Analysis of new cybercrimes in the hyper-connected society: Focusing on the cases of South Korea

Chang-Moo Lee, Ph.D.
Dept. of Industrial Security
Chung-Ang University
Seoul, South Korea

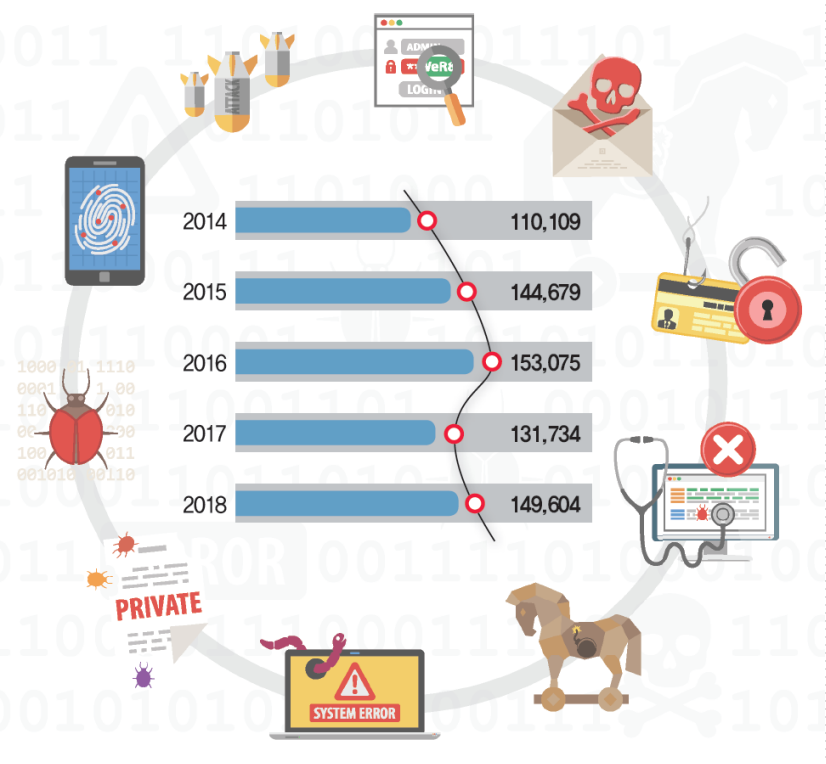
Introduction

- The advent of a hyper-connected society has resulted in a new type of cybercrime that never existed.
- Such new cybercrimes are difficult to predict due to hyper-connectivity and superintelligence. It is also difficult to identify the damage and method of cybercrimes.
- The new cybercrimes cause emotional, psychological and ethical damage as well as economic and industrial damage.

