accenture

2021

Future Cyber Threats

The latest extreme but plausible threat scenarios in financial services

Contents

Foreword

The pandemic has changed how all organizations work. It exposed financial services organizations to exponential growth in potential vulnerabilities through remote workforces both in their institutions and across their third parties. Threat actors took advantage of these exposures in new ways, further advancing their capabilities and targets for data theft and manipulation, fraud and extortion.

Banks are all too aware of the threats. But as they make their best efforts to keep businesses and governments operational, there is the ever-present danger that some of the money flowing through the financial system to keep economies around the globe moving, is not going to legitimate businesses. Instead, loans are being siphoned off by cybercriminals—US$4.2B in 2020 alone according to the FBI's 2020 Internet Crime Report[1].

Clearly, financial institutions must stay alert to attack surfaces and continue to feed transactions and markets that help economies grow. Yet, security teams have been pushed to extremes throughout the pandemic. Adversaries continue to breach software supply chains and target cybersecurity vendors that organizations rely on to keep them safe. Fraudsters continue to find new opportunities for impersonation.

Threat actors are capitalizing on COVID-19 concerns to cause breaches involving malicious or unwitting insiders. Even ransomware actors seem to have become more destructive and less likely to restore systems, even when paid.

As new technologies reinvent our workplace, they are opening up cybercriminal opportunities. Quantum computing is advancing, presenting real potential risk to the controls the financial system uses to protect data. Deepfake capabilities are improving, causing concern for various types of fraud related risks to financial institutions and their customers. These advances pose future threats that could undermine trust in current systems.

To face these threats, financial services organizations should both double down on time-tested mitigation strategies and consider cutting-edge countermeasures. Much of the needed approach boils down to defense in depth and assuming a breach mindset.[2]

We cover all this and more in this report, our latest overview of threats to the financial services sector. We hope our analysis helps you to take the necessary steps to adapt your security strategy and serves to inform the industry with these much-needed insights for the future.

Valerie Abend
Managing Director, Accenture Security

Howard Marshall
Managing Director, Accenture Security

Key threats

In this third annual report, based on research by the Accenture Cyber Threat Intelligence (CTI) team, we review threats from the past two reports. We list a number of ongoing threats we have identified in the past twelve months and explore the likely outcomes of these threats.

For ease of reading, we have broken down our findings into what's happening today and why it matters and we offer insights into the actions financial institutions can take to mitigate further risk.

The five key threat themes are:

01 Supply chain attacks target essential software and services

02 Cyber fraud escalates as disruption opens the door to new avenues and actors

03 Insider threats flourish with remote work

04 Extortion attacks advance their destructive capabilities

05 Emerging technologies continue to reinvent the threat landscape

01
Supply chain attacks target essential software and services

What's happening?

As we have seen with several widescale third-party attacks, supply chains are a major focus for threat actors today—and are likely to be into the future. SolarWinds and Microsoft are prime examples of how threat actors can take advantage of vulnerabilities in cross-sector critical infrastructure to gain access and cause fear, loss of integrity in systems and likely harm the fidelity of the information processed on potentially corrupt systems.

The SolarWinds-based espionage campaign—whose publicly known victims mostly comprise United States federal and local government agencies and information technology (IT) or cybersecurity providers[3]—showed that threat actors can access almost any vulnerable connected downstream organization through its unsecured relationships.

In particular, the actors in this and other campaigns have focused on a key supply chain pain point: information and communications technology products and services, including cybersecurity vendors. Within a few months in 2020 to 2021, reports emerged detailing breaches of:

- Monitoring software at SolarWinds.
- File transfer software at cloud-based provider Accellion, affecting United States law firms, a Singaporean telecommunications company and United States applicants for unemployment relief.
- Systems at cloud provider Blackbaud, affecting numerous nonprofits.

In addition, a ransomware attack against Automatic Funds Transfer Services (AFTS) affected numerous United States cities.[4]

In particular, the SolarWinds breach spans multiple levels of supply chains and goes as deep as build environments and document libraries. The malware infected unrelated software from developers whose build platforms hosted SolarWinds software. The threat actors separately compromised other authentication tools such as Duo[5] and reportedly abused other initial access vectors.[6] The threat actors disguised themselves as trusted vendors delivering a digitally signed software update.[7] The SolarWinds adversaries and others have abused Security Assertion Markup Language (SAML) to obtain access to cloud resources.

Why does it matter?

The broad and deep targeting of supply chains, particularly technical and security service providers, is of concern because such providers serve as gateways to financial services organizations, whether wholesale and retail payments processors, major banks and financial market infrastructures, or regulators.

Threat actors mistreating authentication tools to breach cloud environments can access sensitive internal documents, communications and intellectual property. They can use trusted communications channels for business e-mail compromise (BEC), phishing or introduce malicious links or files.

