468943/usage-of-mobile-banking-apps-worldwide-by-country/

[32] McAfee Labs. "Threats Report: April 2017." April 2017. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

In Latin America and Africa, meanwhile, the spread of broadband internet and 3G and 4G mobile networks is fueling the rapid growth of cybercrime in these regions. Entrepreneurs have taken advantage of technology to bring millions of new customers into the global financial system, but this has created opportunity for cybercriminals, who take advantage of weak cyber defenses and poor cyber hygiene, limited law enforcement capacity, and poor governance to launch attacks with impunity. Some of the fastest-growing countries of origin for cyber attacks are Cuba, Ecuador, Guatemala, Kenya, Morocco, and Peru.[33] They are also increasingly the targets of attacks. Some of the most victimized populations are in Africa and Latin America. For example, 67% of South Africans[34] and 75% of Brazilians[35] have been victims of online crime, well above the global average of 48%.[36]

Case Study: Brazil as a financial cybercrime center

Brazil is one of the fastest-growing centers of financial cybercrime in the world. The Brazilian internet has many features that attract financial cybercriminals. Cybercrime accounts for 95% of the losses incurred by Brazilian banks.[1] 58% of the Brazilian population is connected to the internet,[1] one of the highest rates in the developing world, and 57% of banking transactions are conducted online.[1] Mobile banking transactions grew 96% in 2016, and now account for more than a third of financial transactions in Brazil.[1] The behavior of Brazilian banking customers compounds the problem. New account creation rates are high and users tend to log into their accounts from multiple devices, including mobile phones and public computers, making it more difficult to detect fraud.[1] At the same time, with many users new to the internet, public and business awareness of the threat is low, cyber hygiene education is not widely available, and law enforcement's capacity to combat cybercrime is limited.[1] It is no surprise, then, that banking Trojans are the most prevalent wares in the Brazilian cybercrime underground.[1]

One of the most disruptive bank hacks of 2016 occurred in Brazil. On October 22, a coordinated blitz campaign altered all of Banco Banrisul's 36 domain name system (DNS) registrations, taking over every one of the bank's online domains. The attackers not only hijacked the bank's online banking portal, mobile banking system, and ATM and point-of-sale systems, it even controlled the bank's internal corporate domains and

[33] Alisdair Faulkner. "ThreatMetrix Q1 2017 Cybercrime Report." ThreatMetrix, May 2017. https://www.threatmetrix.com/wp-content/uploads/2017/05/cybercrime-2017-q1-1493750698.pdf?_ga=2.264749387.510841561.1497447173-1576623309.1497447173

[34] Symantec and the African Union Commission. "Cyber Crime & Cyber Security: Trends in Africa." Global Forum for Cybersecurity Expertise Initiative, November 2016. https://www.symantec.com/theme/cyber-security-trends-africa

[35] Gustavo Diniz, Robert Muggah and Misha Glenny. "Deconstructing Cyber Security in Brazil: Threats and Responses." Igarape Institute, December 2014. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

[36] Symantec and the African Union Commission. "Cyber Crime & Cyber Security: Trends in Africa." Global Forum for Cybersecurity Expertise Initiative, November 2016. https://www.symantec.com/theme/cyber-security-trends-africa

email system. When users tried to connect to the banks' legitimate web addresses, they were instead directed to websites set up by the attackers that installed malware on their devices, and stole account credentials, credit card data, and personal information, allowing the attackers to loot customers' accounts. With their email system and website under the attackers' control, the bank was not even able to send a warning to its customers. It took more than five hours to regain control of the bank's web domains.[1]

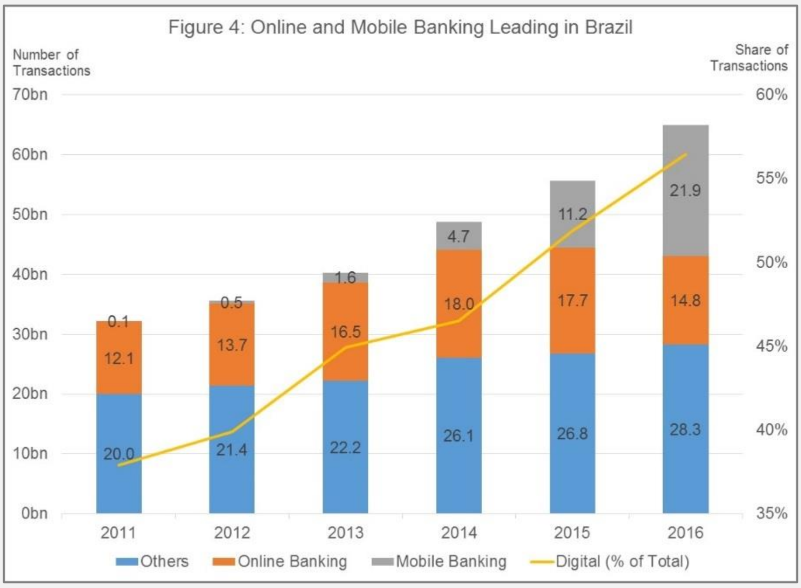
Figure 4: Online and Mobile Banking Leading in Brazil

[1]

The Olympics Effect: Japan in the Crosshairs

The Olympics have become a magnet for cybercriminals. The London Olympics in 2012 were plagued by an incessant wave of attacks on both the games itself and the millions of spectators that turned up to watch the games. The official website of the London Olympics was attacked more than 2.2 million times, and more than 255 million internet "security events" were detected around the Games.[1]

The promise of swarms of foreign tourists coming to the 2016 Olympics in Rio de Janeiro led to a massive uptick in financial cybercrime in Brazil.[1] Some of this was a ramping up of activity by established Brazilian cybercrime groups, but the promise of millions of tourists conducting overseas digital transactions on their foreign credit cards drew new players into the Brazilian cybercrime scene. Law enforcement sources reported seeing known cybercriminals relocate from Europe and the United States to Brazil to join the bonanza. And the end of the games has not coincided with a decline in cybercrime – Brazil remains one of the top originators of cybercrime in the world.[1]

This may help to explain the explosive growth of financial sector cybercrime in Japan, which will host the 2020 summer Olympics, and it is likely to get worse. According to

Symantec, in 2016 Japan was the target of more banking Trojan infections than any other country by a factor of five.[1] While cybersecurity is a top priority for Japan leading up to the Olympics, financial sector cybersecurity is not. According to several senior Japanese officials, efforts to improve cybersecurity for the games are heavily focused on the transportation, electric power, and media sectors because the International Olympic Committee has explicitly required Japan to strengthen their defenses. The financial sector is not receiving the same attention.