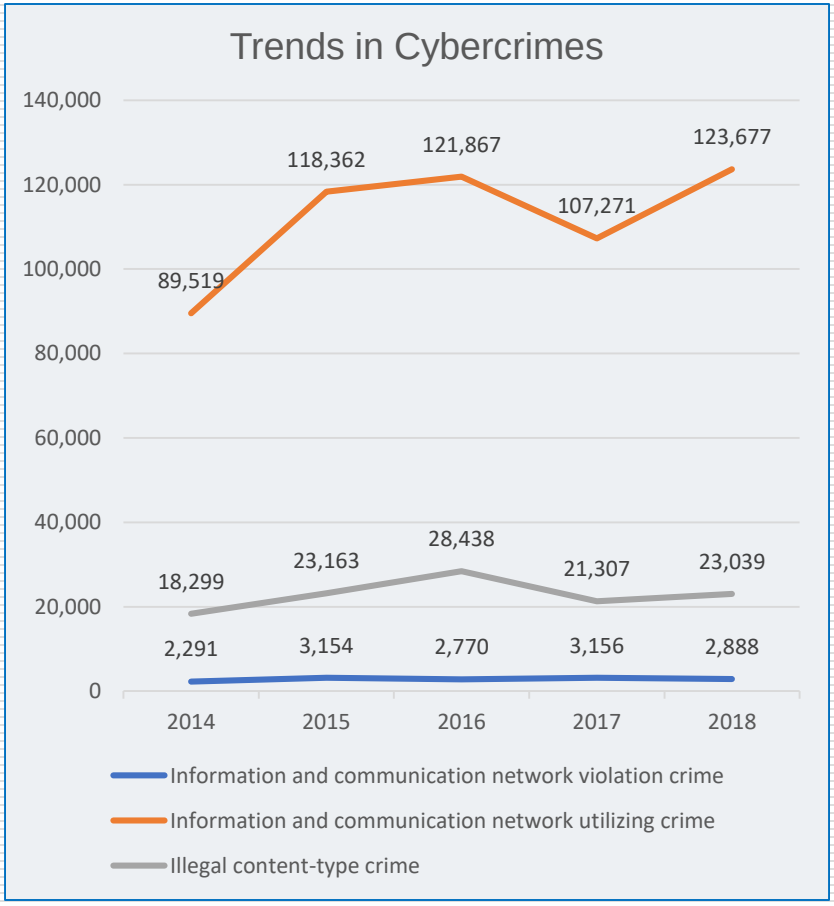
Trends in Cybercrimes in South Korea

- In 2018, there were 149,604 cyber crimes in South Korea, an increase of about 13.6 percent from 131,734 in 2017.

- The number of such incidents is close to the highest level in the last five years (153,075 in 2016), and the trend of stalling increases is continuing again.



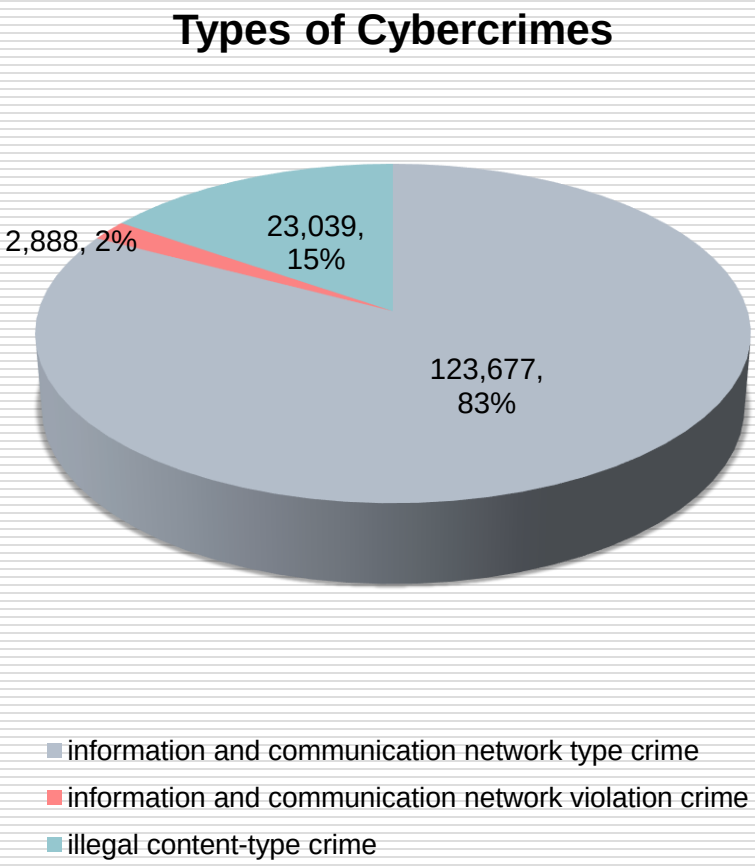
Trends in Cybercrimes in South Korea



- Cyber crimes attacking network such as hacking and distribution of malicious programs reduced by 8.5 percent from 2017 to 2018.
- But cyber crimes using internet, such as internet fraud and cyber financial crimes, increased by 15.3 percent during the same period.
- Cyber crimes of illegal contents, such as cyber pornography and cyber gambling, also increased by 8.1%.

