DHS Science and Technology Directorate

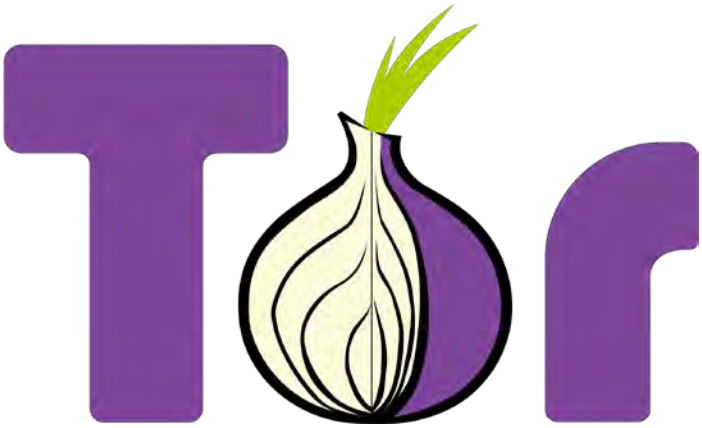
Cyber Security Division - Anonymous Networks & Currencies

Anonymity and encryption attracts criminals

Anonymous networks and cryptocurrencies have many legitimate applications to support the freedom of the press, protect human rights, and allow new methods of payment that protects individual privacy. However, criminals are exploiting the protections built into the encryption and the promise of near anonymity. Applications such as The Onion Router (Tor) and Bitcoin are used to establish marketplaces and websites that facilitate the illegal transaction of drugs, weapons, murder, child pornography, and other illicit contraband. Investigations into anonymous networks and cryptocurrencies are incredibly resource intensive and difficult, requiring significant man-hours to investigate and prosecute criminals involved in illegal trade on anonymous marketplaces and websites.

Developing new tools to identify and unmask the identities illicit identities

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) Anonymous Networks and Cryptocurrencies project is developing cost effective solutions for law enforcement (LE) components to complement and expand their capabilities to investigate crimes committed using anonymous networks and currencies. CSD is researching novel ways to identify illicit anonymous marketplace and website users as well as users facilitating illicit transactions using cryptocurrencies through technology enhancements and automation.



"Tor logo" by the Tor Project; copyright June 19, 2011; source.

DHS S&T is leveraging strong LE partnerships to receive requirements direct from the end users to research and develop solutions that fit specific investigative requirements.

Understanding the legitimate uses of these technologies, CSD is working to provide stronger encryption and protections for LE communications utilizing Tor. Also, important is the development of usage statistics within anonymous networks through safe aggregation of data that protects the privacy and anonymity of users. CSD is also conducting a system analysis, working with LE to generate requirements that can be used to develop broader solutions to investigate criminal activities.

Investigative Impact

The tools developed will complement the investigate techniques LE agencies currently utilize and reduce the resource burden needed to investigate these crimes. DHS S&T CSD will continue to lead research and development and work collaboratively within DHS and the federal, State, and local LE community in combating emerging methods while also protecting the legitimate applications of such services.

Performers

- Sandia National Laboratory
- Naval Research Laboratory
- Ciphertrace

Homeland Security
Science and Technology

To learn more about Cyber Security Forensics, contact Megan Mahle, Program Manager.

03 03 2016