“Emerging Markets for Cybercriminals: Ransom and Purchase of Stolen Data by Victims and Authorized Intermediaries”

Josephine Wolff

The business model of cyber criminals who steal or access protected information and computer systems for the purpose of profiting financially is increasingly shifting from a market in which those criminals sell their stolen information to other criminals and fences to a market dominated by the sale of that data back to its original owners. This strategy of selling data back to its original owners can take multiple forms, including ransomware, in which a victim’s computer systems are compromised and typically encrypted until a payment is made to the perpetrators, or data exfiltration, in which a firm’s proprietary information is stolen and then purchased by that firm itself in attempt to prevent it from being sold to competitors. Both of these forms of victims purchasing their own data—acquiescing to ransomware demands and purchasing stolen data on the black market—present several challenges for law enforcement, provide significant economic incentives to criminals, and raise complicated questions around the ethics and legality of otherwise law-abiding citizens funding criminal endeavors and legitimizing the markets for stolen data. This paper examines the emerging trends in cyber crime that point towards increased activity in selling stolen data back to victims and their authorized intermediaries, and analyzes the relevant legal regimes that might apply to the victims who engage in these activities and current ambiguity around when victims may purchase access to stolen or compromised data. Finally, it proposes policy recommendations intended to disincentivize the payment of ransoms and purchase of stolen data by victims, while incentivizing the implementation of appropriate data protection measures and security controls.

1 This research was made possible by a grant of the Carnegie Corporation of New York.