accenturesecurity

2019

FUTURE CYBER THREATS

EXTREME BUT PLAUSIBLE THREAT SCENARIOS IN FINANCIAL SERVICES

CONTENTS

FOREWORD

While financial services organizations have always been a target for sophisticated criminals, cyber adversaries' capabilities are breaking new ground as they advance rapidly.

Accenture cyber threat intelligence research points to several key threats that, when combined, lay the groundwork for multistage, multiparty attacks that could result in a new wave of extreme cyberattack scenarios for financial services.

Our report describes each of these threats in their earlier and current forms and examines how they could evolve in the future. We explore:

- Credential and identity theft
- Data theft and manipulation
- Disruptive and destructive malware
- Emerging technologies: Blockchain, cryptocurrency and artificial intelligence
- Disinformation

By understanding the past and anticipating the future nature of threats, we aim to help financial services organizations to be better prepared. With a long history of collaboration, we are certain that now, more than ever, financial services organizations need to come together to address security and resilience challenges. As they maintain this spirit of collaboration and gain momentum—both within the sector and with governments around the world—they can secure the trust that is essential to the success and sustainability of the whole financial system.

Valerie Abend
Managing Director, Accenture Security

Howard Marshall
Principal Director, Accenture Security

EXECUTIVE SUMMARY

Trust is the fuel that drives the digital economy—it strengthens an organization's standing and leads to new revenue-generating opportunities.[1] It also underpins the stability of the global financial sector. As cyber threats facing financial institutions evolve over time, adversaries erode trust through well-orchestrated, multistaged cyberattacks. Financial services organizations must continually reassess the wide spectrum of cyber threats targeting the financial sector to sustain cyber resilience.

This report discusses five cyber threats affecting the financial sector today. We assess how these threats are evolving and how they could create major lasting impacts for both organizations and the global sector at large. The threats featured are:

Credential and identity theft: Breaches of enterprise credentials and consumer financial data continue to grow in frequency and scale. As the landscape changes, adversaries may use these large data sets in innovative ways, including simultaneous multiparty access and network abuse.

Data theft and manipulation: Financially, politically, and ideologically motivated adversaries have routinely stolen data from financial institutions. Well-resourced adversaries may evolve to incorporate data manipulation for financial gain, destabilizing financial systems and markets.

Destructive and disruptive malware: Adversaries are using ransomware attacks against the financial sector at exponential rates. Increased deployment has coincided with threat adversaries employing destructive malwares, pseudo-ransomwares and defense

1 Redefine your company based on the company you keep: Intelligent Enterprise Unleashed, Accenture Technology Vision. (2018). Accenture. https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

evasion techniques. Looking ahead, adversaries may deploy wiper malware to conceal their true intentions and stifle the incident response process during financially or politically motivated attacks.

Emerging technologies: Financial services organizations continually explore applications of emerging technologies to deliver faster, more secure and customer-centric services. Increasingly, as financial services organizations leverage blockchain and artificial intelligence, threat adversaries may seek to exploit these emerging technologies as part of a new wave of malicious campaigns.

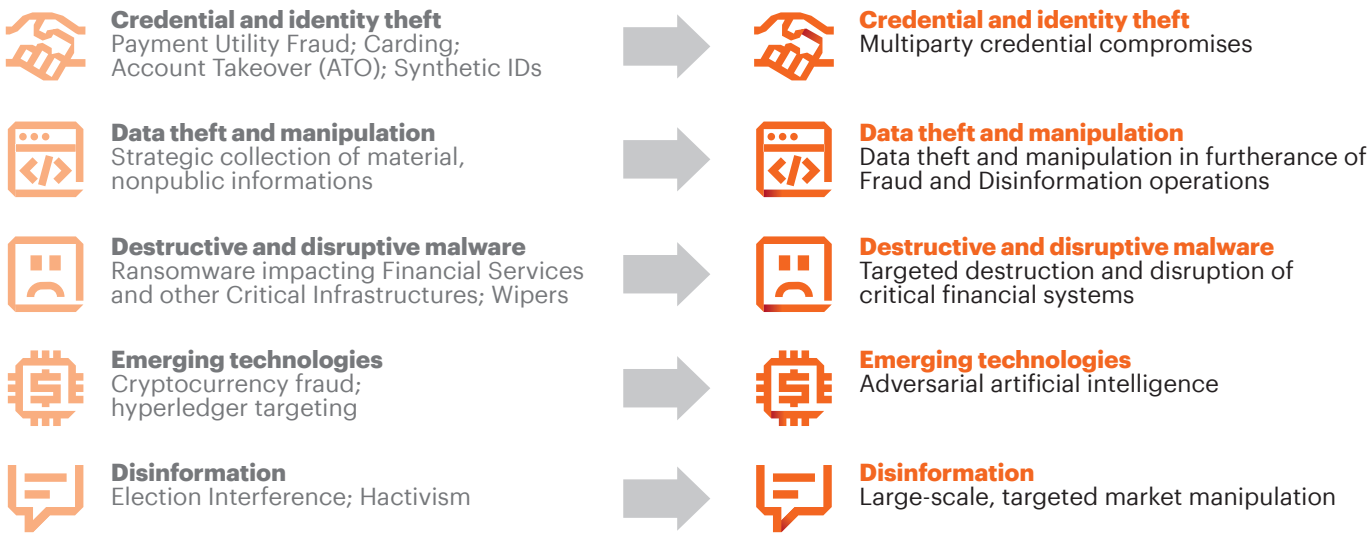
Disinformation: Disinformation has played a role in campaigns targeting financial institutions and markets since the birth of financial transactions. Combined with the other threats, disinformation may factor more prominently during highly targeted, multistage attacks.

