Cybersecurity: Emerging Industry Priorities and Threats
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Cyber threats are no longer a question of if, but when, a breach will occur. It is important to have a cybersecurity plan in place, so you are ready to act if your organization experiences a data breach. Join panelists as they share areas of focus for the year ahead.

Moderator:
Brita Bayatmakou
Senior Director, Cyber and Analytics Unit (CAU)
FINRA Member Supervision

Panelists:
Brian Carter
Vice President, Technology
Sigma Financial

David Kelley
Director, Cyber and Analytics Unit (CAU)
FINRA Member Supervision

Bryan Smith
Section Chief, Cyber Criminal Section
Federal Bureau of Investigation (FBI)

Cybersecurity: Emerging Industry Priorities and Threats Panelists Bios:

Moderator:

Brita Bayatmakou is Senior Director in FINRA's National Cause and Financial Crimes Detection Program where she leads the Cyber and Analytics Unit. Her team's mission is to assess and enhance member firms' cyber controls, support firm examination teams, and conduct complex investigations in the cybersecurity and cyber-enabled fraud disciplines, including crypto-related assets. Additionally, she leads the department's data analytics and technology strategy, which helps to proactively target top financial crime-related threats. Ms. Bayatmakou joined FINRA from Charles Schwab where she built out several functions within the Financial Crimes Risk Management organization including an intelligence team that analyzed and identified emerging and complex fraud, AML and sanctions evasion trends. She also led a team that focused on financial crime threat detection through the use of data science and advanced analytics. Reflecting her AML expertise, Ms. Bayatmakou served as the BSA/AML Officer of Schwab's Mutual Funds, ETFs, Worldwide Funds PLC and Charles Schwab Futures, Inc. Ms. Bayatmakou has authored/co-authored several publications related to financial crimes, cybersecurity, and AML topics. She holds two Masters Degrees, is a Certified Financial Crimes Specialist (CFCS), and Certified Anti-Money Laundering Specialist (CAMS). In addition to English, Ms. Bayatmakou speaks French, Farsi, and Arabic.

Panelists:

Brian Carter is Vice President of Technology for Sigma Financial Corporation and Parkland Securities, LLC. He joined the firm in early 2021 to lead the effort to modernize and transform their technology platform. Mr. Carter brings a passion for implementing technology that helps organizations and people be more effective. How can we create solutions that allow people to shift their time from doing lower-value work to higher-value work? In the Post-COVID World with people working remotely, how do we allow them to do their work effectively while mitigating the constant cybersecurity threats posed by bad actors? These are some of the questions Mr. Carter thinks the most about. He began his 20 plus years of experience in financial services technology as a programmer tasked with building a new commission processing system for National Planning Holdings, a broker dealer network formerly owned by Jackson National Life. From there he moved into various leadership roles, gaining experience in a wide range of technology disciplines. Mr. Carter earned an MBA from Vanderbilt University in 2014, which was a catalyst to transforming his outlook on technology to be more business focused.

Dave Kelley, Director, Member Supervision Specialist Programs, is based out of FINRA's Kansas City office. He has been with FINRA for more than 11 years and leads the specialist team dealing with cybersecurity and information technology controls. Prior to joining FINRA, he worked for more than 19 years at American Century Investments in various positions, including Chief Privacy Officer, Director of IT Audit, Director of Electronic Commerce Controls and AML Officer. He led the development of website controls, including customer application security, ethical hacking programs and application controls. Mr. Kelley is a CPA and Certified Internal Auditor, and previously held the Series 7 and 24 licenses.

Bryan Smith has been employed by the Federal Bureau of Investigation (FBI) as a Special Agent since 2002 and currently serves as the Section Chief for the FBI's Cyber Criminal Section where he is responsible for the FBI's investigations and operations against cybercriminal actors and threats. Prior to his current role, Mr. Smith served as the Assistant Special Agent in Charge over the Cleveland Field Office's Cyber/White Collar Branch, Unit Chief over the FBI's Money Laundering and Bank Fraud unit, and as the FBI's Detailee to the U.S. Securities and Exchange Commission (SEC) where he assisted both agencies in insider trading, market manipulation, and investment fraud matters. His experience crosses over financial crimes, cyber, and virtual currency and he has initiated a number of private sector outreach efforts to better

leverage the complementary knowledge of both. Prior to the FBI, Mr. Smith worked as a consultant for Accenture and Deloitte and Touche and is a graduate of Bradley University with a degree in accounting.

Cybersecurity: Emerging Industry Priorities and Threats

Panelists

- **Moderator**
  - Brita Bayatmakou, Senior Director, Cyber and Analytics Unit (CAU), FINRA Member Supervision
- **Panelists**
  - Brian Carter, Vice President, Technology, Sigma Financial
  - David Kelley, Director, Cyber and Analytics Unit (CAU), FINRA Member Supervision
  - Bryan Smith, Section Chief, Cyber Criminal Section, Federal Bureau of Investigation (FBI)

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/a6eh** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **From a cyber threat perspective, which of the following most keeps you up at night?**
   a. An email phishing attack
   b. The possibility of a ransomware attack
   c. Unauthorized customer account access and theft
   d. A widespread cyber attack on critical infrastructure
   e. Other cyber issue

Polling address: **https://finra.cnf.io/sessions/a6eh**

Polling Question 2

2. **Do you have an established contact within the law enforcement community who you would call if/when a cyber event occurs?**
   a. Yes, the FBI
   b. Yes, the local police
   c. No
   d. I would have to go dig up a business card in the bottom of my desk drawer

Polling address: **https://finra.cnf.io/sessions/a6eh**

Polling Question 3

3. **Have you already implemented some form of multi-factor authentication (MFA)?**
   a. Yes, our firm uses MFA to verify customers when they access accounts online.
   b. Yes, our firm requires employees and reps to use MFA (e.g., for external access to email systems or to access systems that may contain confidential information).
   c. Yes, our firm uses MFA for employees, reps and customers.
   d. No, we don't use MFA today.

Polling address: **https://finra.cnf.io/sessions/a6eh**

Cybersecurity: Emerging Industry Priorities and Threats
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Resources:

- FINRA *Regulatory Notice 21-18, FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts* (May 2021)

  www.finra.org/rules-guidance/notices/21-18

- FINRA *Information Notice – 4/29/19, Imposter Websites Impacting Member Firms* (April 2019)

  www.finra.org/rules-guidance/notices/information-notice-042919

Alert (AA22-110A)

More Alerts

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Original release date: April 20, 2022

Summary

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5(link is external)], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Actions critical infrastructure organizations should implement to immediately protect against Russian state-sponsored and criminal cyber threats:
• Patch all systems. Prioritize patching known exploited vulnerabilities.
• Enforce multifactor authentication.
• Secure and monitor Remote Desktop Protocol and other risky services.
• Provide end-user awareness and training.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations

in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing materiel support to Ukraine. Other cybercrime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive.

This advisory updates joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, which provides an overview of Russian state-sponsored cyber operations and commonly observed tactics, techniques, and procedures (TTPs). This CSA—coauthored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC)—provides an overview of Russian state-sponsored advanced persistent threat (APT) groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge critical infrastructure network defenders to prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity. Refer to the Mitigations section of this advisory for recommended hardening actions.

For more information on Russian state-sponsored cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage. For more information on the heightened cyber threat to critical infrastructure organizations, see the following resources:

- Cybersecurity and Infrastructure Security Agency (CISA) Shields Up and Shields Up Technical Guidance webpages
- Australian Cyber Security Centre's (ACSC) Advisory Australian Organisations Should Urgently Adopt an Enhanced Cyber Security Posture.
- Canadian Centre for Cyber Security (CCCS) Cyber Threat Bulletin Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity(link is external)
- National Cyber Security Centre New Zealand (NZ NCSC) General Security Advisory Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine
- United Kingdom's National Cyber Security Centre (NCSC-UK) guidance on how to bolster cyber defences in light of the Russian cyber threat

Click here for a PDF version of this report.

Technical Details

Russian State-Sponsored Cyber Operations

Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology (OT) networks; and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.
Historical operations have included deployment of destructive malware—including BlackEnergy and NotPetya—against Ukrainian government and critical infrastructure organizations. Recent Russian

state-sponsored cyber operations have included DDoS attacks against Ukrainian organizations. **Note:** for more information on Russian state-sponsored cyber activity, including known TTPs, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.

Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- **The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18**
- **Russian Foreign Intelligence Service (SVR)**
- **Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)**
- **GRU's Main Center for Special Technologies (GTsST)**
- **Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)**

The Russian Federal Security Service

Overview: FSB, the KGB's successor agency, has conducted malicious cyber operations targeting the Energy Sector, including UK and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. FSB has been known to task criminal hackers for espionage-focused cyber activity; these same hackers have separately been responsible for disruptive ransomware and phishing campaigns.

Industry reporting identifies three intrusion sets associated with the FSB, but the U.S. and UK governments have only formally attributed one of these sets—known as BERSERK BEAR—to FSB.

- **BERSERK BEAR (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope)** has, according to industry reporting, historically targeted entities in Western Europe and North America including state, local, tribal, and territorial (SLTT) organizations, as well as Energy, Transportation Systems, and Defense Industrial Base (DIB) Sector organizations. This group has also targeted the Water and Wastewater Systems Sector and other critical infrastructure facilities. Common TTPs include scanning to exploit internet-facing infrastructure and network appliances, conducting brute force attacks against public-facing web applications, and leveraging compromised infrastructure—often websites frequented or owned by their target—for Windows New Technology Local Area Network Manager (NTLM) credential theft. Industry reporting assesses that this actor has a destructive mandate.

The U.S. and UK governments assess that this APT group is almost certainly FSB's Center 16, or Military Unit 71330, and that FSB's Center 16 has conducted cyber operations against critical IT systems and infrastructure in Europe, the Americas, and Asia.

Resources: for more information on BERSERK BEAR, see the MITRE ATT&CK® webpage on Dragonfly.

High-Profile Activity: in 2017, FSB employees, including one employee in the FSB Center for Information Security (also known as Unit 64829 and Center 18), were indicted by the U.S. Department of Justice (DOJ) for accessing email accounts of U.S. government and military personnel, private organizations, and cybersecurity companies, as well as email accounts of

journalists critical of the Russian government.[9] More recently, in 2021, FSB Center 16 officers were indicted by the U.S. DOJ for their involvement in a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data. One of the victims was a U.S. nuclear power plant.[10]

Resources: for more information on FSB, see:

- U.S. DOJ Press Release Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- UK Press Release UK Exposes Russian Spy Agency Behind Cyber Incidents

Russian Foreign Intelligence Service

Overview: SVR has operated an APT group since at least 2008 that has targeted multiple critical infrastructure organizations. SVR cyber threat actors have used a range of initial exploitation techniques that vary in sophistication coupled with stealthy intrusion tradecraft within compromised networks. SVR cyber actors' novel tooling and techniques include:

- Custom, sophisticated multi-platform malware targeting Windows and Linux systems (e.g., GoldMax and TrailBlazer); and
- Lateral movement via the "credential hopping" technique, which includes browser cookie theft to bypass multifactor authentication (MFA) on privileged cloud accounts.[11(link is external)]

High-Profile Activity: the U.S. Government, the Government of Canada, and the UK Government assess that SVR cyber threat actors were responsible for the SolarWinds Orion supply chain compromise and the associated campaign that affected U.S. government agencies, critical infrastructure entities, and private sector organizations.[12][13(link is external)][14]

Also known as: APT29, COZY BEAR, CozyDuke, Dark Halo, The Dukes, NOBELIUM, and NobleBaron, StellarParticle, UNC2452, YTTRIUM [15]

Resources: for more information on SVR, see:

- Joint CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint Advisory Further TTPs associated with SVR cyber actors
- The MITRE ATT&CK webpage on APT29

For more information on the SolarWinds Orion supply chain compromise, see:

- CISA's Supply Chain Compromise webpage
- CISA's webpage on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- NCSC-UK Guidance Dealing with the SolarWinds Orion compromise

GRU, 85th Main Special Service Center

Overview: GTsSS, or Unit 26165, is an APT group that has operated since at least 2004 and

primarily targets government organizations, travel and hospitality entities, research institutions, and non-governmental organizations, in addition to other critical infrastructure organizations.

According to industry reporting, GTsSS cyber actors frequently collect credentials to gain initial access to target organizations. GTsSS actors have collected victim credentials by sending spearphishing emails that appear to be legitimate security alerts from the victim's email provider and include hyperlinks leading to spoofed popular webmail services' logon pages. GTsSS actors have also registered domains to conduct credential harvesting operations. These domains mimic popular international social media platforms and masquerade as tourism- and sports-related entities and music and video streaming services.

High-Profile Activity: the U.S. Government assesses that GTsSS cyber actors have deployed Drovorub malware against victim devices as part of their cyber espionage operations.[16] The U.S. Government and UK Government assess that GTsSS actors used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.[17]

Also known as: APT28, FANCY BEAR, Group 74, IRON TWILIGHT, PawnStorm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, Swallowtail, TG-4127, Threat Group-4127, and Tsar Team [18]

Resources: for more information on GTsSS, see the MITRE ATT&CK webpage on APT28.

GRU's Main Center of Special Technologies

Overview: GTsST, or Unit 74455, is an APT group that has operated since at least 2009 and has targeted a variety of critical infrastructure organizations, including those in the Energy, Transportation Systems, and Financial Services Sectors. According to industry reporting, GTsST also has an extensive history of conducting cyber espionage as well as destructive and disruptive operations against NATO member states, Western government and military organizations, and critical infrastructure-related organizations, including in the Energy Sector.

The primary distinguishing characteristic of the group is its operations use techniques aimed at causing disruptive or destructive effects at targeted organizations using DDoS attacks or wiper malware. The group's destructive operations have also leveraged wiper malware that mimics ransomware or hacktivism and can result in collateral effects to organizations beyond the primary intended targets. Some of their disruptive operations have shown disregard or ignorance of potential secondary or tertiary effects.

High-Profile Activity: the malicious activity below has been previously attributed to GTsST by the U.S. Government and the UK Government.[19][20]

- GTsST actors conducted a cyberattack against Ukrainian energy distribution companies in December 2015, leading to disruption of multiple companies' operations and widespread temporary outages. The actors deployed BlackEnergy malware to steal user credentials and used BlackEnergy's destructive component, KillDisk, to make infected computers inoperable.
- In 2016, GTsST actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware (also known as Industroyer) specifically designed to attack power grids.

- In June 2017, GTsST actors deployed NotPetya disruptive malware against Ukrainian financial, energy, and government organizations. NotPetya masqueraded as ransomware, had a large collateral impact, and caused damage to millions of devices globally.
- In 2018, GTsST actors deployed data-deletion malware against the Winter Olympics and Paralympics using VPNFilter.

The U.S. Government, the Government of Canada, and UK Government have also attributed the October 2019 large-scale, disruptive cyber operations against a range of Georgian web hosting providers to GTsST. This activity resulted in websites—including sites belonging to the Georgian government, courts, non-government organizations (NGOs), media, and businesses—being defaced and interrupted the service of several national broadcasters.[21]22(link is external)][23]

Also known as: ELECTRUM, IRON VIKING, Quedagh, the Sandworm Team, Telebots, VOODOO BEAR [24]

Resources: for more information on GTsST, see the MITRE ATT&CK webpage on Sandworm Team.

Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics

Overview: TsNIIKhM, as described on their webpage, is a research organization under Russia's Ministry of Defense (MOD). Actors associated with TsNIIKhM have developed destructive ICS malware.

High-Profile Activity: TsNIIKhM has been sanctioned by the U.S. Department of the Treasury for connections to the destructive Triton malware (also called HatMan and TRISIS); TsNIIKhM has been sanctioned by the UK Foreign, Commonwealth, and Development Office (FCDO) for a 2017 incident that involved safety override controls (with Triton malware) in a foreign oil refinery.[25][26] In 2021, the U.S. DOJ indicted a TsNIIKhM Applied Development Center (ADC) employee for conducting computer intrusions against U.S. Energy Sector organizations. The indicted employee also accessed the systems of a foreign oil refinery and deployed Triton malware.[27] Triton is a custom-built malware designed to manipulate safety instrumented systems within ICS controllers, disabling the safety alarms that prevent dangerous conditions.

Also known as: Temp.Veles, XENOTIME [28]

Resources: for more information on TsNIIKhM, see the MITRE ATT&CK webpage on TEMP.Veles. For more information on Triton, see:

- CISA Malware Analysis Report (MAR) Hatman – Safety System Targeted Malware (update B)
- CISA ICS Advisory: Schneider Electric Triconex Tricon (Update B)
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- NCSC-UK Advisory TRITON Malware Targeting Safety Controllers

Russian-Aligned Cyber Threat Groups

In addition to the APT groups identified in the Russian State-Sponsored Cyber Operations section, industry reporting identifies two intrusion sets—PRIMITIVE BEAR and VENOMOUS BEAR—as state-sponsored APT groups, but U.S., Australian, Canadian, New Zealand, and UK cyber authorities have

not attributed these groups to the Russian government.