Types of Cybercrimes

- **Illegal content-type crime**
  - Cyber pornography, cyber gambling, cyber defamation …
- **Information and communication network violation crime**
  - Hacking, DDoS, Malware …
- **Information and communication network utilizing crime**
  - Internet fraud, Cyber-Financial Crime, Personal information protection leakage …



Emergence of New Cybercrimes

- Along with the growth of traditional cyber crimes such as internet fraud and cyber defamation, a new type of cybercrime has also emerged.
  - New types of phishing using social engineering techniques have been increasing in recent years.
  - Public interest in cryptocurrencies has decreased, but related crimes such as hacking into cryptocurrency exchanges continue to occur.
  - Cybercrimes through DarkNet, a website that is not connected to regular browsers (chrome, Explorer, etc.), have gradually been growing.

New types of phishing using social engineering techniques

Email hacking (spear phishing, smishing …)

- For email hacking, malicious codes are most commonly used in attachments such as promotional emails disguised as free gift or employment.
- Recently, just accessing a specific website can cause a malicious program (drive by download attack).

1. Providing content that is forced to open email
2. Obtaining with a covert attack

Targeting

Attack

Damage

1. Anyone who can receive external email
2. Server administrator, financial officer, etc.

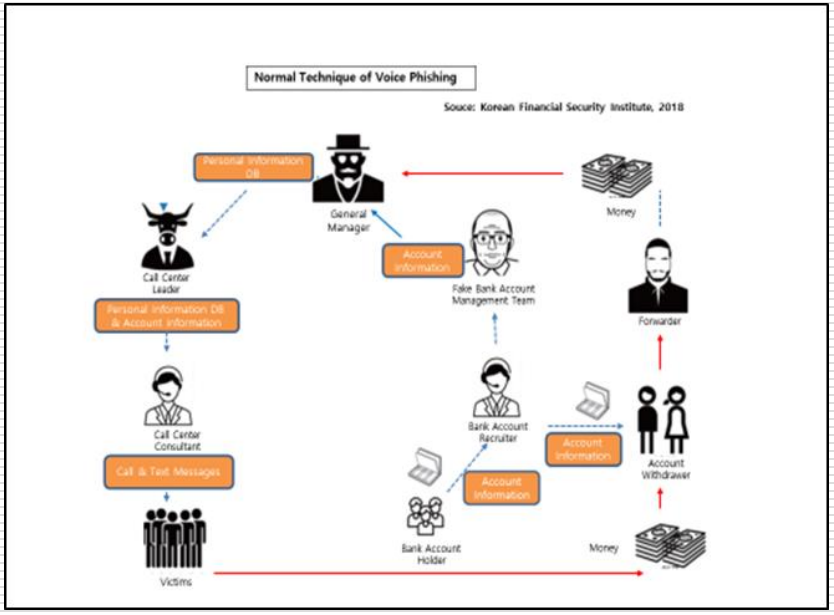
1. Ransomware infection, phishing, etc.
2. Information leakage and security accident

