Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

Georgia State University

Training on Intelligence and Evidence Gathering in Darknet Environments

LEAD PI: DAVID MAIMON

Criminal Investigative Processes

SUMMARY

The internet has accelerated the development of complex illicit supply chain structures which support the flow of illegal goods and services within the underground economy. Investigators need training in cost-effective intelligence and evidence gathering from darknet environments to be able to evaluate threats generated by malicious online actors and collect extensive evidence regarding their operations on darknet platforms. The training provided by this project addresses these gaps by teaching law enforcement agents how to collect and analyze darknet data in a way which could guide the exploration of future policing approaches and application to a wide range of online crime.

PROBLEM STATEMENT

The growth of underground markets creates an increasingly serious threat to global and national security and health; total darknet market sales grew in 2019 to over $790 million, a volume that demonstrates the heightened demand for illicit commodities such as drugs, virtual goods (e.g., malicious malware, credit cards, social security numbers, and online identities), counterfeit money, and fake documents (passports, driver licenses, and health insurance cards). To deal with these new and increasing threats and build successful cases against offenders, law enforcement agencies need to collect extensive evidence from online darknet platforms, while also analyzing longitudinal information to better understand the activities and actors in these ecosystems and formulate the most effective disruption and deterrence strategies.

APPROACH

In this project, we propose a three-day workshop (virtual, in-person, or hybrid) implementing lectures and hands-on exercises to deliver key methodological and technical skills necessary to support cost-effective intelligence and evidence gathering. The training includes topics on OSINT tools and techniques, accessing and navigating darknet markets and forums, encrypted communication channels, cryptocurrency, social networks, the use of data scrapers and parsers, and data maintenance, coding, and analysis. Practice sessions with tools are incorporated into sessions, and trainees are provided with the source code for the scrapers and the parsers to utilize for their organizational needs. The training will leverage the Evidence Based Cybersecurity (EBCS) research group's separate internet network, and is supported by an interdisciplinary team of educators composed of Criminology, Law, Computer Science, and Computer Information System scholars who are committed to supporting participants' development of knowledge in a number of areas as well as critical thinking, which is essential for designing an effective response to online crime challenges.

ANTICIPATED IMPACT FOR DHS

The proposed training is consistent with HSI objectives to reduce cyber-crime incidents through the use of deterrence. A more proactive approach for online policing involves the collection and production of strategic cyber intelligence, which could support identification and understanding of adversarial operational capabilities, partnerships and intentions, and support accurate assessment of offenders' plans. Additionally, the most effective platforms for disseminating deterrence-based cues are still relatively unknown; the empirical data which could guide DHS overall policy related to online policing is also still missing. The proposed training seeks to address these gaps by teaching law enforcement agents how to collect and analyze darknet data in a way which could guide the exploration of future policing approaches to a wide range of online crime.