- **PRIMITIVE BEAR** has, according to industry reporting, targeted Ukrainian organizations since at least 2013. This activity includes targeting Ukrainian government, military, and law enforcement entities using high-volume spearphishing campaigns to deliver its custom malware. According to industry reporting, PRIMITIVE BEAR conducted multiple cyber operations targeting Ukrainian organizations in the lead up to Russia's invasion.

Resources: for more information on PRIMITIVE BEAR, see the MITRE ATT&CK webpage on the Gamaredon Group.

- **VENOMOUS BEAR** has, according to industry reporting, historically targeted governments aligned with the North Atlantic Treaty Organization (NATO), defense contractors, and other organizations of intelligence value. Venomous Bear is known for its unique use of hijacked satellite internet connections for command and control (C2). It is also known for the hijacking of other non-Russian state-sponsored APT actor infrastructure.[29] VENOMOUS BEAR has also historically leveraged compromised infrastructure and maintained an arsenal of custom-developed sophisticated malware families, which is extremely complex and interoperable with variants developed over time. VENOMOUS BEAR has developed tools for multiple platforms, including Windows, Mac, and Linux.[30(link is external)]

Resources: for more information on VENOMOUS BEAR, see the MITRE ATT&CK webpage on Turla.

Russian-Aligned Cybercrime Groups

Cybercrime groups are typically financially motivated cyber actors that seek to exploit human or security vulnerabilities to enable direct theft of money (e.g., by obtaining bank login information) or by extorting money from victims. These groups pose consistent threats to critical infrastructure organizations globally.

Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine. These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations primarily through:

- Deploying ransomware through which cyber actors remove victim access to data (usually via encryption), potentially causing significant disruption to operations.
- Conducting DDoS attacks against websites.
  - In a DDoS attack, the cyber actor generates enough requests to flood and overload the target page and stop it from responding.
  - DDoS attacks are often accompanied by extortion.
  - According to industry reporting, some cybercrime groups have recently carried out DDoS attacks against Ukrainian defense organizations, and one group claimed credit for DDoS attack against a U.S. airport the actors perceived as supporting Ukraine (see the Killnet section).

Based on industry and open-source reporting, U.S., Australian, Canadian, New Zealand, and UK

cyber authorities assess multiple Russian-aligned cybercrime groups pose a threat to critical infrastructure organizations. These groups include:

- **The CoomingProject**
- **Killnet**
- **MUMMY SPIDER**
- **SALTY SPIDER**
- **SCULLY SPIDER**
- **SMOKEY SPIDER**
- **WIZARD SPIDER**
- **The Xaknet Team**

Note: although some cybercrime groups may conduct cyber operations in support of the Russian government, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess that cyber criminals will most likely continue to operate primarily based on financial motivations, which may include targeting government and critical infrastructure organizations.

The CoomingProject

Overview: the CoomingProject is a criminal group that extorts money from victims by exposing or threatening to expose leaked data. Their data leak site was launched in August 2021.[31(link is external)] The CoomingProject stated they would support the Russian Government in response to perceived cyberattacks against Russia.[32(link is external)]

Killnet

Overview: according to open-source reporting, Killnet released a video pledging support to Russia.[33(link is external)]
Victims: Killnet claimed credit for carrying out a DDoS attack against a U.S. airport(link is external) in March 2022 in response to U.S. materiel support for Ukraine.[34(link is external)]

MUMMY SPIDER

Overview: MUMMY SPIDER is a cybercrime group that creates, distributes, and operates the Emotet botnet. Emotet is advanced, modular malware that originated as a banking trojan (malware designed to steal information from banking systems but that may also be used to drop additional malware and ransomware). Today Emotet primarily functions as a downloader and distribution service for other cybercrime groups. Emotet has been used to deploy WIZARD SPIDER's TrickBot, which is often a precursor to ransomware delivery. Emotet has worm-like features that enable rapid spreading in an infected network.

Victims: according to open sources, Emotet has been used to target industries worldwide, including financial, e-commerce, healthcare, academia, government, and technology organizations' networks.

Also known as: Gold Crestwood, TA542, TEMP.Mixmaster, UNC3443

Resources: for more information on Emotet, see joint Alert Emotet Malware. For more information on TrickBot, see joint CSA TrickBot Malware.

SALTY SPIDER

Overview: SALTY SPIDER is a cybercrime group that develops and operates the Sality botnet. Sality

is a polymorphic file infector that was discovered in 2003; since then, it has been replaced by more advanced peer-to-peer (P2P) malware loaders.[35(link is external)]

Victims: according to industry reporting, in February 2022, SALTY SPIDER conducted DDoS attacks against Ukrainian web forums used to discuss events relating to Russia's military offensive against the city of Kharkiv.

Also known as: Sality

SCULLY SPIDER

Overview: SCULLY SPIDER is a cybercrime group that operates using a malware-as-a-service model; SCULLY SPIDER maintains command and control infrastructure and sells access to their malware and infrastructure to affiliates, who distribute their own malware.[36(link is external)][37(link is external)] SCULLY SPIDER develops and operates the DanaBot botnet, which originated primarily as a banking Trojan but expanded beyond banking in 2021 and has since been used to facilitate access for other types of malware, including TrickBot, DoppelDridex, and Zloader. Like Emotet, Danabot effectively functions as an initial access vector for other malware, which can result in ransomware deployment.

According to industry reporting, recent DDoS activity by the DanaBot botnet suggests SCULLY SPIDER has operated in support of Russia's military offensive in Ukraine.

Victims: SCULLY SPIDER affiliates have primarily targeted organizations in the United States, Canada, Germany, United Kingdom, Australia, Italy, Poland, Mexico, and Ukraine.[38(link is external)] According to industry reporting, in March 2022, Danabot was used in DDoS attacks against multiple Ukrainian government organizations.

Also known as: Gold Opera

SMOKEY SPIDER

Overview: SMOKEY SPIDER is a cybercrime group that develops Smoke Loader (also known as Smoke Bot), a malicious bot that is used to upload other malware. Smoke Loader has been available since at least 2011, and operates as a malware distribution service for a number of different payloads, including—but not limited to—DanaBot, TrickBot, and Qakbot.

Victims: according to industry reporting, Smoke Loader was observed in March 2022 distributing DanaBot payloads that were subsequently used in DDoS attacks against Ukrainian targets.
Resources: for more information on Smoke Loader, see the MITRE ATT&CK webpage on Smoke Loader.

WIZARD SPIDER

Overview: WIZARD SPIDER is a cybercrime group that develops TrickBot malware and Conti ransomware. Historically, the group has paid a wage to the ransomware deployers (referred to as affiliates), some of whom may then receive a share of the proceeds from a successful ransomware attack. In addition to TrickBot, notable initial access and persistence vectors for affiliated actors include Emotet, Cobalt Strike, spearphishing, and stolen or weak Remote Desktop Protocol (RDP) credentials.

After obtaining access, WIZARD SPIDER affiliated actors have relied on various publicly available and otherwise legitimate tools to facilitate earlier stages of the attack lifecycle before deploying Conti ransomware.

WIZARD SPIDER pledged support to the Russian government and threatened critical infrastructure organizations of countries perceived to carry out cyberattacks or war against the Russian government.[39(link is external)] They later revised this pledge and threatened to retaliate against perceived attacks against the Russian people.[40(link is external)]

Victims: Conti victim organizations span across multiple industries, including construction and engineering, legal and professional services, manufacturing, and retail. In addition, WIZARD SPIDER affiliates have deployed Conti ransomware against U.S. healthcare and first responder networks.

Also known as: UNC2727, Gold Ulrick

Resources: for more information on Conti, see joint CSA Conti Ransomware. For more information on TrickBot, see joint CSA TrickBot Malware.

The XakNet Team

Overview: XakNet is a Russian-language cyber group that has been active as early as March 2022. According to open-source reporting, the XakNet Team threatened to target Ukrainian organizations in response to perceived DDoS or other attacks against Russia.[41(link is external)] According to reporting from industry, on March 31, 2022, XakNet released a statement stating they would work "exclusively for the good of [Russia]." According to industry reporting, the XakNet Team may be working with or associated with Killnet actors, who claimed credit for the DDoS attacks against a U.S. airport (see the Killnet section).

Victims: according to industry reporting, in late March 2022, the XakNet Team leaked email contents of a Ukrainian government official. The leak was accompanied by a political statement criticizing the Ukrainian government, suggesting the leak was politically motivated.

Mitigations

U.S., Australian, Canadian, New Zealand, and UK cyber authorities urge critical infrastructure organizations to prepare for and mitigate potential cyber threats by immediately (1) updating software, (2) enforcing MFA, (3) securing and monitoring RDP and other potentially risky services, and (4) providing end-user awareness and training.

- **Update software, including operating systems, applications, and firmware, on IT network assets.** Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
  - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
  - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.

- **Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords**. Do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. As Russian state-sponsored APT actors have demonstrated the ability to exploit default MFA protocols and known vulnerabilities, organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios. For more information, see joint CSA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability.
- **If you use RDP and/or other potentially risky services, secure and monitor them closely.** RDP exploitation is one of the top initial infection vectors for ransomware, and risky services, including RDP, can allow unauthorized access to your session using an on-path attacker.
  - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN) or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force attempts, log RDP login attempts, and disable unused remote access/RDP ports.
  - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- **Provide end-user awareness and training** to help prevent successful targeted social engineering and spearphishing campaigns. Phishing is one of the top infection vectors for ransomware, and Russian state-sponsored APT actors have conducted successful spearphishing campaigns to gain credentials of target networks.
  - Ensure that employees are aware of potential cyber threats and delivery methods.
  - Ensure that employees are aware of what to do and whom to contact when they receive a suspected phishing email or suspect a cyber incident.

As part of a longer-term effort, **implement network segmentation to separate network segments based on role and functionality**. Network segmentation can help prevent the spread of ransomware and threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Ensure OT assets are not externally accessible. Ensure strong identity and access management when OT assets needs to be externally accessible.
- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by considering criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

To further prepare for and mitigate cyber threats from Russian state-sponsored or criminal actors, U.S., Australian, Canadian, New Zealand, and UK cyber authorities encourage critical infrastructure organizations to implement the recommendations listed below.

Preparing for Cyber Incidents

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
  - Ensure the cyber incident response plan contains ransomware- and DDoS-specific annexes. For information on preparing for DDoS attacks, see NCSC-UK guidance on preparing for denial-of-service attacks.
  - Keep hard copies of the incident response plan to ensure responders and network defenders can access the plan if the network has been shut down by ransomware, etc.
- Maintain offline (i.e., physically disconnected) backups of data. Backup procedures should be conducted on a frequent, regular basis (at a minimum every 90 days). Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.
  - Ensure the backup keys are kept offline as well, to prevent them being encrypted in a ransomware incident.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure with a particular focus on key data assets.
- Develop recovery documentation that includes configuration settings for common devices and critical equipment. Such documentation can enable more efficient recovery following an incident.
- Identify the attack surface by mapping and accounting all external-facing assets (applications, servers, IP addresses) that are vulnerable to DDoS attacks or other cyber operations.
- For OT assets/networks:
  - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
  - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated from IT networks if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety-critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
  - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
  - Implement data backup procedures.
  - Develop recovery documents that include configuration settings for common devices and critical OT equipment.

Identity and Access Management

- Require accounts with password logins, including service accounts, to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. Consider using a password manager; see NCSC-UK's Password Manager Buyers Guide for guidance.
- Implement authentication timeout and lockout features to prevent repeated failed login attempts

and successful brute-force attempts.
- Create a deny list of known compromised credentials and prevent users from using known-compromised passwords.
- Secure credentials by restricting where accounts and credentials can be used and by using local device credential protection features. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
  - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
  - Ensure storage of clear text passwords in Local Security Authority Subsystem Service (LSASS) memory is disabled. **Note:** for Windows 8, this is enabled by default. For more information see Microsoft Security Advisory Update to Improve Credentials Protection and Management(link is external).
  - Consider disabling or limiting NTLM and WDigest Authentication.
  - Implement Credential Guard for Windows 10 and Server 2016 (refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - Minimize the Active Directory (AD) attack surface to reduce malicious ticket-granting activity. Malicious activity such as “Kerberoasting” takes advantage of Kerberos’ Ticket Granting Service (TGS) and can be used to obtain hashed credentials that malicious cyber actors attempt to crack.
- Audit domain controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
  - Secure accounts.
  - Enforce the principle of least privilege. Administrator accounts should have the minimum permission necessary to complete their tasks.
  - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
  - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- Disable inactive accounts uniformly across the AD, MFA systems, etc.
- Implement time-based access for privileged accounts. The FBI and CISA observed cybercriminals conducting increasingly impactful attacks against U.S. entities on holidays and weekends in 2021. Threat actors may view holidays and weekends—when offices are normally closed—as attractive timeframes, as there are fewer network defenders and IT support personnel at victim organizations. The just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the zero-trust model) by setting network-wide policy to automatically disable admin accounts at the AD level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe.

Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor, ransomware, or other malware. Use network monitoring tools and host-based logs and

monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Implement a firewall and configure it to block Domain Name System (DNS) responses from outside the enterprise network or drop Internet Control Message Protocol (ICMP) packets. Review which admin services need to be accessible externally and allow those explicitly, blocking all others by default.
  - U.S. Defense Industrial Base organizations may sign up for the NSA Cybersecurity Collaboration Center's Protective Domain Name System (PDNS) services.
- Enable web application firewalls to mitigate application-level DDoS attacks.
- Implement a multi-content delivery network (CDN) solution. This will minimize the threat of DDoS attacks by distributing and balancing web traffic across a network.

Vulnerability and Configuration Management

- Use an antivirus programs that uses heuristics and reputational ratings to check a file's prevalence and digital signature prior to execution. **Note:** organizations should assess the risks inherent in their software supply chain (including its security/antivirus software supply chain) in light of the existing threat landscape.
  - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
  - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.
- Disable all unnecessary ports and protocols.
  - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control activity.
  - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Identify business-to-business VPNs and block high-risk protocols.
- Ensure OT hardware is in read-only mode.
- Enable strong spam filters.
  - Enable strong spam filters to prevent phishing emails from reaching end users.
  - Filter emails containing executable files to prevent them from reaching end users.
  - Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.
- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement listing policies for applications and remote access that only allow systems to execute

known and permitted programs under an established security policy.
- Open document readers in protected viewing modes to help prevent active content from running.

Responding to Cyber Incidents

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge network defenders of critical infrastructure organizations to exercise due diligence in identifying indicators of malicious activity. Organizations detecting potential APT or ransomware activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. For DDoS attacks:
   a. Identify the source address originating the attack via the SIEM or logging service. If the attack is originating from a single pool of IP addresses, block IP traffic from suspected IPs via access control lists or by contacting your internet service provider (ISP).
   b. Enable firewall rate limiting to restrict the amount of IP traffic coming in from suspected IP addresses
   c. Notify your ISP and enable remote triggered blackhole (RTBH).
3. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
4. Collect and review relevant logs, data, and artifacts.
5. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
6. Report incidents to appropriate cyber and law enforcement authorities:

- **U.S organizations:** share information about incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov(link sends email) or (888) 282-0870 and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov(link sends email). For ransomware incidents, organizations can also report to the U.S. Secret Service via a U.S. Secret Service Field Office.
- **Australian organizations:** if you have questions about this advice or have indications that your environment has been compromised, call the ACSC at 1300 CYBER1 (1300 292 371). To report an incident see cyber.gov.au/acsc/report.
- **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca(link sends email).
- **New Zealand organizations**: if your organization requires assistance from the National Cyber Security Centre, contact them directly via telephone at (04) 498-7654 or via email at ncscincidents@ncsc.govt.nz(link sends email).
- **UK organizations:** report a significant cybersecurity incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

For additional guidance on responding to a ransomware incident, see the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on

hunting or investigating a network, and for common mistakes in incident handling.

Additionally, CISA, the FBI, and NSA encourage U.S. critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

Note: U.S., Australian, Canadian, New Zealand, and UK cyber authorities strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom does not guarantee that a victim's files will be recovered.

RESOURCES

- For more general information on Russian state-sponsored malicious cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage and joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.
- For alerts on malicious and criminal cyber activity, see the FBI Internet Crime Complaint Center webpage.
- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. government webpage providing ransomware resources and alerts.
- For more information on mitigating DDoS attacks, see NCSC-UK Denial of Service (DoS) Guidance.
- For more information on managing cybersecurity incidents, see NZ NCSC Incident Management: Be Resilient, Be Prepared.
- For information on destructive malware, see joint CSA Destructive Malware Targeting Organizations in Ukraine.
- Critical infrastructure owners and operators with OT/ICS networks, should review the following resources for additional information:
  - Joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
  - CISA factsheet Rising Ransomware Threat to Operational Technology Assets

DISCLAIMER

The information you have accessed or received is being provided "as is" for informational purposes only. CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, and the UK National Crime Agency (NCA) do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.

TRADEMARK RECOGNITION

MITRE and ATT&CK are registered trademarks of The MITRE Corporation. Kubernetes is a

registered trademark of The Linux Foundation.

