Emergency Management and Response Information Sharing and Analysis Center

CIP BULLETIN 7-09 July 29, 2009

NOTE: *CIP Bulletins will be distributed as necessary to provide members of the Emergency Services Sector with timely, important, unclassified information potentially affecting the protection of their critical infrastructures. They are prepared by the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.*

Cybercrime

What is Cybercrime?

The term "cybercrime" is usually referred to as any criminal offense committed against or with the use of a computer or computer network. The US Department of Justice (DOJ) interchangeably uses the terms "cybercrime," "computer crime," and "network crime" to refer to acts such as computer intrusions, denial of service attacks, viruses, and worms.[1] A cybercrime incident can lead to loss of business and consumer confidence, financial loss, productivity loss, and even loss of intellectual property. For something to be considered a crime, however, requires a law to denote it as such, and the laws have, to this point, lagged behind technology. Existing laws relating to cybercrime oftentimes do not apply to specific acts being investigated and those laws vary from state to state. Some cybercrime may be more easily prosecuted if it is simply viewed as a more commonly recognized crime (e.g., vandalism instead of web defacement). To refer to a criminal act as "cybercrime" or "computer crime" tends to place the focus more on the technology, rather than on the crime itself. For these reasons, Anthony Reyes, author of the book *Cyber Crime Investigations*, argues against using the term "cybercrime," and instead prefers to call these acts as "crimes with a computer component."[2] Despite the means used to commit a crime or the target of a crime, whether it is a computer, a business, or someone's data, it is still a crime.

What are the Trends in Cybercrime?

In the 1990s, cybercrime was mainly motivated by notoriety or revenge and predominately defined by the willful destruction of online property or intentional disruption of a business. The current era of cybercrime is dominated by criminals who want to use your computer for illegal activities, to steal data for profit, and organized crime is heavily involved.[3] Attackers exploit vulnerabilities in computer software in order to develop "crimeware," such as viruses, Trojans, and keyloggers, in order for other criminals to carry out their nefarious acts. These "crimeware" creators also utilize the software-as-a-service business model to provide crimeware-as-a-service. Some of their crimeware servers not only act as command and control servers (i.e., machines designed to provide instructions to the crimeware), but also as "data suppliers" or repositories for private stolen information that is harvested by the crimeware.

Personal information is a valuable commodity for criminals. Traditional security tools are becoming increasingly more limited in their ability to mitigate these highly complicated cybercrime attacks.[4] Another trend is that the governments of various countries are suspected of being involved in cybercrimes for political reasons. As governments become more dependent upon technology, those assets will be attacked for various reasons. The cybercrime landscape, as it may be called, has definitely changed, but the criminal motivations are still the same – money, power, and revenge.

What Can I Do?

Fighting cybercrime is problematic for several reasons. Many actions, such as writing crimeware, are currently not defined as illegal and, even if they constitute a crime, can be difficult to prosecute. Location and jurisdiction may also be a problem. For instance, a criminal may reside in one country and use a crimeware server in another country to attack a victim who resides in a third country.[5] Cybercrime can also be perpetrated without a person's knowledge, unlike other types of crimes that may be more noticeable. To adequately defend against cybercrime, you need to follow the traditional best practices for protecting your network or desktop.

If you become a victim of cybercrime, you should report the incident to the appropriate law enforcement authorities. Depending on the scope of the crime, the appropriate agency may be local, state, federal, or even international. The US DOJ maintains a list of federal agencies to which computer related crimes may be reported at the following address: http://www.usdoj.gov/criminal/cybercrime/reporting.htm. In addition, you may report cybercrimes to the Internet Crime Complaint Center (IC3), a partnership among the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA). The IC3 provides a convenient reporting mechanism for both citizens and government agencies that alerts authorities of suspected criminal or civil violations and may be contacted via the following address: http://www.ic3.gov.

[1] "Prosecuting Computer Crimes," February 2007, http://www.usdoj.gov/criminal/cybercrime/ccmanual/00ccma.html.
[2] Reyes, Anthony, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Syngress Publishing, Inc. 2007.
[3] "A Brief History of Data Theft," The ISSA Journal, June 2008.
[4] "The Cybercrime 2.0 Evolution," The ISSA Journal, June 2008.
[5] "Organized Cybercrime," The ISSA Journal, October 2008.

NOTE: The source of this document is the Multi-State ISAC July 2009 Cyber Security Tips