As time goes on, these five threats are likely to overlap and intersect. In doing so, they can create the right conditions for new classes of cyberattacks—ones that simultaneously affect numerous organizations essential to financial services' most critical processes. A proactive cyber defense plan that incorporates multiparty attack simulations to test against these key threats could help financial institutions to be better prepared—not only to recognize cyber threats today, but also to defend them tomorrow.

EXECUTIVE SUMMARY

Financial Services

Current and future state of the threat



Source: Accenture iDefense Threat Intelligence

KEY THREATS

Based on our research of current and evolving cyber threats, the Accenture Security iDefense Threat Intelligence Services Team highlights the following five threats as key for organizations within the financial services sector:

- Credential and identity theft
- Data theft and manipulation
- Destructive and disruptive malware
- Emerging technologies: Blockchain, cryptocurrency and artificial intelligence
- Disinformation

CREDENTIAL AND IDENTITY THEFT

Credential and identity theft
Payment Utility Fraud; Carding; Account Takeover (ATO); Synthetic IDs

Credential and identity theft
Multiparty credential compromises

Social engineering remains the number one threat in breaching security defenses, regardless of the maturity and frequency of security awareness campaigns.[2] Increasingly, most organizations experience frequent and sophisticated phishing and other types of social engineering attacks[3] and, unfortunately, people continue to be the weak link in cybersecurity defense.[4]

The primary and most immediate impact of social engineering attacks is usually theft of customer, employee and other third-party credentials. These attacks often occur through account takeover (ATO) and synthetic identity fraud. In 2018, more than 43,000 breaches across all industries involved the use of customer credentials stolen from botnet-infected clients.[5] Such activity is a concern for financial institutions whose customers routinely repurpose usernames and passwords or where employee or third-party credentials are delegated for enterprise access.

Financially motivated adversaries take advantage of real-time payment networks by using ATO, wire fraud, check fraud, card fraud and a variety of other fraud types to steal funds.[6] The increase in consumer data available to fraudsters is driving fraud losses higher every year,[7]

---

2 Phishing as a Service: The Phishing Landscape. Accenture Security. (2018). https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-71/Accenture-Phishing-As-Service.pdf

3 Microsoft Security Intelligence Report Volume 24. (2019). https://clouddamcdnprodep.azureedge.net/gdc/gdcVAOQd7/original

4 Ninth Annual Cost of Cybercrime. (2019). https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

5 2018 Data Breach Investigations Report. Verizon. (2019). https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

6 Faster Payments, Faster Fraudsters. (2019, March 19). PYMNTS. https://www.pymnts.com/news/security-and-risk/2019/real-time-payments-faster-fraudsters-security/

7 Witt, P. (2019, February 28). The top frauds of 2018. Federal Trade Commission. https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018

propelling the shift from counterfeit cards to identity theft and synthetic identity fraud.[8] Cybercriminals use compromised credentials to quickly and widely establish user profiles. These credentials are easy to obtain firsthand or through criminal marketplaces, where they are sold in large volume at affordable rates. Synthetic identities have become a particular concern for financial institutions. This form of account theft is attractive to fraudsters because it enables them to obtain control of the account, cultivate high credit limits and bypass account alerts—all to facilitate high-dollar transactions with low risk of detection.[9] Fraudsters using synthetic identities are likely to continue to increase alongside traditional fraud.

Credential theft is a rapidly expanding threat for enterprise networks, incorporating e-mail addresses and login credentials; system credentials, such as certificates; and other forms of identification that third parties and employees use to authenticate themselves.[10] Unfortunately, the number of compromised credentials being used continues to rise.[11] In the United States, the Federal Financial Institutions Examination Council (FFIEC) published a statement warning financial institutions of the growing trend of credential theft.[12] It is a reminder that firms need to keep up-to-date with changing tactics, techniques and procedures (TTPs) used by the threat groups who compromise credentials.

Frequently, corporate credential theft is a targeted effort. Adversaries often conduct extensive reconnaissance of individuals at a target

---

8 Chasing ever-shifting payments fraud. (2018, September 6). Accenture. https://bankingblog.accenture.com/chasing-ever-shifting-payments-fraud?lang=en_US

9 Ibid

10 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

11 Goodin, D. Hard-to-detect credential-theft malware has infected 1,200 and is still going. (2019, February 20). Ars Technica. https://arstechnica.com/information-technology/2019/02/hard-to-detect-credential-theft-malware-has-infected-1200-and-is-still-going/

12 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

CREDENTIAL AND IDENTITY THEFT

organization using social media and news channels. Once cybercriminals identify specific users with credentials to access critical data, the adversaries conduct phishing campaigns and create fake websites to gather an individual's credentials.

E-mail lures and fake sites used in corporate credential theft are often far more sophisticated than those used for consumer credential theft.[13] Following a successful compromise, adversaries use a variety of evasive measures so that they can keep using the credentials. Adversaries have been observed modifying permissions, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. Such actions include account activity designed to undermine security policies, such as performing iterative password updates to disrupt password duration policies and preserve the life of compromised credentials.[14]

In recent years, malicious adversaries have taken careful steps to obtain large sets of customer and corporate credentials for the purpose of credential abuse. In particular, privileged credential abuse—where adversaries gain access to critical processes and data within a financial institution or set of financial services organizations—is one of the most popular breach strategies used by organized crime and state-sponsored organizations.[15] In some cases, adversaries may not need to use malware to achieve their objectives when corporate credentials are effective enough on their own.