PURPOSE

This document was developed by U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

REFERENCES

[1] Cybersecurity and Infrastructure Security Agency
[2] Federal Bureau of Investigation
[3] National Security Agency
[4] Australian Cyber Security Centre
[5] Canadian Centre for Cyber Security(link is external)
[6] New Zealand's National Cyber Security Centre
[7] United Kingdom's National Cyber Security Centre
[8] United Kingdom's National Crime Agency
[9] U.S. DOJ Press Release: U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts
[10] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
[11] CrowdStrike Blog: Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign(link is external)
[12] U.S. White House Statement: FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian
[13] Government of Canada Statement on SolarWinds Cyber Compromise(link is external)
[14] UK Government Press Release: Russia: UK and US expose global campaign of malign activity by Russian intelligence services
[15] MITRE ATT&CK: APT29
[16] Joint CSA Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware
[17] Joint CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
[18] MITRE ATT&CK APT28
[19] Joint CSA New Sandworm Malware Cyclops Blink Replaces VPNFilter
[20] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks
[21] U.S. Department of State, Press Statement: The United States Condemns Russian Cyber Attack Against the Country of Georgia
[22] Government of Canada CSE Statement on Malicious Russian Cyber Activity Targeting Georgia(link is external)
[23] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks
[24] MITRE ATT&CK The Sandworm Team
[25] U.S. Department of the Treasury Press Release: Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware
[26] UK Government Press Release: UK exposes Russian spy agency behind cyber incident

[27] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
[28] MITRE ATT&CK TEMP.Veles
[29] NSA and NCSC-UK Cybersecurity Advisory Turla Group Exploits Iranian APT To Expand Coverage Of Victims
[30] CrowdStrike Adversary Profile: VENEMOUS BEAR(link is external)
[31] KELA Cybersecurity Intelligence Center: Ain't No Actor Trustworthy Enough: The importance of validating sources(link is external)
[32] Twitter: Valery Marchive Status, Feb. 25, 2022 1:41 PM(link is external)
[33] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)
[34] Twitter: CyberKnow Status, March 29, 2022, 7:54 AM(link is external)
[35] CrowdStrike Blog: Who is Salty Spider (Sality)?(link is external)
[36] Proofpoint Blog: New Year, New Version of DanaBot(link is external)
[37] Zscaler Blog: Spike in DanaBot Malware Activity(link is external)
[38] Proofpoint Blog: New Year, New Version of DanaBot(link is external)
[39] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)
[40] TechTarget: Conti ransomware gang backs Russia, threatens US(link is external)
[41] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)

ACKNOWLEDGEMENTS

The U.S., Australian, Canadian, New Zealand, and UK cyber authorities would like to thank CrowdStrike, Google, LookingGlass Cyber, Mandiant, Microsoft, and Secureworks for their contributions to this CSA.

Contact Information

U.S. organizations: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at report@cisa.gov(link sends email) or (888) 282-0870 and/or to the FBI via your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov(link sends email). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov(link sends email). **Australian organizations:** visit cyber.gov.au/acsc/report or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca(link sends email). **New Zealand organizations:** report cyber security incidents to ncscincidents@ncsc.govt.nz(link sends email) or call 04 498 7654. **United Kingdom organizations:** report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Revisions

April 20, 2022: Initial version

Contact Us

(888)282-0870

Send us email(link sends email)

Download PGP/GPG keys

Submit website feedback

Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

HSIN

Report

RANSOMWARE GUIDE

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

On September 30, 2020, a joint Ransomware Guide was released, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

- **Part 1: Ransomware Prevention Best Practices**
- **Part 2: Ransomware Response Checklist**

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): https://learn.cisecurity.org/ms-isac-registration
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): https://learn.cisecurity.org/ei-isac-registration
  - Sector-based ISACs - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups/
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov
- Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Ransomware Guide (Sept. 2020)

Expand All Sections

TLP:WHITE

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the Public Power Cyber Incident Response Playbook (https://www.publicpower. org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this Ransomware Guide, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.

Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: https://www.cisa.gov/cyber-resource-hub.
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (https://us-cert.cisa.gov/ncas/alerts/aa20-073a).
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:

- Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on th existing systems or applications) that may break when disabled.
  - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
- Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.
  - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
  - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
  - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
  - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
  - If a third party or MSP is responsible for maintaining and securing your organization’s backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA’s APTs Targeting IT Service Provider Customers (https:// us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers).
  - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.

- Adversaries may spoof the identity of—or use compromised email accounts associated with—entities you has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
  - If you are using passwords, use strong passwords (https://us-cert.cisa.gov/ncas/tips/ST04-002) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
  - Restrict user permissions to install and run software applications.
  - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.
  - Remove unnecessary accounts and groups and restrict root access.
  - Control and limit local administration.
  - Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
  - Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.
- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
  - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology. This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.
  - Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

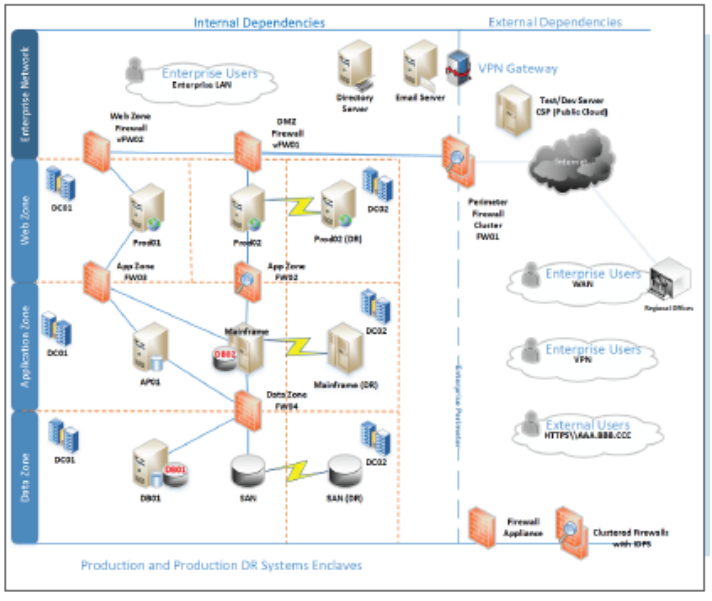


Figure 1. Example Network Diagram

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: https://www.cisecurity. org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/.
- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).
    - The two logs that record PowerShell activity are the "PowerShell" Windows Event Log and the "PowerShell Operational" Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

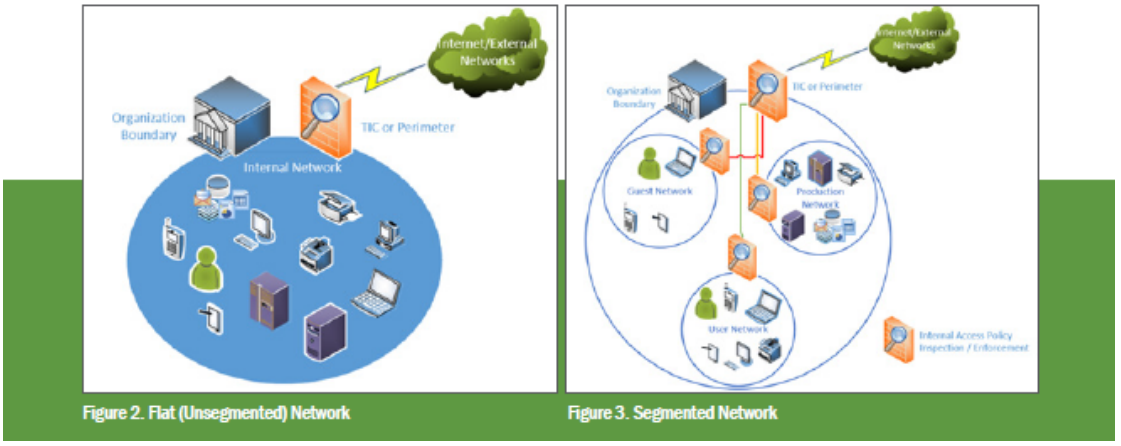


Figure 2. Flat (Unsegmented) Network Figure 3. Segmented Network

- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
  - The following list contains high-level suggestions on how best to secure a DC:
    - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
    - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (https://docs.microsoft.com/ en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-forsecuring-active-directory), when configuring available security features.
    - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
    - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
    - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates

allowing internet access for DCs.

- CISA recommends the following DC Group Policy settings:
  (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
  - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
  - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
  - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.
- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.
  9
  - Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
  - Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.

Contact CISA for These No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: https://www.cisa.gov/cyber-resource-hub
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- CISA Cybersecurity Advisors (CSAs) advise on best practices and connect you with CISA resources to manage cyber risk
- Contacts:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Quick References

- Ransomware: What It Is and What to Do About It (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One -Pager_and_Technical_Document-FINAL.pdf
- Ransomware (CISA): Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: https://www.us-cert.cisa.gov/ransomware
- Security Primer – Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: https://www.cisecurity.org/white-papers/security-primer-ransomware/
- Ransomware: Facts, Threats, and Countermeasures (MSISAC):
  Facts about ransomware, infection vectors, ransomware

capabilities, and how to mitigate the risk of ransomware infection: https://www.cisecurity.org/blog/ransomwarefacts-threats-and-countermeasures/

- Security Primer – Ryuk (MS-ISAC): Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: https://www.cisecurity.org/white-papers/security-primer-ryuk/

Part 2: Ransomware Response Checklist

TLP:WHITE

FEDERAL BUREAU of INVESTIGATION

Internet Crime Report

2021

INTERNET CRIME COMPLAINT CENTER

Contents

INTRODUCTION

Dear Reader,

In 2021, America experienced an unprecedented increase in cyber attacks and malicious cyber activity. These cyber attacks compromised businesses in an extensive array of business sectors as well as the American public. As the cyber threat evolves and becomes increasingly intertwined with traditional foreign intelligence threats and emerging technologies, the FBI continues to leverage our unique authorities and partnerships to impose risks and consequences on our nation's cyber adversaries.

The FBI's Internet Crime Complaint Center (IC3) provides the American public with a direct outlet to report cyber crimes to the FBI. We analyze and investigate the reporting to track the trends and threats from cyber criminals and then share this data with our intelligence and law enforcement partners. The FBI, alongside our partners, recognizes how crucial information sharing of cyber activities is to prepare our partners to combat the cyber threat, through a whole-of-government approach. Critical to that approach is public reporting to IC3 - enabling us to fill in the missing pieces with this valuable information during the investigatory process. Not only does this reporting help to prevent additional crimes, it allows us to develop key insights on the ever-evolving trends and threats we face from malign cyber actors.

In 2021, IC3 continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding $6.9 billion. Among the 2021 complaints received, ransomware, business e-mail compromise (BEC) schemes, and the criminal use of cryptocurrency are among the top incidents reported. In 2021, BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion.

IC3's commitment to cyber victims and partnerships allow for the continued success through programs such as the IC3's Recovery Asset Team (RAT). Established in 2018, RAT streamlines communications with financial institutions and FBI field offices to assist freezing of funds for victims. In 2021, the IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 1,726 BEC complaints involving domestic to domestic transactions with potential losses of $443,448,237. A monetary hold was placed on approximately $329 million, which represents a 74% success rate.

In 2021, heightened attention was brought to the urgent need for more cyber incident reporting to the federal government. Cyber incidents are in fact crimes deserving of an investigation, leading to judicial repercussions for the perpetrators who commit them. Thank you to all those readers who reported crimes to IC3 throughout the year. Without this reporting, we could not be as effective in ensuring consequences are imposed on those perpetrating these attacks and our understanding of these threats would not be as robust. Please visit IC3.gov to access the latest information on criminal internet activity.

The FBI's Cyber Division is working harder than ever to protect the American public and to instill safety, security, and confidence in a digitally connected world. We encourage everyone to use IC3 and reach out to their local FBI field office to report malicious activity. Together we can continue to create a safer and more secure cyber landscape.

Paul Abbate
Deputy Director
Federal Bureau of Investigation

THE IC3

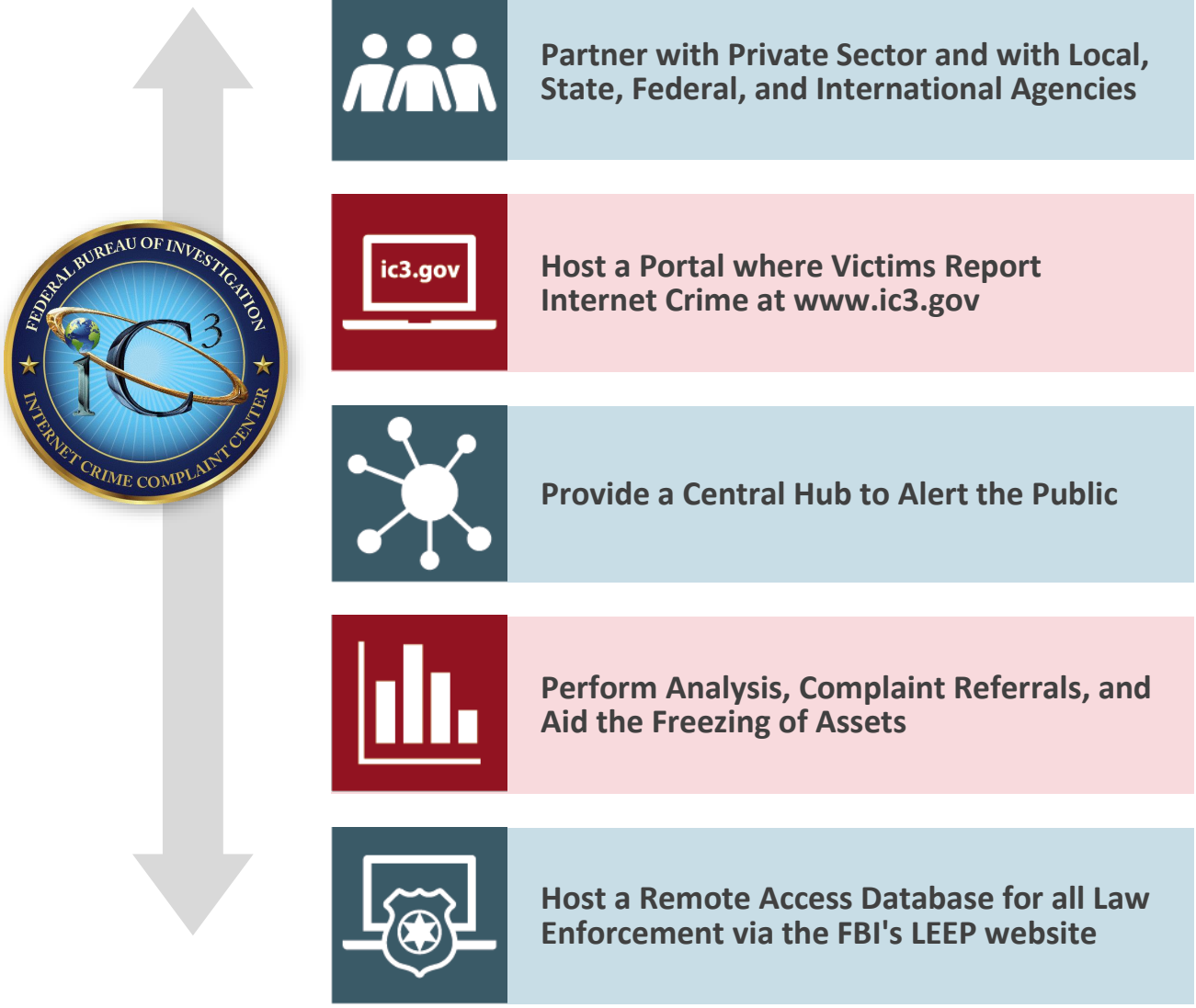
Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber attacks and major criminal threats, and on supporting our many partners with information, services, support, training, and leadership. The IC3 serves those needs as a mechanism to gather intelligence on cyber and internet crime so we can stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints of internet related crime and has received more than 6.5 million complaints since its inception. Its mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected cyber enabled criminal activity, and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and for public awareness.

To promote public awareness, the IC3 aggregates the submitted data and produces an annual report to educate on the trends impacting the public. The quality of the data is directly attributable to the information ingested via the public interface, www.ic3.gov, and the data categorized based on the information provided in the individual complaints. The IC3 staff analyzes the data to identify trends in cyber crimes and how those trends may impact the public in the coming year.

THE IC3 ROLE IN COMBATING CYBER CRIME[1]

What we do



[1] Accessibility description: Image lists IC3's primary functions including partnering with private sector and with local, state, federal, and international agencies: hosting a victim reporting portal at www.ic3.gov; providing a central hub to alert the public to threats; Perform Analysis, Complaint Referrals, and Asset Recovery; and hosting a remote access database for all law enforcement via the FBI's LEEP website.

