SHERLOC SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

UNODC United Nations Office on Drugs and Crime

Case Law Database

Cybercrime

Acts against the Confidentiality, Integrity and Availability of Computer, Data and Systems

- Production/ distribution/ possession of computer misuse tools

Computer-related acts for personal or financial gain

- Copyright/ trademark violations

Drug offences

Offences

- Importation/ exportation

Money laundering

Trafficking in firearms

Offences

- Illicit trafficking

Operation Onymous

Other

Fact Summary

In November 2014, law enforcement and prosecutors in Europe and the US launched Operation Onymous, an international operation aimed at taking down online illegal markets and arresting vendors and administrators of such markets. The operation was coordinated by Europol's European Cybercrime Centre (EC3), Eurojust, the FBI, and the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI). The operation culminated in the arrest of 17 individuals and the seizure of Bitcoins amounting to USD 1 million, drugs, gold and silver.

Among the marketplaces brought down were Silk Road 2.0, an online black market and used to sell drugs and other illegal items. In 2013, the FBI shut down its predecessor, Silk Road 1.0 and arrested its founder Ross Ulbricht, who was convicted in February 2015 in the US. Silk Road 2.0 was launched in November 2013 after the shutdown of its previous version. On 5 November 2015, the alleged administrator of Silk Road 2.0, Blake Benthall, was arrested by the FBI in San Francisco. According to the FBI, as of September 2014, Silk Road 2.0 had sales of at least approximately $8 million per month and approximately 150,000 active users. As a part of the investigation, an undercover HIS agent infiltrated in the administration of Silk Road 2.0 and obtained access to restricted information.

Silk Road 2.0 and other online marketplaces shut down as part of this investigation were operated as TOR hidden services. The TOR (The Onion Router) network is a worldwide network that allows users to establish anonymous communication. A TOR hidden service does not reveal the IP address of the server used . TOR is used for both illicit and licit purposes, with the latter including members of the military as well as activists and journalists evading censorship.

Most transactions on the shuttered marketplaces were carried out in Bitcoins. Bitcoin is a decentralized cryptocurrency, i.e. there is no centralized authority and Bitcoin transactions are processed and validated by a peer-to-peer network. Bitcoin users are anonymity but all its transactions are stored in a public ledger. Information on Bitcoin

users can be obtained from exchanges – institutions converting Bitcoin into other currencies or vice versa – and other points of intersection with the regulated financial system.

Commentary and Significant Features

This case shows how criminals are able to use the internet to trade illegal goods and conceal the proceeds of illegal transactions. In particular, the use of Bitcoin and other digital currencies poses significant challenges in identifying the offenders.

Cooperation between law enforcement and judicial agencies as well as with the private sector contributed significantly to the success of this operation. In particular, obtaining data from Bitcoin exchanges and ISPs helped law enforcement erode Bitcoin's anonymity. Swift international police and judicial cooperation allowed the investigators to obtain crucial information in a timely fashion and locate the offenders.

Cross-Cutting Issues

Liability

... for

- completed offence

... based on

- criminal intention

... as involves

- principal offender(s)
- participant, facilitator, accessory

Offending

Involved Countries

- Bulgaria
- Czechia
- Finland
- France
- Germany
- Hungary
- Ireland
- Latvia
- Lithuania
- Luxembourg
- Netherlands (Kingdom of the)
- Romania
- Spain
- Sweden
- Switzerland

United Kingdom of Great Britain and Northern Ireland

United States of America

Investigation Procedure

Computer specific investigative measures

- Seizure/Confiscation of hardware and/or software
- Remote forensic tools

Special investigative techniques

- Undercover operation(s)/ Assumed identities/ Infiltration

Comments

Law enforcement in the US obtained information from Google, a Bitcoin exchange and the ISP hosting Silk Road 2.0.

International Cooperation

Measures

- International law enforcement cooperation (including INTERPOL)

Defendants / Respondents in the first instance

Defendant: B.B., a/k/a “Defcon"

Gender: Male

Nationality: American

Age: 26

Secret owner and operater of the Darknet website known as “Silk Road 2.0”.

Charges / Claims / Decisions

Defendant: B.B., a/k/a “Defcon"

Charge details:

B.B. was charged with one count of conspiring to commit narcotics trafficking; one count of conspiring to commit computer hacking; one count of conspiring to traffic in fraudulent identification documents; and one count of money laundering conspiracy.

Sources / Citations

Europol press release

FBI press release