At Japanese financial firms, cybersecurity awareness is just starting to develop, and many have only recently begun to build their cybersecurity teams. Investment in cybersecurity is much lower than in the U.S. and Europe, and many of the largest financial institutions in the country have limited expertise in-house.[1] In May 2016, a gang of criminals using stolen credit card data stole $18 million from ATMs across Japan.[1] The attack seems to have served as a wakeup call for the Japanese financial industry, but if history is any guide, it will take significant investment to hold off an Olympic-scale wave of financial cybercrime.

IV. Targeted Attacks on Bank Networks: What is changing?

As making money through consumer fraud gets more difficult, sophisticated adversaries like organized crime groups are increasing their efforts to go after bank networks directly and carry out large-scale robberies. A prime example is the rise of new ATM attacks. As consumer fraud has become less profitable due to improvements in fraud prevention, other types of attacks have been growing. ATM attacks have been around for years, but the tactics used are evolving. A particularly worrisome trend is the rise in attacks on ATMs that come from banks' core networks, compromising the systems that manage the ATM networks instead of the machines themselves. In 2016, criminal groups launched a string of multi-million-dollar ATM hacks in Europe and Asia, breaking into the banks' internal networks and remotely infecting the machines with malware that caused them to spew millions of dollars in cash onto the street.[37]

a) Attackers are becoming more sophisticated, persistent

The incentives that shape attacker behavior are shifting, creating new adversary groups and changing their tactics. With big budgets, access to top cyber talent, and protection from law enforcement, nation state hacking groups pose the most sophisticated threat. Criminals are also becoming more sophisticated, whether organized crime groups launching targeted attacks on banks' core networks or average cybercriminals leveraging the market to launch opportunistic attacks at scale.

[37] Robert McMillan. "Hackers Program Bank ATMs to Spew Cash." *The Wall Street Journal*, November 20, 2016. https://www.wsj.com/articles/hackers-program-bank-atms-to-spew-cash-1479683814

i. “Nation states are robbing banks”

Nation state hackers, whose attention has, in the past, been focused on government networks, military systems, and intelligence targets, have increasingly focused on the financial sector in recent years, recognizing its value as a pain point to influence their adversaries. Not only is the global political climate becoming more tense, but as Rick Ledgett, former Deputy Director of the NSA, alleged at a public event in March, “nation states are robbing banks,” and they’re doing it with computers.[38] Ledgett was referring to the 2015-2016 cyber campaign that targeted dozens of banks in the SWIFT network, in which millions of dollars were stolen from banks in developing countries by submitting fake payment orders via the network.[39] Security researchers linked the attacks to the Lazarus Group, a hacker group working for the North Korean Reconnaissance General Bureau (RGB).[40] The attacks allegedly provided a lucrative means to supplement the North Korean government’s limited access to foreign currency.

Political conditions are also ripe for an increase in traditional espionage and disruption attacks on banks. Rising international tensions could lead to more cyber attacks on the banks by nation states, particularly the rise of nationalist politics, a more confrontational diplomatic environment, and the collapse of international reconciliation efforts led by the Obama administration. The straining of relations between the major cyber powers – the U.S., UK, Russia, China, Israel, Iran, North Korea – could lead to an uptick in the use of cyber attacks as a geopolitical tool. And the field of cyber powers is growing. According to senior U.S. intelligence officials, at least 30 additional countries are currently working to develop offensive cyber capabilities.[41]

ii. Nation state capabilities are now available to criminals

What were once exclusively nation state level capabilities are increasingly available to criminal groups, reflecting the growing overlap between nation state hacking groups and organized crime. The public release of source code for many sophisticated malware families has also contributed to the spread of highly advanced tools, as criminals adopt, adapt, and combine these tools into new crimeware.

The growing overlap between nation state hackers and cybercriminals is a key driver of the adoption of nation state tools and tactics by organized criminal groups. In Russia and Eastern

[38] Elias Groll. “NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist.” *Foreign Policy*, March 21, 2017. http://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/

[39] Danny Palmer. “New wave of cyberattacks against global banks linked to Lazarus cybercrime group.” *ZDNet*, February 13, 2017. http://www.zdnet.com/article/string-of-cyberattacks-against-global-banks-linked-to-lazarus-cybercrime-group/

[40] Dmitry Volkov. “Lazarus Arisen: Architecture, Techniques and Attribution.” Group-IB, March 30, 2017. http://www.group-ib.com/lazarus.html

[41] United States Congress Senate Armed Services Committee. *Hearing on Foreign Cyber Threats to the United States, January 5, 2017.* 115th Congress 1st Session. Washington: GPO, 2017 (Joint Statement for the Record of James Clapper, Marcel Lettre and Admiral Michael S. Rogers). https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

Europe, in particular, the lines between government hacking groups and criminal organizations are often blurred.[42] As U.S. law enforcement officials interviewed for this report described it, some senior leaders of Russian government cyber units are allowing criminals to "monetize their capabilities and infrastructure" in exchange for a cut of the profits, and the Russian government has also hired known leaders of cybercrime syndicates, often under indictment in other countries, to carry out attacks on their behalf.[43] In an even more bizarre twist, leading cybercriminals are getting involved directly in politics. Dmitry Golubov, a member of the Ukrainian Parliament, is considered the "godfather" of carding in the former Soviet Union![44]

iii. Open-source malware libraries provide advanced capabilities to many more actors

Organized crime groups are not the only cybercriminals that are gaining access to nation state capabilities. The release of advanced hacking tools stolen from intelligence agencies has made these tools available to a wide array of actors, from nation states to unsophisticated cybercriminals. The WannaCry ransomware campaign that affected hundreds of thousands of computers in a few days in May 2017 used an exploit called Eternal Blue that was stolen from a U.S. intelligence agency and posted online by a group calling itself the "Shadow Brokers."[45] While some have alleged that WannaCry is linked to North Korea, the exploit has also been detected in low-level criminal attacks on tens of thousands of systems in addition to WannaCry.[46]

Nation state tools are not the only tools being released into the growing open-source malware community. A combination of government takedowns, analysis by security companies, and releases by malware authors has caused the library of open-source malicious code to balloon in recent years. Source code for many sophisticated malware families like Zeus, Mirai, and Nymaim have been released into the wild, leading to the spread of dozens of variants and hundreds of modules that provide a dazzling array of new functionality. Enterprising cybercriminals have started to combine these tools into dangerous hybrids, making them more profitable and more difficult to detect and attribute.[47]