IC3 CORE FUNCTIONS[2]



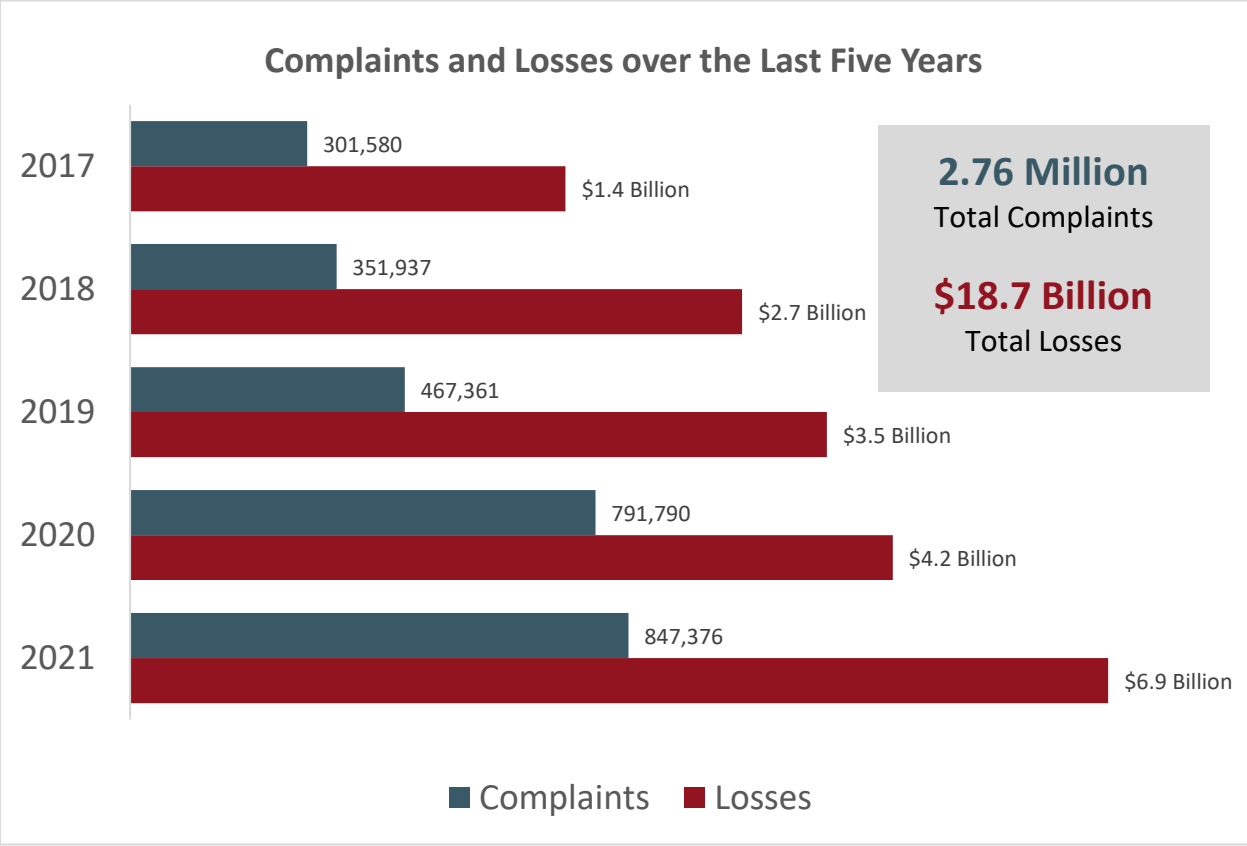

COLLECTION	ANALYSIS	PUBLIC AWARENESS	REFERRALS
The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to Internet crime, as well as any other relevant information necessary to support the complaint.	The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends. In addition, the IC3 quickly alerts financial Institutions to fraudulent transactions which enables the freezing of victim funds.	Public service announcements, industry alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of Internet crimes and the methods used to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.	The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement investigates and determines a crime has been committed, legal action may be brought against the perpetrator.

[2] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

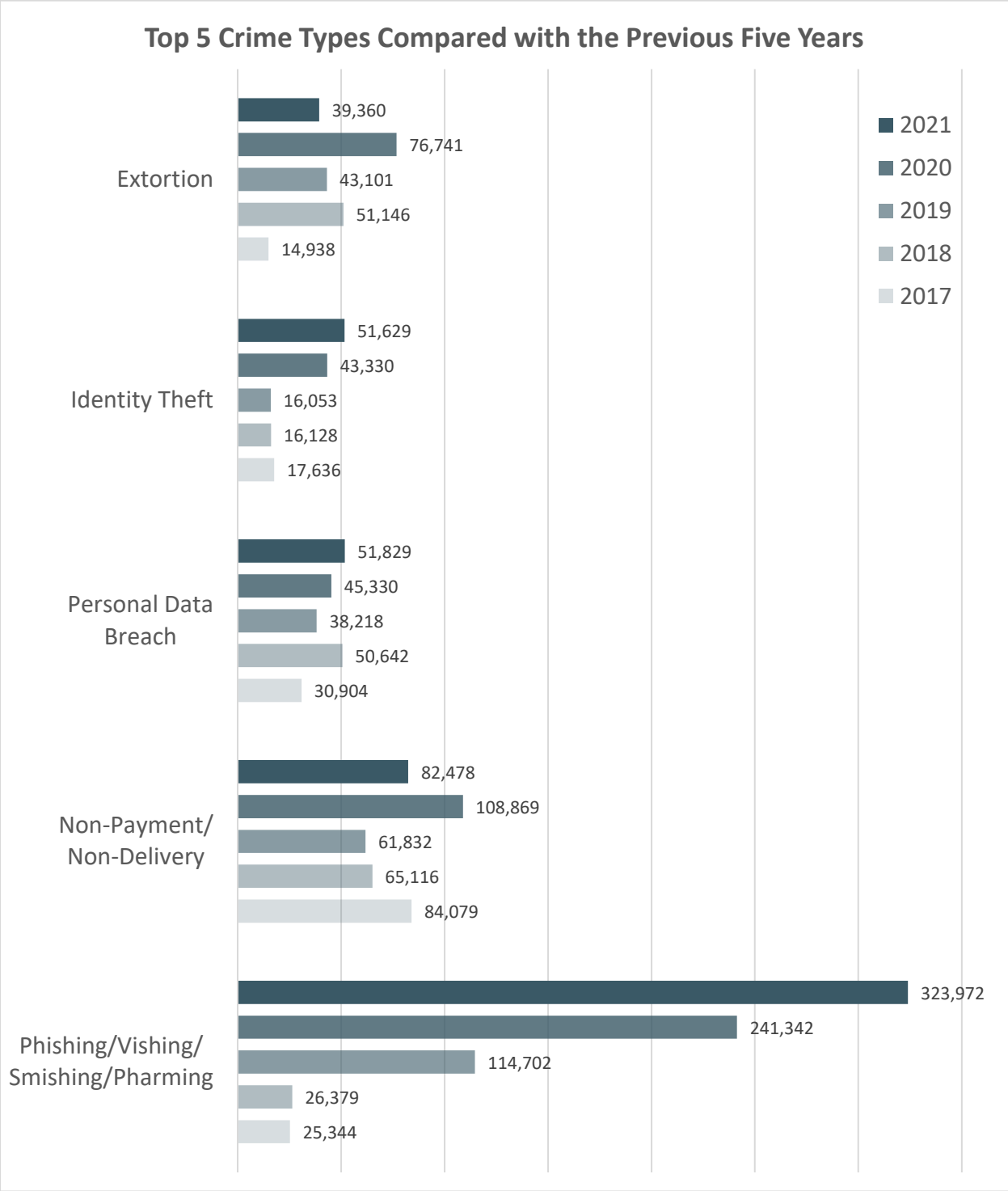
LAST 5 YEARS

Over the last five years, the IC3 has received an average of 552,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[3]



[3] Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2017 to 2021. Over that time, IC3 received a total of 2,760,044 complaints, reporting a loss of $18.7 billion.

TOP 5 CRIME TYPE COMPARSON[4]



[4] Accessibility description: Chart includes a victim loss comparison for the top five reported crime types for the years of 2017 to 2021.

THREAT OVERVIEWS FOR 2021

BUSINESS EMAIL COMPROMISE (BEC)

In 2021, the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses at nearly $2.4 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

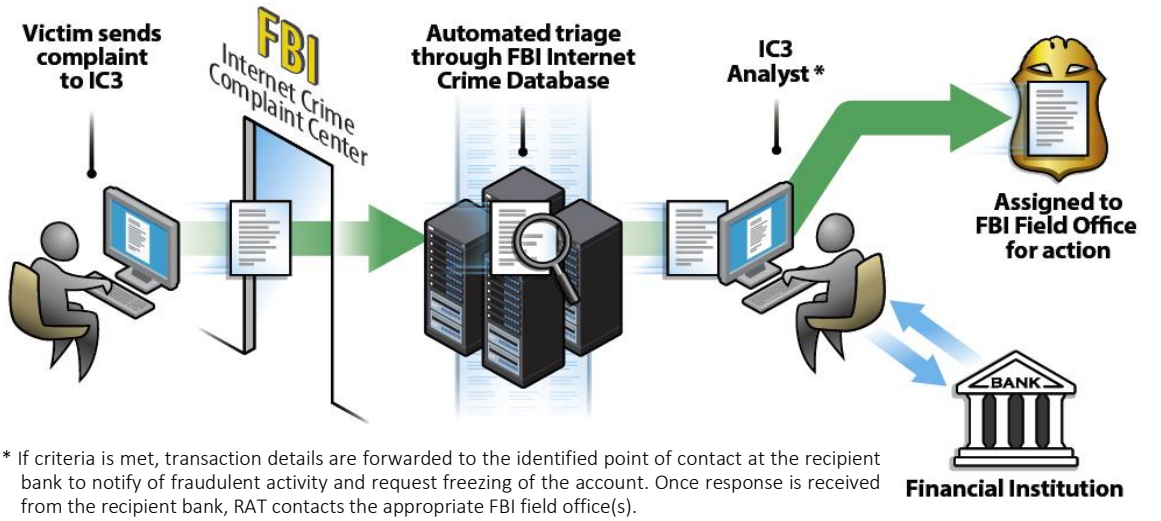
As fraudsters have become more sophisticated and preventative measures have been put in place, the BEC/EAC scheme has continually evolved in kind. The scheme has evolved from simple hacking or spoofing of business and personal email accounts and a request to send wire payments to fraudulent bank accounts. These schemes historically involved compromised vendor emails, requests for W-2 information, targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. Now, fraudsters are using virtual meeting platforms to hack emails and spoof business leaders' credentials to initiate the fraudulent wire transfers. These fraudulent wire transfers are often immediately transferred to cryptocurrency wallets and quickly dispersed, making recovery efforts more difficult.

The COVID-19 pandemic and the restrictions on in-person meetings led to increases in telework or virtual communication practices. These work and communication practices continued into 2021, and the IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions.

IC3 RECOVERY ASSET TEAM

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[5]



* If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

Goals of RAT-Financial Institution Partnership

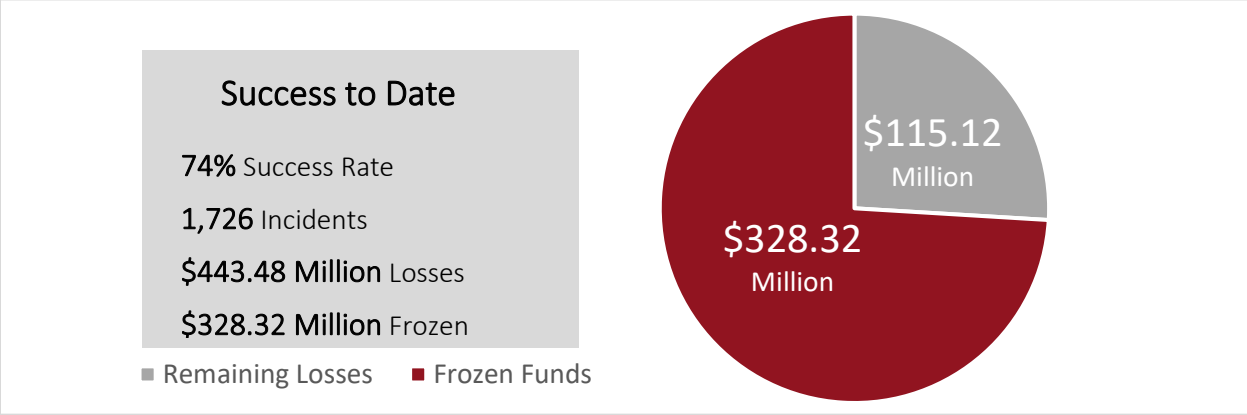
- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, and W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device

[5] Accessibility description: Image shows the different stages of a complaint in the RAT process.

RAT SUCCESSES[6]



The IC3 RAT has proven to be a valuable resource for field offices and victims. The following are three examples of the RAT's successful contributions to investigative and recovery efforts:

Philadelphia

In December 2021, the IC3 received a complaint filed by a victim roadway commission regarding a wire transfer of more than $1.5 million to a fraudulent U.S. domestic bank account. The IC3 RAT quickly notified the recipient financial institution of the fraudulent account by initiating the financial fraud kill chain. Collaboration between the IC3 RAT, the recipient financial institution, and the Philadelphia Field office resulted in learning the subject quickly depleted the wired funds from the original account into two separate accounts held at the same institution. The financial institution was able to quickly identify the second-hop accounts and freeze the funds, making a full recovery possible.

Memphis

In June 2021, the IC3 received a complaint filed by a victim law office regarding a wire transfer of more than $198k to a fraudulent U.S. domestic account. IC3 RAT collaboration with the Memphis Field Office and the recipient financial institution resulted in learning the domestic account was a correspondent account for a fraudulent account in Nigeria. IC3 RAT immediately initiated the international FFKC to FinCEN and LEGAT Abuja, which resulted in freezing the full wired amount. The victim forwarded a note of gratitude for all the work put into their case.

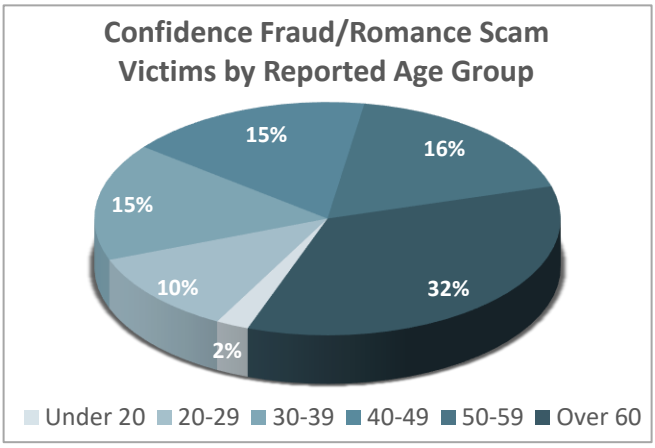
Albany

In October 2021, the IC3 received a complaint filed by a victim of a tech support scam where an unauthorized wire transfer of $53k was sent from their account to a U.S. domestic custodial account held by a cryptocurrency exchange (CE). The IC3 RAT immediately notified the recipient financial institution and collaborated with the CE that held the account. With the knowledge that funds sent to cryptocurrency accounts will be depleted to crypto faster than the usual wire transfer gets depleted, the immediate efforts of initiating the financial fraud kill chain with the CE resulted in the freezing of the funds in the custodial account before they could be depleted to purchase or withdraw cryptocurrency. Further collaboration with the domestic financial institution and the Albany Field Office confirmed the funds were frozen in the account, making a full recovery possible.

[6] Accessibility description: Image shows Success to Date to include 74% Success Rate; 1,726 Incidents; $433.48 Million in Losses; and $328.32. Million Frozen.

CONFIDENCE FRAUD / ROMANCE SCAMS[7]

Confidence Fraud/Romance scams encompass those designed to pull on a victim's "heartstrings." In 2021, the IC3 received reports from 24,299 victims who experienced more than $956 million in losses to Confidence Fraud/Romance scams. This type of fraud accounts for the third highest losses reported by victims.



Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out Romance scams are experts at what they do and will seem genuine, caring, and believable. The scammer's intention is to quickly establish a relationship, endear himself/herself to the victim, gain trust, and eventually ask for money. Scammers may propose marriage and make plans to meet in person, but that will never happen. Scam artists often say they are in the military, or a trades-based industry engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they request money be sent overseas for a medical emergency or unexpected legal fee. Grandparent Scams also fall into this category, where criminals impersonate a panicked loved one, usually a grandchild, nephew, or niece of an elderly person. The loved one claims to be in trouble and needs money immediately.

Con artists are present on most dating and social media sites. In 2021, the IC3 received thousands of complaints from victims of online relationships resulting in sextortion or investment scams.

- Sextortion occurs when someone threatens to distribute your private and sensitive material if their demands are not met. In 2021, the IC3 received more than 18,000 sextortion-related complaints, with losses over $13.6 million. Please see the September 2021 IC3 PSA on Sextortion for more information.[8]
- Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency. In 2021, the IC3 received more than 4,325 complaints, with losses over $429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering" –so named because victims' investment accounts are fattened up before draining, much a like a pig before slaughter. Additional information on "pig butchering" can be found in the September 2021 IC3 PSA I-091621-PSA.[9]

[7] Accessibility description: Chart shows Confidence Fraud/Romance Scam Victim by Reported Age Group. Under 20 2%; 20-29 10%; 30-39 15%; 40-49 15%; 50-59 16%; Over 60 32%

[8] FBI Warns about an Increase in Sextortion Complaints. https://www.ic3.gov/Media/Y2021/PSA210902

[9] Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams.