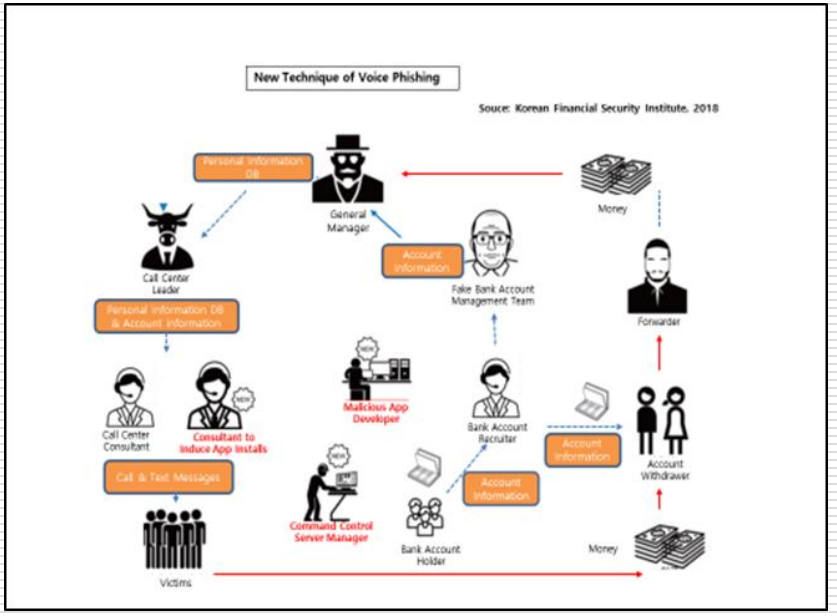
Domain name spoofing

- This method is to create and deceive e-mail addresses similar to those of the counterparties, the most common in South Korea, such as inserting certain characters, changing order, and changing characters that are easy to confuse, such as 1 and l(L).

New Way of Voice Phishing

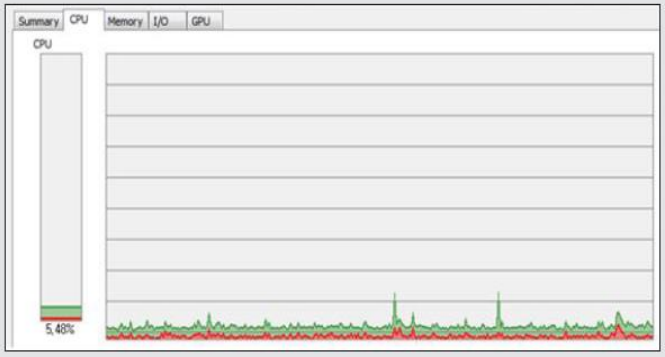
- The voice phishing techniques are getting more and more sophisticated day by day. Voice phishing is divided into two main types: impersonating government agents like police officers, and loan fraud.
- Recently, a new method of introducing a malicious android app to a user by impersonating a financial company, and then intercepting the phone when a user infected with a malicious application tries to dial a financial company.
- When an infected device dials a financial company's primary number, it appears to dial the primary number on the terminal screen, but in reality it is linked to the specific number that the attacker has set up and the victim is deceived by the attacker's social engineering technique.



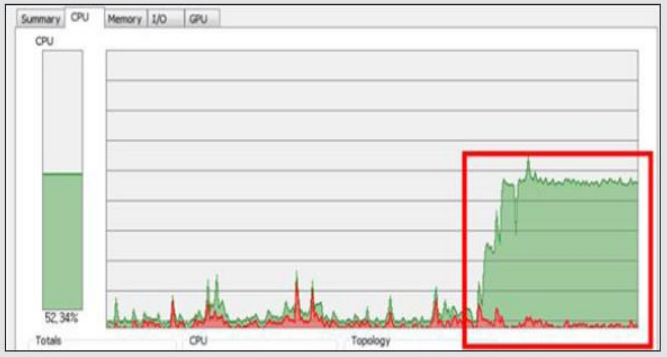


Cryptojacking

- It is a compound word of cryptocurrency and hijacking, and refers to a crime in which a hacker secretly infects a user's PC to a malicious code and uses it for mining a cryptocurrency
- In addition to the computer's poor performance, the infection of these cryptojacking malware causes excessive use of computer resources, which can lead to an explosion in electricity bills.
- Since the recent discovery of a PC infected with a cryptojackling malware shows that it consumes about 2 to 30 times more power than a regular PC, if the electricity bill has suddenly increased, it can be suspected that the PC has infected malicious code.