[42] Michael Schwirtz and Joseph Goldstein. "Russian Espionage Piggybacks on a Cybercriminal's Hacking." *The New York Times*, March 12, 2017. https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html

[43] Michael Schwirtz and Joseph Goldstein. "Russian Espionage Piggybacks on a Cybercriminal's Hacking." *The New York Times*, March 12, 2017. https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html

[44] Kim Zetter. "Ukrainian Cybercrime Capo Now a Politician." *Wired.com*, March 14, 2008. https://www.wired.com/2008/03/ukrainian-cyber/

[45] Symantec Security Response. "What you need to know about the WannaCry Ransomware." Symantec Connect, May 12, 2017. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

[46] Swati Khandelwal. "Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs." *The Hacker News*, April 22, 2017. http://thehackernews.com/2017/04/windows-hacking-tools.html

[47] Candid Wueest. "Internet Security Threat Report: Financial Threats Review 2017." Symantec Corporation, May 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

b) *Law enforcement is struggling to keep up*

Law enforcement's inability to keep up with changes in technology is allowing this underground economy to flourish. While anonymization tools like Tor and VPNs can protect activists and dissidents from oppressive regimes, they have also allowed cybercriminals to hide from law enforcement. The rise of digital wallets and cryptocurrencies like BitCoin has also fueled cybercrime, giving criminals new ways to monetize their attacks without employing legions of mules who relay illicit payments through their accounts, but take a large cut of the profits.

The broad adoption of encryption has also made life difficult for law enforcement, complicating efforts to identify malicious web traffic and track the communications of criminal groups. Criminals have also become savvy at developing their tools to thwart investigators. For example, malware authors increasingly include features in their code that allow it to identify and bypass sandboxes, or include features that prevent the code from executing in virtual environments, making it difficult for investigators to analyze.[48]

Law enforcement has long struggled with a lack of resources to combat cybercrime – funding, skills, equipment and training – but that is only one piece of the challenge. Even more difficult are the challenges of pursuing transnational criminals. In many countries, for example Brazil, legislation criminalizing cybercrime is inadequate, punishments are insufficient and the legal expertise to prosecute cybercrimes is in short supply.[49] There are also significant procedural hurdles, including issues of jurisdiction, challenges in maintaining standards of evidence, and the difficulty of explaining complex digital crimes to juries. The absence of adequate evidence sharing and extradition treaties between countries, lack of capacity in many countries to investigate cybercrimes, identify or locate offenders, or even just take them into custody allow criminals to operate with impunity.

c) *Banks in Asia are top targets*

Adversaries are not only increasingly sophisticated, they are also increasingly global, as are their targets. Financial institutions in Asia, in particular, are facing greater attention from cybercriminals, with a series of high-profile attacks in Japan, Taiwan, the Philippines, Bangladesh, Indonesia and Vietnam in 2016. The five largest banks in the world are based in Asia,[50] and mobile banking and mobile payments penetration in Asia is higher than any other region, presenting an attractive target for cybercriminals.

Unlike Europe and the United States, where a combination of stricter regulations and rising costs of cybercrime have pushed major banks to invest significantly in their cyber defenses,

[48] Candid Wueest. "Internet Security Threat Report: Financial Threats Review 2017." Symantec Corporation, May 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

[49] GRA Quantum. "Cybersecurity: The Greatest Hurdle of the 2016 Olympic Games." July 2017. https://graquantum.com/app/uploads/2016/07/WP_GreatestHurdle2016Olympic_051816_RGBpages.pdf

[50] Relbanks. "The 50 Largest Banks in the World." March 31, 2017. http://www.relbanks.com/worlds-top-banks/assets

many banks in Asia remain comparatively unsophisticated. In Japan and China, for example, many of the largest banks have only appointed CISOs and established dedicated cybersecurity teams in the last few years, and their cybersecurity budgets are much smaller than their western counterparts.

This has a significant impact on cyber incidents. Organizations in Asia are the slowest to detect cyber intrusions of any region – the average time from initial compromise to detection in Asia is 520 days, more than three times the global average of 146 days.[51] Cybercrime cost companies in Asia more than $80 billion in 2015, significantly higher than in Europe or the U.S. Asian banks are also being used to launder the proceeds of global cybercrime.[52] According to multiple officials interviewed for this report, poor anti-money-laundering (AML) and fraud prevention practices at some Asian banks are one of the biggest challenges to following the money in fraud and cybercrime investigations – the money trail goes cold in Asia in as much as 70-80% of cases!

d) *Vectors of compromise – new twists on old themes.*

Manipulating insiders remains the number one vector of compromise for banks. 58% of attacks on financial institutions rely on the company's employees to gain access, but over 90% of those employees are unwitting pawns in the attacks, victims of social engineering or watering hole attacks that manipulate them into giving attackers access to the network.[53] Social engineering remains the number one vector of attack against financial institutions,[54] but attackers are adapting their methods in response to new defenses.

[51] Bryce Boland. "M-Trends Asia Pacific: Organizations Must Improve at Detecting and Responding to Breaches." FireEye, August 24, 2016. https://www.fireeye.com/blog/threat-research/2016/08/m-trends_asia_pacifi.html

[52] Grant Thornton. "Cyber attacks cost global businesses $300bn+." September 22, 2015. https://www.grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/

[53] Michelle Alvarez. "Security trends in the financial services sector." IBM X-Force Research, April 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03129USEN&

[54] Pricewaterhouse Coopers. "Global State of Information Security Survey: 2017." http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html

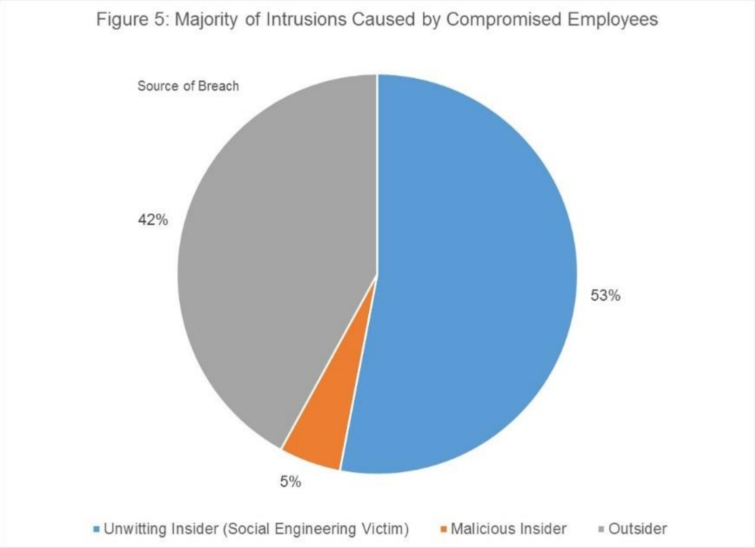
Figure 5: Majority of Intrusions Caused by Compromised Employees

[55]

i. Social engineers are developing new tactics as “don’t click the link” gains traction

Financial institutions have invested heavily in cyber hygiene training and progress is being made in “don’t click the link” campaigns. The sector is one of the least vulnerable to traditional phishing, with only 8.5% of targets opening malicious links or attachments.[56] While this is still a significant number, attackers have taken notice and are adapting their attacks with new twists on an old method.