Vendor e-mail compromise (VEC) also facilitates cyber-fraud operations.[8] At the systemic level, the European Union's Single Resolution Board (SRB) appears among 23 entities researchers have identified on the SolarWinds threat actors' highly selective final target list.[9] A breach of the SRB, which is the central resolution authority for troubled banks, could give threat actors visibility into how the European Union defends the stability of the entire European financial system. Recent supply chain breaches threaten the trust and speed of global transactions and have the potential to erode faith in global financial systems.

What should you do?

To reduce risks associated with cyber supply chains, Accenture suggests considering the following actions:

- Tighten up the privilege and access levels of externally developed software.
- Craft service-level agreements with software suppliers to help ensure they locate and improve vulnerable software prior to deployment.[10]
- Deploy new tools to help detect anomalies and secure software. The Cybersecurity & Infrastructure Security Agency (CISA) developed a tool called Sparrow for detecting malicious activity in Microsoft Azure Active Directory, Office 365, and M365 environments. Accenture has patented a new technique where blockchain could secure software supply chains with self-referencing software bills of materials (SBOMs).[11]
- Refer to the National Institute of Standards and Technology's (NIST) "Best Practices in Cyber Supply Chain Risk Management" to map supply chains, identify critical suppliers and review suppliers' cybersecurity practices.

02
Cyber fraud escalates as disruption opens the door to new avenues and actors

What's happening?

Fraud and business e-mail compromise (BEC) flourished in 2020. As specialized regional threat groups combined their efforts, criminals targeted COVID-19 pandemic relief funds. New tactics, techniques and procedures (TTPs) enabled threat actors to exploit even seemingly low-value stolen credentials from small organizations.

New criminal BEC and money laundering cases show how organized crime groups in Africa, the Middle East, Europe and Asia cooperate in complex conspiracies, each filling a specialized role such as devising lures in target languages, operating malware, spamming targets and controlling mules.[12]

Threat actors have also exploited COVID 19-related disruptions and relief programs.[13] Early in the pandemic, fraudsters began identifying and using dormant corporate bank accounts to file for government funded loans. They also increased the volume and the price for selling legitimate corporate bank account credentials on the Dark Web. Furthermore, cybercriminals have stolen identities and filed fraudulent unemployment insurance claims[14, 15] or redirected benefits to their own bank accounts.[16] Romance scams deceived lonely people into serving as mules for money laundering.[17, 18]

Even as improved anti-fraud systems help detect anomalies in account login activity and user behavior, cybercriminals are perfecting their evasion techniques. Marketplaces like Genesis offer fraud-as-a-service,[19] with features such as cloud credentials, stolen application programming interface (API) keys, access to a compromised computer's credentials and digital fingerprint (IP address, keyboard layout, browser information) and techniques to bypass multi-factor authentication (MFA).[20] Threat actors such as user "Zanko" on the Exploit forum sell access to vendor companies in financial services and other sectors, facilitating VEC attacks.[21]

Amid a pandemic-inspired uptick in the use of peer-to-peer (P2P) payment apps such as PayPal and Venmo, underground forum members frequently discuss using them to trade stolen credentials, launder money, cash out funds, or conduct social engineering.[22]

Why does it matter?

New fraud tools and criminal cooperation networks enable criminals to monetize stolen access credentials—even for seemingly low-value, small organizations. Fraudsters can impersonate a small company's employees and interact with that company's upstream and downstream contacts. Although often regarded as nuisance activity, the effects of business e-mail compromise and other fraud on companies can be significant and can include disruption to company operations, decreased profits, loss of tax revenue, job losses and reputational damage.

Meanwhile, the Corporate Transparency Act authorized by the United States National Defense Authorization Act of 2021 (NDAA) requires businesses to reveal their beneficial owners and introduces new anti-money-laundering and suspicious activity reporting requirements, making financial services organizations more accountable for combating cyber-enabled fraud. The United States Treasury is likely to issue more-specific regulations in 2022.[23]

What should you do?

To mitigate the threat of cyber-fraud, Accenture suggests considering the following actions:

- Conduct user awareness training and enforce policies to combat phishing and social engineering.
- Focus efforts on vulnerable groups like customer service staff and employees with access to payment systems and other high-risk data.
- Limit remote desktop protocol (RDP).
- Seek alternatives to short message service (SMS) for two-factor authentication.
- Adopt strong e-mail authentication protocols such as Domain Message Authentication Reporting (DMARC).[24, 25]

03
Insider threats flourish with remote work

What's happening?

