Бондя Н., курсант Національної академії внутрішніх справ
Консультант з мови: ХарчукН. Р.

COMBATING CYBER CRIME IN UKRAINE

Before starting our discussion first we must know what **“Cyber crime”** is and what are the impacts and the benefits the **“Cyber Criminals”** gain from such activities.

First consider the definition of cybercrime. “Any crime that involves a computer and a network is called a "Computer Crime" or “Cyber Crime” [1].

Another term called “Internet crime” refers to criminal activities for exploiting the internet. These crimes include and are not limited to identity theft, threatening a nation's security, copyright infringement and child pornography. These crimes have become a threat to individual privacy, where confidential data, individual's identity or photos and videos etc. is stolen or intercepted by the attacker.

In "Cyber Crime" such as identity theft, financial theft, espionage mostly non-state agents and government organizations are involved.

Cybercrime is divided into the following types:

1. **Computer Intrusion** is any malicious activity that harms a computer, or causes a computer or a computer network to work in an unexpected manner. These attacks involve spreading of virus, denial of services or exploitation of the operating system or a software feature.

2. **Social Engineering**

The term "social Engineering" means to fool a user by sending him an email or calling him to provide confidential data like passwords etc.

3. **Masquerading.**

In this type of attack a system is fooled into giving access by sending a TCP (Transmission Control Protocol). Packet that has a forged source address which makes the packet appears to come from a trusted host.

4. **Denial of Service (DOS Attack).**

This type of attack intent is to make resources or service unavailable to its intended users. Such DOS attacks are carried out on websites to stop them from functioning.

5. **Smurf Attack.**

This attack generates large amount of traffic on a victim's network, which causes the network to crash. Smurf Attack is a type of DOS attack.

6. **Email Bombing**

Email bombing means sending thousands of email to a victim causing the victim's mail account or mail server to crash.

7. **Logic Bomb**

A logic Bomb is an event driver attack. This type of attack activates only if certain even occurs [2].

INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled crimes.

Most cybercrimes are transnational in nature, therefore INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale.

Our main initiatives in cybercrime focus on:

1. Operational and investigative support
2. Cyber intelligence and analysis
3. Digital forensics
4. Innovation and research
5. Capacity building
6. National Cyber Reviews

Today's world is more interconne cted than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our nation's cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. The Department of Homeland Security (DHS) works with other federal agencies to conduct highimpact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

Cybercrime has become a particularly relevant problem to police around the world and to society at large. The growing presence of the internet and computers in homes around the world means that more people are exposed to cybercrime each year. The rise in popularity of broadband internet access also means a greater risk. In an era where all data is being digitized and stored on computers, protecting computers is integral to personal and national security.

Список використаних джерел:

1. Категорія: Кіберзлочинність. [Електронний ресурс] : [Інтернет-портал].- Режим доступа: Й1рз://ик^ікіреriia.огд/№Ікі/Категорія:Кіберзлочинність

2. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые методы борьбы: Автореф. дис. ... канд. юрид. наук / Юрид. ин-т ДГУ. Каф-ра уг-го права - http://www.crime.vl.ru/docs/stats/stat 178.html;

3. Інтерпол [Електронний ресурс] : [Інтернет-портал]. - Режим доступа: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.