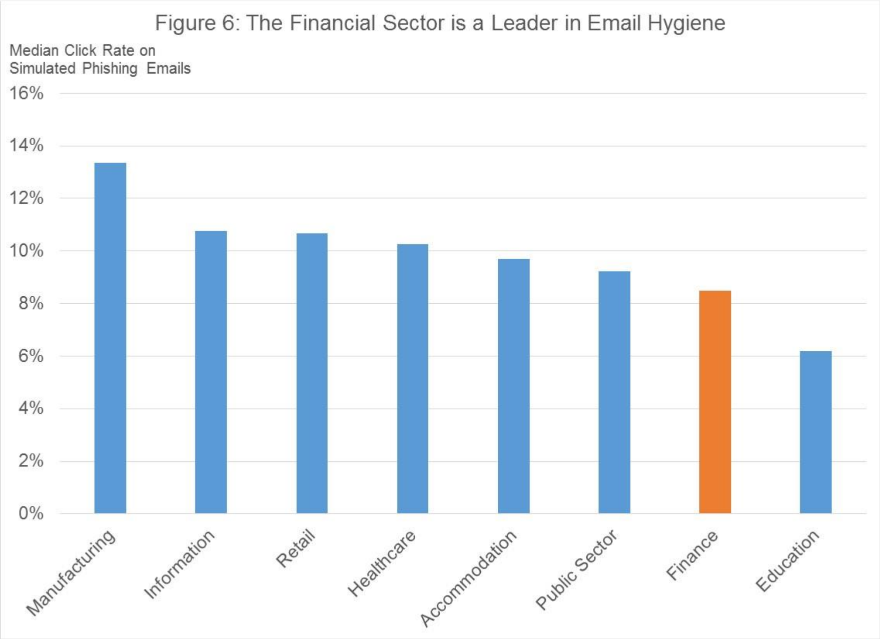
Figure 6: The Financial Sector is a Leader in Email Hygiene

[57]

[55] Michelle Alvarez. “Security trends in the financial services sector.” IBM X-Force Research, April 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03129USEN&

[56] Verizon. “2017 Data Breach Investigations Report: 10th Edition.” http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[57] Verizon. “2017 Data Breach Investigations Report: 10th Edition.” http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Social engineers are returning to pretexting, in which, instead of just sending a link to a "cute cat video" from a phony email account, social engineers are engaging in back and forth exchanges with their targets, posing as colleagues, competitors or service providers and taking their time to gain the target's trust before getting them to provide access to their system. One bank executive described a campaign in which an employee received a phone-call about a supposed security threat on their computer from someone pretending to be in the IT department. After convincing the employee that hackers were already on their computer, they sent an email with a link to provide the "IT guy" with remote access to their desktop in order to "remove the hackers."

It is not just junior employees who are falling for these types of tricks. In Q2 2017 one social engineer was able to engage in extensive email conversations with the CEOs of Barclays, Goldman Sachs, Citi, and Morgan Stanley, as well as the governor of the Bank of England.[58] Using free email accounts, the hoaxer posed as friends and colleagues of the five executives and exchanged emails with them over the course of days. In this case the attacker was not trying to breach the banks' networks, but he did illustrate how easy it was to fool even the most senior officials at some of the most sophisticated banks.

ii. Watering hole attacks on the rise

As employee awareness about phishing emails has improved, watering hole attacks have also increased as a vector of compromise. In a watering hole attack, the attacker compromises a website that they know or guess their target will visit and then uses it to infect their system with malware. Compromises of financial industry related websites are on the rise. In February 2017, a major watering hole attack was discovered that compromised the website of the Polish Financial Supervision Authority. The attack affected over 100 financial institutions in 30 countries,[59] and the initial results of the investigation suggest that the breaches were used to steal data from the banks' networks.[60] The attack has been linked to the RGB/Lazarus Group.[61]

One bank executive also described a new style of watering hole attack that is emerging, in which attackers take advantage of the training being given to bank employees to infect targets who have been trained not to click links, provide remote access to their desktops, or even open emails from strangers. Instead, many companies encourage employees to google the names of people or organizations that cold email them to verify that they are legitimate

[58] Brian McLannahan and Kadhim Shubber. "Three US bank chiefs fall victim to email prankster." *The Financial Times*, June 14, 2017. https://www.ft.com/content/6214a7e0-510d-11e7-bfb8-997009366969

[59] Symantec Security Response. "Attackers target dozens of global banks with new malware." Symantec Connect, February 12, 2017. https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

[60] Peter Falco and Richard Livesley. "FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief: Finalized Cyber Regulations." March 2017. https://icsa.global/sites/default/files/FS-ISAC%20SIRG%20Global%20Cybersecurity%20Brief%20-%20March%20%202017.pdf

[61] Symantec Security Response. "Attackers target dozens of global banks with new malware." Symantec Connect, February 12, 2017. https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

before engaging with them. Some attackers, therefore, are sending phishing emails to their targets, but also creating infected websites for the organization that supposedly sent the email and hoping the employee will open the website to verify the authenticity of the email.

e) Attacks are changing

2016 saw the rise of two new attack types that are a serious concern to bank cybersecurity teams. The number one rising threat identified by every single bank executive, law enforcement official, and expert interviewed for this report was DDoS attacks from internet of things (IoT) botnets. The majority also agreed on the second greatest threat, ransomware attacks.

i. DDoS threats continue to evolve

As banks have invested millions of dollars in DDoS mitigation tools and network monitoring, attackers have transitioned to new modes of attack, using IoT botnets to generate overwhelming floods of traffic or conducting "low and slow" attacks that avoid detection by DDoS prevention software. Most major international banks have contracts with at least one of the major DDoS mitigation services, and as one bank executive put it, for the last few years DDoS has been a nuisance to banks, but not a serious threat that can take them offline.