Pandemic-related operational changes have opened to door to greater exposure for banks to insider threats. Whether malicious or unwitting, insiders have caused disruptions and critical data loss at nearly half of the organizations in a March 2020 survey of 457 cybersecurity professionals commissioned by behavior analytics company Cyberhaven.[26] Ponemon's "2020 Cost of Insider Threats Global Report," based on a survey conducted in 2019 of 964 IT and IT security practitioners worldwide, attributed 62% of insider-related incidents to negligence, 23% to criminal insiders and 14% to stolen credentials.[27] With opportunities expanded in 2020 by pandemic-era work-from-home policies, malicious insiders may exploit lax oversight. Uninformed employees may click on pandemic-related phishing links, while complacent ones may use unsecured collaboration tools.[28]

Insider schemes flourished in 2020. Many institutions described workers that are soliciting non-bank employees to do some or all of their work for them – providing their credentials to directly access bank systems. Many institutions see an increase in "impossible log-in activity" where an individual's credentials are logged in either simultaneously or within short time periods but from geographically diverse locations. An employee at Russian search provider Yandex reportedly sold access to nearly 5,000 user mailboxes.[29] A Tesla employee reported that one criminal conspirator offered him US$1 million to help with a scheme involving distraction by distributed denial-of-service (DDoS), information exfiltration and ransomware for extortion. That conspirator claimed an insider at another company had operated undetected for more than three years.[30] Criminal forums routinely advertise the services of insiders in financial services, telecommunications and other sectors.[31, 32] Insiders have also facilitated subscriber identity module (SIM) swapping,[33, 34, 35] which can enable account takeover.[36]

Recent disinformation trends may also play a role in encouraging irresponsible employee behavior and creating insider threats. Employees deceived by disinformation and conspiracy theories—even high-level, IT-savvy and security staff—have made unsound decisions that could harm an employer's reputation.[37, 38, 39]

Why does it matter?

Insider threats have caused brand damage, lost revenue and negatively impacted competitive edge,[40] as well as exposing organizations to penalties for data leaks.

What should you do?

To minimize the risk of insider threats Accenture suggests nurturing employees' sense of responsibility for the organization's security, as well as applying zero-trust principles in security architectures. These may include:

- Enforcing least privilege for user accounts and data access, creating one-time use passwords for sensitive data access and immediately revoking access from former employees.
- Deploying User and Entity Behavior Analytics (UEBA) to detect anomalous behavior and properly enabling security information and event management (SIEM) solutions to detect unauthorized downloading and use of software and sites.
- Limiting employee use of USB drives.
- Monitoring open and Dark Net sources to uncover potential high-risk employees and stolen information.
- Educating employees with phishing simulations and easy "how-to" guides for common work-from-home situations and clarifying penalties for non-compliance.

04
Extortion attacks advance their destructive capabilities

What's happening?

Some ransomware actors portray themselves as honorable businesses, promising to reliably decrypt a victim's computer and destroy any stolen data after receiving the ransom.[41] However, threat actors do not always hold up their side of the bargain and some have developed new means of extortion.

- **Pseudo-ransomware and wiper malware:** Ransomware recovery company Coveware said in February 2021 that it saw an unspecified uptick in "haphazard data destruction," preventing data retrieval even after ransom payment.[42] The ThiefQuest (EvilQuest) MacOs ransomware, an example of pseudo-ransomware, exfiltrated data but provided no instructions for payment.[43]
- **Cruel extortion:** Name-and-shame sites mushroomed, compounding the embarrassment of ransomware and data leak extortion. The SunCrypt group added DDoS threats to the mix,[44, 45] while Clop ransomware actors targeted top executives in breached companies, apparently seeking blackmail fodder.[46] The same Clop group posted stolen data from file transfer company Accellion but reportedly without even deploying ransomware.[47]
- **Empty promises:** Even after victims pay a ransom, threat actors might fail to delete stolen data as promised.[48, 49] Some threat actors deceptively manipulate exfiltrated data: a group selectively leaked European Medicines Agency (EMA) materials in early 2021 in ways the EMA said "could undermine trust in vaccines."[50] Ransomware actors could potentially do this as well.
- **Resistance to pay:** By the end of 2020, ransomware victims increasingly refused to pay a ransom, according to Coveware; the median paid amount fell 55%, from US$110,532 in the July to September period of 2020 to US$49,450 in the October to December period.[51]
- **Global scope creep:** United States and Canadian officials assessed that some ransomware serves adversary intelligence services as well as criminals.[52] The G7 group of nations warned that some ransomware groups "are vulnerable to influence by state actors" and may help states evade sanctions and pay for weapons of mass destruction (WMD).[53]

Why does it matter?

Victims cannot assume that paying a ransom will restore their data or prevent leaks. Backups and recovery of encrypted data are no longer enough.[54]

Organizations could face fines under European Union General Data Protection Regulation (GDPR) if confidential information becomes public. The United States Treasury Department has warned that financial services entities could also face penalties for paying a ransom to a US-sanctioned group or for facilitating payments to terrorists or Weapons of Mass Destruction developers,[55] with additional strictures for cryptocurrency transfers.[56]

Avoiding ransomware infections entirely—the ideal solution—is challenging. Criminals easily buy credentials for previously compromised accounts.[57, 58] They use garden-variety malware, such as Trickbot and Emotet, to deliver ransomware. After government action crippled those botnets, some now use BazarBackdoor and Buer instead.[59]

It is uncertain whether the apparent decline in ransom payments would continue, making ransomware less attractive to criminals, or whether ransomware operators would further adapt with new extortion variants.