---

13 Shopen, K. is a Credential-Based Attack? (2017, February 16). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack

14 Account Manipulation. MITRE. https://attack.mitre.org/techniques/T1098/

15 Columbus, L. (2019, April 15). CIO's Guide To Stopping Privileged Access Abuse - Part I. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2019/04/15/cios-guide-to-stopping-privileged-access-abuse-part-i/

In an increasingly complex threat landscape, credential abuse across many enterprises at the same time is likely to be the cornerstone of sophisticated cyberattacks that impact financial services.

Compromised employee and third-party credentials may provide initial access to trusted internal systems, enabling adversaries to gain and use system administrator-level access to obtain confidential business information, modify and disrupt information systems, and destroy or corrupt data.

Stolen system credentials can also be used to gain access to internal systems and data to further distribute malware or impersonate the financial institution to facilitate fraud, such as accessing payment processing systems for automated clearing house transactions.[16] Repeating this process across a set of organizations can ensure adversaries maintain end-to-end visibility for their campaigns; it also affords threat adversaries operational resilience. In recent months, advanced adversaries have showcased their capacity to execute multiparty compromises effectively. In April 2018, five banks in Mexico were hacked, forcing them to connect to the domestic payment network, SPEI, via back-up methods.[17]

The applications for multiparty compromises are somewhat limitless when threat adversaries use credential abuse. Paired with ransomware, destructive malware, disinformation, high-dollar fraud or even defacement, multiparty compromises can compound the impact of an attack. The advent of advanced adversaries leveraging their access through compromised credentials to multiple, critical entities concurrently is likely to impact the financial sector's ability to collaborate—in turn, challenging its resilience.

---

16 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

17 Davis, M. (2018, May 29). Mexico Foiled a $110 Million Bank Heist, Then Kept It a Secret. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

DATA THEFT AND MANIPULATION

Data theft and manipulation
Strategic collection of material, nonpublic informations

Data theft and manipulation
Data theft and manipulation in furtherance of Fraud and Disinformation operations

Data is the most critical asset for financial institutions. Maintaining the availability and integrity of data is vital to financial markets globally. Playing such a pivotal role, data is an ideal target for malicious adversaries, with information theft being the most expensive and fastest-rising consequence of cybercrime.[18]

Data breaches are an ever-present threat, with the number of United States data breach incidents hitting a record high in recent years. These breaches have involved the financial sector, including entities such as banks, credit unions, credit card companies, mortgage and loan brokers, investment firms and trust companies, payday lenders and pension funds and even financial authorities.[19] Data loss or data destruction are top-rated concerns for organizations.[20]

The ability to monetize material, nonpublic information through sales on criminal marketplaces or insider trading has attracted financially motivated adversaries to target financial institutions, technology service providers, central banks and relevant government agencies over the years. For example, adversaries stole documents related to a card processing system used by around 200 banks in the United States and Latin America, which could be potentially used for future attacks.[21]

---

18 Ninth Annual Cost of Cybercrime Study. (2019). Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

19 The Impact of Cybersecurity Incidents on Financial Institutions. (2018, February). Identity Theft Resource Center. https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

20 The State of Cybersecurity and Digital Trust 2016. (2016, June 27). Accenture. https://www.accenture.com/t20170510T000709__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Executive-Summary-June.pdf

21 Cuthbertson, A. (2017, December 12). Bank Robber Hackers Steal Millions of Dollars in Silent Heists Across U.S. and Russia. *Newsweek*. https://www.newsweek.com/bank-robber-hackers-steal-millions-dollars-silent-heists-745087

In 2016, adversaries extracted files from the United States Securities & Exchange Commission's EDGAR system to trade on nonpublic earnings results.[22] In 2017, adversaries targeted Poland's financial regulator, KNF, to exfiltrate data from several Polish banks. In what was labelled the most serious attack in Polish history at the time, the incident speaks to the diversity of ways threat adversaries can attempt data theft from critical financial entities.[23] This kind of activity is likely to continue as some institutions support their clients with initial public offerings (IPOs) and large mergers. Financial institutions are direct targets because of the sensitivity of the data they hold.[24] Both financially and politically motivated threat adversaries searching for competitive intelligence may continue to target firms as central repositories of valuable insider information.

As cyber threats progress, adversaries are likely to change as they shift their focus from data theft to strategic data manipulation. Unlike most data theft (where data is stolen because it is valuable) or extortive attacks (when data is imprisoned or destroyed until someone pays to release it), manipulation hacks are hard to detect: they occur when adversaries (or bots) change vital information, often below the threshold of attention.[25] Business is more data driven than ever, but inaccurate and manipulated information threatens to compromise the insights that companies rely on to plan, operate, and grow. Moreover, increasingly, financial services organizations are making use of autonomous, data-driven decision making. Left unchecked, adversaries could cause significant harm through the

---

22 SEC Brings Charges in EDGAR Hacking Case. (2019, January 15). Securities and Exchange Commission. https://www.sec.gov/news/press-release/2019-1

23 O'Neill, P. (2017, February 2). Hackers break into Polish banks through government regulator charged with bank security standards. CyberScoop. https://www.cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/

24 Cyber attacks on financial services sector rise fivefold in 2018. (2019, February 24). *Financial Times*. https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5

25 Cooper, B. (2017, November 20). The dangerous data hack that you won't even notice. University of California, Berkeley. https://news.berkeley.edu/berkeley_blog/the-dangerous-data-hack-that-you-wont-even-notice/