CRYPTOCURRENCY (VIRTUAL CURRENCY)

In 2021, the IC3 received 34,202 complaints involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. While that number showed a decrease from 2020's victim count (35,229), the loss amount reported in IC3 complaints increased nearly seven-fold, from 2020's reported amount of $246,212,432, to total reported losses in 2021 of more than $1.6 billion.

Initially worth only fractions of pennies on the dollar, several cryptocurrencies have seen their values increase substantially, sometimes exponentially. Once limited to hackers, ransomware groups, and other denizens of the "dark web," cryptocurrency is becoming the preferred payment method for all types of scams – SIM swaps, tech support fraud, employment schemes, romance scams, even some auction fraud. It is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim. The IC3 has noted the following scams particularly using cryptocurrencies.

- Cryptocurrency ATMs: Automated Teller Machines (ATMs) used to purchase cryptocurrency are popping up everywhere. Regulations on the machines are lax and purchases are almost instantaneous and irreversible, making this payment method lucrative to criminals. In 2021, the IC3 received more than 1,500 reports of scams using crypto ATMs, with losses of approximately $28 million. The most common scams reported were Confidence Fraud/Romance, Investment, Employment, and Government Impersonation. Read more about crypto ATM scams in IC3 PSA I-110421-PSA.10
- Cryptocurrency support impersonators: Increasingly, crypto owners are falling victim to scammers impersonating support or security from cryptocurrency exchanges. Owners are alerted of an issue with their crypto wallet and are convinced to either give access to their crypto wallet or transfer the contents of their wallet to another wallet to "safeguard" the contents. Crypto owners are also searching online for support with their cryptocurrencies. Owners contact fake support numbers located online and are convinced to give up login information or control of their crypto accounts.
- Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency. In 2021, the IC3 received more than 4,325 complaints, with losses over $429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering." The scammer's initial contact is typically made via dating apps and other social media sites. The scammer gains the confidence and trust of the victim, and then claims to have knowledge of cryptocurrency investment or trading opportunities that will result in substantial profits.

https://www.ic3.gov/Media/Y2021/PSA210916

[10] The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment https://www.ic3.gov/Media/Y2021/PSA211104

RANSOMWARE[11]

In 2021, the IC3 received 3,729 complaints identified as ransomware with adjusted losses of more than $49.2 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally. Although cyber criminals use a variety of techniques to infect victims with ransomware, phishing emails, Remote Desktop Protocol (RDP) exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents reported to the IC3. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.[12]

Immediate Actions You Can Take Now to Protect Against Ransomware:

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.

Ransomware and Critical Infrastructure Sectors

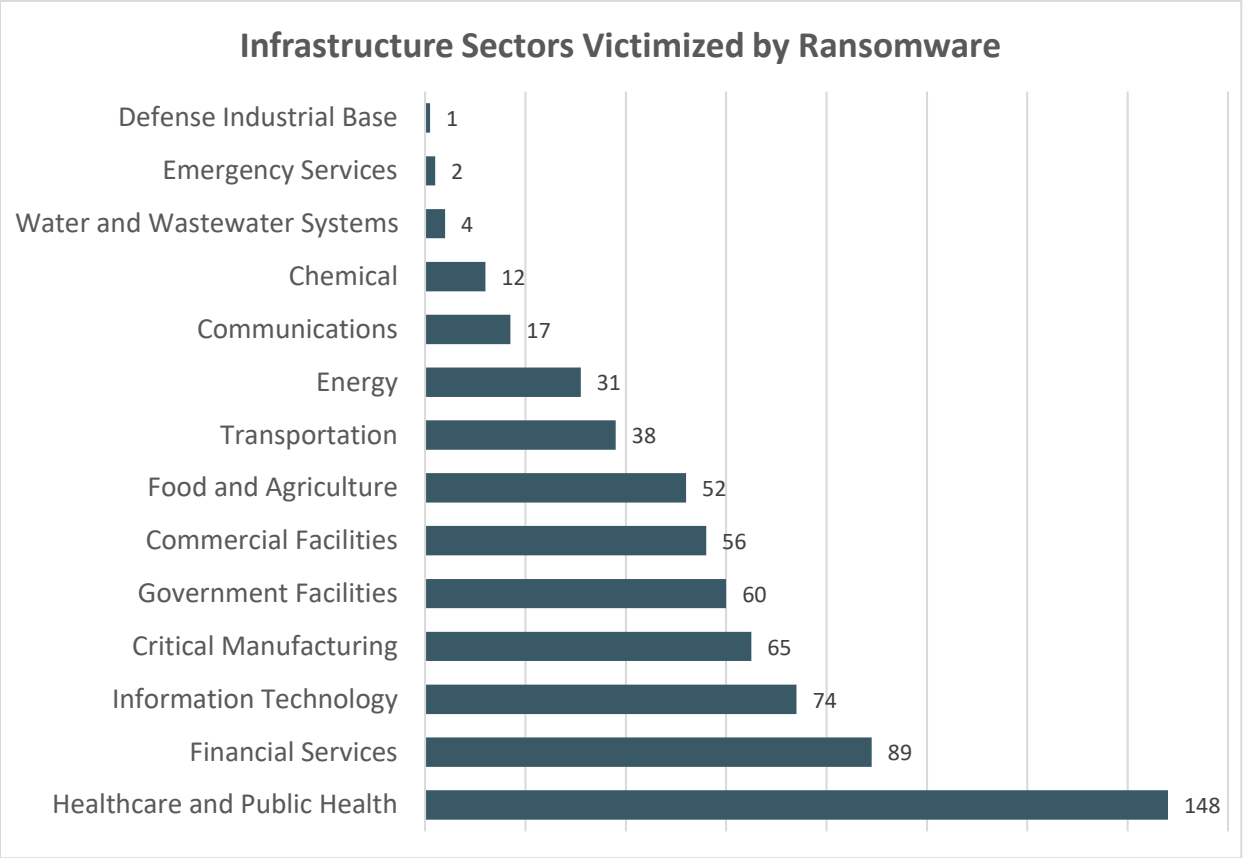
In June 2021, the IC3 began tracking reported ransomware incidents in which the victim was a member of a critical infrastructure sector. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our security, national economy, public health or safety, or any combination thereof.

[11] Accessibility description: Image shows actions you can Take to Protect Against Ransomware: Update your operating system. Implement user training and phishing exercises to raise awareness, secure and monitor Remote Desktop Protocol (DDP) if used, and make an offline backup of our data.

[12] 2021 Trends Show Increased Globalized Threat of Ransomware. https://www.ic3.gov/Media/News/2022/220209.pdf

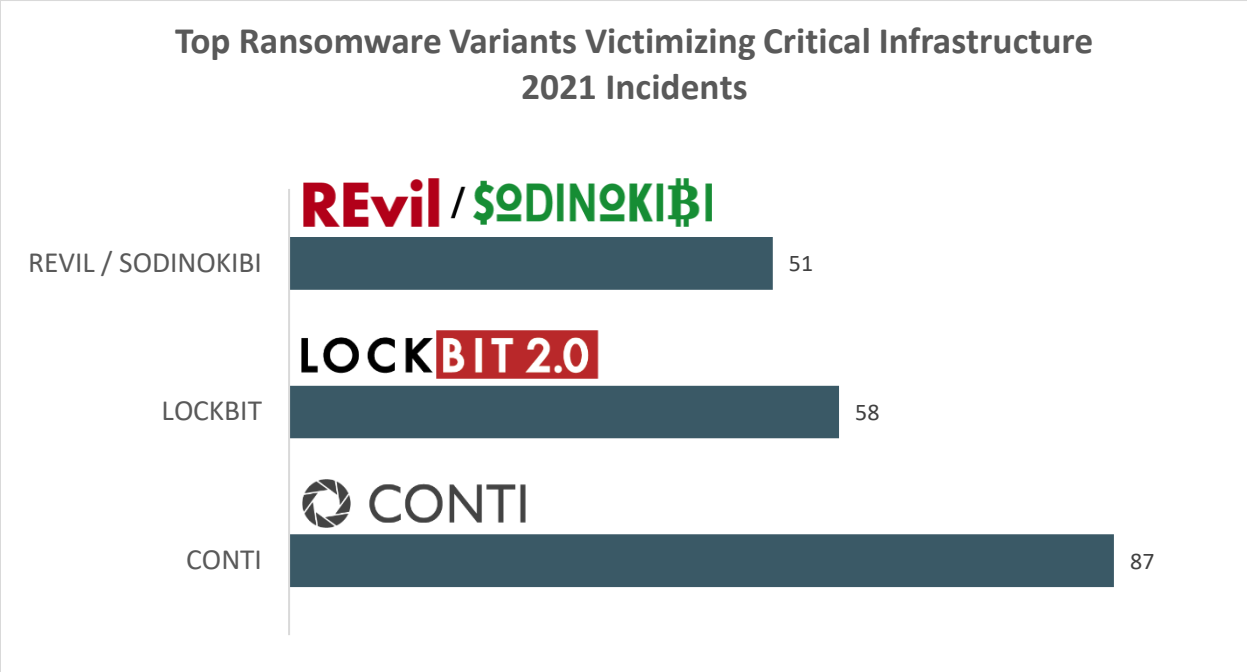
In October 2021, the IC3 posted a Joint Cybersecurity Advisory (CSA) to ic3.gov regarding ongoing cyber threats to U.S. Water and Wastewater Systems. In September 2021, the IC3 posted a Private Industry Notification (PIN) which warned that ransomware attacks targeting the Food and Agriculture sector disrupt operations, cause financial loss, and negatively impact the food supply chain. In May 2021, the IC3 posted an FBI Liaison Alert System (FLASH) report that advised the FBI identified at least 16 CONTI ransomware attacks targeting US Healthcare and First Responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. And in March 2021, the IC3 posted a FLASH warning that FBI reporting indicated an increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom.

The IC3 received 649 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021.[13]



[13] Accessibility description: Chart shows Infrastructure Sectors Victimized by Ransomware. Healthcare and Public Health was highest with 148 followed by Financial Services 89; Information Technology 74; Critical Manufacturing 65; Government Facilities 60; Commercial Facilities 56; Food and Agriculture 52; Transportation 38; Energy 31; Communications 17; Chemical 12; Water and Wastewater Systems 4; Emergency Services 2; Defense Industrial Base 1.

Of the known ransomware variants reported to IC3, the three top variants that victimized a member of a critical infrastructure sector were CONTI, LockBit, and REvil/Sodinokibi.



[14]

According to information submitted to the IC3, CONTI most frequently victimized the Critical Manufacturing, Commercial Facilities, and Food and Agriculture sectors. LockBit most frequently victimized the Government Facilities, Healthcare and Public Health, and Financial Services sectors. REvil/Sodinokibi most frequently victimized the Financial Services, Information Technology, and Healthcare and Public Health sectors.

Of all critical infrastructure sectors reportedly victimized by ransomware in 2021, the Healthcare and Public Health, Financial Services, and Information Technology sectors were the most frequent victims. The IC3 anticipates an increase in critical infrastructure victimization in 2022.

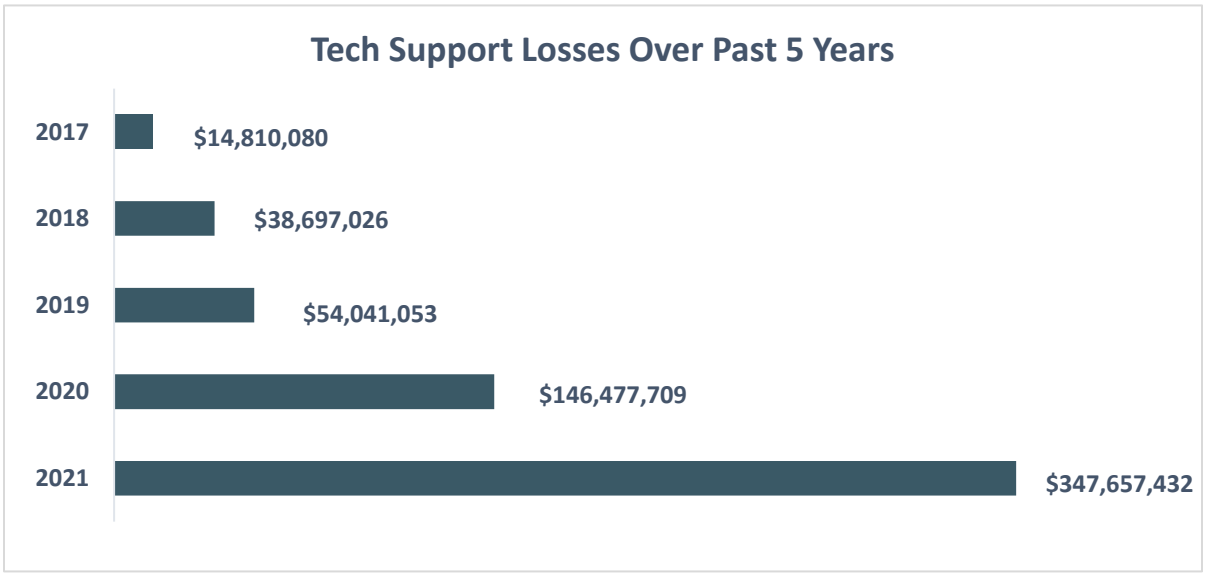
The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and /or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office or the IC3. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

[14] Accessibility description: Chart shows top variants Victimizing Critical Infrastructure 2021 Incidents. REvil/Sodinokibi, Locbit, and CONTI.

TECH SUPPORT FRAUD[15]

Tech Support Fraud involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal.

Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards. In 2021, the IC3 received 23,903 complaints related to Tech Support Fraud from victims in 70 countries. The losses amounted to more than $347 million, which represents a 137 percent increase in losses from 2020. Most victims, almost 60 percent, report to be over 60 years of age, and experience at least 68 percent of the losses (almost $238 million).



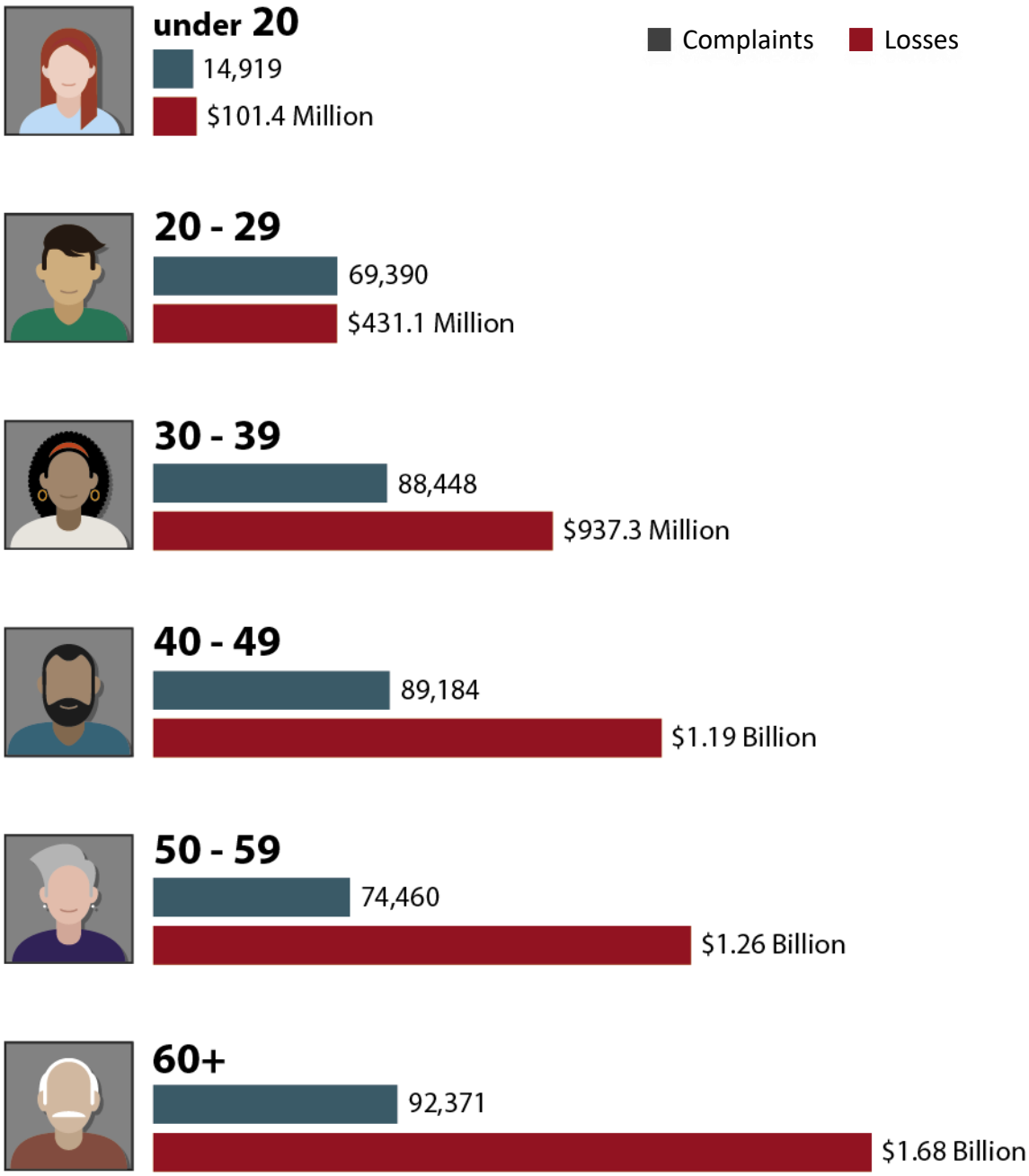
Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues or renew fraudulent software or security subscriptions. However, in 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms, such as financial and banking institutions, utility companies, or virtual currency exchanges.

[15] Accessibility description: Chart shows Tech Support Losses Over Past 5 Years.
2021 $347,657,432; 2020 $146,477,709; 2019 $54,041,053; 2018 $38,697,026; 2017 $14,810,080.

IC3 by the Numbers[16]

[16] Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $6.9 billion were reported in 2021. The total number of complaints received since the year 2000 is over 6.5 million. IC3 has received approximately 552,000 complaints per year on average over the last five years, or more than 2,300 complaints per day.

2021 Victims by Age Group[17]

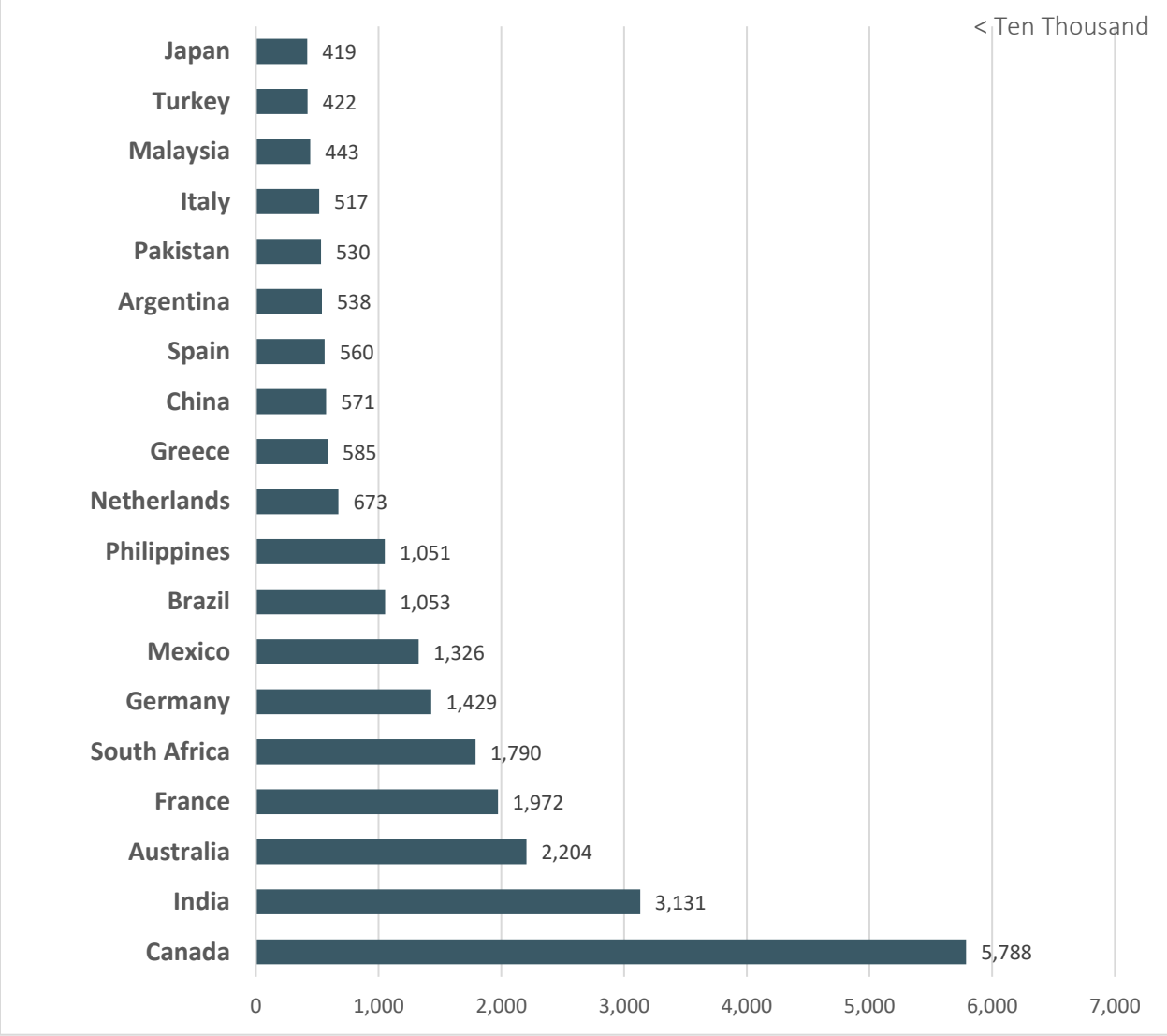


[17] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

Accessibility description: Chart shows number of complaints and Loss for Victims by Age Group. Under 20 14,919 victims $101.4 Million losses; 20-29 69,390 Victims $431.1. Million losses; 30-39 88,448 Victims $937.3 Million losses; 40-49 89,184 victims $1.19 Billion losses; 50-59 74,460 Victims $1.26 Billion losses; 60+ 92,371 Victims $1.68 Billion losses.

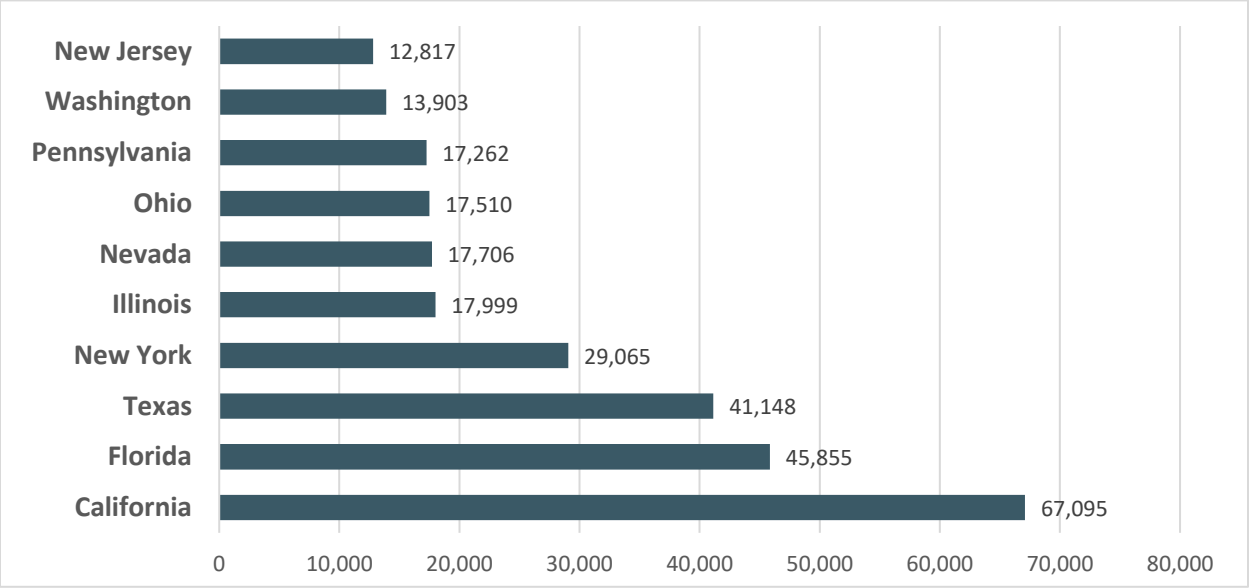
2021 - Top 20 International Victim Countries[18]

Compared to the United States

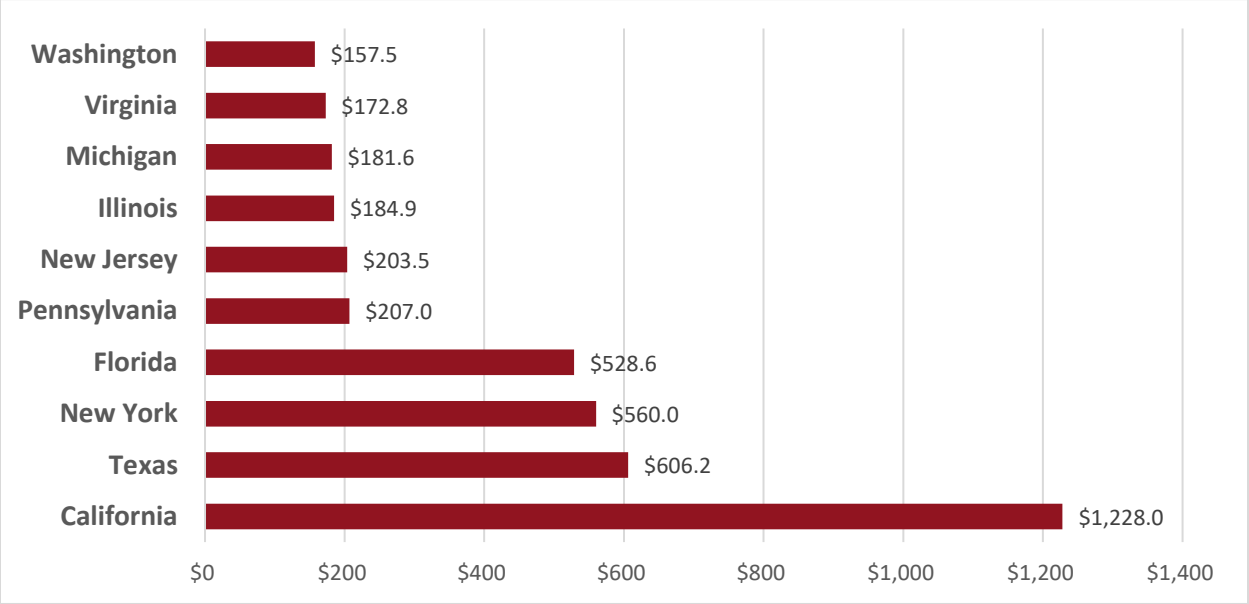


[18] Accessibility description: The charts list the top 20 countries by number of total victims as compared to the United States. The specific number of victims for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding IC3 data.

2021 - Top 10 States by Number of Victims[19]



2021 - Top 10 States by Victim Loss in $ Millions[20]



[19] Accessibility description: Chart depicts the top 10 states based on number of reporting victims are labeled. These include California, Florida, Texas, New York, Illinois, Nevada, Ohio, Pennsylvania, Washington, and New Jersey. Please see Appendix B for more information regarding IC3 data.

[20] Accessibility description: Chart depicts the top 10 states based on reported victim loss are labeled. These include California, Texas, New York, Florida, Pennsylvania, New Jersey, Illinois, Michigan, Virginia, and Washington. Please see Appendix B for more information regarding IC3 data.

2021 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395
*Descriptors**			
Social Media	36,034	Virtual Currency	34,202

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2021 Crime Types continued

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

*Descriptors***			
Social Media	$235,279,057	Virtual Currency	$1,602,647,341

* Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

**These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

Last 3 Year Complaint Count Comparison

By Victim Count			▼ ▲ = Trend from previous Year		
Crime Type	***2021***		*2020*		*2019*
Advanced Fee	**11,034**	▼	13,020	▼	14,607	▼
BEC/EAC	**19,954**	▲	19,369	▼	23,775	▲
Civil Matter	**1,118**	▲	968	▲	908	▲
Confidence Fraud/Romance	**24,299**	▲	23,751	▲	19,473	▲
Corporate Data Breach	**1,287**	▼	2,794	▲	1,795	▼
Credit Card Fraud	**16,750**	▼	17,614	▲	14,378	▼
Crimes Against Children	**2,167**	▼	3,202	▲	1,312	▼
Denial of Service/TDoS	**1,104**	▼	2,018	▲	1,353	▼
Employment	**15,253**	▼	16,879	▲	14,493	▼
Extortion	**39,360**	▼	76,741	▲	43,101	▼
Gambling	**395**	▲	391	▲	262	▲
Government Impersonation	**11,335**	▼	12,827	▼	13,873	▲
Health Care Related	**578**	▼	1,383	▲	657	▲
Identity Theft	**51,629**	▲	43,330	▲	16,053	▼
Investment	**20,561**	▲	8,788	▲	3,999	▲
IPR/Copyright and Counterfeit	**4,270**	▲	4,213	▲	3,892	▲
Lottery/Sweepstakes/Inheritance	**5,991**	▼	8,501	▲	7,767	▲
Malware/Scareware/Virus	**810**	▼	1,423	▼	2,373	▼
Non-Payment/Non-Delivery	**82,478**	▼	108,869	▲	61,832	▼
Other	**12,346**	▲	10,372	▼	10,842	▲
Overpayment	**6,108**	▼	10,988	▼	15,395	▼
Personal Data Breach	**51,829**	▲	45,330	▲	38,218	▼
Phishing/Vishing/Smishing/Pharming	**323,972**	▲	241,342	▲	114,702	▲
Ransomware	**3,729**	▲	2,474	▲	2,047	▲
Real Estate/Rental	**11,578**	▼	13,638	▲	11,677	▲
Re-Shipping	**516**	▼	883	▼	929	▲
Spoofing	**18,522**	▼	28,218	▲	25,789	▲
Tech Support	**23,903**	▲	15,421	▲	13,633	▼
Terrorism/Threats of Violence	**12,346**	▼	20,669	▲	15,563	▼

Last 3 Year Complaint Loss Comparison

By Victim Loss			▼ ▲ = Trend from previous Year		
Crime Type	***2021***		*2020*		*2019*
Advanced Fee	**$98,694,137**	▲	$83,215,405	▼	$100,602,297	▲
BEC/EAC	**$2,395,953,296**	▲	$1,866,642,107	▲	$1,776,549,688	▲
Civil Matter	**$85,049,939**	▲	$24,915,958	▲	$20,242,867	▲
Confidence Fraud/Romance	**$956,039,739**	▲	$600,249,821	▲	$475,014,032	▲
Corporate Data Breach	**$151,568,225**	▲	$128,916,648	▲	$53,398,278	▼
Credit Card Fraud	**$172,998,385**	▲	$129,820,792	▲	$111,491,163	▲
Crimes Against Children	**$198,950**	▼	$660,044	▼	$975,311	▲
Denial of Service/TDoS	**$217,981**	▼	$512,127	▼	$7,598,198	▲
Employment	**$47,231,023**	▼	$62,314,015	▲	$42,618,705	▼
Extortion	**$60,577,741**	▼	$70,935,939	▼	$107,498,956	▲
Gambling	**$1,940,237**	▼	$3,961,508	▲	$1,458,118	▲
Government Impersonation	**$142,643.253**	▲	$109,938,030	▼	$124,292,606	▲
Health Care Related	**$7,042,942**	▼	$29,042,515	▲	$1,128,838	▼
Identity Theft	**$278,267,918**	▲	$219,484,699	▲	$160,305,789	▲
Investment	**$1,455,943,193**	▲	$336,469,000	▲	$222,186,195	▼
IPR/Copyright and Counterfeit	**$16,365,011**	▲	$5,910,617	▼	$10,293,307	▼
Lottery/Sweepstakes/Inheritance	**$71,289,089**	▲	$61,111,319	▲	$48,642,332	▼
Malware/Scareware/Virus	**$5,596,889**	▼	$6,904,054	▲	$2,009,119	▼
Non-Payment/Non-Delivery	**$337,493,071**	▲	$265,011,249	▲	$196,563,497	▲
Other	**$75,837,524**	▼	$101,523,082	▲	$66,223,160	▲
Overpayment	**$33,407,671**	▼	$51,039,922	▼	$55,820,212	▲
Personal Data Breach	**$517,021,289**	▲	$194,473,055	▲	$120,102,501	▼
Phishing/Vishing/Smishing/Pharming	**$44,213,707**	▼	$54,241,075	▼	$57,836,379	▲
Ransomware	**$49,207,908**	▲	$29,157,405	▲	$8,965,847	▲
Real Estate/Rental	**$350,328,166**	▲	$213,196,082	▼	$221,365,911	▲
Re-Shipping	**$631,466**	▼	$3,095,265	▲	$1,772,692	▲
Spoofing	**$82,169,806**	▼	$216,513,728	▼	$300,478,433	▲
Tech Support	**$347,657,432**	▲	$146,477,709	▲	$54,041,053	▲
Terrorism/Threats of Violence	**$4,390,720**	▼	$6,547,449	▼	$19,916,243	▲

Overall State Statistics

Victim per State*					
Rank	*State*	*Victims*	*Rank*	*State*	*Victims*
1	California	67,095	30	Louisiana	4,248
2	Florida	45,855	31	Utah	4,242
3	Texas	41,148	32	Oklahoma	4,156
4	New York	29,065	33	Arkansas	2,745
5	Illinois	17,999	34	Kansas	2,693
6	Nevada	17,706	35	New Mexico	2,644
7	Ohio	17,510	36	Nebraska	2,407
8	Pennsylvania	17,262	37	Mississippi	2,170
9	Washington	13,903	38	West Virginia	2,135
10	New Jersey	12,817	39	Delaware	2,132
11	Arizona	12,375	40	District of Columbia	2,103
12	Virginia	11,785	41	Puerto Rico	1,923
13	Georgia	11,776	42	Idaho	1,882
14	Maryland	11,693	43	Alaska	1,787
15	Indiana	11,399	44	Hawaii	1,615
16	Michigan	10,930	45	New Hampshire	1,487
17	Colorado	10,537	46	Maine	1,402
18	North Carolina	10,363	47	Rhode Island	1,205
19	Missouri	9,692	48	Montana	1,188
20	Massachusetts	9,174	49	South Dakota	951
21	Iowa	8,853	50	Wyoming	735
22	Wisconsin	8,646	51	Vermont	715
23	Kentucky	7,148	52	North Dakota	670
24	Tennessee	7,129	53	Virgin Islands, U.S.	100
25	Oregon	5,954	54	U.S. Minor Outlying Islands	93
26	Minnesota	5,844	55	Guam	64
27	South Carolina	5,426	56	Northern Mariana Islands	29
28	Alabama	5,347	57	American Samoa	25
29	Connecticut	4,524			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Total Victim Losses by State*

Rank	State	Loss	Rank	State	Loss
1	California	$1,227,989,139	30	Louisiana	$38,783,908
2	Texas	$606,179,646	31	Kentucky	$37,953,949
3	New York	$559,965,598	32	Iowa	$33,821,569
4	Florida	$528,573,929	33	Kansas	$26,031,546
5	Pennsylvania	$206,982,032	34	North Dakota	$21,246,355
6	New Jersey	$203,510,341	35	Mississippi	$20,578,948
7	Illinois	$184,860,704	36	District of Columbia	$20,096,921
8	Michigan	$181,622,993	37	Nebraska	$19,743,241
9	Virginia	$172,767,012	38	Hawaii	$18,964,018
10	Washington	$157,454,331	39	South Dakota	$18,131,095
11	Massachusetts	$150,384,982	40	Idaho	$17,682,386
12	Georgia	$143,998,767	41	Arkansas	$15,302,829
13	Ohio	$133,666,156	42	New Hampshire	$15,302,618
14	Colorado	$130,631,286	43	Delaware	$15,041,717
15	Arizona	$124,158,717	44	Puerto Rico	$14,650,062
16	Tennessee	$103,960,100	45	Alaska	$13,070,648
17	Maryland	$99,110,757	46	New Mexico	$12,761,850
18	North Carolina	$91,416,226	47	Rhode Island	$11,191,079
19	Nevada	$83,712,410	48	Wyoming	$10,249,609
20	Minnesota	$82,535,103	49	Montana	$10,107,283
21	Oregon	$75,739,646	50	Vermont	$9,826,787
22	Connecticut	$72,476,672	51	West Virginia	$9,453,607
23	Utah	$65,131,003	52	Maine	$7,261,234
24	Indiana	$60,524,818	53	Guam	$2,168,956
25	Missouri	$53,797,188	54	Virgin Islands, U.S.	$895,946
26	Wisconsin	$51,816,862	55	Northern Mariana Islands	$705,244
27	Oklahoma	$50,196,339	56	U.S. Minor Outlying Islands	$403,844
28	Alabama	$49,522,904	57	American Samoa	$177,533
29	South Carolina	$42,768,322			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Count by Subject per State*					
Rank	*State*	*Subjects*	*Rank*	*State*	*Subjects*
1	California	27,706	30	Nebraska	1,243
2	Texas	13,518	31	Kentucky	1,238
3	Florida	11,527	32	District of Columbia	1,107
4	New York	10,696	33	Utah	1,063
5	Maryland	5,244	34	Delaware	924
6	Ohio	5,182	35	New Mexico	893
7	Pennsylvania	5,168	36	Kansas	876
8	Illinois	4,587	37	West Virginia	863
9	Georgia	4,521	38	Arkansas	831
10	New Jersey	3,913	39	Iowa	723
11	Washington	3,586	40	Mississippi	714
12	Virginia	3,542	41	Montana	681
13	Arizona	3,485	42	Maine	507
14	North Carolina	3,316	43	Idaho	486
15	Nevada	3,308	44	New Hampshire	467
16	Colorado	2,885	45	Hawaii	435
17	Michigan	2,605	46	Alaska	429
18	Tennessee	2,384	47	Puerto Rico	346
19	Massachusetts	2,018	48	Rhode Island	318
20	Indiana	1,976	49	North Dakota	297
21	Oklahoma	1,929	50	Wyoming	251
22	Missouri	1,646	51	South Dakota	216
23	Oregon	1,598	52	Vermont	189
24	Minnesota	1,553	53	U.S. Minor Outlying Islands	34
25	Alabama	1,520	54	Virgin Islands, U.S.	14
26	Connecticut	1,499	55	Guam	11
27	Louisiana	1,398	56	Northern Mariana Islands	7
28	South Carolina	1,358	57	American Samoa	3
29	Wisconsin	1,316			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Subject Earnings per Destination State*

Rank	State	Loss	Rank	State	Loss
1	California	$404,965,496	30	South Carolina	$10,406,812
2	New York	$320,011,292	31	Iowa	$7,960,272
3	Florida	$174,884,203	32	Wyoming	$7,007,308
4	Texas	$168,153,129	33	Idaho	$6,879,088
5	Colorado	$96,949,691	34	Connecticut	$6,586,016
6	Illinois	$82,985,601	35	Kansas	$6,527,306
7	Ohio	$65,567,505	36	New Mexico	$6,441,444
8	Georgia	$62,682,196	37	Kentucky	$6,260,280
9	Washington	$49,643,646	38	Arkansas	$5,511,079
10	New Jersey	$46,773,594	39	Delaware	$5,404,683
11	Nevada	$46,441,562	40	Hawaii	$5,312,553
12	Pennsylvania	$44,661,540	41	Nebraska	$5,156,069
13	Arizona	$44,490,075	42	New Hampshire	$5,082,033
14	Louisiana	$43,427,842	43	Mississippi	$4,245,861
15	North Carolina	$43,281,815	44	Puerto Rico	$4,067,734
16	Virginia	$42,989,608	45	Maine	$3,445,411
17	Maryland	$33,912,104	46	Vermont	$3,357,692
18	Massachusetts	$29,327,619	47	Rhode Island	$3,307,726
19	Michigan	$28,857,054	48	North Dakota	$3,174,006
20	Oklahoma	$19,278,395	49	Montana	$2,946,504
21	Minnesota	$19,039,734	50	Alaska	$2,773,302
22	Tennessee	$18,580,987	51	South Dakota	$2,413,398
23	Utah	$17,137,321	52	West Virginia	$2,269,994
24	Missouri	$16,619,864	53	Northern Mariana Islands	$107,000
25	District of Columbia	$15,656,649	54	U.S. Minor Outlying Islands	$77,350
26	Wisconsin	$14,886,212	55	Virgin Islands, U.S.	$44,453
27	Alabama	$14,639,799	56	Guam	$3,932
28	Indiana	$14,634,699	57	American Samoa	$420
29	Oregon	$10,561,887			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Appendix A: Definitions

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Civil Matter: Civil litigation generally includes all disputes formally submitted to a court, about any subject in which one party is claimed to have committed a wrong but not a crime. In general, this is the legal process most people think of when the word "lawsuit" is used.

Computer Intrusion: Unauthorized access or exceeding authorized access into a protected computer system. A protected computer system is one owned or used by the US Government, a financial institution, or any business. This typically excludes personally owned systems and devices.

Confidence/Romance Fraud: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent's Scheme and any scheme in which the perpetrator preys on the complainant's "heartstrings".

Corporate Data Breach: A data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Credit Card Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH. EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system, or a Telephony Denial of Service (TDoS) floods a voice service with multiple requests, slowing down or interrupting service.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Health Care Related: A scheme attempting to defraud private or government health care programs which usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The illegal theft and use of others' ideas, inventions, and creative expressions – what's called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

Identity Theft: Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (Account Takeover) a fraudster obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer the victims large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

Lottery/Sweepstakes/Inheritance: An Individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

Malware/Scareware/Virus: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Phishing/Vishing/Smishing/Pharming: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Re-shipping: Individuals receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

Social Media: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

Tech Support: Subject posing as technical or customer support/service.

Terrorism/Threats of Violence: Terrorism is violent acts intended to create fear that are perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.

Appendix B: Additional Information about IC3 Data

- Each complaint is reviewed by an IC3 analyst. The analyst categorizes the complaint according to the crime type(s) that are appropriate. Additionally, the analyst will adjust the loss amount if the complaint data does not support the loss amount reported.
- One complaint may have multiple crime types.
- Some complainants may have filed more than once, creating a possible duplicate complaint.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.
- Victim is identified as the individual filing a complaint.
- Subject is identified as the individual perpetrating the scam as reported by the victim.
- "Count by Subject per state" is the number of subjects per state, as reported by victims.
- "Subject earnings per Destination State" is the amount swindled by the subject, as reported by the victim, per state.

Core Cybersecurity Threats and Effective Controls for Small Firms

Sound cybersecurity practices are a key focus of member firms and FINRA, especially given the evolving nature, increasing frequency and mounting sophistication of cybersecurity attacks —as well as the potential for harm to investors, member firms and the markets. Cybersecurity is one of the principal operational risks facing broker-dealers, and FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

The following list updates and expands on the Core Cybersecurity Controls for Small Firms provided in the Report on Selected Cybersecurity Practices – 2018 (2018 Report) by identifying key cybersecurity risks currently faced by small firms and helping them enhance their customer information protection, and cybersecurity written supervisory programs (WSPs) and related controls, including:

- Highlighting the most common and recent categories of cybersecurity threats faced by small firms, including questions to assist firms with addressing such threats;
- Providing a summary of effective core controls small firms should consider, as well as relevant questions for consideration to evaluate their current cybersecurity programs; and
- Including appendices with a glossary of relevant terms and additional resources.

Regulatory Obligations

Rule 30 of the U.S. Securities and Exchange Commission's (SEC) Regulation S-P requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members' operations. Cybersecurity remains one of the principal operational risks facing broker-dealers and FINRA expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms' change- and problem-management practices, or issues related to an increase in trading volumes, can expose firms to operational failures that may compromise their ability to comply with a range of rules and regulations, including FINRA Rules 4370, 3110 (Supervision) and 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

Contact Us

Questions related to this tool or other Cybersecurity topics can be sent to Member Supervision's CyberTech team at cybertech@finra.org.

COMMON CYBERSECURITY THREATS FOR SMALL FIRMS

1 IMPOSTER WEBSITES

☐ Reviewed ✔

Small firms frequently report to FINRA cybersecurity risks related to imposter websites,[1] where fraudsters use registered representatives' names, firm information or both to establish websites that market investment services and products. These sites attempt to steal both personal information and investor funds by leading site visitors to believe that they are investing in a legitimate business or legitimate products. Firms may want to consider asking the following questions, where applicable, with respect to how they monitor for, and address, imposter websites:

- How does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives?
  - Has your firm registered website name variations, including common misspellings or visually similar character substitutions?
  - Does your firm use social media or website monitoring services to watch for imposter websites?
- How does your firm address imposter websites once they are identified? If your firm becomes aware of an imposter website, has it addressed the concern with the hosting provider and domain name registrar, sought assistance from specialists and informed regulators and customers?[2]

2 PHISHING

☐ Reviewed ✔

Phishing is one of the most common cybersecurity threats affecting firms[3] – it may take a variety of forms, but all phishing attempts try to convince the recipient to provide information or take action. The fraudsters typically try to disguise themselves as a trustworthy entity or individual via email, instant message, phone call or other communication, where they request personally identifiable information (PII) (such as Social Security numbers, usernames or passwords), direct the recipient to click on a malicious link, open an infected attachment or application, or attempt to initiate a fraudulent wire transfer or transaction. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate phishing attempts:

- Do your firm's policies and procedures address phishing by, for example:
  - identifying phishing emails;

---

[1] *See* FINRA *Information Notice - 4/29/19* (Imposter Websites Impacting Member Firms) and *Regulatory Notice 20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).

[2] *See Information Notice - 4/29/19* (Imposter Websites Impacting Member Firms).

[3] See, *e.g.*, *Regulatory Notice 12-05* (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts); *Regulatory Notice 21-30* (FINRA Alerts Firms to a Phishing Email Campaign Using Multiple Imposter FINRA Domain Names); *Regulatory Notice 21-22* (FINRA Alerts Firms to Phishing Email From "FINRA Support" From the Domain Name "westour.org"); *Regulatory Notice 21-20* (FINRA Alerts Firms to Phishing Email Using "gateway-finra.org" Domain Name); *Regulatory Notice 20-27* (FINRA Alerts Firms to Use of Fake FINRA Domain Name); *Regulatory Notice 21-08* (FINRA Alerts Firms to Phishing Email Using "finra-online.com" Domain Name); and *Regulatory Notice 20-12* (FINRA Warns of Fraudulent Phishing Emails Purporting to be from FINRA).

- clarifying that staff should not click on any links or open any attachments in phishing emails;
- requiring deletion of phishing emails;
- developing a process to securely notify Information Technology (IT) administrators or compliance staff of phishing attempts;
- confirming requests for wire transfers of a certain type, or above a certain threshold, with the customer via telephone or in person; and
- ensuring proper resolution and remediation after phishing attacks?

- Has your firm implemented email scanning and filtering to monitor and block phishing and spam communication?
- Does your firm regularly conduct phishing email campaign simulations to evaluate employee understanding and compliance of its phishing policies and procedures?

3 CUSTOMER AND FIRM EMPLOYEE ACCOUNT TAKEOVERS (ATOs)

☐ Reviewed ✔

Customer and firm employee email ATOs have become an increasingly problematic area for firms. ATOs can occur either at customer or firm personnel accounts and usually begin with their email account being compromised. Fraudsters can gain unauthorized access to customer and firm employee email accounts through data breaches, phishing emails or websites that trick users into clicking on malicious links allowing them to execute unauthorized transactions in financial accounts, firm systems, bank accounts and credit cards. Fraudsters can also monitor those email accounts, view or download the information contained within messages and even add new email rules to hide legitimate correspondence. In addition, some fraudsters use synthetic identities to establish accounts to divert specific types of payments, such as congressional stimulus funds or unemployment payments, or to engage in automated clearing house (ACH) or wire fraud. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate ATOs impacting broker-dealers or affiliates, as well as those impacting customer accounts:

For ATOs impacting broker-dealers or affiliates:

- Does your firm require multi-factor authentication (MFA) for external access to email systems, vendor portals or other systems that may contain confidential information?
- Does your firm have automated monitoring, alerting or both for suspicious logins?
- For high-risk transactions (*e.g.*, third-party money movements) does your firm have a process to validate these requests?

For ATOs impacting customer accounts:

- What documentary identification (*e.g.*, drivers' licenses, passports) and non-documentary methods (*e.g.*, contacting the customer, obtaining a customer's financial statement) does your firm use to verify customers' identities when establishing online accounts?
- What approaches does your firm take to verify customer identities when they access their online accounts (*e.g.*, MFA, adaptive authentication) and initiate transfer requests (*e.g.*, reviewing the Internet Protocol (IP) address of requests made online or through a mobile device for consistency with past legitimate transactions)?
- How does your firm proactively address potential or reported customer ATOs? What practices has your firm implemented to restore customer account access in a secure and timely manner?
- Do your firm's Suspicious Activity Reporting (SAR) procedures address ACH or wire fraud? Does your firm collaborate with its clearing firm to allocate responsibilities for handling ACH or wire transactions?

- Does your firm educate its customers on account security? Does your firm provide resources to its customers to help them identify potential security threats (*e.g.*, email or SMS text messages for certain types of account activity)?

4 MALWARE

☐ Reviewed ✔

Malware is a catch-all term for multiple types of malicious software (*e.g.*, viruses, spyware, worms) designed to cause damage to a stand-alone or networked computer. Malware most often originates from phishing emails where a user clicked on a link or opened an attachment. Once activated, it can mine a firm's system for PII and sensitive data; erase data; steal credentials; alter, corrupt or delete a firm's files and data; take over an email account; and even hijack device operations or computer-controlled hardware. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to malware attacks:

- How does your firm train employees to recognize and report cyberattacks involving malware?
- What preventative measures does your firm take (*e.g.*, endpoint malware protection) to defend against malware?
- How does your firm monitor for indications of malware on your firm's systems?
- How does your firm's incident response plan address malware infections?
- How does your firm incorporate threat intelligence regarding newly-identified instances of viruses or other types of malware into its IT infrastructure?