What should you do?

Actions to prevent ransomware:

- Protect against common precursor malware such as Trickbot, Emotet, and BazarLoader by promptly applying security patches to software and training employees to recognize phishing e-mails.
- Consider conducting a ransomware self-assessment to gauge vulnerability to ransomware operations.[60]
- Segment systems to minimize the lateral movement of ransomware malware.
- Maintain regularly updated offline backups.
- Deploy and operationalize good logging systems to detect anomalous system behavior.[61]

Actions after a breach has occurred:

- Assume data will be leaked; build a comprehensive understanding of the intrusion and measured impact.
- Put a crisis communications plan in place.
- Work with legal counsel to ensure statutory obligations are fulfilled by reporting an incident to the appropriate authorities.
- Develop and practice incident response playbooks and operational continuity plans.

Actions to predict future behaviors:

- Assess the credibility of threat actors' demands and promises.
- Think twice before paying any ransom;[62, 63] keep up to date with legal and regulatory sanctions.
- Exercise due diligence to avoid facilitating ransom payments. File a suspicious activity report if, for example, a customer new to cryptocurrencies suddenly purchases a large amount of such currency.[64]
- Evaluate current inherent and residual risk measurements and work with the business to identify any risks that go beyond acceptable levels.

05
Emerging technologies continue to reinvent the threat landscape

Threats are agile and organizations should keep pace, too, with emerging technologies. Here are some of the front runners that are reinventing the threat landscape.

Quantum computing and breaking encryption

What's happening?

Quantum computing and cryptography-associated vulnerabilities threaten the security of existing encryption systems. Although practical applications are years in the future, teams in the United States, China and France have, in turn, declared "quantum supremacy." They have shown how quantum computers can solve hard-complexity problems, such as one-day breaking RSA encryption, that would take thousands of years for an ordinary computer.[65] NIST is creating Post-Quantum Cryptography (PQC) standards, with drafts slated for public comment in 2022 to 2023 and final standards likely due in 2024.[66] In the meantime, quantum computing research is surging ahead.[67]

Why does it matter?

Adversaries are getting smarter and more capable just as widely used cryptographic security methods risk being undermined by quantum computing. Cryptographically protected passwords will need additional security protections or stronger standards. Many organizations may struggle to stay compliant with NIST's new PQC standards.[68] Organizations may find themselves experimenting with multiple encryption schemes in an effort to keep up both with standards and with new vulnerabilities.

What should you do?

Accenture suggests that organizations work with partners to develop "crypto-agility,"[69] modular security protocols that can support new algorithms and cryptographic suites and switch back and forth between them. Crypto-agility enables interoperability between new and deprecated algorithms, so organizations can drop old cryptographic practices as stronger options appear.

While crypto-agile modules and PQC are being developed, Accenture also suggests that organizations:

- Double key lengths and select quantum-resistant solutions, where possible.
- Run development tests and benchmarking to evaluate PQC feasibility and impact.
- Automate private key rotation to mitigate future threats while transitioning to PQC where possible.
- Transition to Keccak-derived hash functions (such as SHAKE256) which could provide the most crypto-agility for hashes with variable length outputs.
- Investigate whether Quantum Key Distribution (QKD) methods (such as BB84, E91) are suitable for your organization.
- Automate software development and code reviews to find new vulnerabilities in cryptographic methods.
- Consider adopting authentication schemes that do not rely on passwords.

Biometrics and deepfakes

What's happening?

Biometric authentication for online payment systems and know-your-customer (KYC) systems bears great promise—but also risks. Retailers and payment processors have experimented with payment authorization systems, including facial recognition and fingerprint-authorized contactless payments.[70] Organizations have also explored biometric technologies like iris recognition, heartbeat analysis and vein mapping.[71]

Banks face pandemic-enhanced demand for mobile-friendly onboarding for new bank customers; in the United States, online users accounted for 64% of primary checking account openings, according to biometrics vendor Thales. In a typical mobile-onboarding KYC procedure, the new customer uploads a driver's license and a selfie; the bank checks the validity of the license, compares the selfie with the license photo and checks the selfie for "liveness."[72, 73]

However, artificial intelligence-fed "deepfakes" could enable threat actors to falsify biometric data. The Carnegie Endowment for International Peace warned in a mid-2020 report that techniques like deepfake voice phishing could deceive financial organizations.[74]