DATA THEFT AND MANIPULATION

manipulation of these autonomous processes or via the large volumes of data that fuel this type of decision making.[26]

Both politically and financially motivated threat groups can benefit from manipulating data, a sentiment echoed by the United States Intelligence Community in recent years. In the future, firms are likely to see cyber operations that involve changing or manipulating electronic information, instead of simply deleting it or disrupting access to it. Should highly-resourced threat groups manipulate and disrupt access to key data sets, they could undermine the trust in the organization's systems and the organization itself. Decision making by senior government officials, corporate executives, investors, or others could be impaired if they cannot trust the information they are receiving.[27] Manipulating credit scores, bank account numbers, and also market data (including pricing and transaction volumes) is a natural evolution from yesterday's big data breaches, where the personal information on millions of consumers, healthcare patients and government workers could already be in use for such manipulation schemes.[28]

From an enterprise perspective, successful cyber threat operations, targeting the integrity of information, can overcome institutionalized checks and balances that are designed to prevent the manipulation of data; for example, market monitoring and clearing functions in the financial sector.[29] Evidenced by the large-scale data theft and financial crime over

---

26 Redefine your company based on the company you keep: Intelligent Enterprise Unleashed, Accenture Technology Vision 2018. (2018). Accenture. https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

27 Clapper, J. (2015, September 10). Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

28 Overfelt, M. (2016, March 9). The next big threat in hacking — data sabotage. CNBC. https://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html

29 Clapper, J. (2015, September 10). Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

the past decade, both financially and politically motivated groups have positioned themselves as adversaries capable of penetrating the defenses of institutions of all sizes and may set their sights on data manipulation.

Critical pieces of intellectual property for financial organizations, such as algorithmic trading code, may play a central role in advancing the threat landscape for data. The globalization of asset trading, the emergence of ultrafast information technology and interconnected communications has made it impossible for humans to efficiently participate in a routine, low-level decision-making process.

Today, most trading decisions in equities and electronic futures contracts are made by algorithms: they define where to trade, at what price, and what quantity.[30] Malicious insiders at financial institutions have a storied history of stealing this trading algorithm code, including the use of credential stealers and malware designed to capture encryption keys for trading models.[31] This tendency is likely to evolve to include the alteration of these algorithms. Influencing trading algorithms to behave abnormally or ineffectively in small increments may be difficult for organizations to identify. Eventually, these changes could begin to accumulate, causing algorithms to become unstable, leading to extremely diverse outcomes including catastrophic failures.[32]

Financial services organizations should work to combat the manipulation of data by employing countermeasures aimed at early detection of alteration—provenance, threat modeling and alerting. By verifying the

---

30 Bacoyannis, V., et al. (2018, November 30). Idiosyncrasies and challenges of data driven learning in electronic trading. https://arxiv.org/pdf/1811.09549.pdf

31 Computer Engineer Arrested For Theft Of Proprietary Trading Code From His Employer. (2017, April 7). U.S. Attorney's Office Southern District of New York. https://www.justice.gov/usao-sdny/pr/computer-engineer-arrested-theft-proprietary-trading-code-his-employer

32 Know your Threat: AI is the New Attack Surface. (2019). Accenture. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

DATA THEFT AND MANIPULATION

history of data from its origin throughout its life cycle, firms can certify and recertify the authenticity of their data. Assessing a firm's enterprise data landscape for inaccurate data and subsequently quantifying the trust within that data could enable security teams to forecast targeting through plausible, but extreme, threat models for cyberattacks.

In the future, firms are likely to see cyber operations that involve changing or manipulating electronic information instead of simply deleting it or disrupting access to it.

DESTRUCTIVE AND DISRUPTIVE MALWARE

Destructive and disruptive malware
Ransomware impacting Financial Services and other Critical Infrastructures; Wipers

Destructive and disruptive malware
Targeted destruction and disruption of critical financial systems

The cost of business disruption—including diminished employee productivity and business process failures that happen after a cyberattack—continues to rise at a steady rate. The financial consequences of ransomware alone have increased 21 percent in the last year.[33] Ransomware is overtaking banking trojans in financially motivated malware attacks, a trend that is predicted to continue in the near future.[34] The risk of large-scale disruption in financial services may rise as threat adversaries develop variants of extortive malware.

In recent years, financial services organizations have been among the most targeted organizations from adversaries conducting ransomware campaigns.[35] One insurance company that provides protection against ransomware attacks has observed that, of all the attacks they noted, 20 percent targeted financial institutions. That said, successful infections have been significantly lower and have primarily affected smaller banks and credit unions—some more than once.[36] Organized cybercriminal groups continue to target firms they deem likely to pay the ransom. In some ways, this explains the lack of successful infections reported by large financial institutions, often perceived by adversaries to have more mature cybersecurity postures.

