Cybercrime Prevention from the Perspective of Anti-cyber-attack Technology

— — the Thinking and Practice of the Enterprise

Dr. Liyun HAN
360 Dipper Research, the Future Security Labs
2020.07.29 @ UN IEG Conference
The Overall Scale of Cyber Underground Economy

- **Top companies paying for cyber security vulnerabilities per minute in 2018**: $25/min

- **Global economic loss per minute due to cybercrime in 2018**: $2.9 million/min

- **Estimated global economic loss per minute due to ransomware attacks in 2019**: $222,184/min

From: The Cybersecurity Law Research Center of the Third Research Institute of the Ministry of Public Security P.R.C.
360 Mobile Guard Statistics: Mobile Malware

The development trend of mobile malware

Unit: 10 thousand

- The number of malicious programs blocked
- Increased number of malicious programs
- Linear (the number of malicious programs blocked)
360 Mobile Guard Statistics: Internet Fraud

The distribution of Internet fraud types

Statistics according to the number of reports:
- Financial management: 30.2%
- Gambling: 14.3%
- Fake shopping: 8.7%
- Online game trading: 8.7%
- Making friends: 8.5%
- Identity theft: 7.2%
- Virtual merchandise: 2.4%
- Others: 2.2%

Statistics according to the amount involved:
- Financial management: 37.8%
- Gambling: 31.1%
- Fake part-time job: 15.9%
- Identity theft: 11.5%
- Fake part-time: 9.0%
- Making friends: 4.1%
- Fake shopping: 3.3%
- Account theft: 0.7%
- Red envelope: 0.6%
- Others: 0.3%
How to Understand Cyber crime?

### Typical Cybercrime

1. **Traditional E-crime**
   - **Tech**: Fake IP address, URL redirection, botnet
   - **Crime**: Telecom fraud, Internet gambling, spreading pornography via chatroom, online social suicide, copyright infringement

2. **Crime enabled by hacking and defense technology**
   - **Tech**: exploiting Vulnerabilities, ransomware, Malicious Trojan
   - **Crime**: Illegal intrusion, control, and destruction of computer information systems, stealing data, production and spread of viruses, and paralysis of systems

### Typical Characteristic

- **Industrialization, the chain is long and tight**
  - The upper reaches: the hackers to provide technologies
  - The middle reaches: black production gangs
  - The lower reaches: various related organizations who support black production gangs.

- **Grouped Form**
  - It involves cross-department, cross-industry, cross-platform and even cross-border criminal actions, forming a close network loop

- **Increasingly enhanced technical means and anti-reconnaissance capabilities**
Long Chain Attack by Hacker Penetration

Criminal

Exploiting vulnerability

Smart Appliances

Get phone permissions by Malicious Trojan

Employee’s phone

OA server

Industrial Control Server

Intranet

Target to attack

Obtain legal credentials to entry

Send messages with legal identity

Production shutdown

Obtain valid credentials and legally entry

Serious security incidents may happen though the hacker’s behavior in the intranet environment seems to be legal.
Black Production Chain of Malware

Exploiting the malicious Trojan

01
- Remote control
- Traffic hijacking
- Botnet
- Hacking
- Malicious downloading

Spreading via smartphone

02
- Downloading maliciously implanted viruses through APP
- Spreading malware through mobile web pages
- Spreading malware through scanning QR codes by mobile phone users
- Spreading through communication software email

03

Main types of cybercrime

07.

1. DDOS attack, traffic hijacking
2. Illegal trading of personal information stolen by malicious programs
3. Use malware as tools to implement fraud and extortion
Three Key Steps for Cyber Crime Governance

1. **Individual Protection**
   - Prevention can kill crime in the cradle

2. **Governance of Public Network Environment**
   - The key influencing factor of prevention is the capability of network attack and defense tech

3. **The judicial punishment**
   - To improve the pre-capability and the capability of identifying, detecting, responding, and controlling
Case: Anti-phishing Websites Protection

- Accurately detecting phishing sites
- Detecting the rogue base station
- Blocking phishing websites through threat intelligence sharing mechanism and reporting in real time

Protection

- All round blocking phishing websites
- For PCs and mobile devices

Investigation & Analysis

- Real-time query of phishing websites
- Malicious sample storage
- Customized report
Technology-driven Cybercrime Prevention

**Technology**
- Big data analysis
- Multi-dimensional detection engine
- Vulnerability mining
- PC & mobile endpoint protection technology
- Traffic monitoring
- Deception defense

**Platform**
- Security analysis and response platform
- Financial fraud prevention platform
- Telecom fraud prevention
- Microscope APP scanning platform
- Cloud security service

**Crime prevention scenario**
- Identification, detection, interception during anti-fraud, anti-gambling, anti-pornography and others underground economy industry combating process
- Security enhancement in industrial internet and various fields of information infrastructure, such as BFSI, server provider, Energy and others.
Cases and efforts of 360

1. Malware Blocking 110 million times per day

2. Vulnerability Discovering
   Discovered more than 2,000 CVE vulnerabilities from mainstream global vendors including Apple, Google, Microsoft, Huawei, Qualcomm, VMWare, etc, and assisted them in vulnerability location and repair, which can reduces the possibility of criminals exploiting vulnerabilities to commit crimes

3. 360 University of Cybersecurity
   Committed to cybersecurity education for users and cyber security practitioner in China and some developing countries
Responsibility · Cooperation · Ecosystem

High-level responsibility
- Promote the industrial safety ecosystem
  - The Security + Internet

Public Responsibility
- Prevent cybercrime

Industry Collaboration
- Security data sharing
- Promote industry safety standards

Platform Responsibility
- Security technology operation and maintenance
- Platform information governance

Communication with Academia and Industry

Combination of Prevention Combating

Multi-participating And collaborative ecosystem

Innovative Technology Platform

Combination of Prevention Combating
We are looking forward to the further discussion and research with you.

Email:
Dr. HAN Liyun
Hanliyun1@360.cn

For academic cooperation please contact via:
Futurelab@360.cn

THANKS