While most known deception techniques currently involve methods like conductive ink, latex masks and splicing frames into camera feeds,[75, 76, 77] artificial intelligence provides new ways to deceive biometric authentications. Leaks from fingerprint scanners and facial recognition systems have shown the vulnerability of such tools.[78, 79] Privacy activists and researchers have developed "cloaking" apps to fool facial recognition systems.[80] Researchers have trained optical character recognition (OCR) to misread information—with potential applications for online banking fraud[81]—and have trained neural networks to hide the exfiltration of sensitive accounting data with steganographic techniques.[82]

Accenture, along with other organizations, is developing tests to detect model extraction and poisoning techniques as well as deepfake products. Deepfake detection technology still struggles to assess "liveness" in low-resolution or low-light photos.[83, 84] Researchers are exploring deepfake prevention techniques—such as altering pixels to disrupt an algorithm from outputting realistic deepfake images—but these require further research.[85]

Why does it matter?

Financial organizations have strong incentives to adopt time-saving artificial intelligence methods—Accenture assessed in 2017 that AI technologies could add some US$1.2T to the financial sector by 2035.[86] However, many users remain distrustful of AI. The European Union, NIST, and other entities have developed non-binding guidelines for "Trustworthy AI" that is unbiased, transparent, under human control and secure.[87]

What should you do?

Accenture suggests that as organizations develop machine-learning models, they should consider steps to improve security. These can include:

- Rate-limiting how individuals can submit inputs to a machine learning system.
- Validating and simplifying the inputs.
- Simplifying model structures to provide natural resistance to adversarial examples.
- Including adversarial examples during the training phase to "inoculate" the algorithm against them.[88]

When onboarding new accounts, banks may consider techniques for using geolocation, device IP address and user keying patterns to learn legitimate customer behavior and discover anomalies.[89]

Ready for resilience

Financial services are the bedrock of global economies. For governments, the stability of the finance sector is fundamental to decision making. For customers, knowing that their finances are safe and sound and their privacy protected is essential for consumer confidence.

Vulnerabilities remain high, but there are steps financial institutions can take to improve security in the long term.

1. **Know your operations** by modeling threats against your end-to-end value chain and taking full account of third-party risks.
2. **Strengthen defenses** across people, process and technology. Encourage security leaders to be active in demonstrating why security is critical to business strategy.
3. **Be agile** to keep pace with new variants and enhanced tactics and outrun cybercriminals.
4. **Proactively collaborate** so that everyone knows how to work together before, during and after an event.
5. **Plan for resilience** by maintaining high standards of security hygiene and focusing on business and operational risks.

Contacts

Valerie Abend

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

Howard Marshall

Managing Director, Accenture Security
howard.marshall@accenture.com

References

1 FBI releases the Internet Crime Complaint Center 2020 Internet Crime Report, including COVID-19 Scam Statistics, FBI News, March 17, 2021. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

2 Microsoft Security Team, Sophisticated cybersecurity threats demand collaborative, global response, 4 February 2021, https://www.microsoft.com/security/blog/2021/02/04/sophisticated-cybersecurity-threats-demand-collaborative-global-response/

3 In addition to publicly reported United States federal agencies, researchers have publicly listed 23 victims of end-stage malware. In addition to domains associated with United States government agencies and information, communications and technology (ICT) or cybersecurity companies, the list includes domains associated with health organizations; the European Union's Single Resolution Board, an apparent local affiliate of Fox news, and Chevron Texaco. "Finding Targeted SUNBURST Victims with pDNS," 7 January 2021, https://www.netresec.com/?page=Blog&month-2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS

4 Lawrence Abrams, US cities disclose data breaches after vendor's ransomware attack, 18 February 2021, https://www.bleepingcomputer.com/news/security/us-cities-disclose-data-breaches-after-vendors-ransomware-attack/

5 Julian E. Barnes and David E. Sanger, White House Announces Senior Official Is Leading Inquiry Into SolarWinds Hacking, 10 February 2021, https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html

6 US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, CISA, Alert (AA21-008A) Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments , 8 January 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-008a

7 SITREP: Post-Compromise Authentication Abuse Tactics Expose Cloud Services, 18 December 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/e3492fe0-a676-4c7c-a288-74e9c0563895

8 Accenture Cyber Defense, Cyber Defense Looking back to see the future: CIFR DeLorean—2021 edition , 10 February 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition

9 Erik Hjelmvik, Twenty-three SUNBURST Targets Identified, 25 January 2021, https://www.netresec.com/?page=Blog&month=2021-01&post=Twenty-three-SUNBURST-Targets-Identified

10 Accenture Cyber Defense, Cyber Defense Looking back to see the future: CIFR DeLorean—2021 edition, 10 February 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition

11 Alireza Salimi and Benjamin Glen McCarty, Information assurance (ia) using an integrity and identity resilient blockchain, 29 July 2020, https://patents.google.com/patent/EP3687107A1

