Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

COVID-19: Cybercrime Opportunities and Law Enforcement Response

Kristin Finklea
Specialist in Domestic Security

March 19, 2020

Opportunistic criminals and other malicious actors exploit the internet and rapidly evolving technology to their advantage. Criminals can compromise financial assets; hacktivists can flood websites with traffic, effectively shutting them down; and spies can steal intellectual property and government secrets. And, they capitalize on ever changing world events. Federal officials have cautioned about scams relating to the outbreak of disease caused by a previously unidentified strain of coronavirus, designated Coronavirus Disease 2019, or COVID-19. They have noted that "[c]yber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes."

Indeed, analysts and officials have reported criminals using public interest in COVID-19 to their advantage. For instance, the Department of Justice (DOJ) cites "reports of individuals and businesses selling fake cures for COVID-19 online and engaging in other forms of fraud, reports of phishing emails from entities posing as the World Health Organization or the Centers for Disease Control and Prevention, and reports of malware being inserted onto mobile apps designed to track the spread of the virus." In one scheme reported by security experts, hackers sold a malware infection kit that used an interactive map of coronavirus infections produced by Johns Hopkins University. The kit was designed to spread malware to steal passwords.

Cybercrime Investigations

Federal law enforcement has the principal role in investigating and attributing cyber incidents, including those that may take advantage of heightened public interest in the COVID-19 pandemic, to specific perpetrators, and this responsibility has been codified within the broader framework of federal cyber incident response. Specifically, DOJ—through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF)—is the designated lead in responding to these threats.

Congressional Research Service
7-....
www.crs.gov
IN11257

FBI Cyber Investigations

The FBI pursues cybercrime cases ranging from computer hacking and intellectual property rights violations to child exploitation, fraud, and identity theft. Its top cyber priorities involve combating computer and network intrusions and investigating ransomware. The FBI's cyber efforts are focused on "high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors."

One key challenge involves moving away from reacting to malicious cyber events and toward preventing them. As such, the FBI has focused resources on enhancing cyber capabilities in a number of ways, including bolstering the FBI's cyber workforce, strengthening the NCIJTF, expanding Cyber Task Forces (CTFs) and focusing their efforts on computer/network intrusion investigations, and increasing information sharing and coordination with the private sector.

Task Forces and Partnerships

The NCIJTF was established by National Security Presidential Directive-54/Homeland Security Presidential Directive-23 in January 2008. The NCIJTF's mission is to "serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations." Led by the FBI, the NCIJTF coordinates over 20 federal agencies, including law enforcement, intelligence, and the military. It also collaborates with the private sector and international partners. Early on, there were concerns that "the NCIJTF was not always sharing information about cyber threats among the partner agencies." There were also criticisms that the NCIJTF was perceived as an extension of the FBI's Cyber Division instead of as a multiagency effort. However, DOJ's Inspector General has since noted that these issues have improved.

The FBI leads several other task forces and partnerships focused on cyber threat response. For instance, there is a CTF at each field office. CTFs focus on local cybersecurity threats, respond to incidents, and maintain relationships with companies and institutions. CTFs also support the national effort to combat cybercrime by participating in national virtual teams on certain cyber issues and providing cyber subject matter experts or enhanced capability outside of their assigned areas, when needed. Additionally, the FBI has established and maintained Cyber Action Teams of agents and computer scientists that can be rapidly deployed around the world to assist in computer intrusion investigations. In addition to domestic field offices pursuing international leads in investigations, the FBI has positioned cyber assistant legal attachés (ALATs) in some foreign countries. ALATs work with law enforcement in host countries to share information, collaborate on investigations, and enhance relationships with partner agencies. ALATs focus on "identifying, disrupting, and dismantling cyber threat actors and organizations."

Going Forward: DOJ Cyber Priorities

Countering cyber threats is among DOJ's top priorities, and countering threats related to the COVID-19 pandemic is receiving heightened attention. On March 16, 2020, Attorney General William Barr issued a memorandum to the U.S. Attorneys regarding DOJ's COVID-19 priorities. Noting that criminals may take advantage of the COVID-19 pandemic, the memorandum stated that "[e]very U.S. Attorney's Office is thus hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic." Congress, in examining DOJ's cyber priorities going forward, may look to the resources DOJ has placed toward countering cyber threats broadly as well as specific nefarious activity capitalizing on the COVID-19 pandemic.

DOJ has highlighted a number of challenges that law enforcement faces in countering cybercrime, and Congress may continue to conduct oversight and debate legislation in these arenas, including the following:

- Transnational Crime. Cybercriminals have specialized their activities and, because they can operate anywhere in the world, networks of expert cybercriminals—and digital evidence of their activity—may exist in various countries. There are sometimes investigative challenges in gathering evidence, working with international law enforcement, and bringing perpetrators to justice in the United States.
- Evolving Technology. While some note that law enforcement may have access to more digital information than ever before, others contend that law enforcement is "going dark" as some investigative capabilities are outpaced by the speed of technological change. These hurdles for law enforcement reportedly include strong, end-to-end (or what law enforcement has sometimes called "warrant-proof") encryption, which can prevent access to certain communications and information. The tension between privacy of electronic communications and law enforcement's ability to investigate crimes remains of congressional interest.