

December 12, 2016

International Cyber Sweep Nets DDoS Attackers

California Grad Student Arrested in Operation Aimed at Young Hackers



A 26-year-old student in California was among nearly three dozen suspects arrested last week in a cyber crime sweep involving 13 countries.

Sean Sharma, a graduate student at the University of Southern California, was arrested December 9, 2016 and charged with cyber crimes for his role in a distributed denial of service (DDoS) attack that knocked a San Francisco chat service company's website offline. DDoS attacks flood websites and their servers

with massive amounts of data, leaving them inaccessible to users. Sharma purchased a tool to mount his cyber attack, according to the charges against him.

The arrest occurred during an operation aimed at users of “DDoS for hire” services, which can be used to target computers and websites of their choosing. Over five days beginning on December 5, law enforcement agencies conducted 101 interviews and arrested 34 suspects in the sweep, which was coordinated from The Hague in the Netherlands by Europol’s European Cyber Crime Centre (EC3). Europol, the law enforcement agency of the European Union, assisted participating countries in their efforts to identify suspects—many under the age of 20—by sharing intelligence and analytical support. Actions within the United States were coordinated by the International Cyber Crime Coordination Cell, or IC4, hosted by the FBI in the Washington, D.C. area.

The case against Sharma is being investigated by the FBI San Francisco Field Office’s San Jose Resident Agency. If convicted, Sharma could face up to 10 years in prison. In a statement released today, the FBI said the nature of cyber crimes often requires a coordinated response, since subjects could be operating from anywhere in the world.

The operation marked the kick-off of a prevention campaign to raise awareness of the risks of young adults being lured into committing cyber crimes. In a press release about the operation, Europol said teenagers who become involved in cyber crimes often have skill sets that could be put to positive use through a career in computer programming or cyber security.

“DDoS tools are among the many specialized cyber crime services available for hire that may be used by professional criminals and novices alike,” said Steve Kelly, FBI unit chief of IC4. “While the FBI is working with our international partners to apprehend and prosecute sophisticated cyber criminals, we also want to deter the young from starting down this path.”

Europol identified examples of cyber crimes that involve predominantly young offenders. They include:

- Hacking, or gaining access into someone’s computer network without their permission, and then taking control and/or taking information from other people’s computers.
- Making, supplying, or obtaining malware (malicious software), viruses, spyware, botnets, and remote access Trojans.
- Carrying out a DDoS attack or “booting” a DDoS—booting someone offline, for example, while they are playing online games.

“Today’s generation is closer to technology than ever before, with the potential of exacerbating the threat of cyber crime,” said Steve Wilson, head of the EC3. “Many IT enthusiasts get involved in seemingly low-level fringe cyber crime activities from a young age, unaware of the consequences that such crimes carry.”

Last week’s law enforcement actions took place in Australia, Belgium, France, Hungary, Lithuania, the Netherlands, Norway, Portugal, Romania, Spain, Sweden, the United Kingdom, and the U.S.

The arrest of Sharma in La Canada, California, was just one of the investigative activities conducted last week by cyber task forces in the U.S. The efforts included interviews that did not result in arrests but highlighted the seriousness of engaging in cyber crimes, which is a top priority of the FBI. In a statement released today, the FBI said the nature of cyber crimes often requires a coordinated response, since subjects could be operating from anywhere in the world.

“No law enforcement agency or country can defeat cyber crime alone,” the Bureau statement said. “This demands a collective global approach.”

Resources:

- Europol press release
(<https://www.europol.europa.eu/newsroom/news/joint-international-operation-targets-young-users-of-ddos-cyber-attack-tools>)
- More on FBI efforts to combat cyber crime
(<https://www.fbi.gov/investigate/cyber>)

“While the FBI is working with our international partners to apprehend and prosecute sophisticated cyber criminals, we also want to deter the young from starting down this path.”

Steve Kelly, FBI unit chief, International Cyber Crime Coordination Cell (IC4)