12 US Department of Justice, Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe, 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and; David Dawkins, Nigerian Influencer Ramon 'Hushpuppi' Abbas Laundered Funds For North Korean Hackers, Says U.S. Department Of Justice, 19 Feb 2021, https://www.forbes.com/sites/daviddawkins/2021/02/19/nigerian-influencer-ramon-hushpuppi-abbas-laundered-funds-for-north-korean-hackers-says-us-department-of-justice/?sh=37d0842f1dd5; Gary Warner, Hushpuppi and Mr.Woodbery, BEC scammers: Welcome to Chicago!, 5 July 2020, http://garwarner.blogspot.com/2020/07/hushpuppi-and-mrwoodbery-bec-scammers.html; Catalin Cimpanu, Three suspects arrested in Maltese bank cyber-heist, 31 January 2020, https://www.zdnet.com/article/three-suspects-arrested-in-maltese-bank-cyber-heist/

13 Profile of Successful Cybercriminal Fingerprinting and Credential Store "Genesis," 7 Oct 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/8396081f-8482-4c07-adb2-f03220ab8579

14 Brian Krebs, U.S. Secret Service: "Massive Fraud" Against State Unemployment Insurance Programs, 16 May 2020, https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/

15 US Attorney's Office, Southern District of New York, Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise, 17 February 2021, https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting

16 Center for Security Studies, ETH Zuerich, The Evolving Cyber Threat Landscape during the Coronavirus Crisis, December 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/23122020_CyberThreatLandscapeCoronaCrisis.pdf

17 US Attorney's Office, Southern District of New York, Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise, 17 February 2021, https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting

18 People aged 70 or older reported median losses of US$9475 from these romance scams, according to a February 2021 US Federal Trade Commission report. Emma Fletcher, Romance scams take record dollars in 2020, 10 Feb 2021, https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020

19 Profile of Successful Cybercriminal Fingerprinting and Credential Store "Genesis" https://intelgraph.idefense.com/#/node/intelligence_alert/view/8396081f-8482-4c07-adb2-f03220ab8579

20 iDefense Explains: Cybercriminal Exploitation of Multi-Factor Authentication 19 February 2021, https://intelgraph.idefense.com/#/node/intelligence_report/view/a03d5d06-1be9-4638-bfac-3cffc458edec

21 Zanko, https://intelgraph.idefense.com/#/node/threat_actor/view/0c09a560-50d9-468d-a494-4feae480d044; Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise, October 2019, https://www.agari.com/cyber-intelligence-research/whitepapers/silent-starling.pdf

22 Fraudulent P2P Payment App Use - Dark Web Chatter and Pandemic Lockdowns Align, 15 February 2021, https://intelgraph.idefense.com/#/node/intelligence_alert/view/cdf50597-1c7b-4699-b653-e83889dd62b2

23 Franca Gutierrez Harris et al, 2021 AML Trends and Developments, 19 February 2021, https://wp.nyu.edu/compliance_enforcement/2021/02/19/2021-aml-trends-and-developments-part-iz-of-iii/

24 How to Fight Business Email Compromise (BEC) with Email Authentication? 22 February 2021, https://thehackernews.com/2021/02/how-to-fight-business-email-compromise.html?m=1

25 Alex Weinert, It's Time to Hang Up on Phone Transports for Authentication, 10 November 2020, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/it-s-time-to-hang-up-on-phone-transports-for-authentication/ba-p/1751752

26 Cyberhaven Survey: Lack of Awareness, Cloud App Usage, and Remote Workers Create Perfect Storm for Insider Attacks, 22 April 2020, https://www.prnewswire.com/news-releases/cyberhaven-survey-lack-of-awareness-cloud-app-usage-and-remote-workers-create-perfect-storm-for-insider-attacks-301043845.html

27 Ponemon Institute, 2020 Cost of Insider Threats Global Report, April 2020, https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

28 SitRep: Cybersecurity Risks Related to COVID-19, 28 April 2020, https://www.accenture.com/_acnmedia/PDF-124/Accenture-SITREP-COVID-19-20200428-V8-Final-Edit.pdf

29 Yandex internal security team uncovers data breach, 12 February 2021, https://yandex.com/company/press_center/press_releases/2021/2021-12-02

30 The Evolving Threat of Initial Access Brokers: Enabling Ransomware Groups, 11 Sept 2020, https://intelgraph.idefense.com/#/node/intelligence_report/view/960c74c3-ee02-4193-8cb7-9df3e776d05e; https://www.zdnet.com/article/russian-arrested-for-trying-to-recruit-an-insider-and-hack-a-nevada-company/

31 Current Underground Trends Further Aid Malicious Insiders, https://www.darkreading.com/endpoint/how-the-dark-web-fuels-insider-threats/a/d-id/1337599, 27 April 2020