5 RANSOMWARE

☐ Reviewed ✔

Ransomware attacks are an increasingly common threat for small firms, and can quickly cripple their business operations, as well as expose firms to risks of data exfiltration and publication. This type of highly sophisticated malware commonly encrypts a firm's files, databases or applications to prevent firm employees from accessing them until a ransom demand is paid to the fraudster. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to ransomware attacks:

- Has the firm evaluated capabilities to detect and block sophisticated attacks, using tools such as endpoint detection and response (EDR), a host-based intrusion detection system (HIDS) and a host-based intrusion prevention system (HIPS)?
- Does your firm keep offline backups of systems and data? Are recovery capabilities tested on a regular basis?
- Does your firm's incident response plan include a scenario for potential ransomware attacks? If so, does your plan address factors such as:
    - making cybersecurity insurance claims;
    - engaging cybersecurity experts to conduct forensics investigations and to assist in recovery efforts;
    - assessing and mitigating the impact of these attacks; and
    - notifying affected parties (*e.g.*, customers, employees, regulators) as required by data breach notification laws applicable to your firm?

6 DATA BREACHES

☐ Reviewed ✔

Data breaches are another serious threat to small firms that can expose sensitive customer or firm information to an unauthorized party and may result in customer harm, reputational damage to a firm or both. If a data breach has been identified, firms must determine whether sensitive data is impacted and the various data privacy concerns, including the required notifications to regulators and customers because of the breach. Firms may want to consider asking the following questions, where applicable, with respect to how they investigate, monitor for, prevent and respond to data breaches:

- How does your firm investigate data breaches?
- Do your firm's contracts with vendors define "breach" – in the context of data and systems the vendor is involved with – as well as address the manner and timing of the vendor's notification to the data owner of a security breach, and the requirements as to who is responsible for notifying customers along with any related costs?
- Has your firm established a formal data loss prevention (DLP) program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (*e.g.*, appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- Does your firm have a process to notify regulators and customers about data breaches?

EFFECTIVE CORE CYBERSECURITY CONTROLS FOR SMALL FIRMS

The following are some of the effective cybersecurity controls observed at small firms they should consider, as well as relevant questions for consideration they could use to evaluate their current cybersecurity programs. In addition to the following controls, FINRA has provided a number of cybersecurity resources for small firms that provide additional information on these and other controls, including the Cybersecurity and Technology Governance section of the 2022 Report on FINRA's Examination and Risk Monitoring Program, the 2015 FINRA Report on Cybersecurity Practices, the 2018 Report, the Small Firm Cybersecurity Checklist and the Cybersecurity Topic Page.

1 GOVERNANCE AND RISK MANAGEMENT

☐ Reviewed ✔

A firm's governance framework should enable it to become aware of relevant cybersecurity risks, estimate their severity and decide how to manage (*i.e.*, to accept, mitigate, transfer or avoid) each risk. Because there is no one-size-fits-all approach to cybersecurity, any governance framework should also include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available. Firms may want to consider asking the following questions, where applicable, with respect to how they implement and maintain their cybersecurity-related governance framework and risk management policies:

- Does your firm use well-established, relevant industry frameworks[4] and standards to implement and maintain its cybersecurity program, including policies that are appropriate for the firm's size, business model and cybersecurity threat environment, particularly in areas such as:
    - data protection;
    - vendor management;
    - asset management;
    - risk management;
    - incident management and responses; and
    - branch controls?
- Has your firm conducted program risk assessments that include prioritization, tracking and follow up for all required implementation items for your cybersecurity program (*e.g.*, leveraging FINRA's Small Firm Cybersecurity Checklist)?
- Does your firm have a Chief Information Security Officer (CISO) or otherwise designate a single staff person to lead the firm's overall cybersecurity program, such as your firm's Chief Compliance Officer (CCO), IT leader or another member of senior management with sufficient knowledge of cybersecurity risks and controls?
- Has your firm established conducted documented meetings or assigned accountability for action items discussed in meetings?
- Does your firm's cybersecurity leadership engage your firm's executive management in all risk-based decisions aligned to the overall organization's goals and corresponding risks?

2 VENDOR MANAGEMENT

☐ Reviewed ✔

Member firms – including small firms – have increasingly leveraged vendors to implement systems and perform key functions (*e.g.*, customer relationship management systems, clearing arrangements, account statement generation) and often contract with Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs), respectively, to oversee their IT infrastructure and cybersecurity programs. Relying on vendors may help small firms reduce operating costs, improve efficiency and concentrate on core broker-dealer operations. However, due to the recent increase in the number and sophistication of cyberattacks during the COVID-19 pandemic, FINRA reminds firms of their obligations to oversee, monitor and supervise cybersecurity programs and controls provided by third-party vendors.[5] Firms may want to consider asking the following questions, where applicable, with respect to how they select, conduct due diligence on and document relationships with cybersecurity vendors:

- Does your firm have a process for its decision-making on outsourcing, including the selection of cybersecurity vendors? Does this process engage key internal stakeholders and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?

[4] Examples of these relevant frameworks include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Center For Internet Security (CIS): Critical Security Controls and Federal Trade Commission (FTC): Cybersecurity for Small Business.

[5] Firms can find relevant guidance in *Regulatory Notice 21-29* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) and the Cybersecurity and Infrastructure Security Agency's (CISA) Risk Considerations for Managed Service Provider Customers.

- Does your firm implement risk-based due diligence on vendors' cybersecurity practices critical to managing risks present in a firm's environment, including the ability to protect sensitive firm and customer non-public information?[6]
- Does your firm document relationships with vendors in written contracts that clearly define all parties' roles and responsibilities related to cybersecurity, such as evidencing compliance with federal and state securities laws and regulations, and FINRA rules; protection of sensitive firm and customer information; and notifications to your firm of cybersecurity events, and the vendor's efforts to remediate those events?
- Does your firm conduct independent, risk-based reviews to determine if vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the vendors' response to such events?

3 ACCESS CONTROLS

☐ Reviewed ✔

Small firms may face a unique set of challenges related to access controls due to their reliance on third party providers such as clearing firms, client management systems and IT services, including cloud-based providers. Third party providers may be especially appealing to small firms with fewer internal resources. However, this may result in vendor employees wearing multiple hats and having more access to systems and data than needed to fulfill their functions. Firms may want to consider asking the following questions, where applicable, with respect to how they grant access to firm and customer data, establish and enforce access and authentication controls, and detect and resolve anomalies within privileged accounts:

- Does your firm maintain WSPs in crucial areas, such as identity governance, onboarding, offboarding and periodic access reviews?
- Does your firm follow the Principle of Least Privilege when granting entitlements?
- Has your firm established identity and access management protocols for registered representatives and other staff, including managing the granting, maintenance and termination of access to firm and customer data?
- Does your firm enforce complex password standards and authentication controls (*e.g.*, MFA, password reuse, password change intervals, minimum length, character types and length, change frequency)?
- Has your firm implemented enhanced procedures (*e.g.*, monitoring, alerts) to detect anomalies in privileged accounts, such as a privileged user assigning herself or himself extra access rights, performing unauthorized work during off-hours or logging in from different geographic locations concurrently? Do your firm's procedures also account for logging the occurrence of anomalies, and how firms resolve them?
- Has your firm established physical access controls across office locations or access controls for remote work?

[6] *See id.*, at Section II for steps small firms can take when performing due diligence (*e.g.*, talking to industry peers; collecting and reviewing American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 reports, if available).

4 DATA PROTECTION

☐ Reviewed ✔

Data protection is one of the most important facets of a small firm's cybersecurity program. Small firms have information assets (*e.g.*, employee and customer information, firm sensitive data) that, if inadequately protected, could result in harm to the customers, individuals or the firm's reputation. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method; they can also prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. Firms may want to consider asking the following questions, where applicable, with respect to how they establish a formal DLP program, and applicable WSPs and controls, to protect sensitive customer and firm data:

- Has your firm identified where sensitive information is stored and transmitted?
- Has your firm established a formal DLP program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (*e.g.*, appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- How does your firm implement encryption for confidential data at rest or in transit?
- Does your firm prohibit the storage of sensitive customer or firm data in unapproved or prohibited locations (*e.g.*, a file server, cloud provider or thumb drive transmitted without encryption)?
- What is your firm's policy regarding storing sensitive data on removable media or personal devices, as well its retention and secure disposal?
- How does the firm ensure that third parties involved in maintaining or storing sensitive information have reasonable data protection safeguards and cybersecurity controls? Are third parties' data protection responsibilities mutually agreed upon?

5 TECHNICAL CONTROLS

☐ Reviewed ✔

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred. However, small firms may not have sufficient resources to ensure adequate safeguards around all possible attack surfaces, especially in today's hyperconnected world and ever-changing risk landscape. Small firms can use a cybersecurity risk assessment to determine which threats are most significant for each branch and then identify and implement appropriate technical and other controls to mitigate those threats. Firms may want to consider asking the following questions, where applicable, with respect to how they assess the cybersecurity risks at each of their branches, and implement appropriate controls to mitigate those risks:

- Does your firm understand where its cybersecurity risks lie, including its technology hardware and software asset inventories?
- Do your firm's staff in cybersecurity positions have the technical skillsets to properly configure tools and applications?
- How does your firm verify that its critical and sensitive systems have adequate protection and detection controls?

- What cyber hygiene controls (*e.g.*, endpoint, MFA, email encryption, DLP) does your firm implement?
- Does your firm enable automatic patching and updating features of operating systems and other software to help maintain the latest security controls?
- Does your firm prohibit the sharing of passwords among firm staff?

6 BRANCH CONTROLS

☐ Reviewed ✔

Overseeing IT and cybersecurity controls across a branch network can be especially challenging for small firms, including firms with independent contractor models. A branch network may present challenges for a firm' seeking to implement a consistent firm-wide cybersecurity program. Some firms may experience increased challenges if their branches may, for example, purchase their own assets, allow Bring Your Own Devices (BYOD), use nonapproved vendors, or not follow their firm's software patching and upgrade protocols. As a result, firms should evaluate whether they need to enhance their branch-focused cybersecurity measures to maintain robust cybersecurity controls and protect customer information across their organizations. Firms may want to consider asking the following questions, where applicable, with respect to how they supervise their branch network:

- What policies and procedures regarding cybersecurity and annual attestations of compliance have been established for each of your firm's branch offices?
- What cybersecurity training required when onboarding new branch locations or new staff?
- How does your firm confirm each of its branches meet firm cybersecurity standards, use firm-recommended vendors or other vendors meeting firm standards? What consequences does the firm impose (such as fines, sanctions or termination) on branches and registered representatives engaging in repeat violations of firm standards?
- What compliance and technology support does your firm provide its branches and registered representatives implementing firm cybersecurity protocols?
- What are your firm's configuration requirements for physical security and technical controls at each branch (*e.g.*, hard drive encryption, virus protection, MFA, patching and removable storage media)? How does your firm monitor these controls? Are these controls reviewed during branch inspections or monitored through the use of automated tools?
- How does your firm confirm that each of its branches use only secure, encrypted wireless settings for office and home networks?
- If a review of one of your firm's branches identifies material deficiencies or reported material cybersecurity incidents, how does it confirm that the branch has implemented corrective action?

7 INCIDENT MANAGEMENT AND RESPONSE

☐ Reviewed ✔

Incident response plans can help small firms address cybersecurity threats from bad actors. Developing and implementing an incident response plan may require contracting with an outside specialist but doing so may aid firms in responding to threats rapidly and effectively. Cybersecurity-related incidents may also require firms to file a SAR with the Financial Crimes Enforcement Network (FinCEN), as well as notify the FBI through their Internet Crime and Complaint Center (IC3) and the Federal Trade Commission (FTC). Firms may want to consider asking the following questions, where applicable, with respect to how they develop and implement their incident response plans:

- Does your firm maintain an incident response plan to identify and escalate incidents in a timely manner?
- Does your firm have the data inventory, assets inventory, and controls to assess the impact of incidents?
- Does your firm have capabilities for incident detection, containment, mitigation, and recovery either from internal resources or with help from a third party? If from a third party, have you established the relationship with defined service level agreements (SLAs)?
- What communication plans does your firm prepare for outreach to relevant stakeholders (*e.g.*, customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies) if an incident occurs?
- Do your firm's post incident reviews aim for improvements, including evaluating the incident management process, policy updates and control effectiveness?
- Have you tested the incident response plan within the past year?[7]
- Has the firm investigated or considered cybersecurity insurance?

8 TRAINING

☐ Reviewed ✔

A well-trained staff is an important defense against cyberattacks. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks, so effective training helps reduce the likelihood that such attacks will be successful. Firms may want to consider asking the following questions, where applicable, with respect to how they design internal cybersecurity training, what personnel they require to take the training and how frequently they conduct and evaluate the training:

- How frequently and consistently does your firm conduct cybersecurity training? Are all individuals or third parties at the firm included in cybersecurity training? How often does your firm conduct training?
- Is your firm's training tailored to the cybersecurity risks applicable to its business? Does the training encompass a variety of methods (*e.g.,* reminder emails, online formal training, discussions of actual events)?
- Does your firm's training include simulated phishing exercises to validate employee understanding and track participation metrics? What consequences do employees face if they don't pass (*e.g.*, mandatory retraining)?
- How does your firm ensure that IT personnel are trained and kept abreast of the cybersecurity threat landscape to continuously assess the effectiveness of technical controls?
- Has your firm considered incorporating a formal or informal evaluation of the staff's understanding of and compliance with firm cybersecurity requirements into its training program?

[7] For additional guidance, *see* the NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.

Appendix 1 – Glossary

Account Takeover (ATO) – a form of identity theft where a fraudster uses stolen login credentials to gain unauthorized access to another individual's online account.

Bring Your Own Device (BYOD) – a policy that allows firm employees to use their personal devices (*e.g.*, computers, smartphones, tablets) to access the firm's network.

Data Loss Prevention (DLP) – a set of technologies, products, and techniques that prevent end users from moving key information outside the firm's network.

Endpoint Detection and Response (EDR) Tools – integrated endpoint security solutions that combine real-time continuous monitoring and collection of endpoint data with rules-based automated responses and analysis capabilities.

Host-Based Intrusion Detection System (HIDS) and Host-Based Intrusion Prevention System (HIPS) – software that protects computer systems from malware and other unwanted, negative activity utilizing advanced behavioral analysis and the detection capabilities of network filtering to monitor running processes, files, and registry keys within an operation system.

Multi-Factor Authentication (MFA) – an authentication method that requires a user to provide two or more verification factors to gain access. Verification factors include something you know (password), something you have (token), something you are (biometrics), or somewhere you are (Geolocation).

Managed Service Providers (MSP) – third-party companies that remotely manage a customer's information technology (IT) infrastructure and end-user systems.

Managed Security Service Providers (MSSP) – providers of outsourced monitoring and management of security devices and systems, which may include security hardening, security monitoring, incident response and forensics services.

Personally Identifiable Information (PII) – data or information that allows the identity of an individual to be directly or indirectly inferred.

Principle of Least Privilege – the information security practice that any user, program or process should have the bare minimum privileges necessary to perform a function.

Service Level Agreement (SLA) – a contract between a service provider and a customer that identifies the types of provided services, and the standards the customer expects the service provider to meet.

Appendix 2 – Additional Resources

FINRA

Guidance

- *Regulatory Notice* *21-29* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
- *Regulatory Notice* *21-18* (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)
- *Regulatory Notice* *20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
- *Regulatory Notice* *20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- *Regulatory Notice* *12-05* (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts)

Reports

- 2022 Report on FINRA's Examination and Risk Monitoring Program – Cybersecurity and Technology Governance
- Report on Selected Cybersecurity Practices – 2018
- Report on Cybersecurity Practices – 2015

Compliance Tools and Other Resources

- Compliance Vendor Directory
- Cybersecurity Topic Page
- Firm Checklist for Compromised Accounts
- Small Firm Cybersecurity Checklist

Non-FINRA Resources

- CIS: Critical Security Controls
- FBI: Internet Crime and Complaint Center (IC3)
- FinCEN: SAR Filing Instructions
- FTC: Cybersecurity for Small Business
- FTC: ReportFraud.ftc.gov
- NIST: Cybersecurity Framework
- NIST: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

FINRA Compliance Tool Disclaimer

This optional tool is provided to assist member firms in fulfilling their regulatory obligations. This tool is provided as a starting point, and you must tailor this tool to reflect the size and needs of your firm. Using this tool does not guarantee compliance with or create any safe harbor with respect to FINRA rules, the federal securities laws or state laws, or other applicable federal or state regulatory requirements. This tool does not create any new legal or regulatory obligations for firms or other entities.

Updates – This tool was last updated on May 5, 2022. This tool does not reflect any regulatory changes since that date. FINRA periodically reviews and update these tools. FINRA reminds member firms to stay apprised of new or amended laws, rules and regulations, and update their WSPs and compliance programs on an ongoing basis.

Member firms seeking additional guidance on certain regulatory obligations should review the relevant FINRA Topic Pages, including the Cybersecurity Topic Page.

Staff Contact(s) – FINRA's Office of General Counsel (OGC) staff provides broker-dealers, attorneys, registered representatives, investors and other interested parties with interpretative guidance relating to FINRA's rules. Please see Interpreting the Rules for more information.

OGC staff contacts:

Jeanette Wingler
FINRA, OGC
1735 K Street, NW
Washington, DC 20006

(202) 728-8000