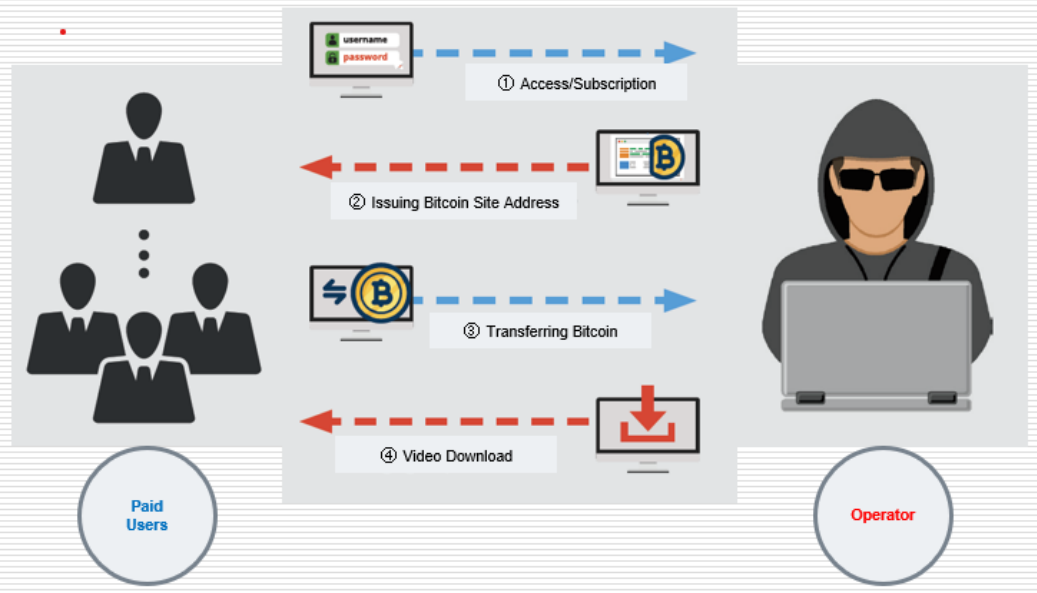


CPU use rate before infection with a cryptojacking malware

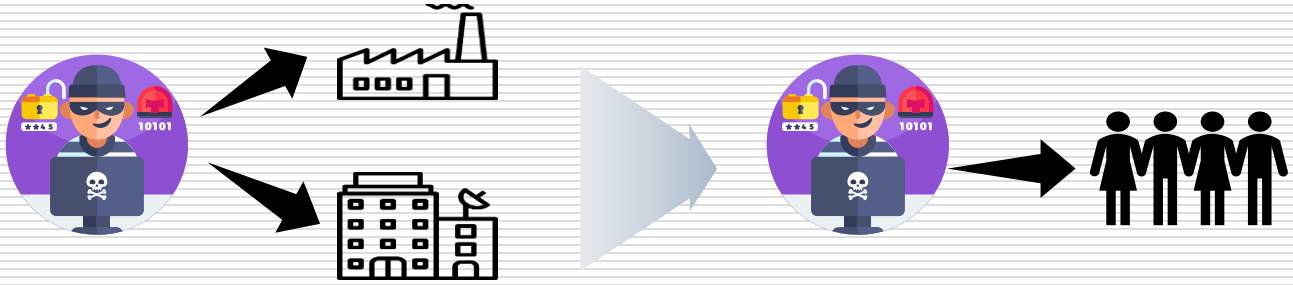


CPU use rate after infection with a cryptojacking malware (50% ↑)

- Cybercrime through DarkNet
  - Cyberspace, called 'DarkNet,' is characterized by a separate encrypted network that can only be accessed through a specific browser, making it difficult to trace IP.
  - Due to these characteristics, transactions of personal information, drugs, and hacking tools through the dark net are actively carried out.
  - The recent case: a cybercriminal ran a site that provided child pornography on the dark net.
  - The Web site operated by the criminal had more than 1 million members and 360,000 video downloads. There were 4,000 paid members, 156 of them Koreans, and all Korean suspects were arrested.



