GOING DARK: THE USE OF ANONYMIZING TECHNOLOGIES IN DARK WEB CRIMES

Date: 12 June 2017

By: Clifford C. Histed, Nicole C. Mueller

Like an iceberg, the majority of the internet is concealed from plain sight. The "Dark Web," or websites and content that use anonymizing networks to provide untraceable access to unindexed sections of the web, comprises a segment of what lies beneath that which is visible through a Google search. On May 3, 2017, then-FBI Director James Comey discussed the same when he testified before the United States Senate in a hearing relating to the FBI's oversight:

> Virtually every national security threat and criminal problem that the FBI currently faces has an element that is digitally-based or facilitated. Unfortunately, there is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as 'Going Dark.'

Former Director Comey cited examples such as "online pedophiles who hide their crimes and identities behind layers of anonymizing technologies, or drug traffickers who use virtual currencies to obscure their transactions." He went on to state that, "[t]he FBI is actively engaged with relevant stakeholders, including companies providing technological services, to educate them on the corrosive effects of the Going Dark challenge on both public safety and the rule of law."

Comey's concerns about cybercriminals Going Dark is shared by European law enforcement authorities. On March 13, 2017, Europol and Eurojust (the European Union's judicial cooperation unit) published a joint paper called "Common Challenges in Combatting Cybercrime." One challenge identified in the paper was the "widening criminal use of decentralized virtual currencies and the increase of tumbler/mixer services" which the paper defined as a service "that attempts to break the links between the original and the final address by using several intermediary wallets." The paper asserted that the use of such services effectively prevents law enforcement from "following the money" and "significantly complicates the possibilities for asset recovery and the prevention of fraudulent transactions."

These law enforcement concerns are playing out in real time in the criminal case *United States v. Michael Richo*, currently pending in federal court in Connecticut. In October 2016, the FBI arrested Richo and charged him with money laundering, fraud, and other crimes arising from his alleged theft of bitcoins from Dark Web users. According to the criminal complaint, Richo created phishing pages to steal logins for bitcoin wallets escrowed on dark web marketplaces, catching 10,000 users whose details were later found in a database on his laptop. Richo is alleged to have monitored the account balances of the users' bitcoin wallets, withdrawing bitcoins as they were deposited before selling them back to other users for U.S. dollars, and depositing the laundered money into a

bank account he controlled. Richo is estimated to have allegedly stolen "six figures" worth of bitcoins. Of course, bitcoins are routinely used for buying or selling services on the Dark Web because they allow anonymity for bitcoin owners, particularly for those who use mixer or tumbler services to hide the origins of the bitcoins. Richo allegedly used a mixer called Bitcoin Fog to attempt to hide his trail.

The *Richo* case is worth watching because it provides a window into the FBI's playbook for conducting such investigations. According to the complaint, the FBI had been investigating Richo since November 2013. In November 2014 (nearly two years before Richo's arrest in this case) the FBI executed a search warrant at his home and he confessed to stealing bitcoins from users on the Dark Web in the manner described above. However, the FBI took two years to arrest and charge Richo. When Richo was ultimately arrested in 2016, he was allowed to post bond and was released immediately. Though Richo had the right to a probable cause hearing within 21 days of his arrest, and the right to be indicted within 30 days of his arrest, neither have yet happened in the eight months since his arrest. In a court pleading filed March 19, 2017, Richo requested that those deadlines be extended while he considers a plea agreement and engages in discussions with the government concerning a possible pre-indictment resolution of this matter. It is reasonable to wonder whether Richo is assisting the FBI in other Dark Web investigations.

