Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

December 21, 2022

Justice Department's Evolving Efforts on Ransomware

Ransomware attacks, such as the one carried out by the cybercrime group DarkSide against Colonial Pipeline in May 2021 that disrupted pipeline operations, have highlighted federal law enforcement efforts to counter cybercriminals and their use of malicious technology.

Ransomware Conceptualized

Ransomware is malware that targets systems and data for the purpose of extortion. It is used against individuals, businesses, and government networks, locking users out of their systems or data and demanding a ransom payment to supposedly regain access to or prevent exposure of the system's content. There is no guarantee users will get their data back, even if they pay, or that their data or systems will not have been otherwise compromised. Reportedly, cybercriminals have increasingly used a Ransomware-as-a-Service (RaaS) model wherein certain criminals develop the malware and then sell or lease the tool to others to carry out ransomware campaigns. Both the developer and attacker then receive portions of the criminal proceeds.

Cyber Incident Response

Federal law enforcement has the principal role in investigating and attributing cyber incidents to specific perpetrators, and this responsibility has been established within the broader framework of federal cyber incident response. The 2016 Presidential Policy Directive/PPD-41 on U.S. Cyber Incident Coordination outlined how the government responds to *significant* cyber incidents—those that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Responding to cyber incidents involves (1) threat response, (2) asset response, and (3) intelligence support. The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF), leads the nation's threat response to significant cyber incidents. Asset response and intelligence support responsibilities are led by other federal agencies. Specifically, *threat response* is conceptualized in PPD-41 to mean:

> conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

DOJ's Comprehensive Cyber Review

In April 2021, DOJ announced it was launching a four-month strategic review to evaluate how it responds to cyber threats, in part because of growing ransomware concerns. DOJ's *Comprehensive Cyber Review* report, released in July 2022, notes that "a central goal of the Comprehensive Cyber Review [was] to identify concrete and actionable ways the Department can draw on its full range of criminal, civil, national security, and administrative authorities and resources to confront the multidimensional cyber challenge." With specific mention of ransomware, the review recommended that DOJ comprehensively evaluate its various sources of information to identify priority criminal targets—such as prolific cybercriminals using multiple ransomware variants to carry out their attacks.

The review also noted that today's cyber threats cannot be conceptualized as distinct criminal threats or national security threats; rather, they are blended in nature. It delineates that cybercriminals, including those linked to transnational criminal organizations in Russia and Eastern Europe, profit from levying ransomware and digital extortion attacks against U.S. businesses and organizations. These attacks have "increased in scale, prevalence, and consequence," and attacks that target critical infrastructure networks including pipelines, schools, food supply, hospitals, and emergency services have implications for national security.

Evolving DOJ Actions on Ransomware

As the threats posed by cybercriminals using ransomware develop (at the time of the *Comprehensive Cyber Review*, DOJ noted it was investigating over 100 different ransomware variants) and the amount of money paid by victims increases (a study by Sophos estimates that the average payment was over $812,000, and average recovery costs were $1.4 million in 2021), DOJ has acknowledged that consequences extend beyond ransomware payments and remediation costs, and include associated "mayhem" (e.g., challenges to patient care during attacks against hospitals' systems). DOJ has taken a number of actions intended to bolster investigations, enhance law enforcement information sharing, and increase public awareness.

Investigations

Augmenting cyber investigations is among DOJ's top priorities, because cyber threats, including ransomware attacks, pose risks to national security. For instance, in April 2021, DOJ created a Ransomware and Digital Extortion Task Force comprised of the FBI, Executive Office for the United States Attorneys (EOUSA), and representatives from their Criminal, Civil, and National Security Divisions. The task force's efforts include increasing training and resources; enhancing intelligence

and information sharing; using all investigative leads, including human intelligence and links between criminals and nation states; and improving DOJ coordination on cases—all to disrupt, investigate, and prosecute ransomware cases. DOJ notes that this task force helped seize the proceeds ($2.3 million in bitcoin) from the 2021 DarkSide ransomware attack on the Colonial Pipeline.