---

33 Ninth Annual Cost of Cybercrime Study. (2019). Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

34 2018 Internet Organised Crime Threat Assessment (IOCTA). (2019). Europol. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

35 Crosman, P. (2016, November 3). Ransomware: Should Banks Prepare to Pay or Be Ready to Refuse? *American Banker*. https://www.americanbanker.com/news/ransomware-should-banks-prepare-to-pay-or-be-ready-to-refuse

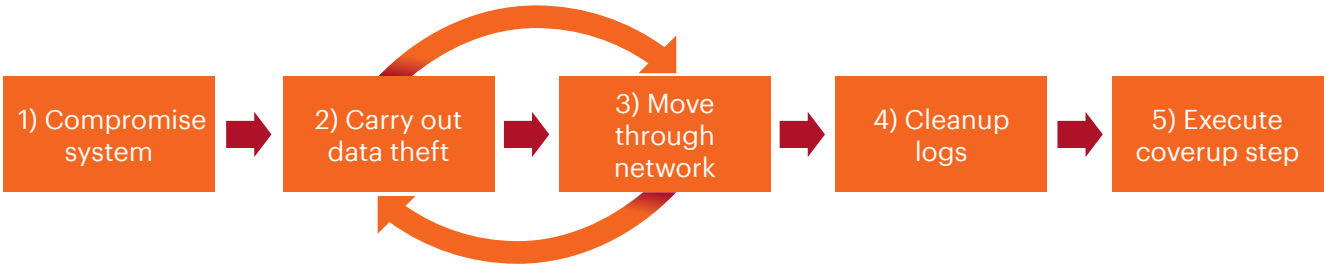
36 Yurcan, B. (2018, June 15). Ransomware is taking a toll on banks. Here's how they're fighting back. *American Banker*. https://www.americanbanker.com/news/ransomware-is-taking-a-toll-on-banks-heres-how-theyre-fighting-back

DESTRUCTIVE AND DISRUPTIVE MALWARE

The same threat groups operating ransomware also operate banking trojans that hit banks' consumer and commercial clients with wire fraud and automated clearing house fraud.[37] To help reduce the effectiveness of these attacks, banks should consider threats holistically, rather than looking at each specific attack. By doing so, organizations can better anticipate specific vulnerabilities and gaps as future TTPs evolve.

A critical advancement in adversaries' TTPs has been their ability to evade detection through deploying destructive malware, often referred to as wiper ware, that erases data including logs used to monitor for suspicious activity. Usually, an adversary's malware, tools, or other activity leaves traces behind indicating what was done within a network and how. Adversaries are incentivized to remove these files over the course of an intrusion to minimize their footprint or remove it as part of the post-intrusion cleanup process.[38]

Anatomy of the coverup



Source: Accenture iDefense Threat Intelligence

Several threat adversary groups have incorporated these TTPs into their attacks that specifically target financial institutions.[39] As this type of activity continues to become more targeted, threat adversaries may take

37 Crosman, P. (2016, November 3). Ransomware: Should Banks Prepare to Pay or Be Ready to Refuse? *American Banker*. https://www.americanbanker.com/news/ransomware-should-banks-prepare-to-pay-or-be-ready-to-refuse

38 File Deletion. MITRE. https://attack.mitre.org/techniques/T1107/

39 Ibid

advantage of system encryption and file destruction for greater impact to critical systems supporting the delivery of core financial services.

With this evolution, cyber defense operators supporting financial institutions could face challenges around deciphering the differences between the attack and the coverup. Data manipulation and theft, followed by ransomware or a wiper malware, impedes incident responders' ability to perform forensics, stop the attack, and remove the adversaries from their systems.

Institutions also face attackers fighting back after they are detected, trying to circumvent defenses and the investigation into the attack. Adversaries are leaving behind destructive malware and using Distributed Denial-of-service (DDoS) to create smokescreens during events.[40] In 2018, adversaries reportedly deployed wiper malware that affected 9,000 workstations and 500 servers inside Chile's largest financial institution to shield their theft of US$10 million.[41]

Cyber-espionage campaigns, aimed at targeting the financial sector, use destructive malwares and pseudo-ransomware. More than 40,000 systems were rendered inoperable during an attack on South Korea's banking and communications sectors in 2013. Affecting four large banks, as well as several subsidiaries, there were widespread outages that had an impact on Automated Teller Machines (ATMs), payment terminals, and mobile banking services.[42] More generally, the use of destructive malware is increasing in

---

40 Higgins, K. (2018, May 22). Cybercriminals Battle Against Banks' Incident Response. DarkReading. https://www.darkreading.com/endpoint/cybercriminals-battle-against-banks-incident-response/d/d-id/1331869

41 Seals, T. (2018, June 13). Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist. Threatpost. https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/

42 Martin, D. (2015, November 20). Tracing the Lineage of DarkSeoul. SANS Institute. https://www.sans.org/reading-room/whitepapers/warfare/tracing-lineage-darkseoul-36787

DESTRUCTIVE AND DISRUPTIVE MALWARE

frequency and scale, as shown by the Petya[43] and Shamoon[44] campaigns of 2017 and 2018 respectively.

Considering this growing threat, financial organizations should incorporate destructive attacks into their incident response playbooks and adversary simulations. Mindful of the dissolving siloes between financial, political, and ideologically motivated operations, financial institutions should prepare for likely increases in destructive computer network attacks aimed at disrupting and degrading their infrastructure.

43 Global Ransomware Outbreak Cripples Major Companies Worldwide. (2017, June 27). iDefense IntelGraph.

44 Assessing the 2018 Shamoon Campaign. (2018, December 21). iDefense IntelGraph.

EMERGING TECHNOLOGIES: BLOCKCHAIN, CRYPTOCURRENCY AND ARTIFICIAL INTELLIGENCE (AI)

Emerging technologies
Cryptocurrency fraud; hyperledger targeting

Emerging technologies
Adversarial artificial intelligence

Financial organizations are often early adopters of new technologies in their business processes. A recent example is financial organizations' exploration of blockchain technologies to enable real-time multiparty transactions with increased transparency and instant audit trails.

