DORSEY
DORSEY+WHITNEY LLP

Cybercrime Trends: A Midyear Review

by Seth Goertz and Dustin Berger

Cybercriminals continue to outpace the best efforts of regulators, law enforcement, and cybersecurity professionals. Recent reporting from the Federal Bureau of Investigation demonstrates that cybercriminals are increasingly utilizing remote work and artificial intelligence to exploit vulnerable networks, bypass security protocols, and defraud unsuspecting victims.[1] In particular, the FBI reported on a wide-scale scheme involving remote IT professionals, the use of AI to scale already-known schemes, and the continued prevalence of ransomware attacks.

Remote Work Fraud Schemes

One of the most pressing concerns involves the Democratic People's Republic of Korea's ("North Korea") ongoing effort to sponsor a cyber fraud involving remote IT professionals. In short, North Korean nationals are impersonating U.S. citizens and then applying for remote positions as IT professionals at various U.S. companies. These fake IT professionals are currently targeting Fortune 500 companies, U.S. banks, and other financial service providers. To date, the FBI estimates that the scheme has successfully defrauded over 300 U.S. companies.[2]

The fraudulent IT professionals are using a variety of tools to conceal their identities—such as, pseudonymous emails, disguised payment platforms, false websites, proxy computers, and fraudulent ID documents. Once hired, the IT professionals are given near-complete access to a company's network, which they are using to steal sensitive intellectual property and to initiate fraudulent wire transfers.

AI-Enhanced Business Email Compromise

Business email compromise (BEC) scams continue to receive heightened focus, accounting for nearly $3 billion in fraud throughout 2023, the second highest cyber fraud reported to the FBI. Typically, a BEC scam involves a compromise to an employee's business email account through phishing, social engineering, or other intrusion tactics. Once compromised, the bad actor then obtains whatever sensitive data is stored within

Related People

- Seth Goertz
- Dustin Berger

Related Capabilities

- Government Enforcement & Corporate Investigations
- Privacy & Social Media
- Artificial Intelligence
- Technology
- Banking & Financial Institutions

the email account and will then seek to use the legitimate email account for fraudulent purposes—such as impersonating the account holder to facilitate fraudulent financial transactions.

Utilizing developments in AI technology, BEC scams have grown in scale because scammers now have the ability to clone voices and images, which they are using to further large-scale frauds.[3] For instance, scammers who successfully compromised a real estate company's email account were then able to use AI-impersonation technology to redirect wire transfers to a fraudulent bank account following a real estate closing. This follows a wave of cybercrime directed at title companies, title agents, and others involved in real estate transactions because they typically have access to private financial information and are responsible for facilitating large-scale transactions.[4]

Ransomware via Software Vulnerabilities

Ransomware is a malicious software that cybercriminals use to take over a company's systems by encrypting all of the data accessible from the system, rendering the data and system unusable. Once employed, cybercriminals effectively hold the company's data hostage, only providing a key to unencrypt the company's data if the company pays a ransom. Even if a company pays the ransom and is able to recover its data, cybercriminals sometimes leverage the threat of disclosing the previously encrypted data to extort victims for a second ransom payment. According to the FBI, actors associated with the Iranian Government's Islamic Revolutionary Guard Corps ("IRGC") are currently leveraging Microsoft Exchange and Fortinet vulnerabilities to gain access to the systems of a broad range of targets.

Likewise, the FBI provided an update on "Black Basta," a ransomware operator that frequently targets healthcare organizations because of their size and access to sensitive personal identifying information. According to the FBI, Black Basta actors are utilizing phishing techniques and software vulnerabilities to obtain network access and will then initiate a "double extortion" model by encrypting a network and threatening to disclose the affected data.[5]

Investment Scams Continue to Proliferate

The highest reported losses from any crime in 2023 remain attributable to investment scams. Among the most pervasive, are cryptocurrency-related schemes that rely on social engineering—where a bad actor builds a relationship of trust with their victim, introduces the victim to a crypto-investment scheme, and then steals the victim's money. Because of the rise in advanced technology, including AI, these schemes are especially dangerous because fraudsters can create seemingly legitimate investment platforms that fabricate financial gains and similarly use AI to impersonate company executives and others voicing support for the underlying "investment."

Best Practices are Critical

Beyond the concerns that cybercriminals pose, regulators have also signaled that

companies and their executives can be liable for their own lack of due diligence if they fail to implement an adequate cybersecurity program. It's no longer enough to have a cybersecurity program, it must also be defensible in the wake of a breach. For instance, one of the main allegations the SEC has levied against Solar Winds following its well-publicized breach, is that the Solar Winds chief information security officer publicly misrepresented the company's cybersecurity posture.

As a result, companies must take a strategic approach to cybersecurity, including these best practices:

- Have a plan, know your plan: In addition to having a well formulated incident response plan, it's critical that companies and their compliance/regulatory staff review it often, ensuring that it is up to date and continues to evolve with the cyber landscape.
- Prepare, prepare, and prepare: Engage in sophisticated incident response exercises —including tabletop and red team drills—and do so with outside counsel. Leveraging outside counsel to facilitate training exercises, internal systems review, and incident response, ensures that the attorney-client privilege will apply as broadly as possible and that any protocols survive regulatory scrutiny.
- Details matter: From multi-factor authentication ("MFA") to employee education, focusing on details is critical. Specific attention to MFA is especially important to ensure it is truly "multi-factor" and de-coupled from systems that are routinely compromised—such as email or a device.
- Document and validate: Companies should document their cybersecurity program and use regular audits or assessments to ensure that their program is effective, complaint with legal requirements, and working as intended.

[1] FBI Releases Internet Crime Report — FBI

[2] Office of Public Affairs | Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers | United States Department of Justice

[3] FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence — FBI

[4] FinCEN Analysis of Business Email Compromise in the Real Estate Sector Reveals Threat Patterns and Trends | FinCEN.gov; US Secret Service Cyber Investigations Division Updates on Real Estate Scams: Real Estate Scams - Vacant Properties.pdf (certifid.com); file (alta.org)

[5] #StopRansomware: Black Basta (ic3.gov)