CRS Insights

Attribution in Cyberspace: Challenges for U.S. Law Enforcement

Kristin Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

April 17, 2015 (IN10259)

"Who did it?" Attribution, some may argue, is a challenge "as old as crime and punishment." In the cyber realm too, criminal attribution is a key delineating factor between cybercrime and other threats. When investigating a given incident, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat.

Blurry lines between various types of malicious activity in cyberspace may make it difficult for investigators to attribute an incident to a specific individual or organization. Without knowing the criminal intent or motivation, some activities of cybercriminals and other malicious actors may appear on the surface to be similar, causing confusion as to whether a particular action should be associated with a *criminal* or other actor. Further, "[t]he speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all." Moreover, officials have noted cooperation and blurring of lines between types of actors, including nation states, organizations, and individuals, which can complicate or stymie attribution.

Attribution in the Sony Pictures Entertainment Breach

The attribution issue is highlighted in the November 2014 revelation of a breach at Sony Pictures Entertainment (SPE) by actors claiming responsibility and calling themselves the "Guardians of Peace." The Federal Bureau of Investigation (FBI), in its investigation of the breach, notes that it "consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations." Hackers further threatened a September 11, 2001-type of attack on movie theaters that showed "The Interview," a spoof about journalists tasked with killing North Korea's Supreme Leader, Kim Jong-un. There has been debate about the true source of the breach. As of December 2014, the FBI—leading an interagency effort—had attributed the hack to the North Korean government. In its attribution, the FBI cited malware linked "to other malware that the FBI knows North Korean actors previously developed," "significant overlap between the infrastructure used in this attack and other malicious cyberactivity the U.S. government has previously linked directly to North Korea," and tools similar to those used in a 2013 North Korean cyberattack against South Korean banks and media outlets. Nonetheless, experts critical of this attribution note that the evidence linking North Korea to the SPE breach is not definitive. Further fueling concerns that the hack may be mis-attributed, U.S. officials have not revealed specifics surrounding how the attribution was reached.

As a response to North Korea's "numerous provocations, particularly the [2014] cyber-attack targeting Sony Pictures Entertainment and the threats against movie theaters and moviegoers," President Obama signed an Executive Order on January 2, 2015, authorizing additional sanctions against certain individuals and entities associated with the North Korean government.

Attribution in the Anthem Inc. Breach

In February 2015, it was revealed that one of the nation's largest health insurance companies, Anthem Inc., had suffered a data breach involving the personal information—including Social Security numbers—of potentially 80 million individuals. However, Anthem does not believe that banking, credit card, or certain medical information was compromised. Law enforcement has not publicly attributed this attack. Notably, "security experts involved in the ongoing forensics investigation into the breach say the servers and attack tools used in the attack on Anthem bear the hallmark of a state-sponsored Chinese cyberespionage group known by a number of names, including 'Deep Panda,'" as well as a professor at Southeast University in China. Nonetheless, a definitive attribution for the Anthem Inc. breach has not been made.

Federal Efforts to Enhance Attribution

Determining the actor (and actor's motivation) involved in a cyber incident will in turn help guide how the United States responds. If a criminal—motivated by profit—is the perpetrator, the investigation and response may be led by law enforcement using the tools of the criminal justice system. If the perpetrator is deemed to be a state-sponsored actor, the United States may utilize diplomatic or military tools in its response. Notably, the criminal justice system has standards of proof for attributing an incident to an individual. It is less clear in other domains —such as attribution as a basis for war or a response to cyberterrorism—what the standard of attribution or proof may be.

A number of issues may pose challenges for accurate, timely attribution. For instance, the anonymizing tools that lie within the Internet through means such as The Onion Router (Tor) can help mask the identities of actors. While such tools can help protect privacy online, they can also help hide malicious, illegal activity. Policymakers may consider how Congress can assist law enforcement and others in enhancing attribution of cyber incidents within the framework of today's rapidly changing technology space. They may question whether law enforcement has sufficient resources—authorities, technological capabilities, and manpower.

While attribution remains a challenge, the Director of National Intelligence notes that "[g]overnmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions." The FBI has reportedly bolstered its efforts to better attribute cyberthreats and attacks. Through the Next Generation Cyber Initiative, the FBI is developing agents to connect with critical infrastructure components and computer scientists to "extract hackers' digital signatures" and determine their identities, all to help concretely attribute a specific actor to a cyber incident. Similarly, the Department of Defense has reportedly "made significant investments in forensics to address this problem of attribution." Congress has already shown interest in understanding whether accurate attribution can help deter cyberattacks as well as in ensuring that investigators have the tools and skills to accurately attribute incidents.