But attackers continue to try, and are developing new attack methods and monetization strategies. DDoS attacks were the number one type of security incident in the financial sector in 2016.[62] One in three financial institutions experiences at least one DDoS attack a month, and those attacks are becoming larger, more complex, and are being combined with other forms of cybercrime.[63]

IoT botnets are the biggest new concern. The discovery of and release of the source code for the Mirai IoT malware family in 2016 has led to the proliferation of dozens of new IoT botnets,[64] some capable of generating hundreds of Gbps of traffic. A new IoT botnet family called Leet, unrelated to Mirai, emerged in December 2016 with comparable power.[65] While banks have invested millions in DDoS mitigation services to protect themselves from traditional DDoS attacks, their capacity is finite, and the threat of massive IoT botnets overwhelming these services looms over financial institutions that depend on constant connectivity.

[62] Verizon. "2017 Data Breach Investigations Report: 10th Edition." http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[63] Neustar Inc. "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World." October 2016. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf

[64] Brian Krebs. "Source Code for IoT Botnet 'Mirai' Released." *Krebsonsecurity.*com, October 1, 2016. https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[65] Avishay Zawozni and Dima Bekerman. "650 Gbps DDoS Attack from the Leet Botnet." Imperva Incapsula Blog, December 26, 2016. https://www.incapsula.com/blog/650gbps-ddos-attack-leet-botnet.html

ii. Ransomware wave hitting banks

Ransomware is another top worry for financial institutions. 2016 saw a massive increase in ransomware activity. While modern crypto-ransomware really started in 2013 with the rise of CryptoLocker, 2016 saw an enormous uptick in attack activity, development of new malware families, ransom payments, and cost to businesses. Despite high investment in cybersecurity in the financial industry, financial institutions are not immune.

While there have been few major ransomware attacks on banks reported in the media, a survey by SANS in early 2016 found that 55% had been subjected to ransomware attacks.[66] The majority of victims that could quantify the cost of these attacks put it between $100k-$500k.[67] Most of the financial institutions that are successfully infected are small and medium enterprises and banks in emerging markets. For example, the Russian Central Bank confirmed that it was targeted in the May 2017 WannaCry attack, although it was not infected, but several Russian banks were impacted.[68] Bank of China's ATM network was also impacted.[69]

The Year of Ransomware

2016 was the year of ransomware. Security firm SonicWall detected 638 million attempted ransomware attacks in 2016, a 167x increase from the 4 million attempts detected in 2015.[1] These attacks utilized 247 distinct malware families in 2016, up from just 29 in 2015.[1] The FBI reported $209 million in ransom was paid in the first quarter of 2016, and estimated that the total would reach over $1bn by the end of the year. By comparison, the FBI recorded just $24 million in ransom payments in all of 2015.[1] The total economic cost of these attacks, including downtime, recovery costs, investigation, and reputational harm, is likely much higher.[1] What prompted such explosive growth?

The real turning point came in late 2015. From January 2012 – October 2015 there were just 33 new ransomware brands released on the market, but from October 2015 – May 2016 70 new ransomware families were released.[1] There are a number of factors that contributed to this turning point. First, in October 2015 a senior FBI agent was quoted as saying that the FBI's advice to ransomware victims was to "just pay the ransom."[1] Second, as CERT-UK noted in a report in 2016, around the same time the takedown of the highly successful Dridex banking Trojan encouraged cybercriminals to move away

[66] G. Mark Hardy. "From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector." October 2016. https://www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337

[67] G. Mark Hardy. "From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector." October 2016. https://www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337

[68] Alexander Winning and Jack Stubbs. "WannaCry cyber attack compromised some Rusian banks: central bank." *Reuters*, May 19, 2017. http://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V

[69] Wolf Richter. "China's use of pirated software left it vulnerable to the WannaCry ransomware attack." *Business Insider*, May 16, 2017. http://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5

from longer-term infections like banking Trojans toward new scams that turned a quicker profit.[1]

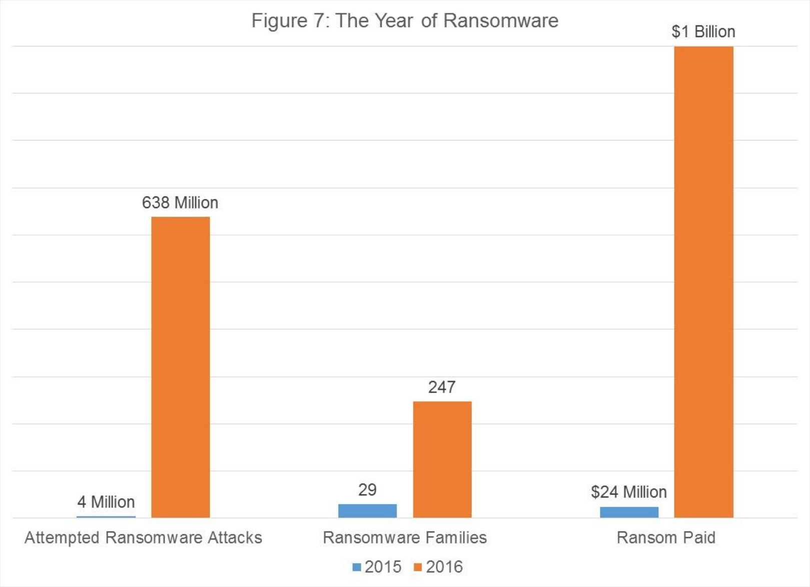
Figure 7: The Year of Ransomware

[1]

The most important driver, however, was the emergence of ransomware-as-a-service (RaaS). Before 2015, ransomware campaigns were largely run by vertically integrated organized crime groups.[11] RaaS had been speculated about but was first truly documented in 2015,[1] and allowed ransomware authors to operate at scale and with relatively little exposure. Starting with distribution, by offering their code on the market ransomware authors outsource distribution to specialists in social engineering or website compromise for a fee, helping to infect a large number of victims and insulating the malware’s author from its victims. The attackers can monitor and communicate with the victims securely, including unlocking the files when they get paid, using encrypted communications through the Tor network. Finally, they can receive payment in Bitcoin, making it difficult for law enforcement to track the payment.

iii. Ubiquitous automation is transforming attacks

Automation is also transforming the threat landscape. Combined with the widespread availability of off-the-shelf exploit kits and malware in underground markets, automation is allowing unsophisticated criminals to launch more advanced campaigns against a wide range of targets. Instead of attempting a sophisticated attack against a well-defended target, a small-time cybercriminal can buy an automated tool that finds vulnerable systems and uses a cheap, out-of-date exploit to infect vulnerable systems. Even if only a small number of financial institutions are vulnerable to the attack, it is so cheap for the criminal to set up and deploy that it can still be highly profitable. One computer security researcher described how he would launch an automatic ransomware attack on financial institutions:

> “Why should I bother to launch the attack myself? I can use a bot to search Project Unicorn or Shodan [search engines that allow cybercriminals to search for exploitable

> systems] for banks that use Apache Struts, which is widely used by banks and contains a lot of known vulnerabilities, and then drop off-the-shelf ransomware that exploits those vulnerabilities. These kinds of low-level attacks are easy to automate, then you can attack thousands of targets for cheap."

The payloads themselves also increasingly employ automated features. Polymorphic and metamorphic features that make malware harder to detect and block have been around for a few years, and have become the norm in malware attacks. Symantec catalogued 430 million unique pieces of malware in their 2016 threat report, almost all of them polymorphisms of a much smaller number of malware families.[70] Self-propagating malware is another serious threat. In May 2017, the first self-propagating ransomware attack, WannaCry, was released, targeting hundreds of thousands of systems in over 150 countries in just a few days.[71]

Machine learning threatens to take automation to the next level, both for offense and defense. Machine learning is a type of analytical modeling which uses iterative algorithms to identify patterns and find insights in data without being explicitly programmed where to look.[72] Financial institutions are increasingly employing machine learning algorithms for security purposes, primarily in fraud prevention.[73] Some executives also said they are investing in machine learning solutions for email filtering and traffic management. Machine learning cybersecurity products seek to improve on traditional pattern-based detection methods and take a proactive approach to threat detection and prevention. The same tools, however, can be used by attackers. According to McAfee, criminals are already starting to use machine learning algorithms for target selection, and it is only a matter of time before they are incorporated into attacks themselves.[74] If a machine learning algorithm can write Shakespearean sonnets, why can't it be applied to more nefarious writing purposes, like composing tailored, personalized spear-phishing emails?

iv. Hybrid attacks combine tactics to monetize breaches in multiple ways

Perhaps the most disturbing trend, however, is the rise of hybrid attacks. DDoS attacks, for example, increasingly use combinations of tactics and are used to draw attention away from breaches to the target's network. While traditional DDoS attacks used one method (e.g. UDP flood, application layer attacks) and generated profits by extorting victims, 57% of DDoS attacks now combine multiple DDoS methods,[75] and 53% of DDoS attacks in 2016 were used

[70] Paul Wood and Ben Nahorney et. al. "Internet Security Threat Report Volume 21." Symantec, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[71] EY. "'Wannacry' ransomware attack: EY response to the global cybersecurity incident." May 2017. http://www.ey.com/Publication/vwLUAssets/EY_response_to_WannaCry_ransomware_attack/$File/EY%20response%20to%20WannaCry%20ransomware%20attack-may-2017.pdf

[72] SAS. "Machine Learning: What it is and why it matters." Retrieved July 5, 2017. https://www.sas.com/en_us/insights/analytics/machine-learning.html

[73] Martin Desvazeaux, Mathieu Couturier and Yasmine El Himdi. "The New Methods in the Fight Against Online Bank Fraud." Wavestone, March 2017. https://www.wavestone.com/app/uploads/2017/03/online-bank-fraud-fighting-new-methods.pdf

[74] "2017 Threats Predictions." McAfee Labs, November 2016. https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

[75] "Verisign Distributed Denial of Service Trends Report: Volume 4, Issue 1 – 1st Quarter 2017." Verisign, May 2015. https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf

to distract defenders from breaches on the target's network which were used to steal or manipulate data, implant malware, or commit fraud.[76] Perhaps the scariest threat lurking behind these DDoS smokescreens is ransomware – nearly 20% of financial services firms that experienced DDoS attacks in 2016 encountered ransomware in conjunction with the DDoS attack.[77]

This cross-pollination is supported by the market structure of the underground hacker economy, in which specialists with narrow skillsets can contribute to highly complex, modular criminal enterprises that generate multiple revenue streams from their attacks. This decentralized market structure allows a small number of orchestrators to create highly sophisticated campaigns that multiply the value of each exploited system, using a combination of monetization strategies.[78] The Carbanak gang, for example, stole an estimated $1bn from banks by worming their way into banks' networks and then launching multiple cash-out schemes, compromising online banking accounts, manipulating payment systems, altering account balances, and launching ATM attacks.[79]

v. Attackers target seams in the financial systems

As major international financial institutions invest in stronger defenses on their internal networks and better fraud prevention and transaction authentication, attackers have shifted their approach. The most sophisticated nation states and organized crime groups have begun targeting the "seams" between these well-defended networks, exploiting weaker institutions in the global financial system to pull off massive heists.

A prime example is North Korea's campaign to steal money through the SWIFT network. Recognizing the difficulty of pulling off large-scale thefts from a single major western bank, the RGB targeted smaller, less sophisticated banks in developing countries like Bangladesh, Vietnam and Ecuador.[80] After compromising these banks' systems, they then used the victim banks' credentials to send what looked like legitimate SWIFT fund transfer requests to larger

[76] Neustar Inc. "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World." October 2016. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf

[77] Neustar Inc. "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World." October 2016. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf

[78] CSIS and McAfee. "Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity." March 1, 2017. https://www.csis.org/events/tilting-playing-field-how-misaligned-incentives-work-against-cybersecurity

[79] Alex Drozhzhin. "The greatest heist of the century: hackers stole $1 bln." Kaspersky Lab Blog, February 16, 2015. https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/

[80] Symantec Security Response. "SWIFT attackers' malware linked to more financial attacks." Symantec Connect, May 26, 2016. https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

banks in other countries.[81] These requests at first appeared legitimate to the receiving banks, since they were sent from legitimate partner banks through the established channels, so in some cases the money was transferred.

Other groups are moving to copy this strategy, inspired by the massive payouts achieved by the Lazarus Group/RGB's campaign. In October, Symantec discovered a group called Odinaff that targeted financial institutions around the world, stealthily infiltrating their networks and employing a range of cash-out strategies over the course of months, including a variation of the Lazarus Group's tactics that targeted banks' SWIFT connections.[82] The group does not appear to be linked to the RGB, but rather to Carbanak, a sophisticated cybercrime organization that has specialized in high-end bank attacks since at least 2013.[83]

The genius of this strategy is that it allows the attackers to get massive payouts while taking advantage of multiple banks in multiple countries, making every step of the response more difficult for defenders. Detecting the theft in the first place is hard because the request looks legitimate to the bank that transfers the money, while the bank that has been compromised does not lose any money in its own accounts. Mitigating and investigating the attack is all the more difficult because the bank that transfers the money to the attackers has not actually been hacked, while the bank that has been hacked is usually chosen because it has limited expertise and resources for cybersecurity, and is often located in a country whose law enforcement have little capacity to combat cybercrime.