New technologies often provide opportunities for malicious cyber adversaries to expose gaps in security or in business processes. As crypto-assets and distributed ledger technology evolves, institutions and policy makers are working to understand how to best use these technologies while managing potential risk.[45]

One of the most discussed technologies in the financial services industry today is blockchain banking, enabling banks to process payments more quickly and more accurately while reducing transaction processing costs. Adversaries are likely to be targeting blockchain transactions already. Researchers in the security community have simulated attacks against hyper-ledger-derived frameworks being developed by major financial institutions.[46] As firms continue to explore the applications of blockchain within the sector and partner with third-party service providers to bring offerings to market, adversaries may continue to exploit opportunities.

But, targeting hyper-ledgers and derivative payment solutions was far from the first foray of cybercriminals into the cryptocurrency and blockchain space. For several years, financially motivated hackers have made use of cryptocurrency as a key mechanism for laundering ill-gotten funds and demanding ransom during extortive campaigns.

---

45 Wigglesworth, R. (2019, April 12). IMF and World Bank explore crypto merits with blockchain project. *Financial Times*. https://www.ft.com/content/1cfb6d46-5d5a-11e9-939a-341f5ada9d40

46 Haro, J. (2018). Targeted Attacks on the Blockchain (Hyperledger). CODE BLUE 2018.

EMERGING TECHNOLOGIES: BLOCKCHAIN, CRYPTO CURRENCY AND ARTIFICIAL INTELLIGENCE (AI)

It is widely accepted that technology, and cybercrime with it, develops so fast that law enforcement cannot keep up.[47] Senior law enforcement officials estimated last year that criminals crypto-laundered US$4.2 billion to US$5.6 billion in Europe alone.[48] Accenture Security has observed adversaries across English—and Russian—speaking marketplaces offering cryptocurrency "mixing" services that enable users to hide their identities while exchanging bitcoins and alternative cryptocurrencies, such as Monero and Ethereum.[49] These laundering services have seemingly succeeded in moving stolen and tainted digital currency at scale while protecting the anonymity of criminal groups.

In addition to using cryptocurrency to launder money, cybercriminals have also developed lucrative schemes to steal the coins and to conduct illicit coin mining. Numerous cryptocurrency exchanges have reported thefts of digital currency at alarming rates. More than US$1 billion worth of cryptocurrency was stolen in the first half of 2018.[50] The trend has carried into 2019 with exchanges in New Zealand, Israel and Singapore reporting breaches and reinforcing the global nature of this threat.

Another threat to blockchain and cryptocurrency is blockchain reorganization, which was undertaken by malicious adversaries in early 2019. In what is dubbed a "51 percent attack," adversaries stole nearly US$1.1 million in Ethereum Classic coins by hijacking more than 50 percent of the blockchain. The adversaries were able to "sell" Ethereum Classic coins for cash while rewriting the blockchain to steal both the

---

47 2015 Internet Organised Crime Threat Assessment (IOCTA). (2016). Europol. https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf

48 Crypto money-laundering. (2018, April 26). *The Economist*. https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

49 The Money Laundering Networks Facilitating The Cyber-criminal Underground. (2018, July 13). iDefense IntelGraph.

50 Rooney, K. (2018, June 7). $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. CNBC. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

cash and the coins. In a conventional payment system, it is up to banks and other central enforcers to stop this from happening. There is no such enforcement for cryptocurrency.[51]

With the price of cryptocurrency declining throughout 2018, hackers set their sights on cryptojacking. Malicious programs designed to mine cryptocurrency on infected machines plagued many organizations. Total CoinMiner malware grew as much as 4,000 percent in 2018.[52] Coupled with information stealers, mining malware became a feature of other campaigns as well. The Xbash malware, for example, combined botnet, coin mining, data-destructive ransomware and self-propagation into one package.[53] Financial services firms should continue to track the evolving nature of cryptojacking targeting corporate networks, especially as a possible indicator of a more severe malware infection.

Recently, some banks have started to endorse cryptocurrency exchanges and explore launching their own exchanges to capitalize on the potential business opportunity.[54, 55] Additionally, legislation in France opened the door for some insurance companies to offer life insurance contracts exposed to cryptocurrencies through specialized funds.[56] However, if a

---

51 Brandom, R. (2019, January 9). Why the Ethereum Classic hack is a bad omen for the blockchain. Verge. https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto

52 McAfee® Labs Threats Report, December 2018. (2018, December 19). McAfee Labs. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

53 Claud, et al. (2018, September 17). Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

54 Alexandre, A. (2019, February 26). Bahrain Central Bank Releases First Crypto Exchange to Graduate Its Regulatory Sandbox. CoinTelegraph. https://cointelegraph.com/news/bahrain-central-bank-releases-first-crypto-exchange-to-graduate-its-regulatory-sandbox

55 BelTA. (2019, January 28). Belarusbank might set up cryptocurrency exchange. Belarusian Telegraph Agency. https://eng.belta.by/economics/view/belarusbank-might-set-up-cryptocurrency-exchange-118236-2019/

56 Bloch, R. (2019, April 11). EXCLUSIF : Le bitcoin a désormais sa place dans les contrats d'assurance-vie. *Les Echos*. https://www.lesechos.fr/finance-marches/banque-assurances/exclusif-le-bitcoin-a-desormais-sa-place-dans-les-contrats-dassurance-vie-1008678

cybercriminal successfully targeted these funds, it could prove devastating for the insurers.