32 Actor lalalamag Seeks Insiders at Large Companies , 15 December 2020, https://intelgraph.idefense.com/#/node/malicious_event/view/86eb93f1-bb82-4458-aa8d-d33330aacb9a

33 UK Law Enforcement Arrests Eight for Celebrity SIM Swapping, 12 Feb 2021, https://intelgraph.idefense.com/#/node/intelligence_alert/view/9f67ed26-c9c2-4fc3-8315-ce6e8281f8eb

34 Brits arrested for sim swapping attacks on US celebs, accessed 1 March 2021, https://www.nationalcrimeagency.gov.uk/news/brits-arrested-for-sim-swapping-attacks-on-us-celebs

35 Prosecutor charges former phone company employee in SIM-swap schemeArs Technica: https://apple.news/A3EAN5wzfRtaKI1OeKmubIA

36 SIM Swap Fraud: An old but resilient enemy, 3 December 2020, https://blogs.lexisnexis.com/fraud-and-identity-in-focus/sim-swap-fraud/

37 Joe Ondrak and Nick Backovic, QAnon Key Figure Revealed as Financial Information Security Analyst from New Jersey. 10 September 2020. https://www.logically.ai/articles/qanon-key-figure-man-from-new-jersey; Kyle Rempfer, Army PSYOP officer resigned commission prior to leading group to DC protests. 11 January 2021. Army Times. https://www.armytimes.com/news/your-army/2021/01/11/army-psyop-officer-resigned-commission-prior-to-leading-group-to-dc-protests/; From Navy SEAL to Part of the Angry Mob Outside the Capitol, 26 January 2021 https://www.nytimes.com/2021/01/26/us/navy-seal-adam-newbold-capitol.html; Dave Troy, 14 February 2021, https://twitter.com/davetroy/status/1360992025848524800?s=12

38 People at the US Capitol riot are being identified and losing their jobs, updated 9 January 2021, https://www.cnn.com/2021/01/07/us/capitol-riots-people-fired-jobs-trnd/index.html

39 Behind the Nashville Bombing, a Conspiracy Theorist Stewing About the Government, 24 February 2021, https://www.nytimes.com/2021/02/24/us/anthony-warner-nashville-bombing.html

40 Communication, Cloud & Finance Apps Most Vulnerable to Insider Threat, https://www.darkreading.com/cloud/communication-cloud-and-finance-apps-most-vulnerable-to-insider-threat/d/d-id/1337636 and conducted by Cybersecurity Insiders

41 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion; Azim Khodzhibaev et al, Interview with a Lockbit Ransomware Operator, 4 January 2021, https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

42 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

43 2021 State of Malware Report, February 2021, https://resources.malwarebytes.com/files/2021/02/MWB_StateOfMalwareReport2021.pdf

44 Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect, 6 Nov 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/f469943c-a0c5-46c8-ad91-2b0f7e84febd

45 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion.

46 Catalin Cimpanu, Some ransomware gangs are going after top execs to pressure companies into paying, January 9, 2021, https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/

47 Andrew Moore et al, Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, 22 February 2021, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html (data appeared on its CL0P^_- LEAKS site)

48 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion.

49 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

50 EMA Vaccine Data Potentially Leaked for Disinformation, 19 Jan 2021, https://intelgraph.idefense.com/#/node/intelligence_alert/view/e7fd82c5-058a-4cfb-83f0-3858af5fbae2

51 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020. The average paid ransom declined 34%, from US$233,817 in Q3 to US$154,108 in Q4.

52 US Cybersecurity and Infrastructure Security Agency, Alert (AA20-205A) NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, 23 July 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-205a; Canadian Centre for Cyber Security, Cyber Threat Bulletin: Modern Ransomware and Its Evolution, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution, 30 November 2020.

53 Ransomware Annex to G7 Statement, 13 October 2020, https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf

54 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure.com/podcast-ransomware-mikko/

55 US Treasury Department, Ransomware Advisory, 1 October 2020, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

56 Frost Brown Todd LLC, Ransomware and Bitcoin - Tax Troubles?, 10 Feb 2021, https://www.lexology.com/library/detail.aspx?g=d06237b0-9685-48c4-819a-ab0b3fb5f551

57 Paul Mansfield and Thomas Willkan, Shady deals: The destructive relationship between network access sellers and ransomware groups, 12 October 2020, https://www.accenture.com/us-en/blogs/cyber-defense/destructive-relationship-between-network-access-sellers-and-ransomware-groups

58 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure.com/podcast-ransomware-mikko/

59 Accenture CTI. Threat Actor Memeos Offers Buer Loader as Malware-as-a-Service on Exploit and XSS Forums. 11 November 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/82a84bd9-062a-44f6-a350-e8f997ee6e96