V. Conclusion: More Threats, More Complexity, More Sophistication

The threat landscape for financial institutions is becoming bigger, more complex, and more sophisticated, and as financial institutions strengthen their protections against consumer fraud, attacks increasingly target financial institutions directly. While the big multinational banks in the U.S. and Europe have invested heavily in their defenses, they face a growing number of well-resourced, sophisticated adversaries. These attackers have the patience to take their time and go for one very big score instead of opportunistically going after softer targets, and they increasingly have the tools, skills, and knowledge necessary to overcome new defenses.

At the top of the growing cadre of advanced persistent threats (APTs) are nation states. The combination of massive budgets, access to top talent, and protection from law enforcement make them the most dangerous adversaries for financial institutions. As more and more countries invest in offensive cyber capabilities and tensions between the cyber powers rise,

[81] Danny Palmer. "New wave of cyberattacks against global banks linked to Lazarus cybercrime group." *ZDNet*, February 13, 2017. http://www.zdnet.com/article/string-of-cyberattacks-against-global-banks-linked-to-lazarus-cybercrime-group/

[82] Symantec Security Repsonse. "Odinaff: New Trojan used in high level financial attacks." Symantec Connect, October 11, 2016. https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

[83] Symantec Security Repsonse. "Odinaff: New Trojan used in high level financial attacks." Symantec Connect, October 11, 2016. https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

we could see a significant uptick in espionage and disruptive attacks on financial institutions. Furthermore, the apparent success of North Korea's ongoing campaign against banks may inspire other marginalized countries looking to inflate their national budgets to dabble in cybercrime.

The threat from organized criminal groups is also growing as these groups become larger, wealthier, more coordinated, and gain access to more sophisticated tools. The rapid growth of the open-source malware community has made very advanced tools available to a much wider array of criminals, and underground markets for automated tools and cybercrime-as-a-service allow criminals with minimal technical skills to orchestrate opportunistic cyber campaigns with little effort.

These sophisticated actors are developing new strategies and methods for their attacks. By exploiting seams in the financial system, attackers can pull off major thefts from well-defended financial institutions by exploiting their connections to smaller organizations with much weaker defenses. They can also multiply their profits by launching hybrid attacks, exploiting a single point of access to engage in multiple crimes simultaneously. Bringing together a range of technical specialists, combining sophisticated malware families that have been released to the public or are available for a fee through online forums, these groups can attempt multiple attacks simultaneously and then employ multiple simultaneous cash-out strategies to maximize their profits.

Low-level cybercriminals are also a growing threat, particularly to banks' customers. The maturation of online markets for cybercrime tools and services has lowered barriers to entry, even for technically unsophisticated criminals. Using automated targeting services and cheap exploit kits that target known vulnerabilities, criminals can launch opportunistic attacks on thousands of targets simultaneously at little cost, allowing them to profit even from attacks with very low success rates. For smaller financial institutions that have managed to avoid the attention of elite hacking groups, the growing sophistication of small-time cybercriminals poses a significant risk.

The attack surface these criminals can exploit is becoming wider and more diverse, and they are quicker to recognize the profit potential of hacking new devices than defenders are. New styles of ATM attacks take advantage of the difficulty of maintaining the defenses of machines that are spread across wide areas and difficult to monitor and update. The proliferation of cheap, poorly secured IoT devices that are always on and always connected has created a new generation of botnets with unprecedented power. And the spread of mobile banking and mobile payments has multiplied the number of endpoints that connect to banks' networks, causing an explosion of mobile malware.

As more of the world is brought online and begins to bank online, the geography of financial cybercrime is changing. Weak bank cyber defenses, high mobile penetration rates, and lack of law enforcement capacity has put financial institutions in Asia at the top of the target list for criminal groups. Latin America and Africa appear poised to follow suit. The strategy of information and communications technology for development (ICT4D) has helped to give millions of people access to the global financial system, but it has also created a breeding ground for cybercriminals. As a new generation are brought online across these regions, they are joining an even softer security environment, with weak governance and the fastest growth rates of online bank account creation, mobile banking, and e-payments in the world. ICT4D has become ICT4C – ICT for crime!

Defenders continue to make progress, but despite significant gains in technical security, attackers continue to innovate and humans remain the weak link in network defense. Avoiding complacency is critical. While DDoS mitigation has made a significant dent in financial institutions' losses to denial of service, hybrid DDoS attacks that include low-and-slow application attacks, IoT botnets, and coordinated campaigns employing multiple botnets may push the balance back toward the attackers. "Don't click the link" campaigns are reducing the success rate of traditional phishing emails, but as social engineers adapt their tactics, training programs must continue to evolve to keep up with the newest scams.

In order to get ahead, financial institutions will need to develop new approaches to fighting cyber threats. The financial system is global and it is integrated, and defenders need to become more global and better integrated to keep up. While the big global banks have invested in multi-layered, cutting edge defenses, small and medium banks and financial institutions in emerging markets serve as easy entry points to the global financial system. The industry's leaders will need to strengthen their smaller partners and help build cyber awareness and capacity in emerging markets to stay ahead of attackers who are sophisticated and savvy enough to exploit the weakest links in the system.

Supporting efforts to secure the broader ecosystem is also important. Protecting financial networks not only requires financial institutions to improve the security of their own systems, but to change the security balance of the entire internet environment. As internet banking becomes more and more prevalent, mobile banking brings millions of new customers into the financial system, and billions of IoT devices come online, cyber threats to financial institutions will increasingly come from billions of insecure devices outside their own networks. In order to defend against these threats, banks will need to strengthen authentication and monitoring measures for devices that connect to their networks, improve cybercrime education and awareness for their customers, and support efforts to build law enforcement capacity to combat cybercrime around the world.

As long as banks exist, criminals will try to rob them, and as financial transactions increasingly occur in cyberspace, so will the robberies. While physical bank robberies were once everyday occurrences, and robbing banks was a leading form of crime, improvements in banks' physical security have significantly reduced their frequency and cost. The same is possible with financial cybercrime. Many financial institutions recognize the risk and are investing the time and money necessary to strengthen their cyber defenses, but as changes in the attack surface, attacker incentives, and defenses evolve, so will the threats.