Along with blockchain, artificial intelligence (AI) is another technology that presents great opportunities for the financial services sector. Many institutions are incorporating AI into their business processes to find efficiencies, improve their decision making, and offer better customer experiences. Even though AI attack surfaces are just emerging, future security strategies should take account of adversarial AI, with the emphasis on engineering resilient modeling structures and strengthening against attempts to introduce adversarial manipulation.[57]

As adversarial AI has emerged over the past five years, Accenture has seen an increasing number of adversarial attacks exploiting machine learning models.[58] Such exploitation could multiply with the magnitude of threats facing financial services companies. As adversaries benefit from efficiencies gained through AI and machine learning, the return on investment for their malicious activities may increase. The ability to use autonomous target reconnaissance and vulnerability exploitation could decrease the turnaround time for campaigns for both well-resourced and less-skilled cyber adversaries. The ability to authenticate data and validate its integrity may be challenged by the adversarial application of AI, fracturing the basis of trust across many institutions through data theft, manipulation and forgery.

New attacks may also arise using AI systems to complete tasks that would be otherwise impractical for humans. Malicious adversaries may exploit the vulnerabilities of AI systems deployed by defenders—an important point

57 Know your Threat: AI is the New Attack Surface. (2019). Accenture. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

58 Ibid

to remember as information security teams construct their organization's threat models.[59]

When considered on its own or coupled with other threats that are increasing in frequency and potency, the malicious application of AI could be a linchpin for both financially and politically motivated adversaries throughout the many phases of their campaigns.

Accenture has seen an increasing number of adversarial attacks exploiting machine learning models.

59 Brundage, et al. (2018, February). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

DISINFORMATION

Disinformation
Election Interference; Hactivism

Disinformation
Large-scale, targeted market manipulation

Troll farms, Twitter bots and fake news—disinformation has taken center stage in the public sphere. Despite its recent prominence, disinformation has always been a tool deployed by financial, ideological, and politically motivated adversaries throughout history—the information age has simply increased the scale and speed of its impact.

The Accenture Security iDefense Threat Intelligence team has reported on the increasing significance of disinformation since the mid-2000s. In April 2007, protests over a controversial statue in Estonia were suspected of being exacerbated by false news reports of Soviet war grave defacements. Riots broke out in Tallinn—hundreds were detained, dozens injured, and one person died.[60] Beginning in 2014, Ukraine faced an onslaught of disinformation through television, online news, and other websites to split families along ethnic, political and regional lines—ultimately to damage the morale of Ukrainian soldiers.[61]

More recently, hacktivists adopted disinformation in campaigns targeting the financial sector. In January 2019, a firm was targeted by an elaborate hoax involving a spoofed letter purporting to be written by the fund group's chief executive officer.[62] The letter claimed the firm was divesting in coal companies in its actively-managed funds and changing voting patterns to take a stronger stance on climate change.[63] The adversaries

60 Van Puyvelde, D. (2015). Hybrid war – does it even exist? Nato. https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

61 Vasilyeva, N. (2018, November 26). Russia's conflict with Ukraine: An explainer. Military Times. https://www.militarytimes.com/news/your-military/2018/11/26/russias-conflict-with-ukraine-an-explainer/

62 Smith, P. (2019, January 9). BlackRock targeted by fake letter on climate change. *Financial Times*. https://www.ft.com/content/bd2113e4-198e-11e9-b93e-f4351a53f1c3

63 Morris, M. (2019, January 19). Someone wrote a fake letter pretending to be BlackRock CEO Larry Fink and some reporters got duped. *Business Insider*. https://www.businessinsider.com/larry-fink-fake-letter-on-climate-change-2019-1

also created a website that looked like the large investment management corporation's genuine webpage. Several thousand people received the fake letter and large news outlets initially picked up the letter as a legitimate communication. It was eventually revealed that the letter and website were the work of an activist seeking to raise awareness for social issues, such as the environment. The incident emphasized the low barrier to entry for an effective disinformation campaign.

These incidents remain dangerous indicators for the future of cyber threats to financial institutions and financial market infrastructures. A well-orchestrated disinformation campaign may have serious consequences on brand reputation, specific markets, and even market stability. The tools required to implement a successful campaign are well within the capability for ideologically, financially, and politically motivated threat adversaries already targeting the financial sector.[64]

Central Banks have voiced concerns regarding information operations, warning of their ability to undermine the trust in a country's banking sector. Recently, the governor of the Romanian National Bank stressed that: "as impatience has filtered into many domains, an erosion of confidence in independent, accountable public institutions like central banks has emerged."[65] To cope with this, central banks worldwide have boosted their defensive efforts related to fake news and negative campaigns.

As malicious adversaries use disinformation to maximize the effectiveness of multi-dimensional cyberattacks, trust in financial services could continue to be tested.

---

64 Trends: The Increasing Significance of Disinformation Efforts. (2008, October 5). iDefense IntelGraph.

65 Isărescu, M. (2019, March 25). Central bank communication as a policy tool – an ongoing challenge. https://www.bis.org/review/r190327d.pdf

PROACTIVE DEFENSE

THE FUTURE OF ADVERSARY SIMULATION

Cyber defense teams continuously prepare their organizations for extreme scenarios to advance cyber resilience to the next level of maturity and effectiveness.[66] Cyber threat intelligence drives these operations, enabling organizations to establish an intelligence-led cyber defense strategy. As part of this process, simulation exercises need to reflect the evolving threat landscape for the financial sector.

The attack landscape has shifted over the years. Now, the door is opening for adversaries to gain access to a wider array of capabilities ranging from targeted credential theft to destructive malware and autonomous tools. When mixed with disinformation, organized cybercriminals and politically motivated adversaries are equipped with a harmful cocktail of TTPs at their disposal.