The National Cryptocurrency Enforcement Team (NCET) was created in October 2021 to investigate and prosecute criminals who misuse cryptocurrency, including crimes committed by cryptocurrency exchanges, mixing and tumbling services, and money laundering services. DOJ specifically notes that the NCET will assist in recovering assets, such as cryptocurrencies, paid to ransomware groups.

In addition to establishing new tools and task forces to respond to ransomware threats, DOJ has acknowledged that, because of the transnational nature of cybercrime, such as ransomware attacks, fostering international partnerships is a priority. For instance, the FBI's international operations division and legal attaché offices liaise with foreign law enforcement partners on cases. DOJ also established the International Virtual Currency Initiative to work with international partners to counter illicit activity involving digital assets, including tracing virtual currencies gleaned from ransomware schemes.

Information Sharing

In June 2021, Deputy Attorney General Lisa O. Monaco issued a memorandum to federal prosecutors requiring that they notify the Computer Crime and Intellectual Property Section (CCIPS) and the National Security and Cyber Crime Coordinator for the EOUSA of any significant developments in existing ransomware or digital extortion cases. They must also notify CCIPS and the EOUSA of all new instances of ransomware or digital extortion attacks in their districts and file an Urgent Report in the instance of new attacks or those affecting ongoing cases. Essentially, federal prosecutors are now to report ransomware incidents in the same way they report critical national security threats. The memorandum also reinforced CCIPS as the coordinating entity for ransomware and digital extortion cases. In this role, CCIPS coordinates with EOUSA and relevant DOJ components and identifies instances when potential ransomware cases are related to other open investigations.

In addition to information sharing on cases, DOJ provides training to state, local, tribal, and territorial law enforcement agencies to enhance cyber capacity, for instance, through the Law Enforcement Cyber Center and the National White Collar Crime Center. This includes training on emerging and specialized topics such as ransomware.

Public Awareness

DOJ leads several public awareness activities on ransomware. For instance, the NCIJTF organized an interagency group of subject matter experts from over 15 government agencies to develop public awareness materials to help educate the public about preventing and responding to ransomware attacks. NCIJTF and the FBI's Internet Crime Complaint Center (IC3), among others, have published materials on the threats posed by ransomware, where to report it, and how to respond. Victims are encouraged to report ransomware incidents to their local FBI field office, NCIJTF, IC3, or the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security. Federal law enforcement discourages the payment of ransom. DOJ specifically notes that doing so "may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware and/or fund illicit activities."

Congressional Considerations

As Congress conducts oversight and debates legislation on DOJ's efforts to respond to cyber incidents, and specifically threats posed by ransomware, policymakers may consider how these efforts could be affected by resource constraints, evolving technology, and the often transnational nature of cybercrime.

Resources

DOJ specifically identified ransomware as a threat in its FY2023 congressional budget submission, where it requested addition resources to bolster cybersecurity and counter cybercrime. Policymakers may debate whether law enforcement's workforce and monetary resources, as well as DOJ's new initiatives to investigate ransomware are commensurate with the threat. Policymakers may also examine how DOJ evaluates various national security threats facing the country to determine resource allocations to counter cybercrimes such as ransomware relative to other threats such as those posed by terrorist organizations.

Evolving Technology

As technology evolves, some contend that law enforcement's investigative capabilities may not be able to keep pace; some specifically cite strong, end-to-end (or what law enforcement has sometimes called "warrant-proof") encryption, which can prevent access to certain communications and information. Congress may continue to examine this tension between the privacy of electronic communications and law enforcement's ability to investigate cybercrime in the context of ransomware investigations.

Transnational Nature of Cybercrime

Because cybercriminals, including those engaging in ransomware, can operate anywhere in the world, networks of these criminals—and digital evidence of their activity—may exist in various countries. This may lead to investigative challenges in gathering evidence, working with international law enforcement, and holding perpetrators accountable in the United States. Policymakers may examine how these challenges could affect DOJ investigations of criminals engaging in ransomware and RaaS.

Kristin Finklea, Specialist in Domestic Security

IF12294

Disclaimer