60 Ransomware Self-Assessment Tool, October 2020, Developed by the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service, https://www.csbs.org/sites/default/files/2020-10/R-SAT_0.pdf

61 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure.com/podcast-ransomware-mikko/

62 Accenture Security. 2020 Cyber Threatscape Report. https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-Threatscape-Report.pdf#zoom=50

63 Ryan LaSalle, Securing your business and the world from ransomware , 30 November 2020, https://www.accenture.com/us-en/blogs/security/securing-business-and-world-from-ransomware

64 FinCen Advisory FIN-2020-A006, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments , 1 October 2020, https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

65 Martin Koppe, A CNRS collaboration achieves quantum supremacy, 23 February 2021, https://news.cnrs.fr/articles/a-cnrs-collaboration-achieves-quantum-supremacy; Tom Simonite, China Stakes Its Claim to Quantum Supremacy, 12 March 2020, https://www.wired.com/story/china-stakes-claim-quantum-supremacy/

66 Dustin Moody, NIST PQC Standardization Update-Round 2 and Beyond. 23 September 2020. https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf

67 Accenture, The race to crypto-agility, 2021, https://www.accenture.com/_acnmedia/PDF-145/Accenture-Crypto-Agility-POV-v7-0

68 Dustin Moody, NIST PQC Standardization Update-Round 2 and Beyond. 23 September 2020. https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf

69 Accenture, The race to crypto-agility, 2021, https://www.accenture.com/_acnmedia/PDF-145/Accenture-Crypto-Agility-POV-v7-0

70 The Thales Group, Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news), 20 February 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

71 Davey Winder, New Hand Gesture Technology Could Wave Goodbye To Passwords, 9 September 2019, https://www.forbes.com/sites/daveywinder/2019/09/09/exclusive-new-hand-gesture-technology-could-wave-goodbye-to-passwords/#31aee09d5286

72 The Thales Group, Liveness in biometrics: spoofing attacks and detection, 4 December 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/liveness-detection

73 FaceTec Raises Biometric Spoof Bounty to US$100,000 Total, 5 August 2020, https://findbiometrics.com/facetec-raises-biometric-spoof-bounty-to-100000-total-908051/

74 Jon Bateman, Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios. 1 July 2020. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237

75 The Thales Group, Liveness in biometrics: spoofing attacks and detection, 4 December 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/liveness-detection

76 Critical Vulnerabilities Present in GeoVision Fingerprint Scanner and Surveillance Security Devices, iDefense Global Research Intelligence Digest for July 1, 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/e7b76cea-a163-40ef-8fc3-c961b6d2f17b

77 FaceTec Raises Biometric Spoof Bounty to US$100,000 Total, 5 August 2020, https://findbiometrics.com/facetec-raises-biometric-spoof-bounty-to-100000-total-908051/

78 Acronis Security, Backdoor wide open: critical vulnerabilities uncovered in GeoVision , 26 June 2020, https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision

79 Zack Whittaker, Security Lapse Exposed Clearview AI Source Code, 16 April 2020, https://techcrunch.com/2020/04/16/clearview-source-code-lapse/

80 Thales, Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news), 20 February 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

81 Accenture Labs, Know Your Threat: AI Is the New Attack Surface, 2019, https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

82 Marco Schreyer, Leaking Sensitive Financial Accounting Data in Plain Sight using Deep Autoencoder Neural Networks. 13 Dec 2020. https://arxiv.org/abs/2012.07110.

83 Ruben Tolosana et al, DeepFakes Evolution: Analysis of Facial Regions and Fake Detection Performance, 2 July 2020, https://arxiv.org/pdf/2004.07532.pdf

84 Deepfake Detection Challenge, https://ai.facebook.com/datasets/dfdc/

85 Ruben Tolosana et al, DeepFakes Evolution: Analysis of Facial Regions and Fake Detection Performance, 2 July 2020, https://arxiv.org/pdf/2004.07532.pdf

86 Mark Purdy and Paul Daugherty, How AI Boosts Industry Profits and Innovation, 2017, https://www.accenture.com/fr-fr/_acnmedia/36dc7f76eab444cab6a7f44017cc3997.pdf

87 Dave Nyczepir, NIST methodically releasing guidance on trustworthy AI, 12 November 2020, https://www.fedscoop.com/nist-guidance-trustworthy-ai/; European Union, ALTAI - The Assessment List on Trustworthy Artificial Intelligence, accessed 1 March 2021, https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence

88 Malek Ben Salem, The New Cyberattack Surface: Artificial Intelligence - Know your threat, 3 August 2020, https://thecyberwire.com/stories/e6909452135l4cd78a5cb9dcf91e4d06/the-new-cyberattack-surface-artificial-intelligence-know-your-threat

89 The Thales Group, Risk management cloud services for an optimised digital banking experience, accessed 1 March 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/fraud-prevention

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 537,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at **www.accenture.com/security**