For financial services, such attacks could upend the stability and trust that sustains the entire system. The combination of the multifaceted and multistaged campaigns of disinformation, paired with cyberattacks, can be expected to continue in coming years.

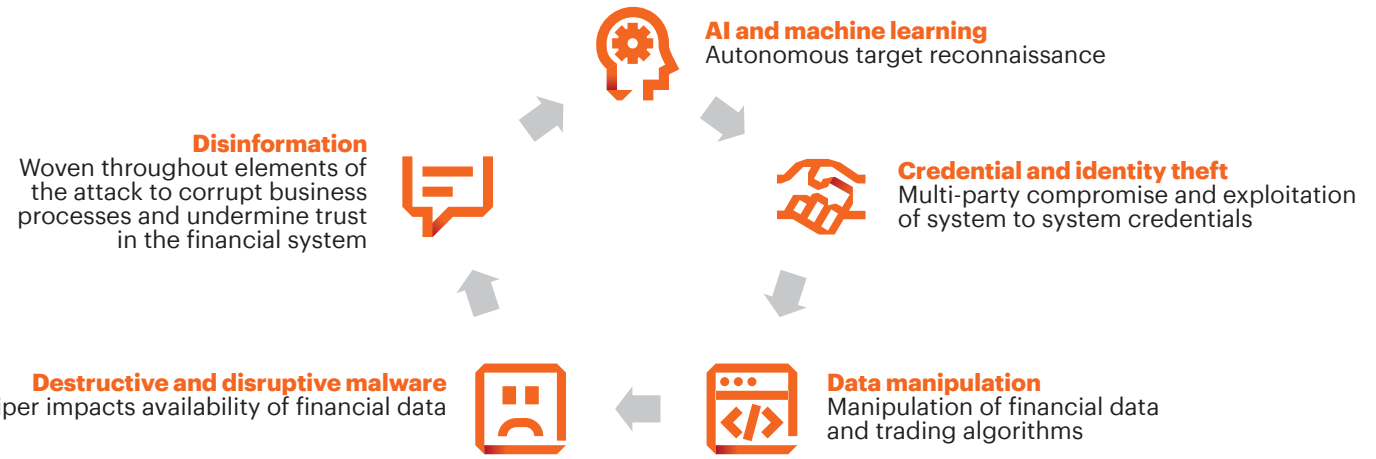
Here are five actions financial services organizations may wish to consider in the face of new threats and adversaries:

- **Collaborate** with peers and third parties on multistage exercises.
- **Invest** in people, processes and tools that identify potential disinformation concerning their firms.
- **Strengthen** insider threat programs to detect and prevent malicious adversaries from gaining access to key systems and data.

66 Duffy, S. (2019, February 21). Accenture Adversary Simulation Service: Fueled by iDefense Threat Intelligence. Accenture. https://www.accenture.com/us-en/blogs/blogs-accenture-adversary-simulation

- **Improve** online accountability through threat informed approaches to authentication and authorization.
- **Simulate** adversarial threats using disinformation, emerging technologies and compromised corporate credentials.

Simulating multiparty attacks – extreme, but plausible scenarios



Source: Accenture iDefense Threat Intelligence

GLOSSARY

Name	Type	Description	Mentioned on page:
Blockchain reorganization	Attack	Also referred to as a 51 percent attack, blockchain reorganization refers to an attack on a blockchain by a group of miners controlling more than 50 percent of the network's mining hashrate, or computing power. The attackers are able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.[67]	**22**
Petya	Malware	Petya is a ransomware that appeared in March 2016. It was first delivered to victims via an e-mail from an applicant seeking a job. Petya overwrites the Master Boot Table (MBT) to deny victims access to their computer and files. On June 27, 2017 government and business entities were paralyzed by a global campaign delivering the malware.	**20**
Shamoon	Malware	Shamoon, also known as DistTrack, is a destructive implant highly likely created by the BLACKSTURGEON threat group. Shamoon was identified in August 2012 and was publicly identified in November 2016 as part of a campaign targeting organizations in the government and resources verticals. The latest wave of Shamoon was identified in December 2018.	**20**
Xbash	Malware	Xbash is a malware that has ransomware and coin mining capabilities. It also has self-propagating capabilities and spreads by attacking weak passwords and unpatched vulnerabilities. Xbash is data-destructive; destroying Linux-based databases as part of its ransomware capabilities. The malware has been tied to the Iron Group, also known as Rocke, a Chinese-speaking hacking group that has grown in notoriety for its use of cryptojacking malware that leverages a backdoor from HackingTeam's leaked code.[68, 69]	**23**

67 Frankenfield, J. (2019, February 7). 51% Attack. Investopedia. https://www.investopedia.com/terms/1/51-attack.asp

68 Claud, et al. (2018, September 17). Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

69 O'Neill, P. (2018, September 18). Chinese-speaking cybercrime group launches destructive malware family. CyberScoop. https://www.cyberscoop.com/iron-group-cybercrime-destructive-malware-palo-alto-networks/

CONTACT US

Valerie Abend
Managing Director, Accenture Security
valerie.abend@accenture.com

Rikki George
Associate Principal, Accenture Security
rikki.george@accenture.com

Howard Marshall
Principal Director, Accenture Security
howard.marshall@accenture.com

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

LEGAL NOTICE & DISCLAIMER

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Accenture provides the information and content on an "as-is" basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.