Questions from the Research

In conducting the research and interviews for this report, two major questions came out that have experts and practitioners stumped. The people we interviewed had very different views on these questions. Their arguments, and our analysis, are below.

Question One: Is sophisticated bank hacktivism dead, or will it come back with a vengeance?

Hacktivist activity has plummeted off the radar of financial institutions. Once considered a top threat, the financial institutions and law enforcement officials interviewed for this project no longer view it as a serious risk at all. Will it come back? The people we interviewed suggested two possible scenarios.

i. First hypothesis: Sophisticated hacktivism is dead. Skilled hackers recognize that it is not impactful and do not want to waste their time or risk their legitimate businesses or criminal empires by engaging in hacktivism.

After the LulzSec takedown in 2012, skilled hackers realized that hacktivism is risky and draws a lot of attention from law enforcement, but is not very impactful. Old-school black hats that used to participate in hacktivism have either retired or gone legitimate, and do not want to risk their legitimate businesses by engaging in illegal hacktivism. At the same time, professional cybercriminals who run sophisticated operations that generate thousands of dollars of profits do not want to waste their time or attract police attention to their money-making activities. The hacktivists that remain are glorified script-kiddies whose capabilities have not kept up with the significant investment and innovation in cyber defenses in the financial sector.

ii. Second hypothesis: A hacktivist wave is just around the corner. While high-level hacktivism has been dormant in recent years, conditions are ripe for a resurgence.

Hacktivism against banks has waned because hating the banks became passé. Occupy failed, Anonymous disintegrated, and fighting the power got old. But with the rise of the Trump Era, Brexit, and a growing focus on corruption and cronyism around the world, banks are being dragged back into the limelight in the worst way. Against this backdrop, hacktivism against banks will see a renaissance, as sophisticated hackers once again target the banks to make a political statement.

Our view: Sophisticated hacktivism against banks is dead.

Sophisticated hackers haven't abstained from hacktivism against financial institutions because they can't do it – the risk/reward balance has shifted. For people with high-end computer skills, lucrative careers in the legitimate tech and cybersecurity industries or in high-end organized cybercrime are not worth risking to moderately inconvenience a bank for a day or two. Hacktivism is attention-grabbing by nature, and hacktivists actively take credit for their crimes, meaning that law enforcement is much more likely to identify and take action against hacktivists than attackers that try to avoid detection.

Questions from the Research

In conducting the research and interviews for this report, two major questions came out that have experts and practitioners stumped. The people we interviewed had very different views on these questions. Their arguments, and our analysis, are below.

Question Two: Why aren't small and medium-sized financial institutions the target of more cyber attacks?

The big international financial institutions invest billions in cybersecurity, but still get hit with hundreds of millions of dollars a year of losses due to cyberattacks. With millions of dollars in their accounts, small dedicated cybersecurity budgets, few to zero cybersecurity professionals on staff, poor patching practices, and off-the-shelf infrastructure often decades old, why are small and medium banks, credit unions, and insurance companies not suffering massive losses from cyber attacks?

i. First hypothesis: Back end service providers are secretly great at cybersecurity.

Most small and medium-sized financial institutions outsource many of their IT services and back-office functions to a small group of outside service providers. These back-end service providers' (in the US we have the Big 4 – FIS, Fiserv, D+H, and Jack Henry) customers, primarily smaller financial firms and regional banks and credit unions, often have no in-house cybersecurity capacity, so they depend on their service providers for security. While some of the people we interviewed were skeptical about the cybersecurity abilities of the Big 4, perhaps their results speak for themselves.

ii. Second hypothesis: There are no mid-market cybercriminals to target these businesses.

The cybercrime economy is divided into two tiers of attackers. The first are highly sophisticated organized criminal groups, many based in the former USSR, that target big financial institutions for enormous payouts. The second group are low-level criminals that do not even bother to attack financial institutions directly, but impose a lot of cost on them through fraud and illicit transactions targeting their customers. Small and medium-sized financial institutions slip through the cracks between the two groups, protected enough to avoid the low-level criminals, but too small to be worthwhile for major criminal syndicates with high overhead and the sophistication to go after bigger targets.

iii. Third hypothesis: Hacker culture emphasizes the coolest and most impressive hacks, and hacking local banks and credit unions is not "cool."

The local credit union isn't exactly a fortress. Your grandma banks there. The admin password is "password," and you know the teller will click on any link to a cat video. It doesn't take any "skillz" to get in, so why would anyone be impressed that you did it? For skilled hackers that are in it for the reputation as much as the money, there is no reason to go after small banks that are soft targets.

Our view: Small and medium-sized financial institutions have slipped between the cracks because there are no mid-market cybercriminals, but that is changing.

For large, sophisticated criminal organizations with the capacity to take on big multinational financial institutions, small and medium sized banks are too small to be worth the time, effort, and risk of exposure. Launching fewer, more lucrative attacks on the major banks offers a better risk/reward for these groups than launching multiple attacks on a range of smaller financial institutions. The proliferation of high-end hacking tools and crime-as-a-service in the underground criminal economy is changing this dynamic, however, giving previously small-time criminals access to the resources and skills to launch more complex and lucrative attacks against bigger targets. While they would probably still struggle to exploit a major international bank, smaller, less sophisticated financial institutions are likely within reach.

Banks in developing markets are also likely to face growing threats. For sophisticated attackers looking to exploit the seams in the global financial system, smaller banks in developing countries provide easy access points, and it is easier to go undetected and avoid law enforcement. Adversaries like the Lazarus Group/RGB and the Carbanak Gang have already taken advantage of the weaker defenses of these smaller banks in emerging markets, and other adversary groups that have seen the success of these campaigns are likely to follow suit.

About the Author

William A. Carter is the Deputy Director of the Technology Policy Program at CSIS. His work focuses on international cyber and technology policy issues, including financial sector cybersecurity, data localization, surveillance and privacy, cyber conflict and deterrence, and law enforcement and technology, including encryption. He has spoken at events and conferences around the world, including leading a table-top exercise on cyber-financial crises for the ASEAN regional forum in Singapore in 2015, and he participates in Track 2 dialogues on cyber and technology policy issues. Before joining CSIS, he worked at Goldman Sachs, advising private and institutional clients on their short- to medium-term asset allocation decisions. In this role, he performed research and analysis on geopolitics and the macro economy and produced reports and presentations on international affairs and current events and their impact on markets. He previously worked at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University with a B.A. in economics.

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).