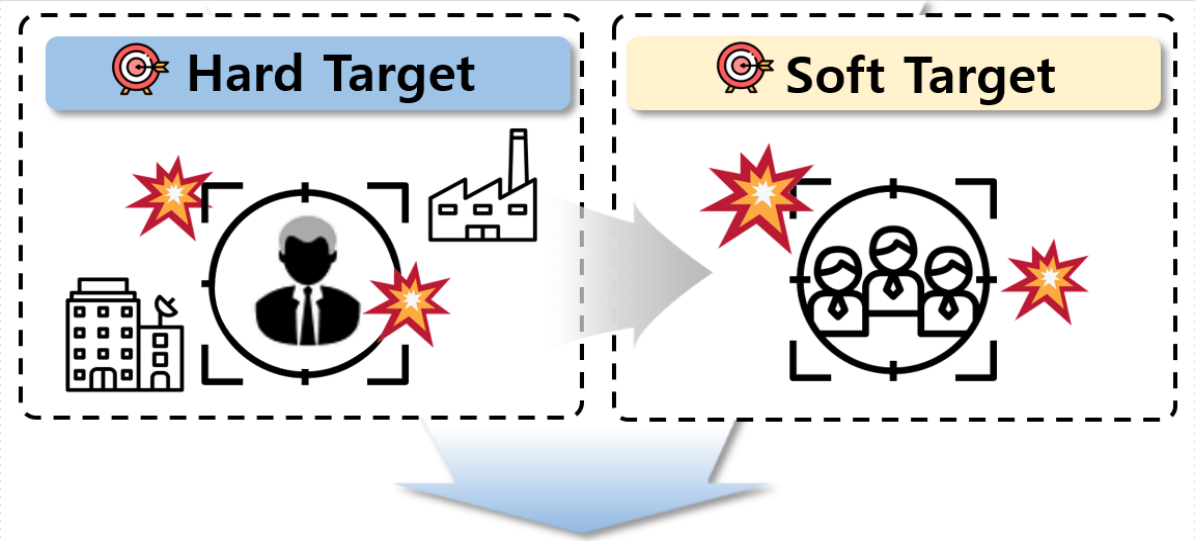
Analysis of New Cybercrimes



Target of Traditional Cybercrimes
"System · Network" : Specific Target

Target of New Cybercrimes
"User" : General Target

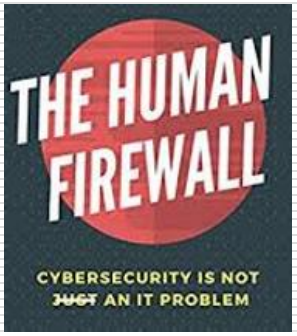
Evolution of Cybercrime



- The scope of security threats is expanding due to the expansion of cybercrime domains.
- Social risks are also increasing due to an increase in cybercrimes targeting human beings such as users.

Cybercrime & Human Factor

- Cyber Security depends on
  - Technology
  - Process
  - People



- All of these factors are important, but "**people**" factor has been overlooked.!!
  - Advances in security technologies lead to access to the most vulnerable "people" who can have direct access to important information
  - Need to consider **human factor**

Human Factor & Social Engineering Technique

- Cybercrime utilizing human factor usually depends on **social engineering techniques** such as spear phishing, pretexting, and so on.
- Social engineering refers to a comprehensive technique of obtaining important information by using ‘people.'
- “Social engineering is an attempt to appeal to potential victims with human emotions such as excitement or fear, or instill confidence and responsibility or persuade them through human relationships.” Gao & Kim (2007),
- Many hackers use social engineering methods because **'people'** are the weakest and most vulnerable to security.
- The stronger the technical security system, the more socio-engineering method is preferred.

Countermeasure against New Cybercrimes

- Effective countermeasures should include the solutions based on human factors

- Example: Malicious email mock drills
  - Malicious e-mails are regularly sent to executives and employees to identify vulnerable personnel and to provide training to prevent recurrence.

Title of email	Sender's address
[email] Find Wrong Picture EVENT~!	Good Opportunity / shopping@gnarket.com
[National Police Agency] Notice of Traffic Violation & Imposition Fine	National Police Agency / police@mail.com
[Guide] Gccgle Password Change Request	help@gccgle.com

- As a result of the mock training in South Korea, the rate of opening malicious mail has decreased from 50 percent to 30 percent.

Conclusion

- Despite the rapid growth of new types of cybercrimes, the countermeasures against them seem to be ineffective.
- This is mainly because new types of cybercrimes have been **utilizing human factors**, while current measures mostly depend upon technological solutions.
- Therefore, it is necessary to consider **human factors** for the effective solutions of new cybercrimes, such as building **human firewalls**.
- Human firewalls could be built by strengthening **security awareness** and continuing **security education**. Otherwise, cyber victimization will be repeated.

Thank You