Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Department of Justice Efforts to Counter Ransomware

July 2, 2021

Ransomware attacks, such as the one carried out by 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

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 systems or data. 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. RaaS was involved in the attack on Colonial Pipeline.

DOJ's Role in Cyber Incident Response

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. Specifically, this threat response includes

> 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.

Congressional Research Service
https://crsreports.congress.gov
IN11698

In April 2021, DOJ announced it was launching a four-month strategic cyber review to evaluate how it responds to cyber threats, in part because of growing ransomware concerns.

Evolving DOJ Actions on Ransomware

As the threats posed by cybercriminals using ransomware develop (the FBI is investigating about 100 types of ransomware) and the amount of money paid by victims increases (one study estimates the average payment is over $170,000, and average recovery costs increased from $761,106 in 2020 to $1.85 million in 2021), DOJ has acknowledged that the consequences extend beyond ransomware payments and remediation costs and include the associated "mayhem" (e.g., ensuring 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, as cyber threats, including ransomware attacks, pose risks to national security. For instance, DOJ created a Ransomware and Digital Extortion Task Force comprised of the FBI, Executive Office for United States Attorneys (EOUSA), and representatives from their Criminal, Civil, and National Security Divisions. The task force's intended 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.

Information Sharing. In June 2021, Deputy Attorney General 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 must 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 where potential ransomware cases are related to other open investigations.

Awareness. DOJ leads several public awareness activities on ransomware. For instance, the NCIJTF "convened an interagency group of subject matter experts to [among other things] educate the public on ways to prevent ransomware attacks." In addition, 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). Notably, federal law enforcement discourages the payment of ransom, noting 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 may be affected by resource constraints, evolving technology, and the often transnational nature of cybercrime.

- In its FY2022 budget justification requesting resources to bolster cybersecurity and counter cybercrime, DOJ specifically identified ransomware as a threat. Policymakers may debate whether law enforcement's manpower and monetary resources as well as DOJ's new initiatives to investigate ransomware are commensurate with the threat.
- 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.
- 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. There may be 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.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer