



We Will be a **Global Leader**
in the **Internet & Security Field**

KrCERT/CC
Intelligence Cooperation Team
Thomas Kim



1

What is it like to be working in a field of Cyber SECURITY?



My boss thinks that I am



My co-worker thinks that I am



My friends think that I am



My ex-girlfriend thinks that I am



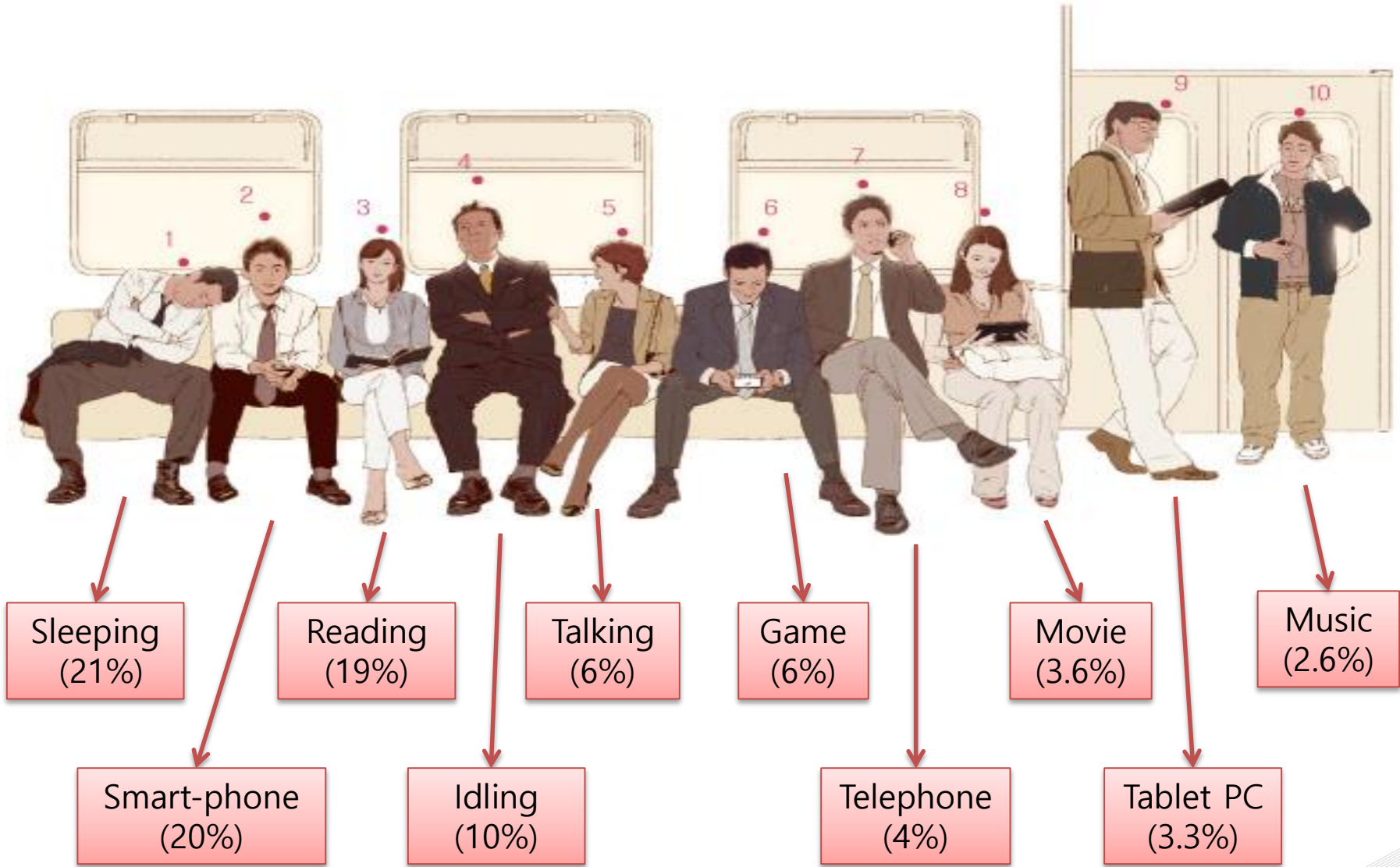
My parents think that I am

2 What is like to live in...?



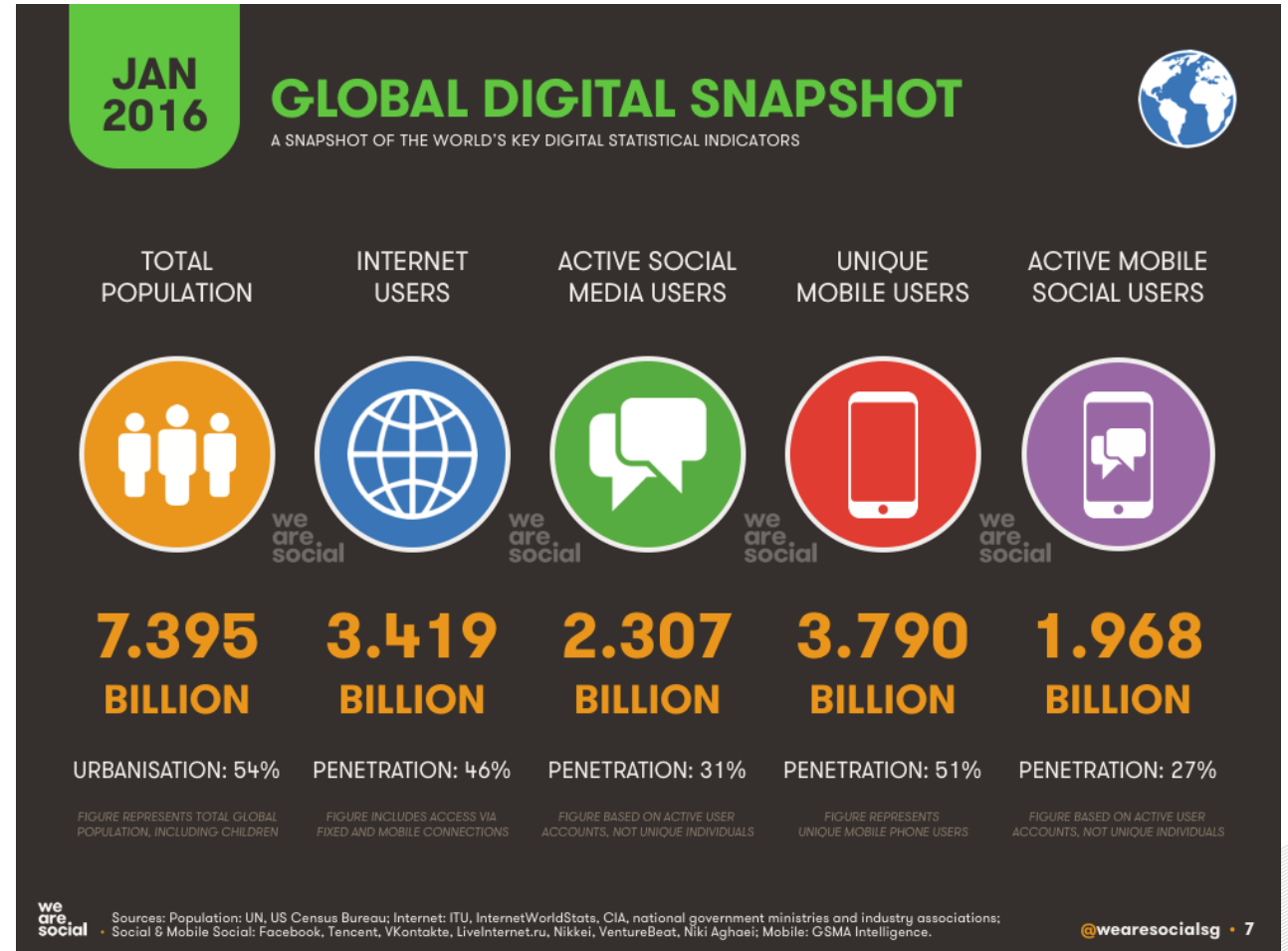
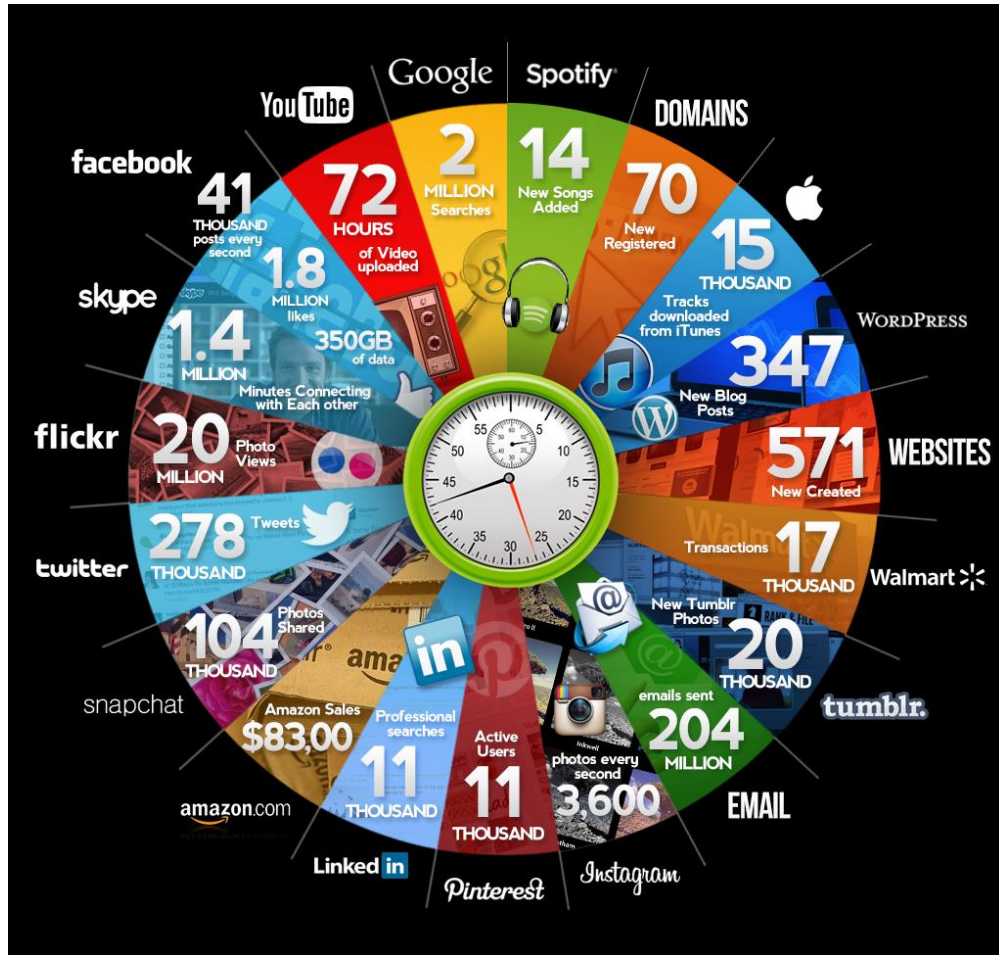
3

Snapshot of South Korea Subway

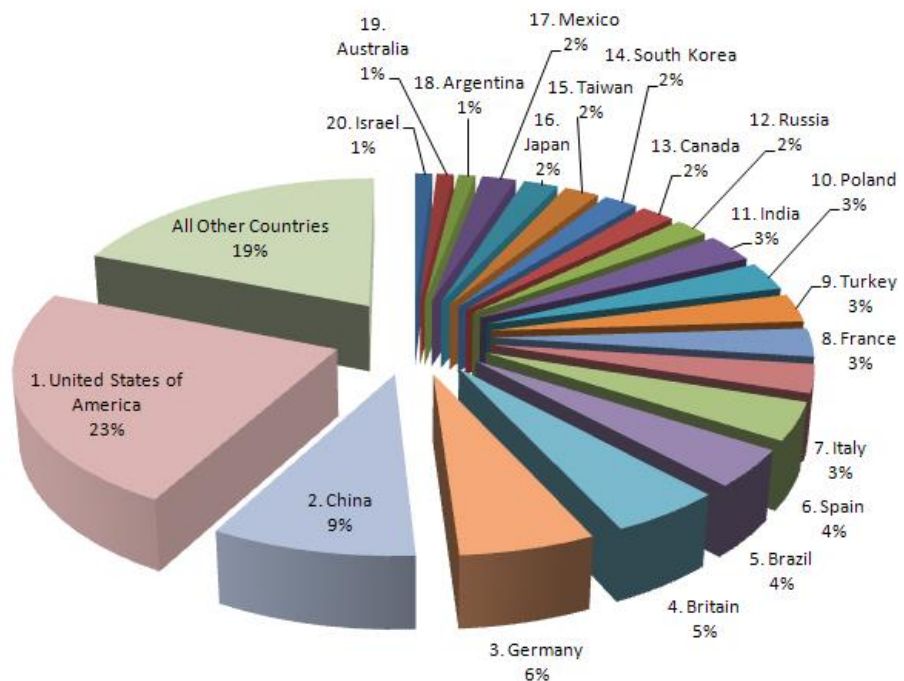


4

What is happening in the “http://world-wide-web”

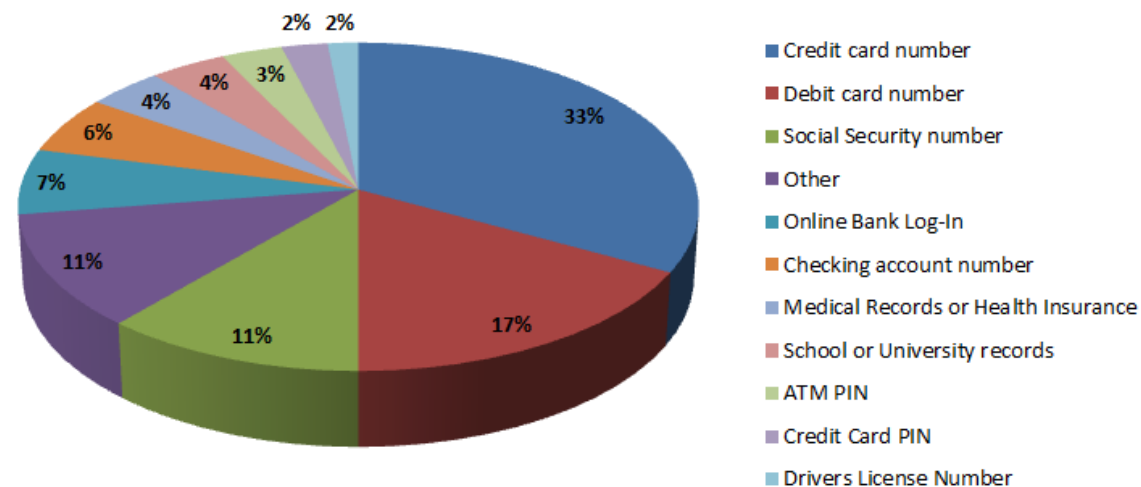


2016 Cyber Threat Report



Cybercrime: Top 20 Countries

What is stolen the most?



For more info please visit :

<http://map.norsecorp.com>

<https://www.fireeye.com/cyber-map/threat-map.html>

<https://cybermap.kaspersky.com/>

<https://threatmap.fortiguard.com/>

<https://community.blueliv.com/map/>

<http://www.pixalate.com/map/>

<http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17255&view=map>

<https://map.lookingglasscyber.com/>

<https://threatmap.checkpoint.com/ThreatPortal/livemap.html>

<https://www.threatmetrix.com/threatmetrix-labs/web-fraud-map/>

<http://globalsecuritymap.com/>

<https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp>

So what is “Cyber Security”?

- **Cyber Security?** → is to protect and make safe environment for users from hacking, DDoS, web-defacement, spam, phishing and etc.



Hacking
(Extract information)



Spam
(Email)



DDoS attack
(Distribute Denial of Service)



Web Defacement




Phishing

So what is “Cyber Incident”?(1/5)


Hacking

- **Unauthorized access to targeted system**
 - Gain ID, Password to extract information
 - Use S/W vulnerability to destroy system or manipulate
- **Spread malware, remote control**

The 10 Most Popular iPhone Passwords, Starring '1234'
By Chris Gaymer on June 13, 2011



Easy Password




Gain ID, PW




S/W vulnerability



Unauthorized access



Extract Confidential Information



Destroying target System

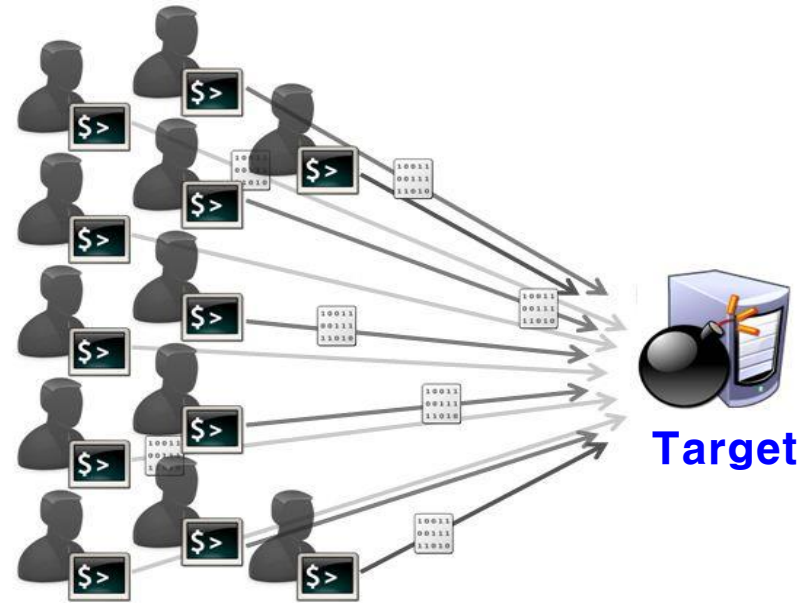
So what is “Cyber Incident”?(2/5)

Distribute Denial of Service

- DDoS(Distributed Denial of Service) – use all the resources
- Attacker must have many infected PC(bots) to create a massive traffic to targeted system



Bottleneck in highway

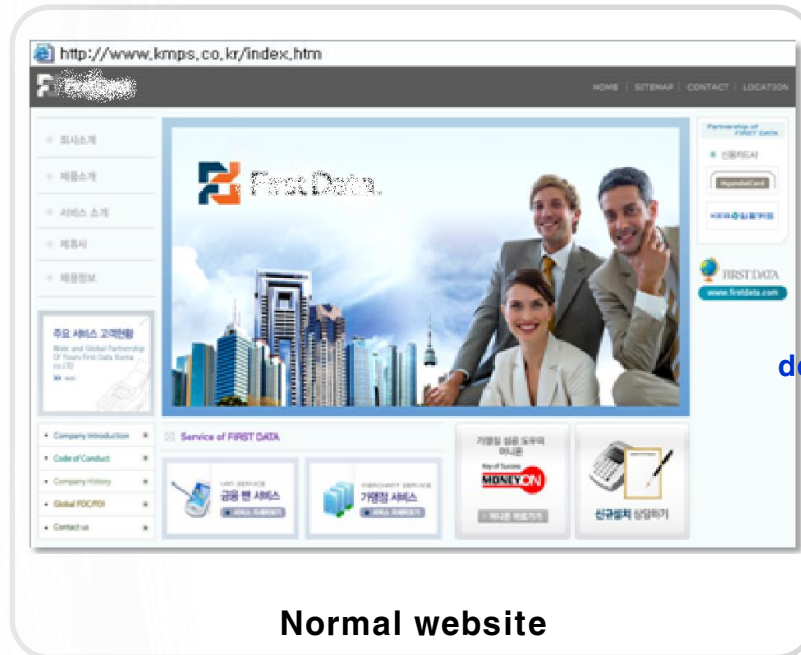


Infected PC(bots)

So what is “Cyber Incident”?(3/5)

Homepage Defacement

- Switch website image to reveal hacking
- Let society or certain group to acknowledge their fault and trust



Web defacement



So what is “Cyber Incident”?(4/5)

Phishing and smishing

- (Voice Phishing) Pretend as gov. official or banker to extract money
- (Phishing Site) Fake website(gov., Internet bank, shopping mall)
- (Smishing) SMS+Phising, send URL(infection site) through TEXT msg.



보이스 피싱



가짜 KB국민은행 웹사이트



세월호 침몰 관련 스미싱

So what is "Cyber Incident"?(5/5)

SPAM

- SPAM used to be a commercial focused email but it can be used as a text msg.
- Personal information is already extracted before sending SPAM

Major Media

Email SMS/MMS Web board

Fax Instant Messenger Telephone

Major Content

gambling Loan

Illegal drug Adult site

Security Trend - Malware

- Enhanced and sophisticated malware now targets Nation-wide terror
- Acceleration Step
 - 1986, 'Brain' Virus : USA to ROK took **3 years**
 - 1998, 'CIH' Virus : Taiwan to ROK **1 month**
 - 2003, 1.25 Terror : 'Slammer worm' took **a few min.** spread to World wide
 - 2009, 7.7 DDoS Attack : **(Realtime)** Changed its target(USA to ROK)
 - 2011, 3.4 DDoS Attack : **(Realtime)** Changed its method of attack
 - 2013, 3.20 Cyber Terror : **Fiancial/News** Server(33),PC(31,609),ATM(16,320)
 - 2014, Nuclear Power Plant : Expanded its target to **Critical infrastructure**



Auto-reproduction, showing off
Single bombing ('90)



Infection spread
Financial purpose
Carpet bombing (early/middle '00)

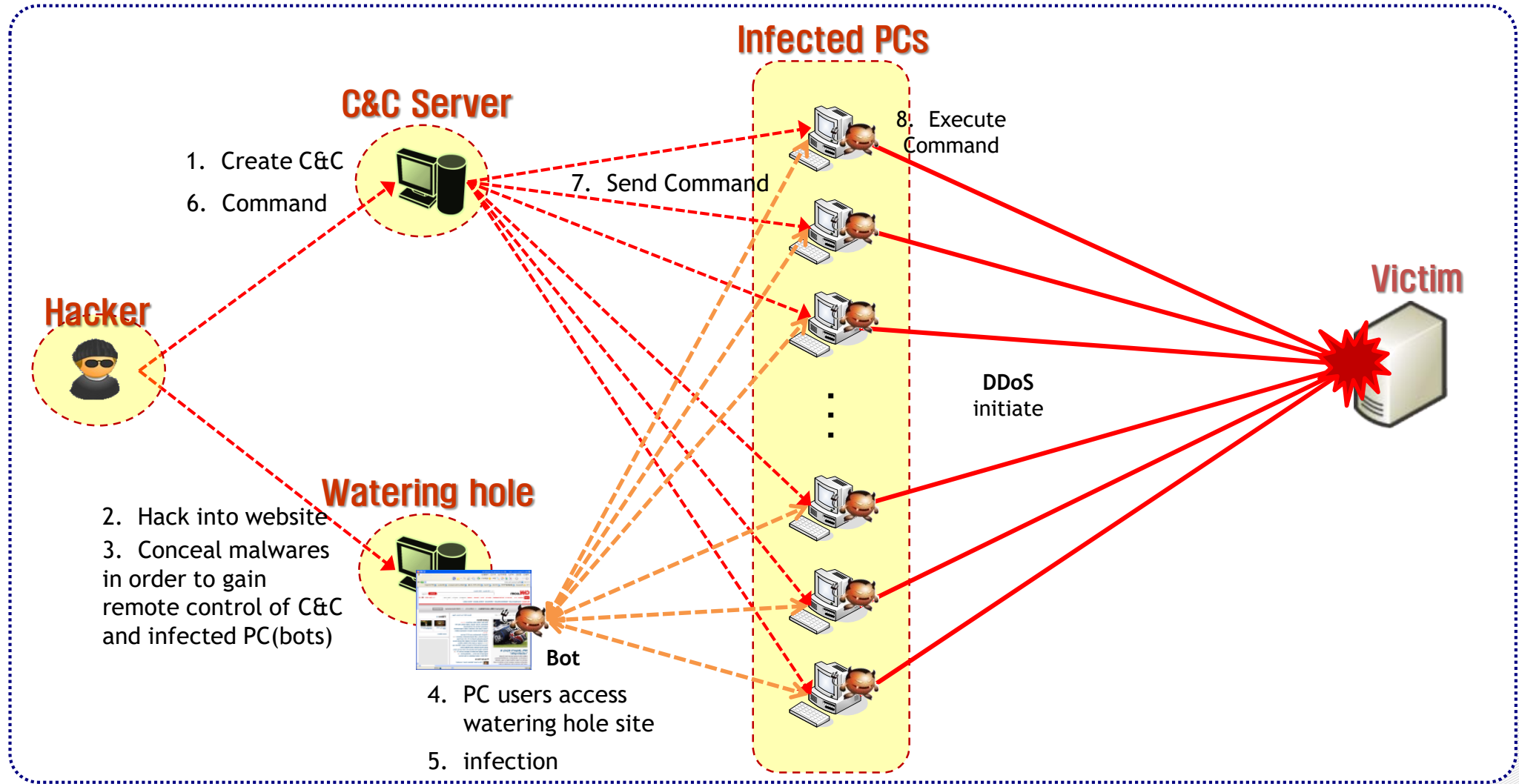


Conceal, sophisticated,
politic focused cyber terror
Targeted bombing (middle '00)

※ **Malicious Code/Malware?**

- **Malware**, short for **malicious software**, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Security Trend - DDoS



Cyber Incident in per day



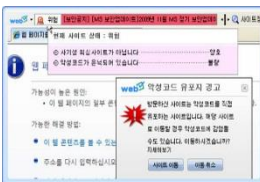
- **Emerge of Malicious Code: 1,435**
(Collected by KISA : 523,624)



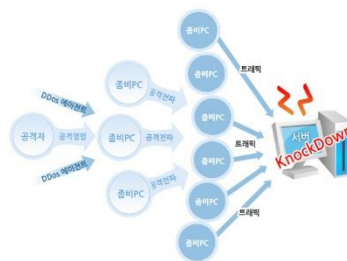
- **Emerge of Mobile Malicious Code: 101**
(McAfee : 36,699)



- **Web Defacement : 8.7**
(Detected by KISA : 3,157)



- **Malicious Code Distribution Websites : 35.7**
(Detected & treated by KISA : 13,018)



- **Zombie PC : 8,821**
(Average Flow in KISA sinkhole)
(per day)



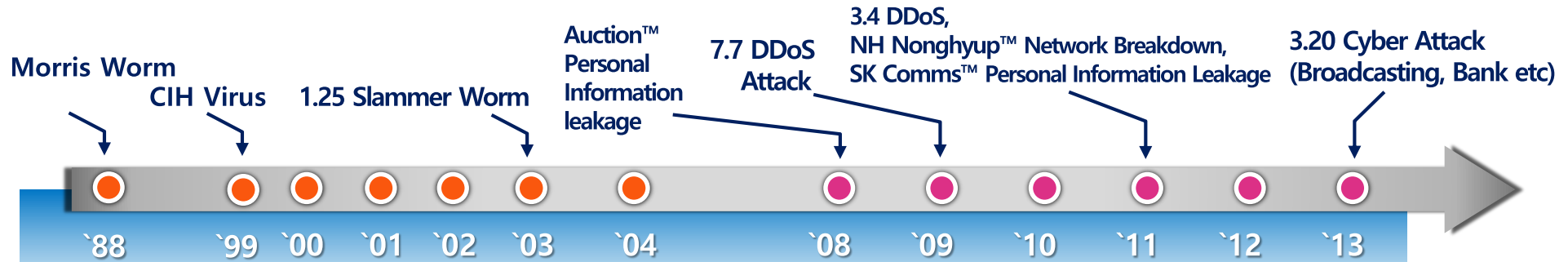
- **DDoS Attack : 1.5**
 - * Report from KISA : 91
 - * Detected by KISA IX line : 318
 - * KISA Cyber Shelter : 138
- **Phishing Website : 19**
(Responded by KISA : 6,944)



- **illegal Spam : 89,628**
(Responded by KISA : 32,714,062)

Chronological order Internet Incident Event

◆ Targeting Enterprise/Government using DDoS attack and APT



Internet incident occurs targeting enterprises using APT

- Targeting and attacking specific subject such as Broadcasting, NH NongHyup™, Game Company, etc

DDoS attack continuously occurs, but purpose has changed

- Financial Issue → Social Disorder(3.4 DDoS), Political issues and etc

Websites that are Impersonating Public organization(Rapid growth of Phishing websites)

- Impersonating financial, personal, portal websites → Public Prosecutor's office, national police, Financial Supervisory Service and etc

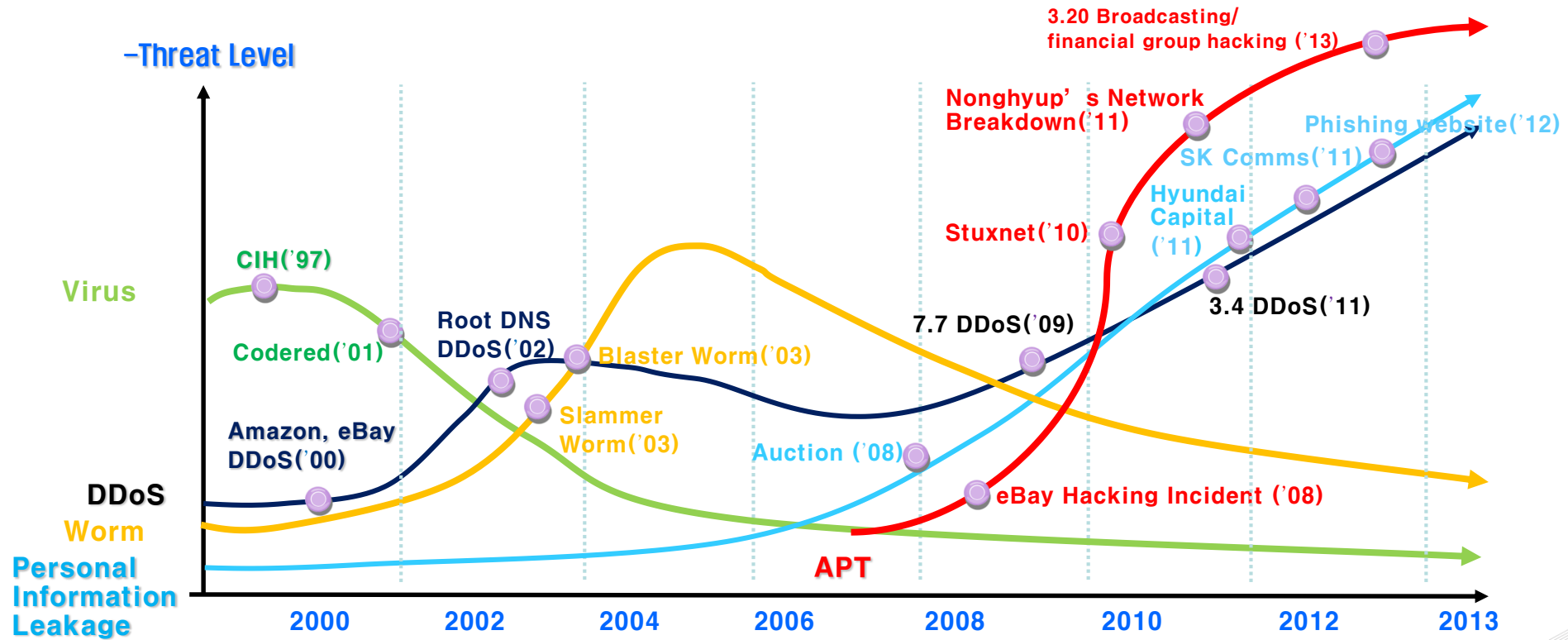
Spreading Malicious codes using the advantage of Popular Keywords, Social Issues

- Disguise as Boston terrorist, Credit card detailed statement and using popular keywords and social issues



Cyber Security Trends : Threat Increases Rapidly

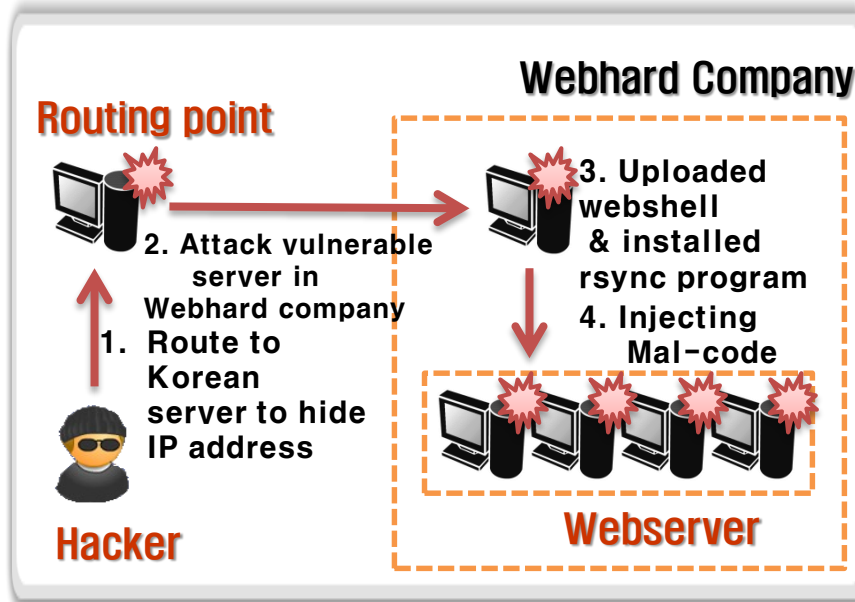
- ◆ Curiosity, self-esteem → extort money(by blackmail) → **social chaos, cyber terror**
- ◆ Manual → concealment, automation → **organized, intelligent**
- ◆ Individual system → large scale of network → **social infrastructures, nations**



▶ **APT(Advanced Persistent Threat)** are a cybercrime category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful.

Cause of Major Hacking Case

- Hackers are interested in vulnerable webhard websites**
 - 7.7('09), 3.4 ('11) DDoS attacks and NH Nonghyup incident ('11) were initiated using vulnerable webhard company's website(used as a distribution point)



< Case of OO Webhard company >

- Webhard hacking (total 194 cases) 64(33%) cases in 2012
- Recurrence percentage of 73%
37 website were hacked(total 233)

- KISA detected 162 webhard hacking cases

Num of incident	Num of site	Num of incident	Num sites
-	196	6 times	2
1 times	10	7 times	5
2 times	6	8 times	2
3 times	4	10 times	1
4 times	2	13 times	1
5 times	3	19 times	1

< Webhard hacking in 2012, KISA >

Security Advisory

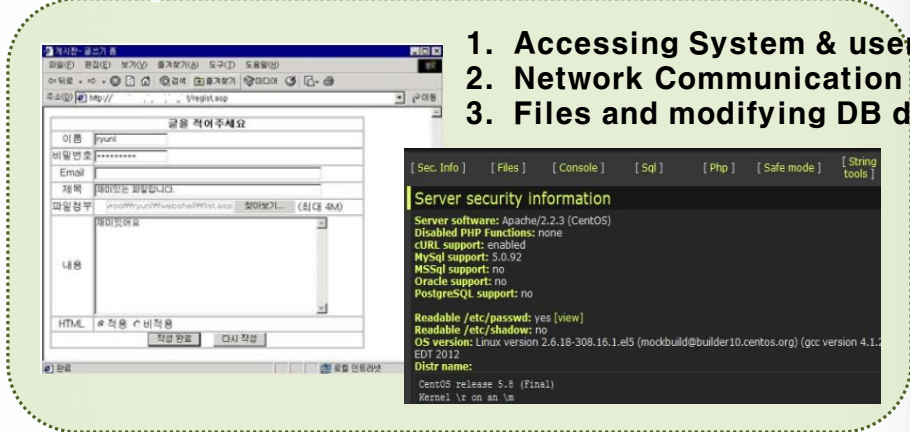
- Hacking activities in weekend(off duty for Admin) can create massive zombie PC
- Hacker's attacking webhard company will be continued and expected to get increased
- necessary to monitor webhard provider's website and increase security level

Cause of Major Hacking Case

- Abusing vulnerability of uploading webshell in web board(for 80% of incident)
- Once **Admin PC** is hacked, everything falls apart

Uploading Webshell

- Hacker uploaded a webshell as a attached file to web board. Shell script is executed when one open up the file



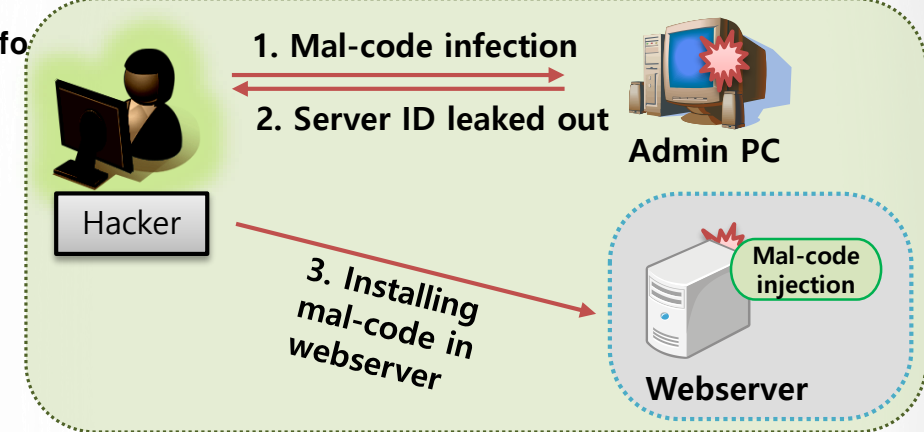
The image shows a web browser window with a login form and a terminal window. The login form has fields for '이름' (Name), '비밀번호' (Password), 'Email', '전화' (Phone), '관리자명' (Admin Name), and '내용' (Content). The terminal window displays 'Server security information' including details about Apache/2.2.3, MySQL support, OS version (Linux), and other system details.

1. Accessing System & user info
2. Network Communication
3. Files and modifying DB data

- ### Method of Prevention and Checking
- **check web board security config (security update)**
 - checking webshell installation using whistle(provided by KISA)

Hacking Admin PC

- IDs were leaked out when admin PC is hacked
- Hacker uses IDs from the target to access



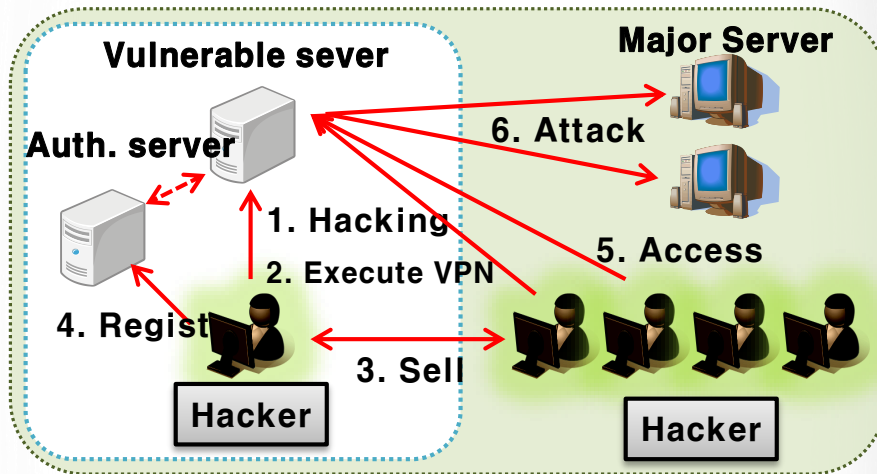
- ### Method of Prevention and Checking
- Use Admin PC in closed-network ONLY
 - execute weekly security patch and vaccine program

Cause of Major Hacking Case

- Used vulnerable(Domestic/International) website as mal-code routing point
- Used Rsync program to vulnerable servers as hacking tool

Abusing VPN Service

- Hacker sells auth keys to other hackers



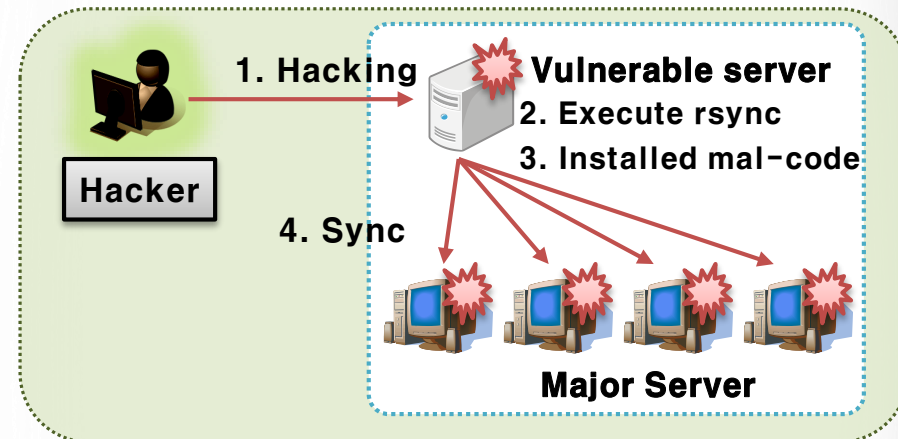
Method of Prevention and Checking

- check 1723 port for VPN service

```
tcp 0.0.0.0:1723 0.0.0.0:* LISTEN 11758/pptpd
```

Abusing rsync Program

- Used rsync program to synchronize target servers



Method of Prevention and Checking

- check rsync program config file(rsync.conf)

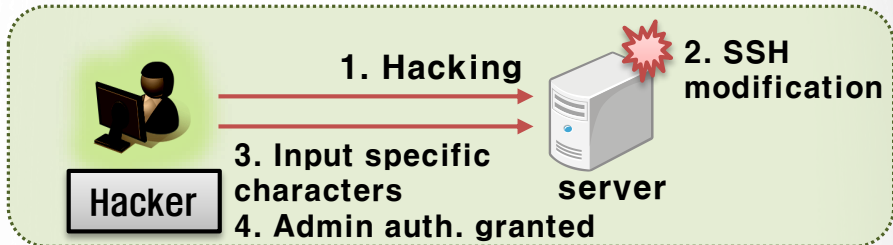
Ex of vulnerable config : `path = / ; uid = root ; gid = root`

Cause of Major Hacking Case

- SSH modification is the most favorite backdoor method of hacker
- Anyone can check the stroke key backdoor easily

SSH(Secure Shell) Backdoor (Linux)

- Hacker modified SSH program to use as backdoor



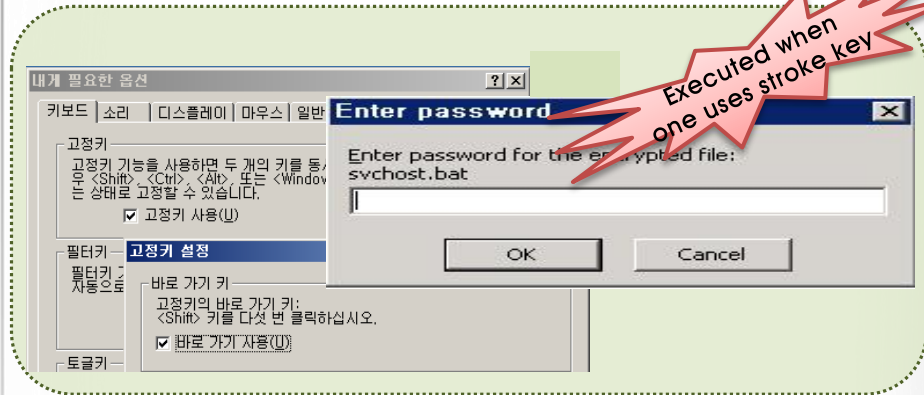
Method of Prevention and Checking

- tracing system call using strace command
- Check if there is any backdoor key using ssh, sshd, pam_unix.so

```
- Ex. of hacked file : (pam_unix.so)
-UN*X-PASS
KiTrapODExp!!! → Backdoor Key
Password:
%s :: %s → Key logging characters
```

Using Sticky Key & Backdoor(windows)

- Hacker uses stroke key(already registered in regist list) to initiate automate backdoor
- Stroke key function is for user convenience



Method of Prevention and Checking

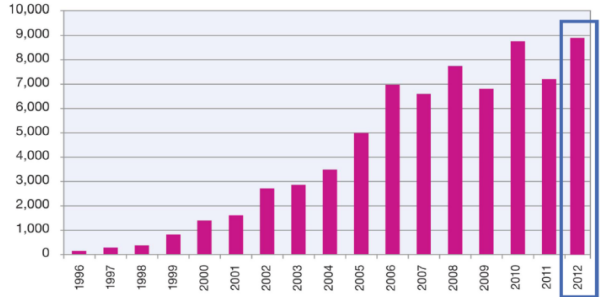
- pressing shift key 5 times,
- Check the execution of malicious code that hacker installed

Security Vulnerability trends

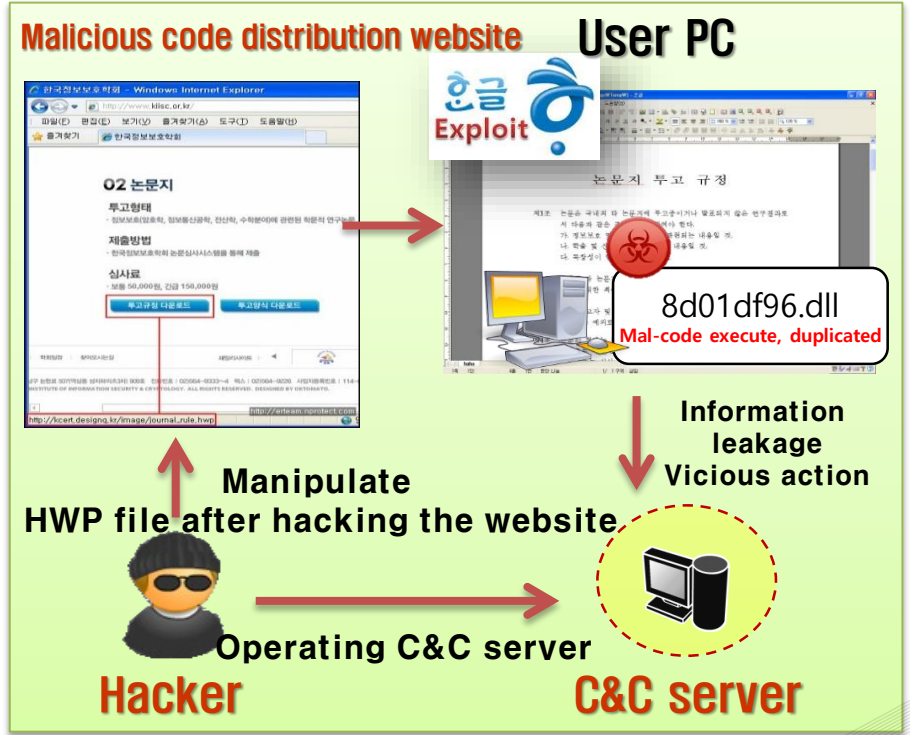
- ◆ Using H/W, S/W problem, insufficient security level that causes unauthorized users to access prior action or information
 - Security Patch : improving and fixing security vulnerabilities to prevent malicious code infection and errors

Vulnerability

● Security vulnerabilities are increasing due to development of ICT and new equipment & programs



- ◁ 1996-2012.6 security vulnerability, IBM ▷
- In Korea, malicious code was first introduced using HWP word processor file in 2011 and was rapidly increased in 2012
- Korea Information Protection Association announcement white paper(May, 2012)
- Zaoyutu dominium conflict paper (Nov 2012)

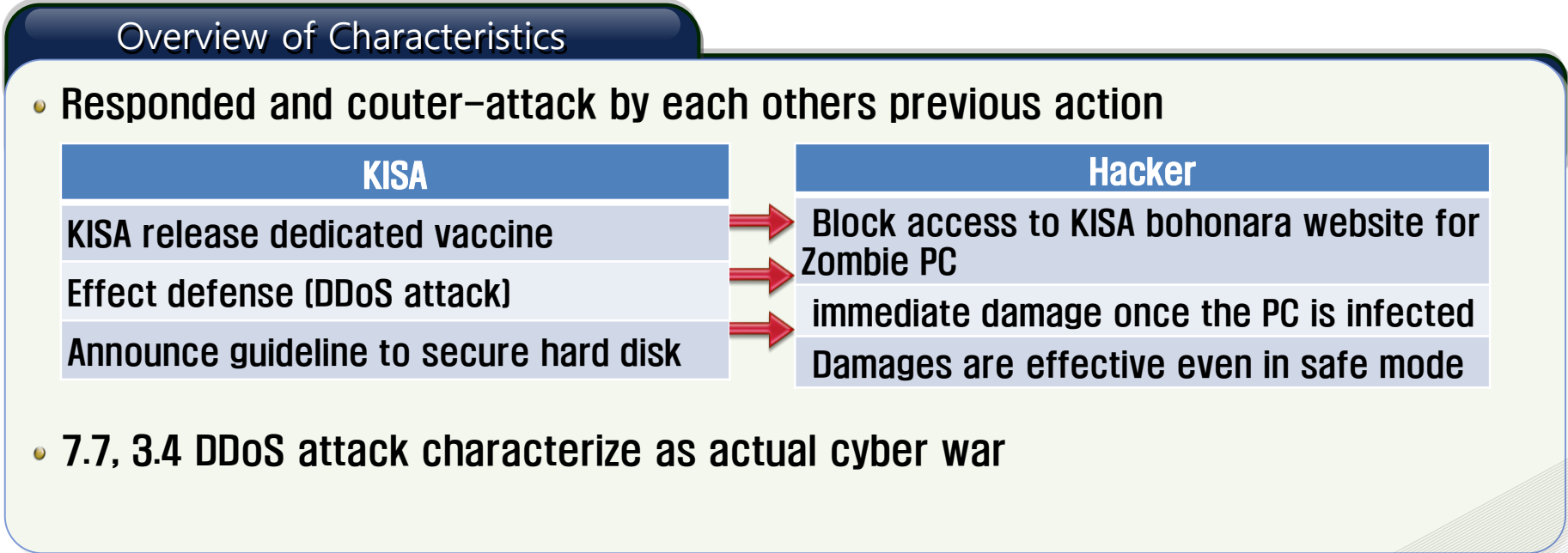


◁ Vulnerability case, using Hangeul word processor ▷

3.4 DDoS Attack

- **March 4th DDoS attack was more sophisticated attack than July 7th DDoS attack in 2009**
 - **Using Webhard Company(management oversight) as a distribution point to initiate DDoS attack targeting major website in Korea**

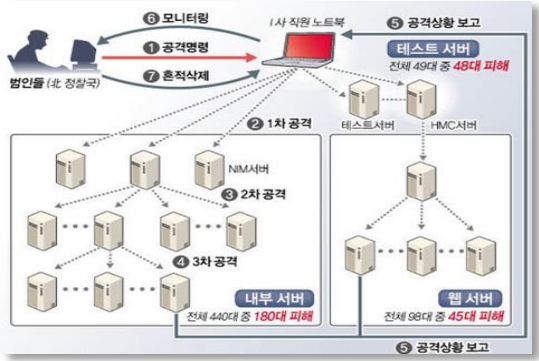
	3.4, 2011	7.7, 2009
• 40 Targets : 24 government • public institutes, 9 financial and 7 portal • online shopping mall		
• infection route and number of zombie PCs were very similar to July 7th but more destructive and intelligent		
	Number of Zombie PC	116,299
	Targets	40
	Number of blocked malware hidden website	748
	Tech support call for malfunction of hard disk	756
		1466



NH Nonghyup Bank Network Breakdown

❑ Created a social chaos by hacking NH Nonghyup network

Overview and Response



- '10. 9. 4 – maintain employee laptop was infected
 - ※ Hacker monitored more than 7 months and took out critical information secretly
- '11. 4.12 – installed attackable files → attack initiated → attack logs are wiped out
- '11. 4.13 – prosecutors office started to investigate
- '11. 4.19 – KISA cooperated to analyze evidence
- '11. 5. 3 – prosecutors office announced report (Hacked from NKorea)

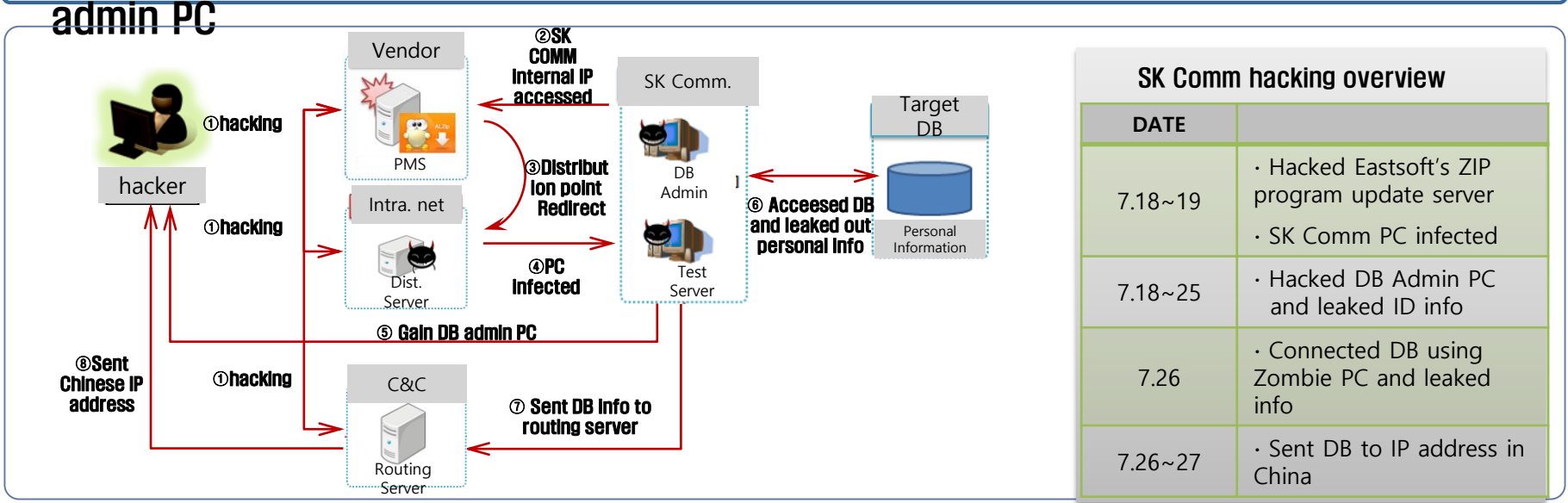
Cause and Fact

- **management oversight** : security monitoring system inadequate
 - management of maintains company → **unauth. laptop**
 - network policy → **a laptop can access from external network**
 - rely on maintains company (insufficient experts)
- **low budget support to information security**
 - information security budget compare to 2010 : **3.12%** : banking 3.4%, stock market 3.1%, credit card 3.6% (government suggested 5%)
 - ※ **81.4% of private company invest less than 1% on information security**
 - **NH Nonghyup invested 1.5%**, compare to '08 decreased 1/3



SK Communication Personal Information

□ SK Comm., Cyworld™ and NATE™ **3.5 million** personal info leaked out in 2011
 – remotely leaked out personal info from DB server after infecting SK Comm



What was the problem?

- Low security on free software (ZIP Program)
- SK Comm **insufficient internal security management**
 - using free ZIP software, DB admin PC was connected to external network

Overview of hacking characteristics

- Advanced Persistence Threat
- SK Comm DB sent to IP address in China

3.20 Cyber Terror

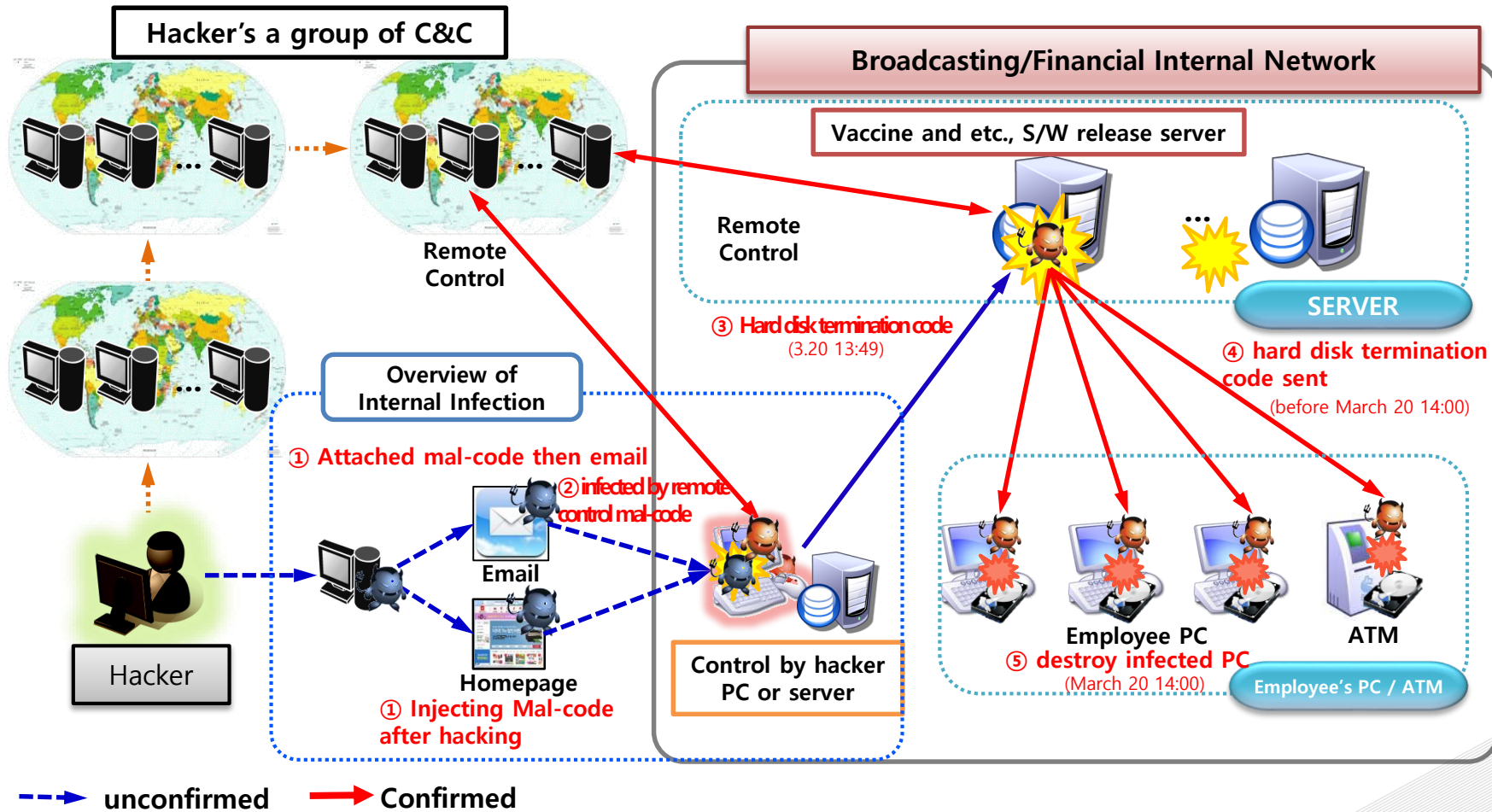
- **Destroyed 48,700 PC, servers and ATMs of 6 broadcasting, Financial institutes were damaged by cyber (March 20th)**
 - Using "www.nalsee.com" website as distribution point to infect users PC (about 800 PCs) (March 25th)
 - destroyed 58 Digital YTN website server's hard disk(main website service unavailable)(March 26th)
 - Wiped out the data of 14 North Korea(related) · conservative group's webpage (March 26th)

- **Number of 6 broadcasting · Financial institutes 'damaged systems were completely recovered (March 29)**
 - Digital YTN's 58 webserver are recovered(100%) (April 12)

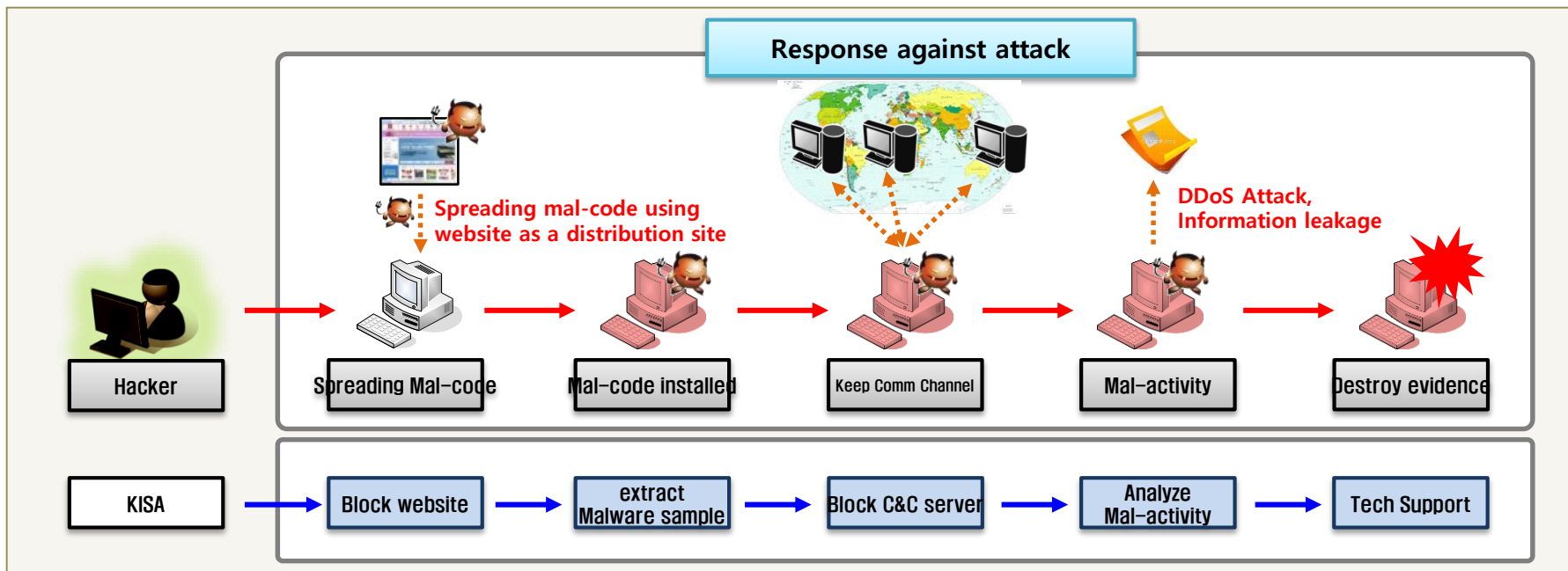


3.20 Cyber Terror(Details)

- Disguise as vaccine update to install mal-code after gaining control of internal server and PC
 - Spread mal-code to internal network as vaccine update using vaccine S/W release server
 - At 14:00 hacker commanded to destroy hard disk



3.20 Cyber Terror



- Dispatched agents to KBS, MBC, YTN, NH Nonghyup, Shinhan Bank(28 times)
- Confirmed location of hacker after analyzing Server, PC, firewall logs
 - Cooperated with vaccine companies (extracted 76 different types of malware) and released dedicated vaccine

Suggested security advisory to the victims and vulnerable targets

※ Security advisory : deleted malwares, increased security level

3.20 Cyber Terror

- 734 malware was reported, analyzed 76 malwares that has direct relationship with this incident
 - Confirmed 49 C&C IP addresses and blocked IP addresses
 - Prevented further malware activates(destroy hard disk, remote control)

<forced termination vaccine>

<extract info on mal-code development>

<Receive date from C&C>

<C&C IP address>

<Analysis in encryption methods >

<Analyzing System termination time and methods of coding>

3.20 Cyber Terror



Characteristics of 3.20 cyber terror

- Attacker hacked S/W update server and gained access to internal PC(Installed malware)
- Attacker analyzed targets' network and operating system then found vulnerabilities
- In admin PC, web server, s/w update server(attacker used various types of attack method)
- Attacker interferes using code obfuscation method, encryption to delay analysis process and used various types of malwares



접속시간	계정	PC이름	접속지역·IP
2012.06.28 15:12	AhnLab	WN2010	미국 209.237.253,
2012.06.28 16:51~16:53	AhnLab	WN2010	북한 175.45.178,
2012.07.02 05:58~06:09	AhnLab	WN2010	북한 175.45.178,
2012.07.06 19:31~19:32	AhnLab	WN2010	북한 175.45.178,
접속시간	계정	PC이름	접속지역·IP
2013.02.05 01:34~01:38	AhnLab	WN2010	북한 175.45.178,19
2013.02.05 01:55~01:56	AhnLab	WN2010	북한 175.45.178,19
2013.02.05 01:57~01:58	AhnLab	WN2010	북한 175.45.178,19

접속시간	계정	PC이름	접속지역·IP
2013-02-22 17:01:18	2013-02-22	17:01:18;235328	북한(해커)
2013-02-23 09:27:52	2013-02-23	09:27:52;2785671	미국(경유지)
2013-02-27 13:58:43	2013-02-27	13:58:43;162195062	
2013-02-27 17:49:00	2013-02-27	17:49:00;36725953	
2013-03-20 19:09:55	2013-03-20	19:09:55;41685281	
2013-03-12 18:07:32	2013-03-12	18:07:32;186786968	
2013-02-27 17:58:43	2013-02-27	17:58:43;36703312	

2012년 애경시 감염신호 생성코드

File pos: 1465800, 1465801, 1465802, 1465803, 1465804

금번 사용안 감염신호 생성코드

File pos: 1986, 1987, 1988, 1989, 1990

North Korea prepared for long time(from N.Korea)

- ①used 6 PCs in NKorea. Tried to access (in NKorea or route outside of country) 1,509 times
- ②used PCs in NKorea and uploaded 3 types of malware into financial institutes
- ③used IP address 222XXXXXXX (NKorea IP) tested their operation

Similar to previous attack methods

- ④used 22 malware distribution website(Previously 49)
- used same malware (number of 30 out of 76) through code analysis; code was very similar to previous malware.
- We think the attacker is same as before
- used same distribution website
- used malware that destroys hard disk
- left some characters (HASTATI, PRINCPES)

Comparing Incidents(1/3)

Category		7.7 DDoS	3.4 DDoS	NH Nonghyup	3.20 Attack
Attack Method		DDoS Attack	DDoS Attack	APT Attack	APT Attack
Target		36 domestic/international institutes webserver	40 Major institutes Web server	NH Noinghyup Servers	6 Broadcasting financial institutes and work PC
Preparing time		-	-	At least 7 months	At least 9 months
Malicious code infection System		Zombie PC (115,044)	Zombie PC (116,299)	Laptop that has access auth. to internal network	Internal update server and work PC (48,832)
Malicious code	characteristic	Planned DDoS attack	Planned DDoS attack	Used internal PC(that has access auth.) to attack servers	Attacked PCs using internal located server as planned
		Hard disk damaged (towards unspecific majority) (1,466)	Hard disk damaged (towards unspecific majority) (756)	Hard disk damaged (273)	Hard disk damaged (48,832)
	Infection route	Using vulnerable webhard website and end-user's PC	Using vulnerable webhard website and end-user's PC	Using vulnerable webhard website Laptop that has access authen. to internal network	Web vulnerability, email and web server
Code Obfuscation		○	○	○	○

Security Problem and Advisory

Category	Problem	Security advisory
Management system	o Security management oversight on Admin PC	o Increase security management level for information on management servers
	o Keeping access information to servers in Admin PC	
	o Any IP or ID can access critical server	
Managing update S/W	o Security management oversight on server security patch	o Increase security level for public use PC(S/W security updates)
	o No Check on defacement, modification of update files, authentication	
	o Exists on weak auth. process in update server	
System security management	o Exists development server that has low security level also that are connected to same network	o System management and security policy needs to be confirmed when introducing new system in internal network
	o Exists possibilities of abuse as hacker's routing point for attack	
	o No Password change	
	o No limitation to use any command (delete, format)	
	o Access granted to external connection	

Silly Mistakes in major Infrastructure

Major infra. Discrete network (Management oversight)	Critical infra needs to be separated from external network but it is connected to public Internet
Vulnerable Admin PC	Admin PC needs to be separate location but some management PC can access Admin PC
Vulnerable to remote management	Maintain employ needs to manage infrastructures in remote control
Vulnerable Outsourcing IT employee	Unauth. USB, laptop are used by outsourcing agents
Vulnerable security level of Internal PC	Low security level in USB solution, virus check and PC vaccine update
Lack of risk response manual	Insufficient detail guideline when there is cyber attack to recover and backup
Insufficient information security personnel	Insufficient security expert

KISA, Korea Internet & Security Agency

Brief History

- 2009.07 Korea Internet & Security Agency (merger of KISA, NIDA and KIICA)
- 2002.01 Korea IT International Cooperation Agency (KIICA)
- 1999.06 National Internet Development Agency (NIDA)
- 1996.04 Korea Information Security Agency (KISA)

Main Tasks

- Internet Promotion
 - New Internet Industry Promotion Support
 - Internet Address Resources Activation
- Internet Security
 - Information Security Countermeasure Development
 - Protection of Personal Information
- International Cooperation
 - Overseas Expansion of the Internet Industry
 - Global Collaboration on Internet Security

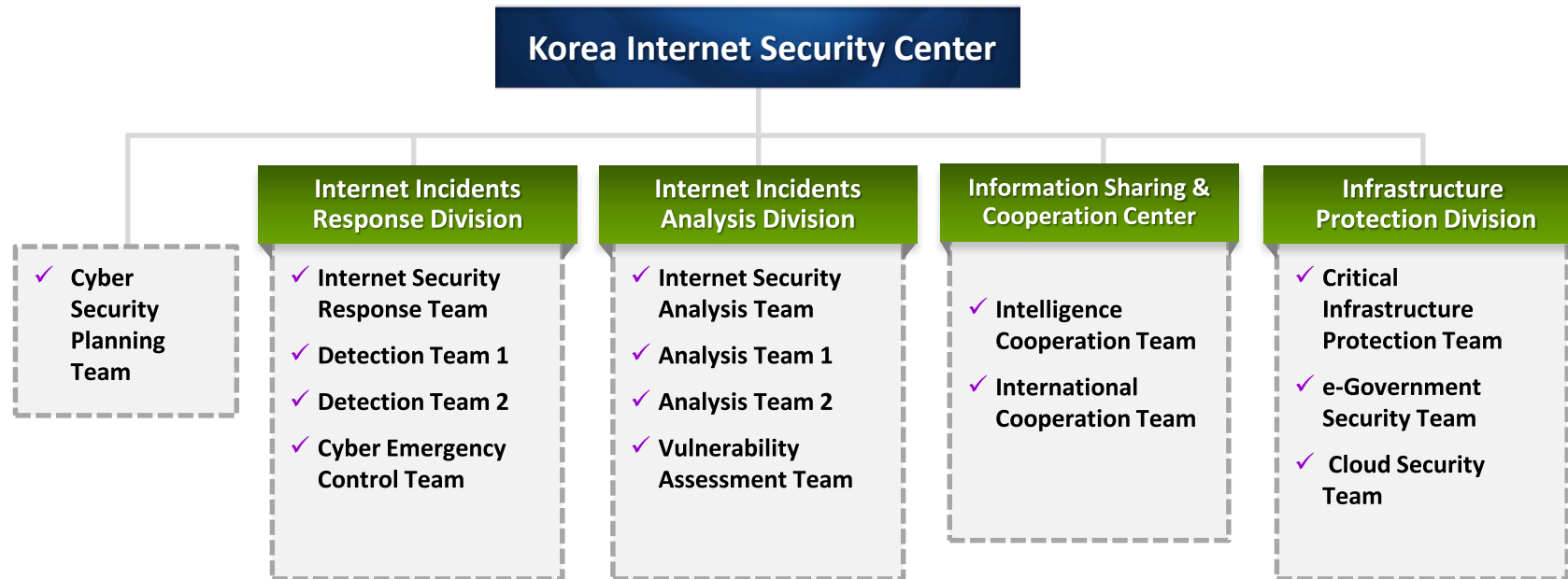


2 KISC, Korea Internet Security Center (KrCERT/CC)

Mission

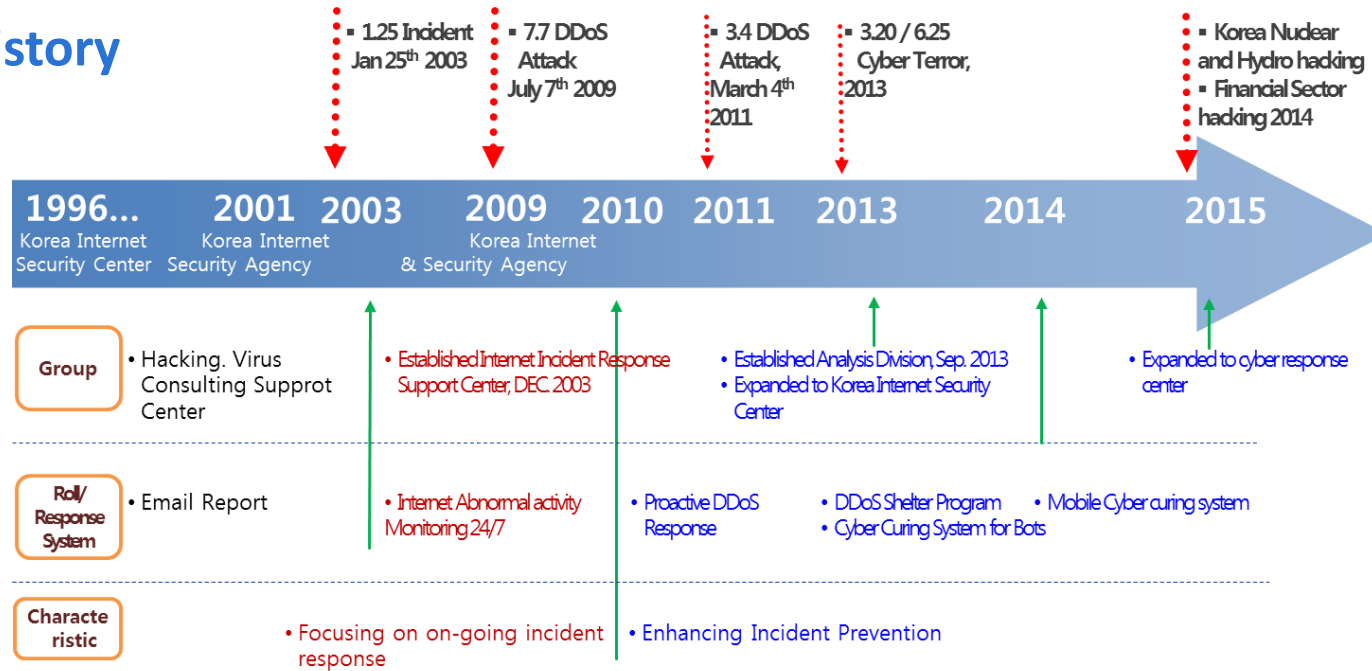
- Preventing Cyber Attacks and Enhancing Countermeasures

Organization

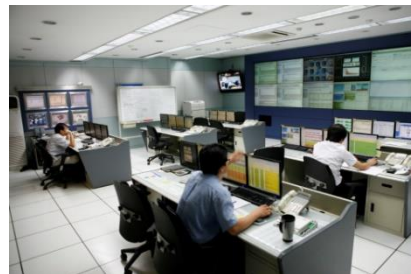


KISC, Korea Internet Security Center (KrCERT/CC)

History



Hacking Virus Consulting Support Center, April 2000



Internet Incident Response Support Center, DEC 2003



Korea Internet Security Center DEC 2010



Korea Internet Security Center DEC 2016

Government Structure in Cybersecurity



Cheong Wa Dae

National Security Office

Private [MSIP, KISC of KISA]

Mobile Subscriber : 59M
(Smartphone : 44 M)
High-speed Internet Subscriber : 20M
Internet Users : 41M (85.1%)

Finance [FSS]

Bank, Stock, Insurance

Public [NCSC of the NIS]

Central Administrative Agency
Local Government Agency
Government Office

Private Sector

IT Services
IPTV, VoIP, IoT,
Cloud, Big Data,
Fin-Tech

Smartphone

PC

Commercial
Company

Portal

IDC

Military [ROK.CC of the MND]

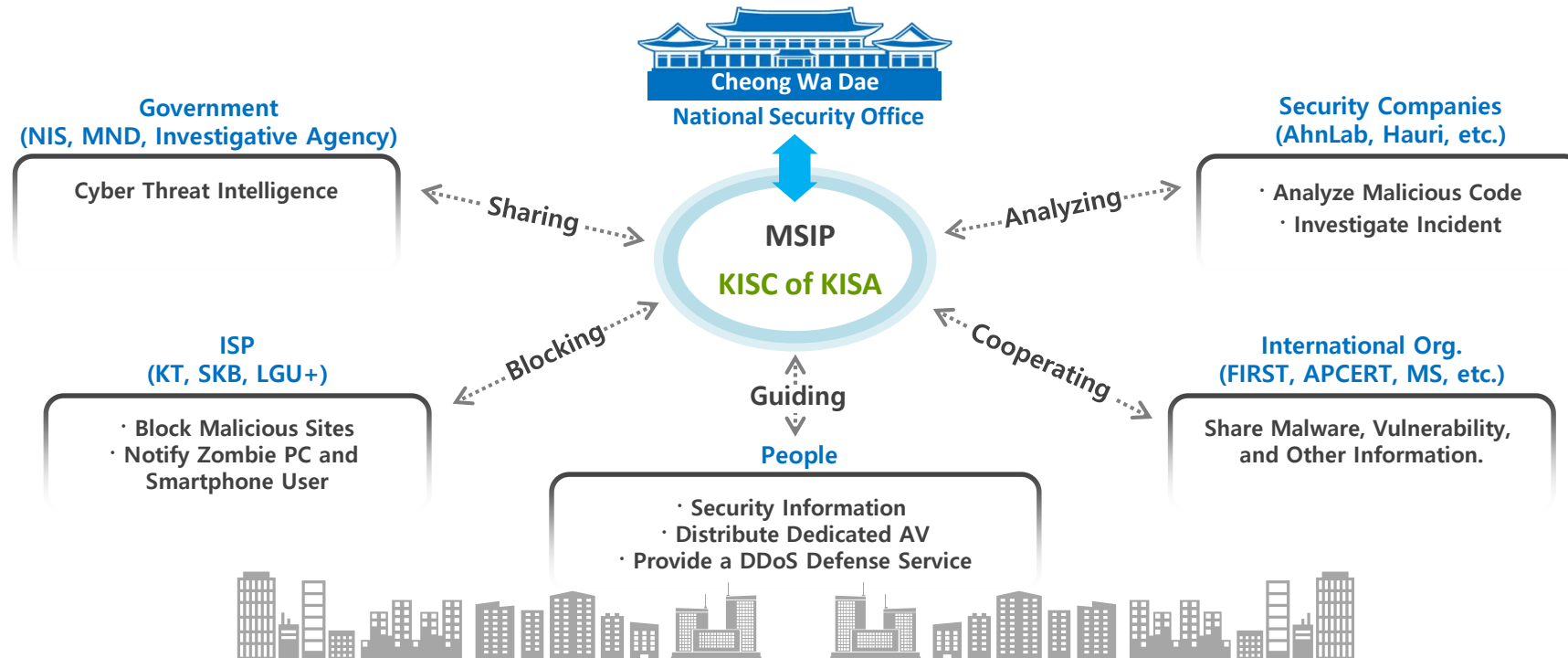
Army
Navy
Air Force

ISP

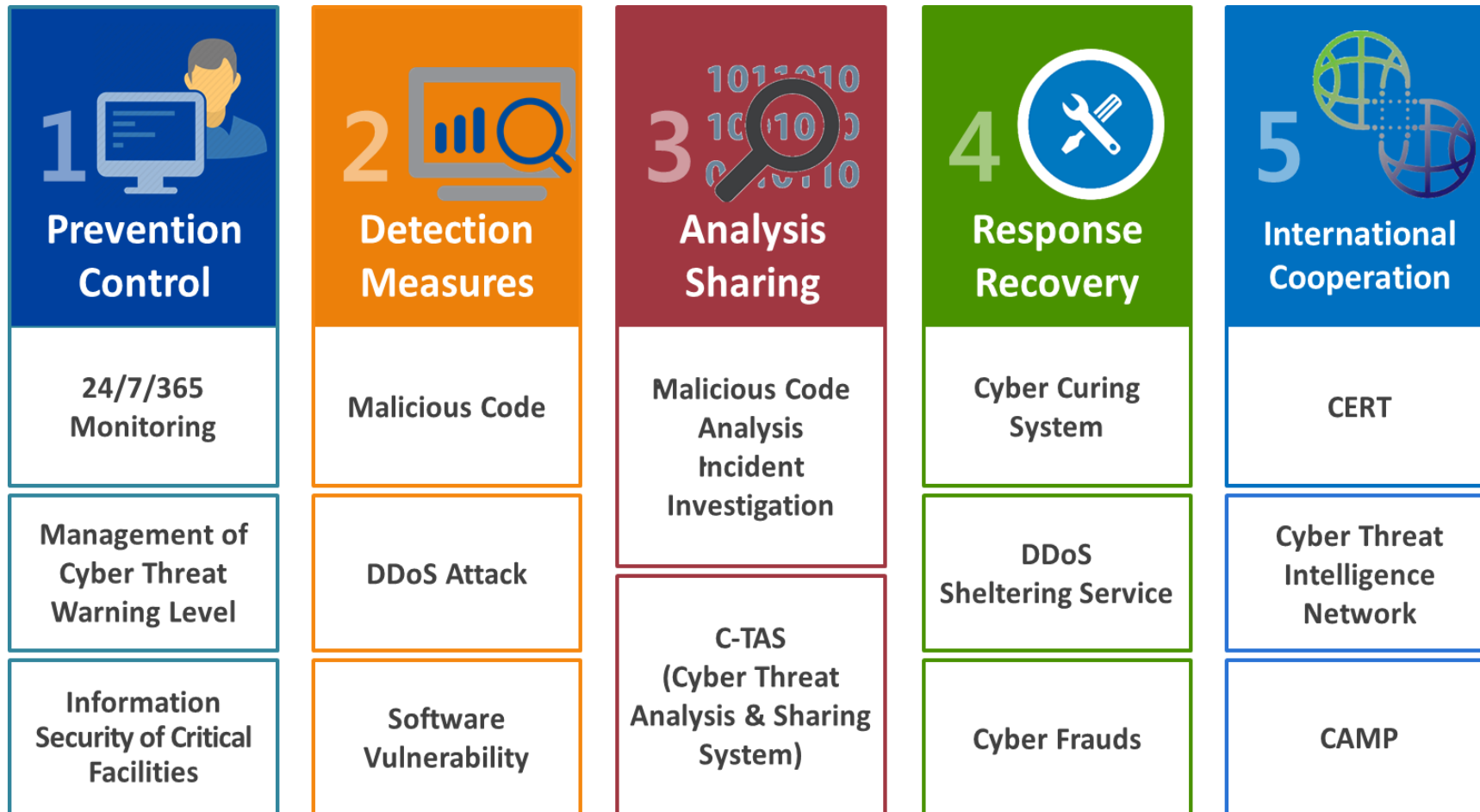


Wired · Wireless Internet

Cyber Threat Response Cooperation




Five Main Activities



Nation-Wide Prevention and Control

Monitor internet network in Korea for abnormal signs 24/7

- Traffic : local Internet Service Provider Traffic, Ports, Protocols, Attacks
- Web Servers : 1,000+ Major Domestic Web servers
- DNS : 13 Root DNS, KR DNS, Major Domestic ISP, Hosting DNS
- Security Information : Major Anti-Virus, System/Software/Security Company sites
- Monitor web-embedded malicious code
- Hotline : ISPs, Anti-Virus Vendors, NCSC, etc.
- Incident Call Services : +82-118 (free)

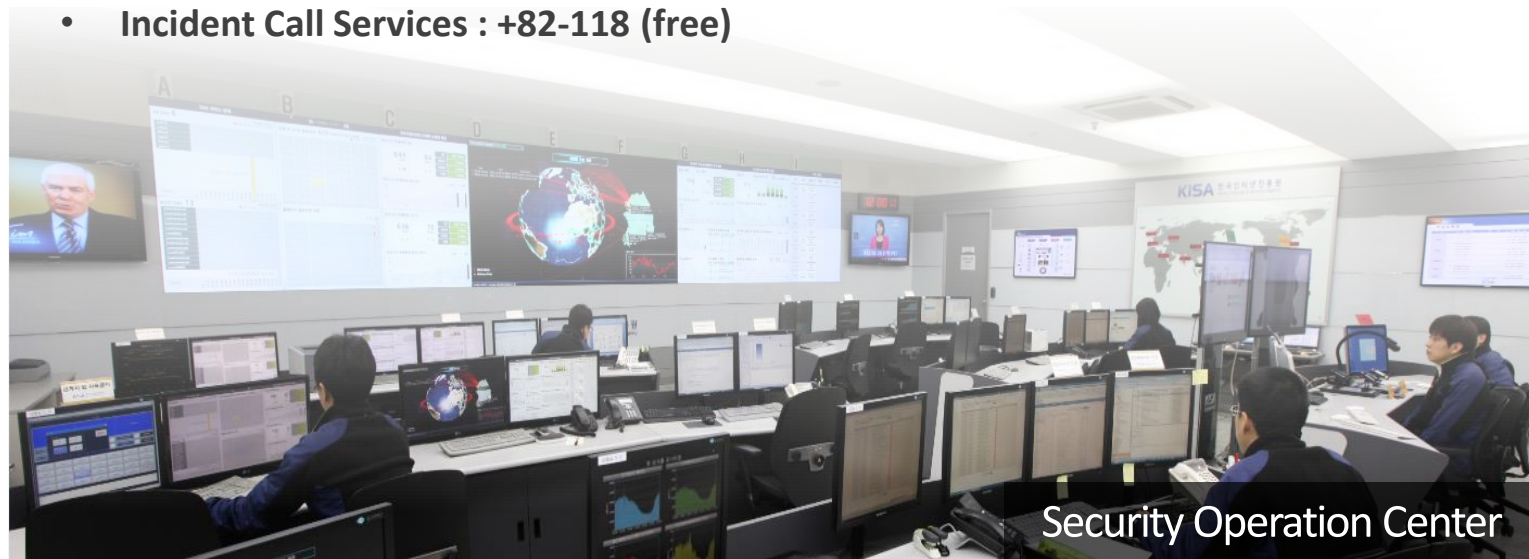


1
**Prevention
Control**

**24/7/365
Monitoring**

Management of
Cyber Threat
Warning Level

Information
Security of Critical
Facilities



Nation-Wide Prevention and Control

Cyber Threat Detection and Cyber Threat Warning Level Management

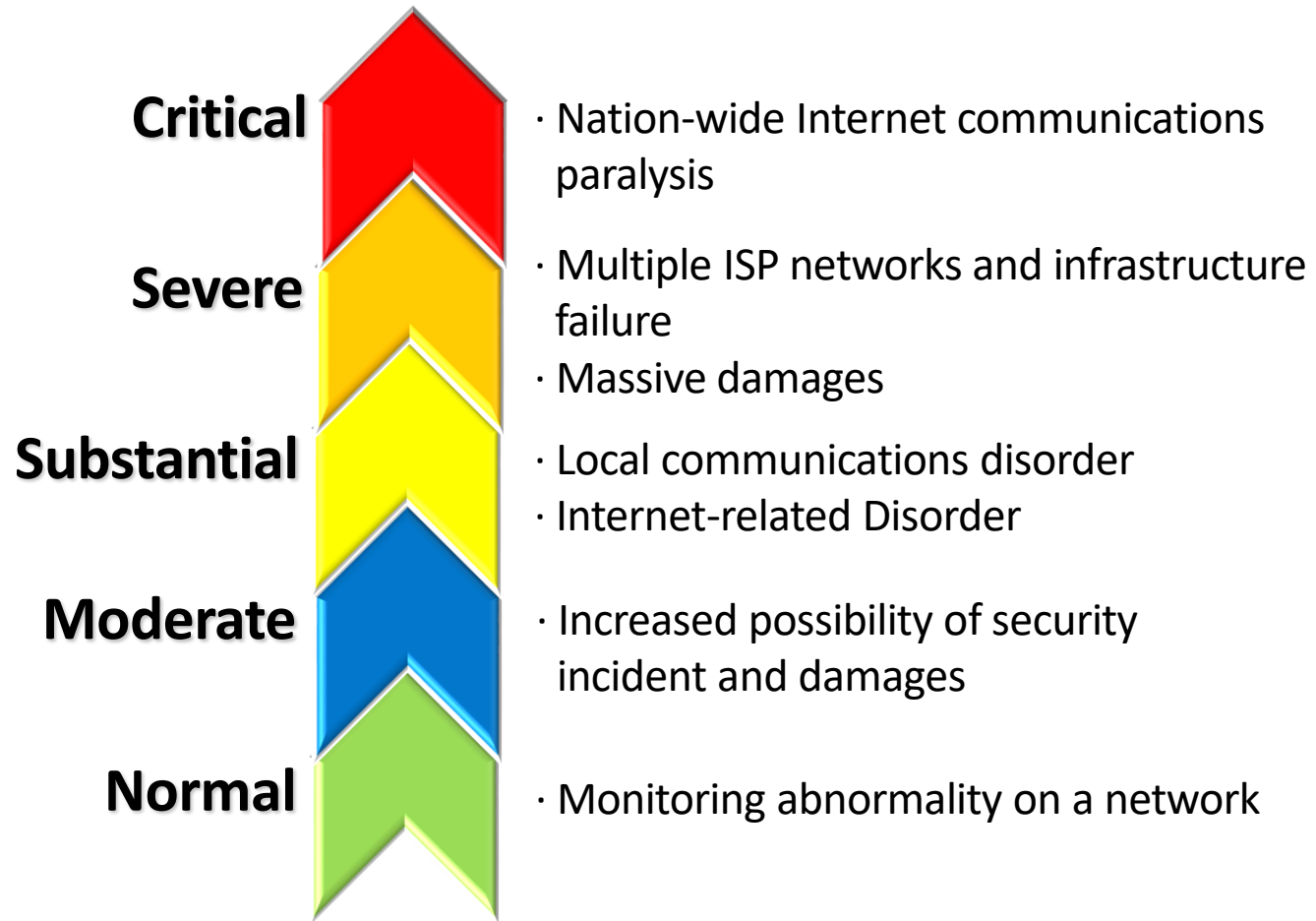


1
Prevention Control

24/7/365
Monitoring

**Management of
Cyber Threat
Warning Level**

Information
Security of Critical
Facilities



Nation-Wide Prevention and Control

Security Threat Specialized in Korea

- Raise of Tension Between South & North
- Growing of Possibilities In Cyber Attack After 4th Nuclear Test

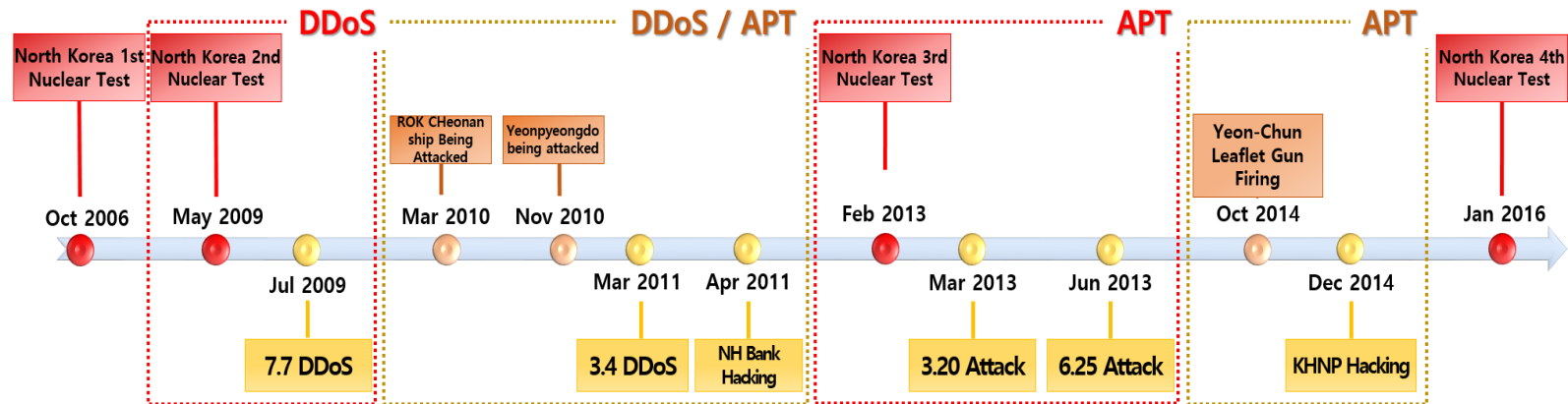
1 Prevention Control



24/7/365 Monitoring

Management of Cyber Threat Warning Level

Information Security of Critical Facilities



2nd Nuclear Test → 7.7 DDoS (after 37 days),

3rd Nuclear Test → 3.20 Attack (after 43 days), 6.25 Attack (4 months later)

Nation-Wide Prevention and Control

Information Security of Critical Facilities

- Designate national Critical Information Infrastructure and manage systematically



- ISMS(Information security management system), PIMS(Personal Information management system)

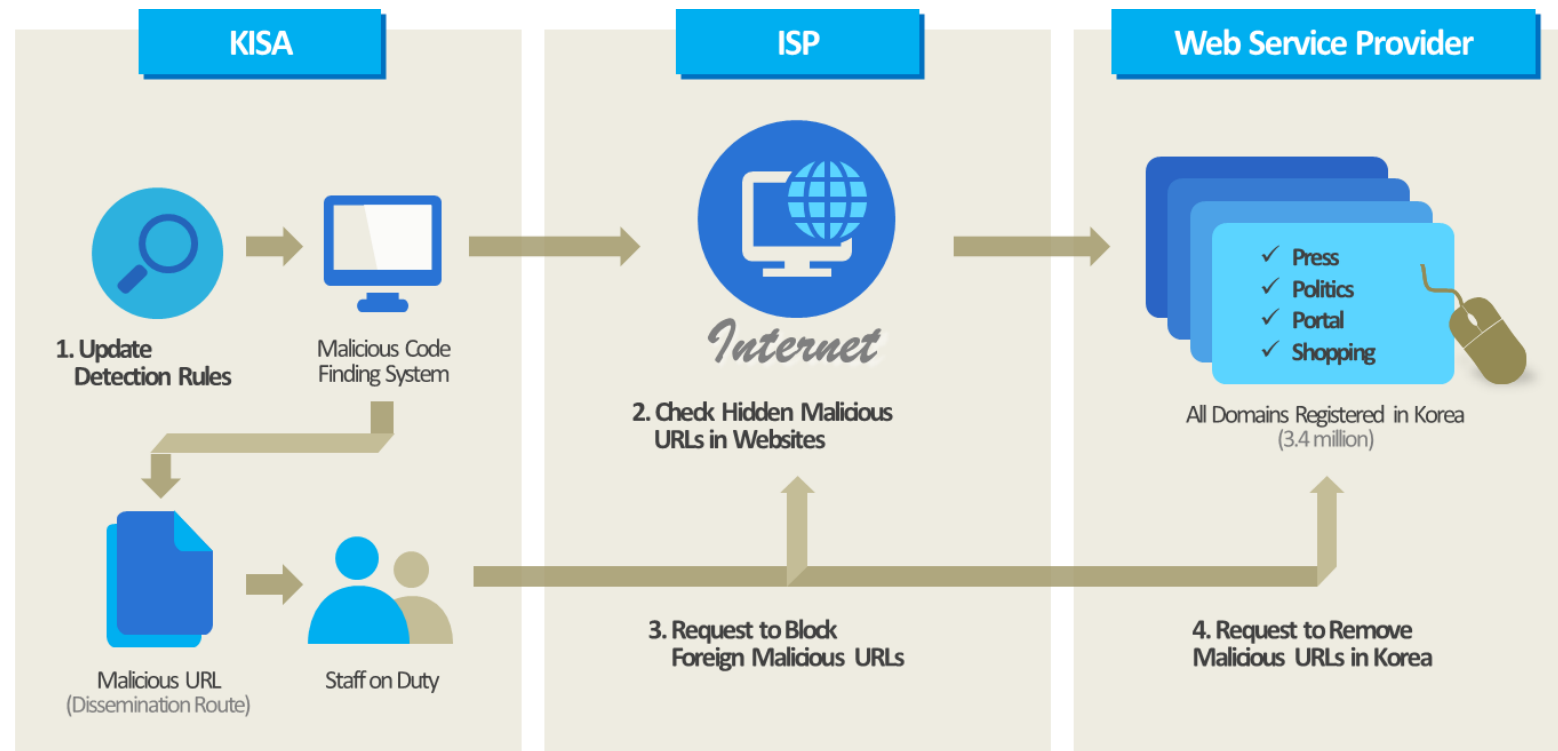


<p style="font-size: 2em; margin: 0;">1</p>  <p style="margin: 0;">Prevention Control</p>
<p>24/7/365 Monitoring</p>
<p>Management of Cyber Threat Warning Level</p>
<p>Information Security of Critical Facilities</p>

Cyber Attack Detection and Measures

Malicious Code Detection System

- Monitor web-embedded malicious codes (3.4 million domestic websites)
- Enhance security of domestic websites and Internet users



Cyber Attack Detection and Measures

DDoS Defense System

- Early Detection of DDoS Attacks at Internet Exchange (IX) Node

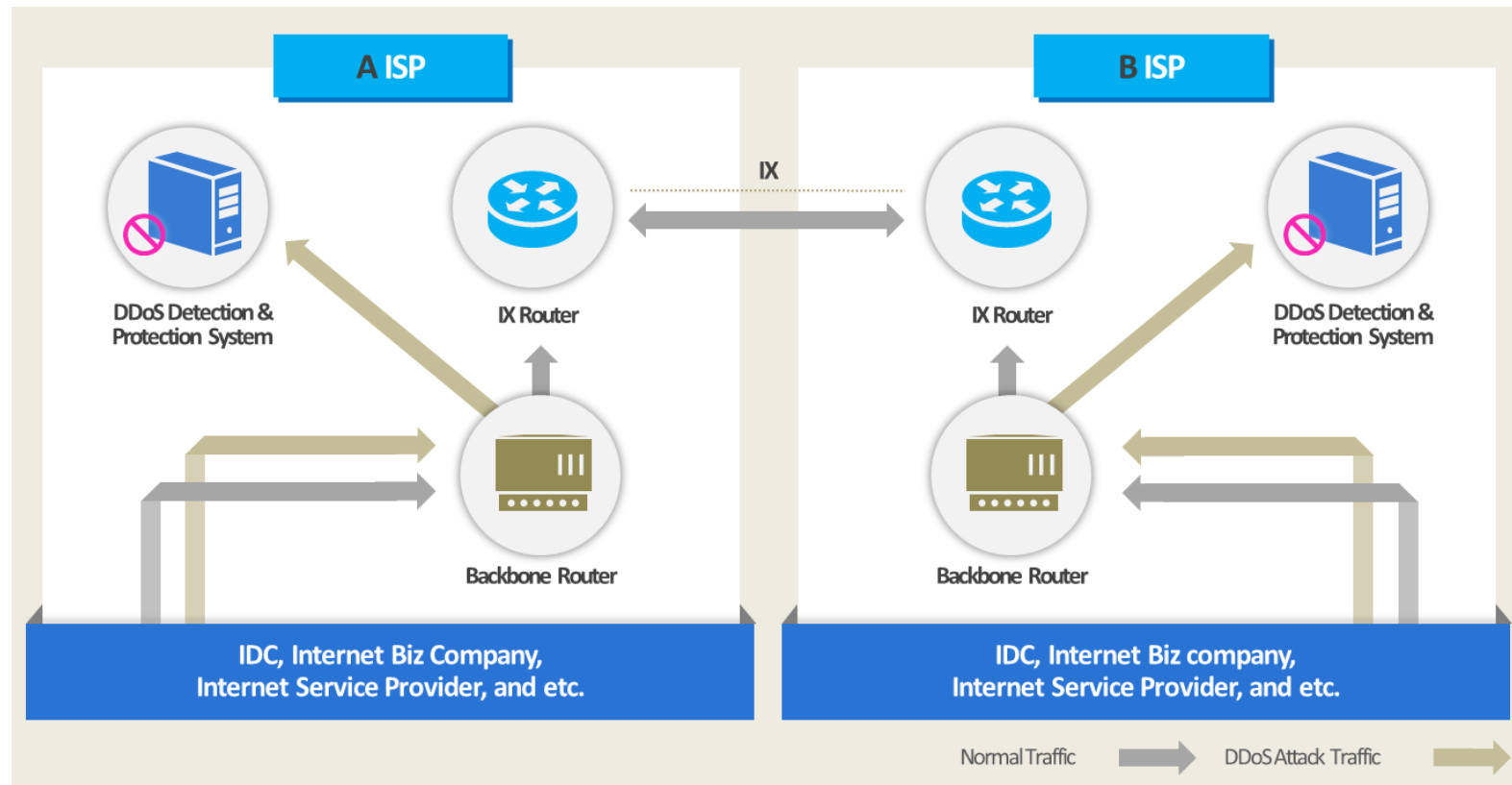
2 

Detection Measures

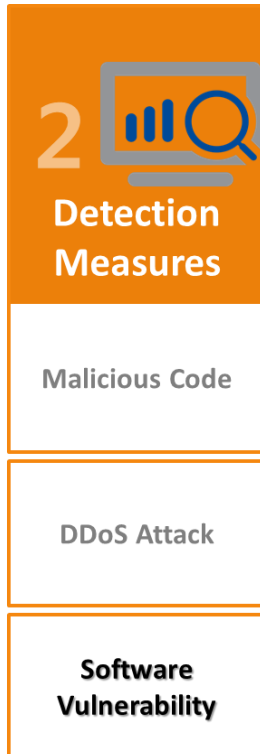
Malicious Code

DDoS Attack

Software Vulnerability

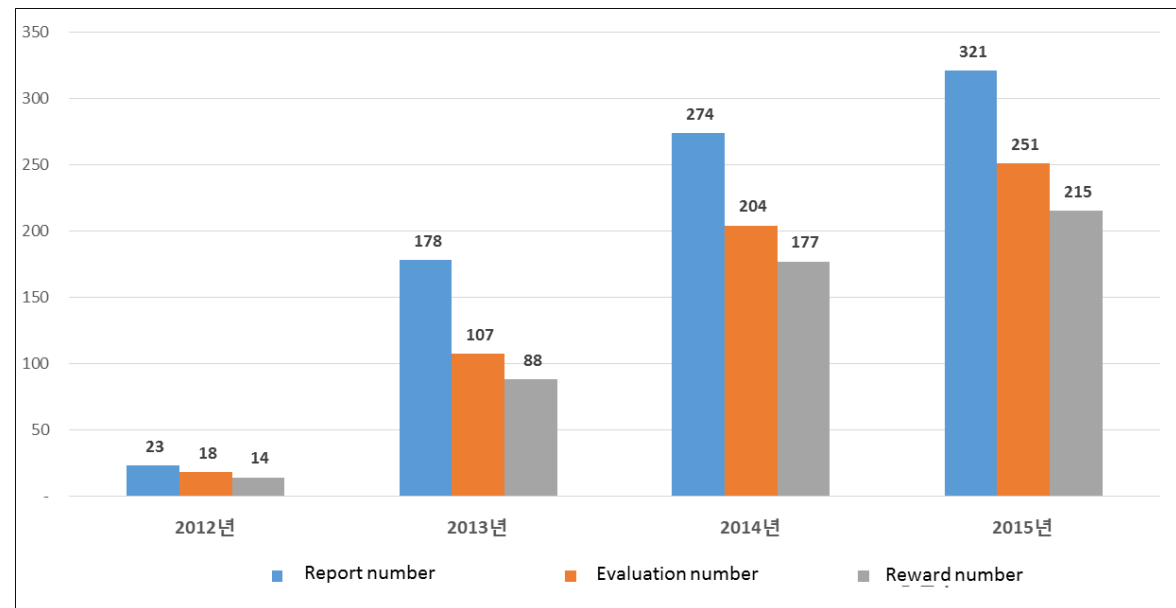


Cyber Attack Detection and Measures



Bug Bounty program

- Conditions for participation : Korean located locally and abroad
- Eligibility of rewards : Zero-day vulnerabilities found in the latest version of software
- Vulnerabilities not eligible for rewards : ongoing web services or low risk issues
- Rewards amounts : \$270 ~ \$4,520
- Reward assessment process
 - Verification of vulnerability → Internal review(KrCERT/CC) → External assessment



Malicious Code Analysis and Sharing

Malicious Code Analysis & Incident Investigation

- Analyze malwares and Provide remote or on-site technical support

C-TAS (Cyber Threat Analysis & Sharing System)

- Provide threat intelligence to relevant organizations
- Analyze cyber threat intelligence based on big-data and share results

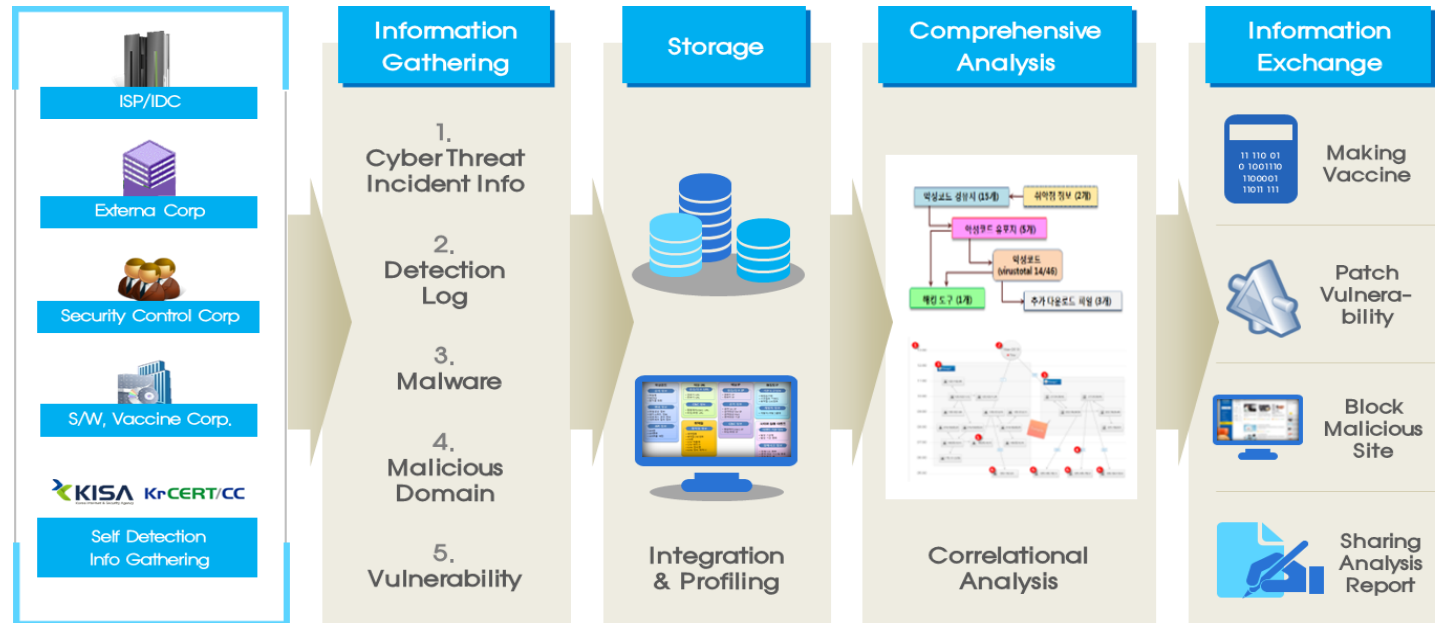
1011010
101010
010110

3

Analysis Sharing

Malicious Code Analysis
Incident Investigation

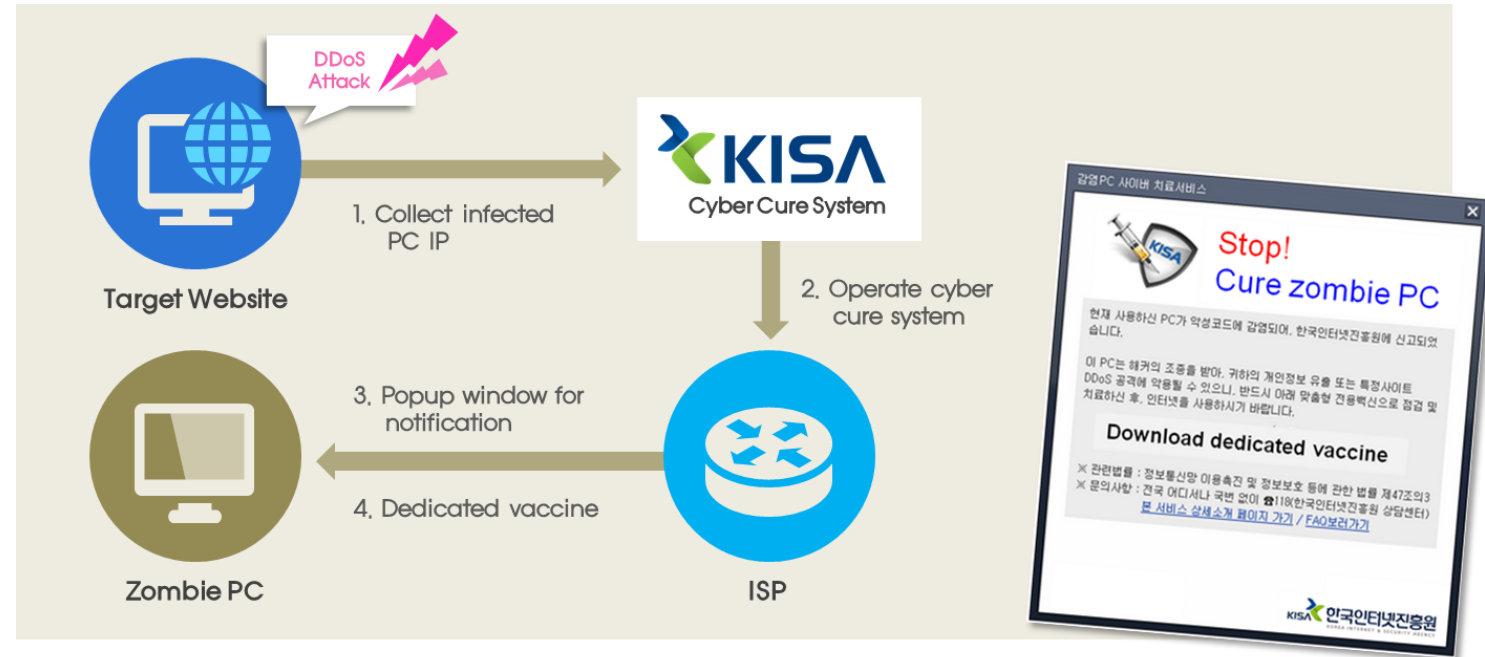
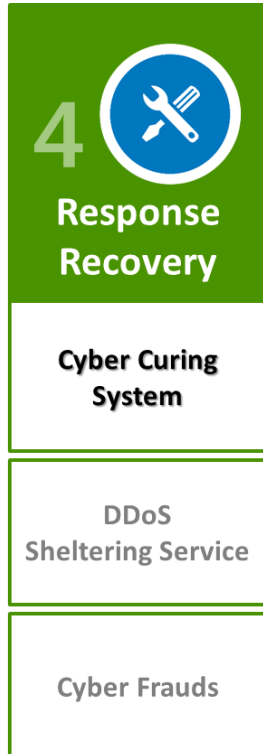
C-TAS
(Cyber Threat Analysis & Sharing System)



Cyber Attack Response and Recovery

Cyber Curing System

- **Zombie PC** : Create a popup window to notify malware infection and guide dedicated AV download




Cyber Attack Response and Recovery

Mobile Cyber Curing System

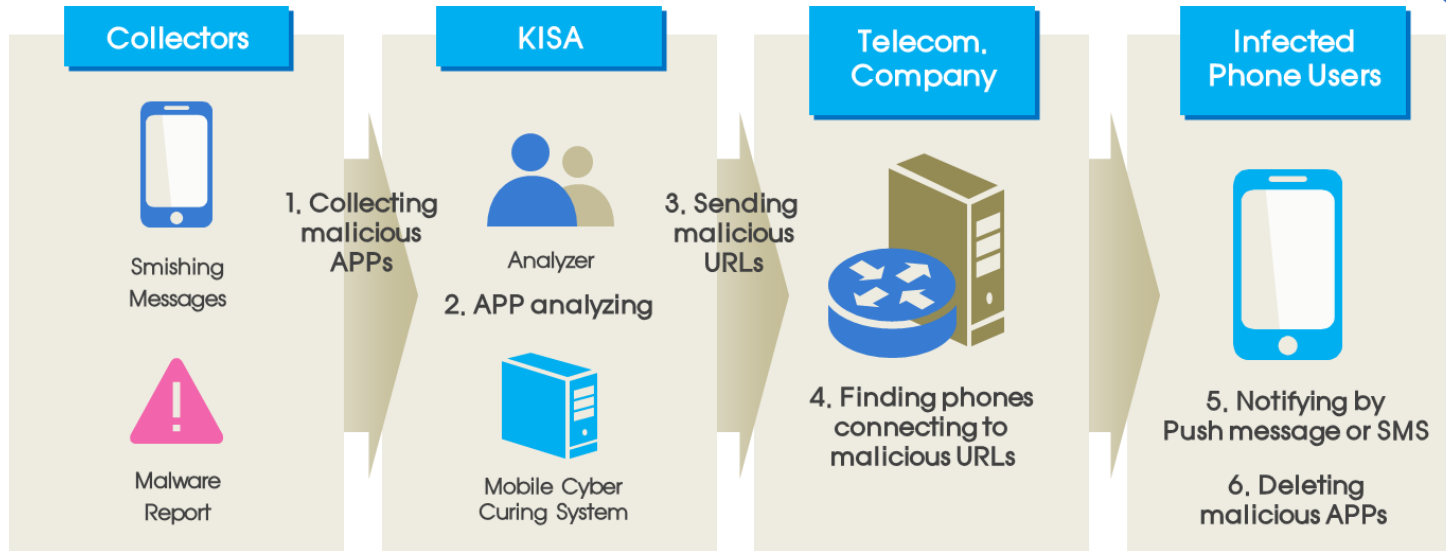
- Infected Smartphones : Notify malware infection and guide dedicated AV download




4 

Response Recovery

- Cyber Curing System
- DDoS Sheltering Service
- Cyber Frauds

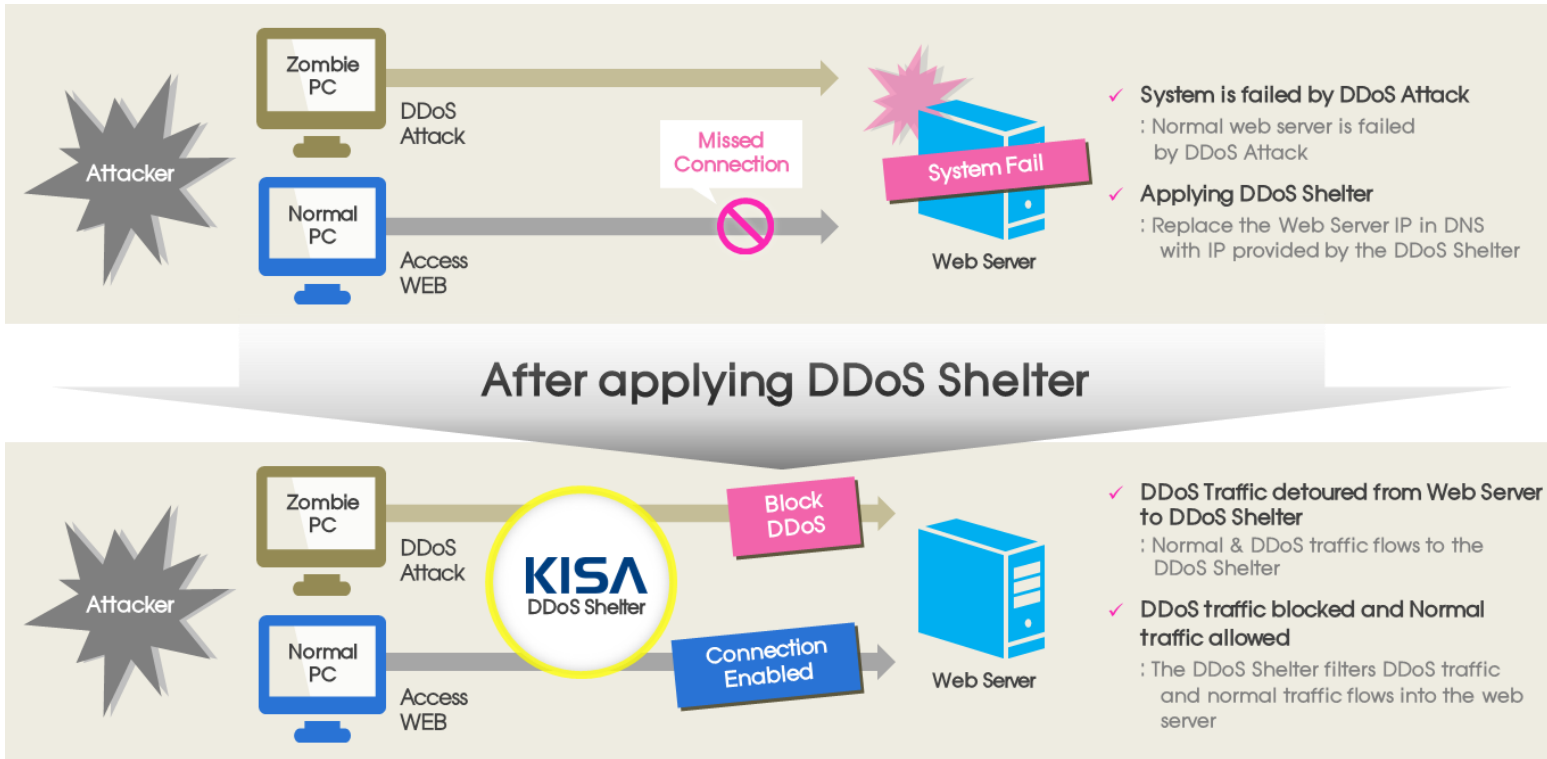


Cyber Attack Response and Recovery

<p>4 </p> <p>Response Recovery</p>
<p>Cyber Curing System</p>
<p>DDoS Sheltering Service</p>
<p>Cyber Frauds</p>

DDoS Sheltering Service

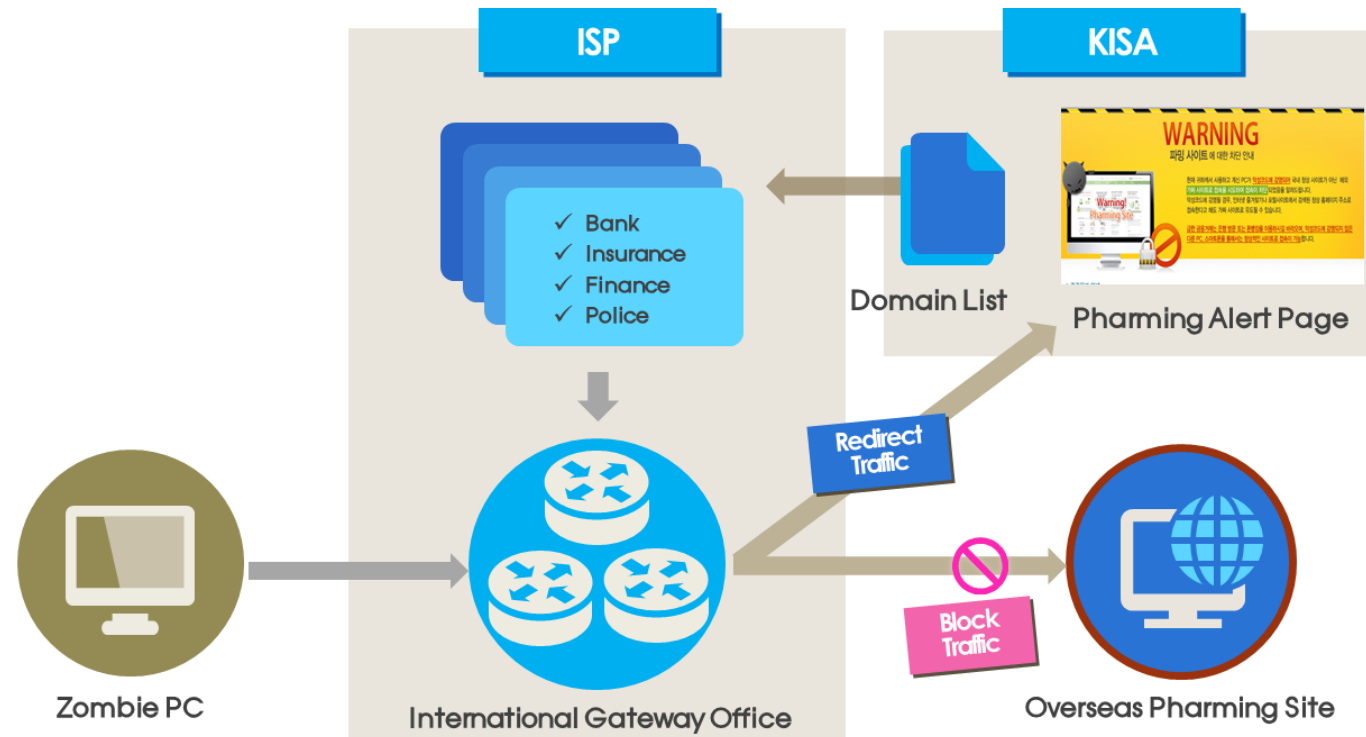
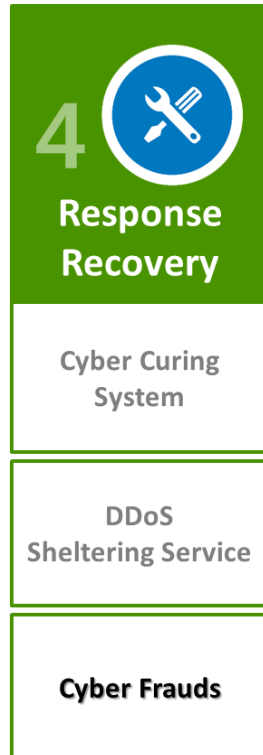
- Block DDoS attacks and support SMEs to provide normal web services



Cyber Attack Response and Recovery

Cyber Frauds

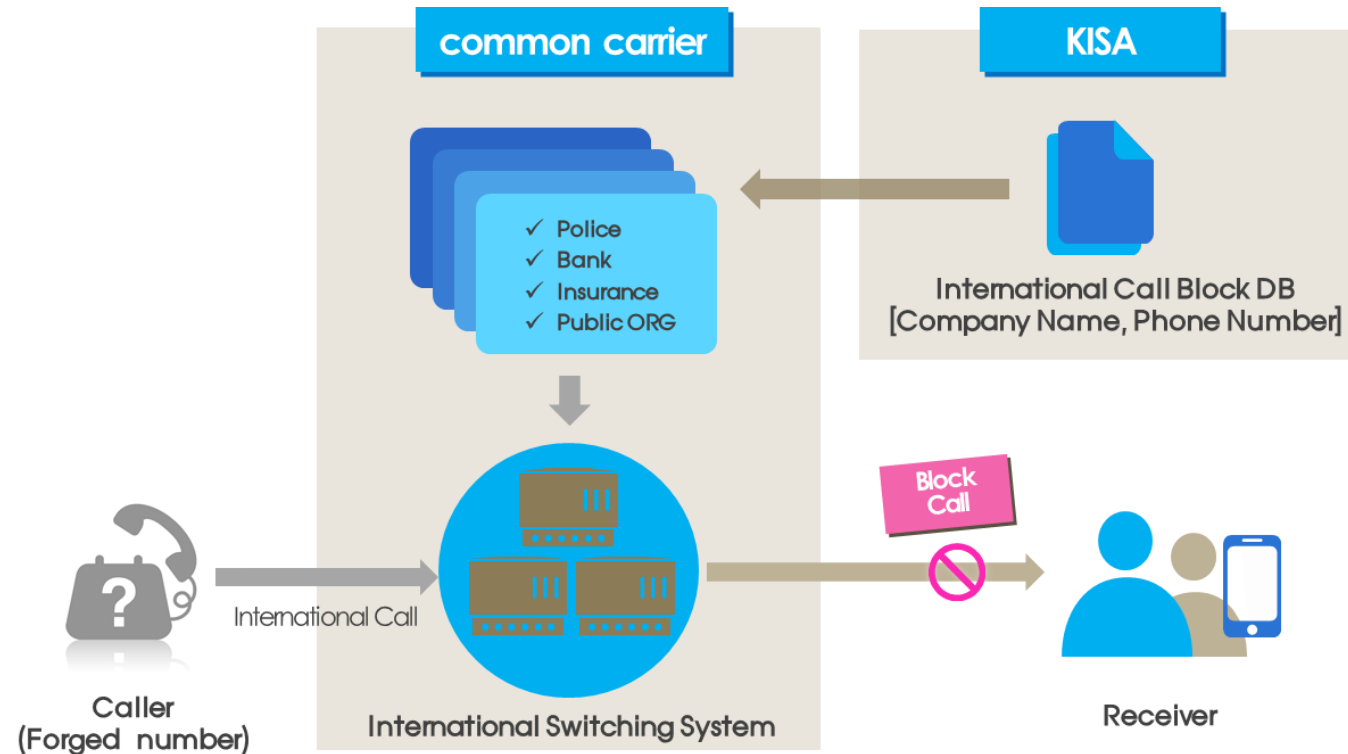
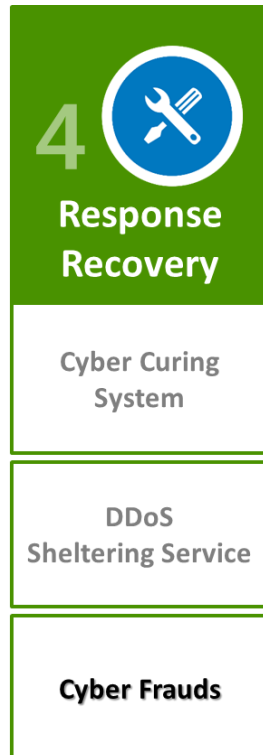
- Pharming alert service : Detecting IPs that are accessing overseas, even though website is located in domestic server(Redirect to KISA alert page)



Cyber Attack Response and Recovery

Cyber Frauds

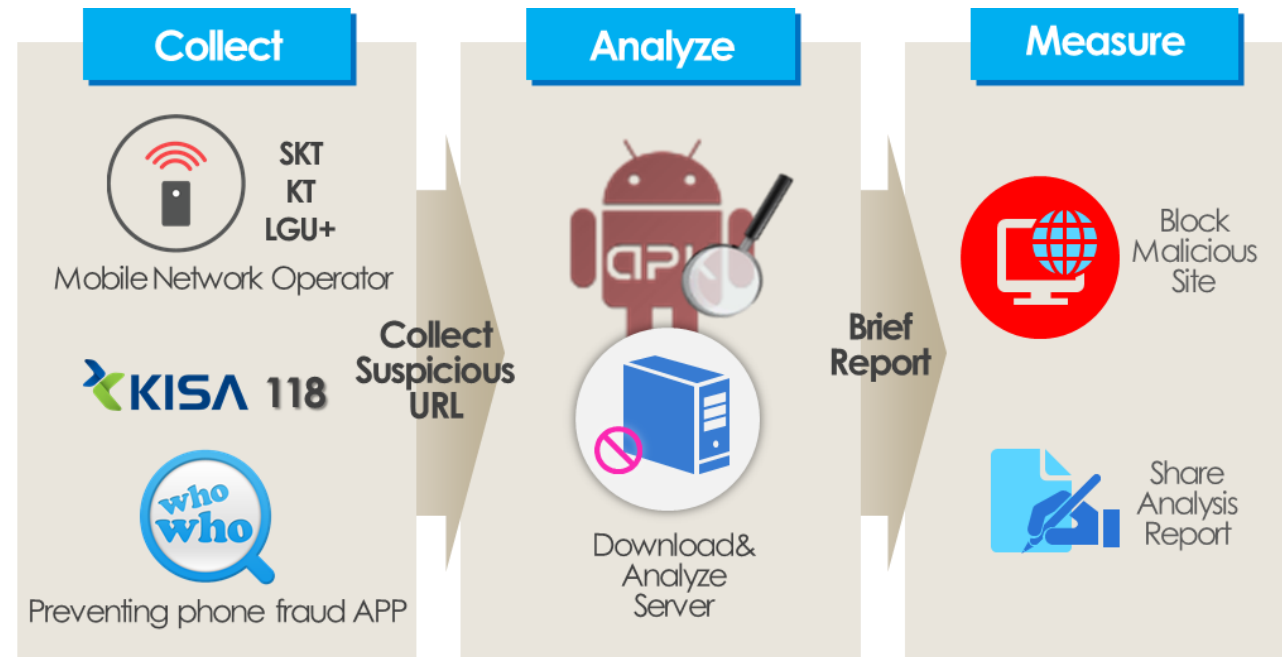
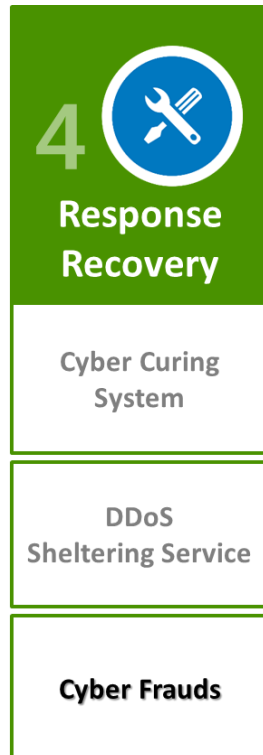
- Forged caller's phone number Block Service : Identify and block domestic spoofed phone numbers



Cyber Attack Response and Recovery

Cyber Frauds

- Smishing Response System : Identify malicious apps by verifying Smishing suspicious characters with URLs



Leading Global Cooperation

5
 International Cooperation

CERT

Cyber Threat Intelligence Network

CAMP

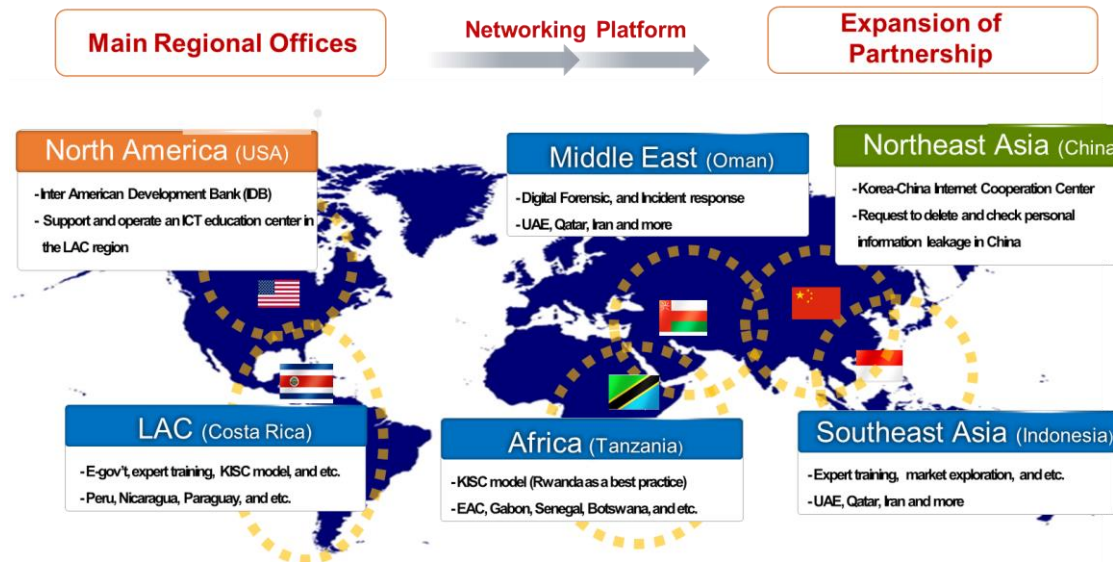
CERT

- (Multilateral) FIRST, APCERT, and APISC
- (Bilateral) Signed MOU with 10 national CERTs

Cyber Threat Intelligence Network

- (Local) Ahnlab, Hauri, ESTsoft, INCA Internet, NSHC, Bitscan
- (Global) FireEye, Fortinet, McAfee, Microsoft, Palo Alto Networks, Symantec

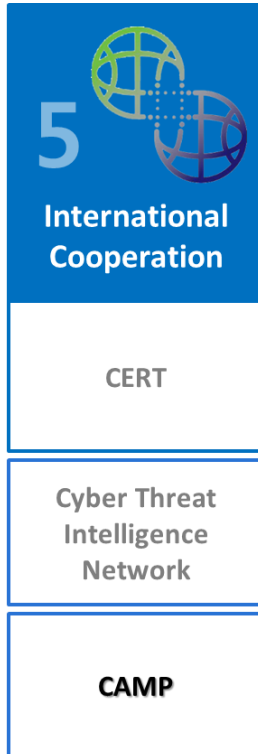
Regional Offices



Leading Global Cooperation

CAMP (Cybersecurity Alliance for Mutual Progress)

- **Members : Ministries, Government Bodies and Non-Profit Org.**
- Members : 47 organizations from 35 nations (July, 2016)
- **Mission and Vision : A network platform to lift up the overall level of cybersecurity of the members.**
- **1st Annual Meeting : Agreed to create Operations Committee and Working Groups.**
-Technology & Industry, Policy & Culture, and Capacity Building



Website : www.cybersec-alliance.org

E-Mail : camp@kisa.or.kr

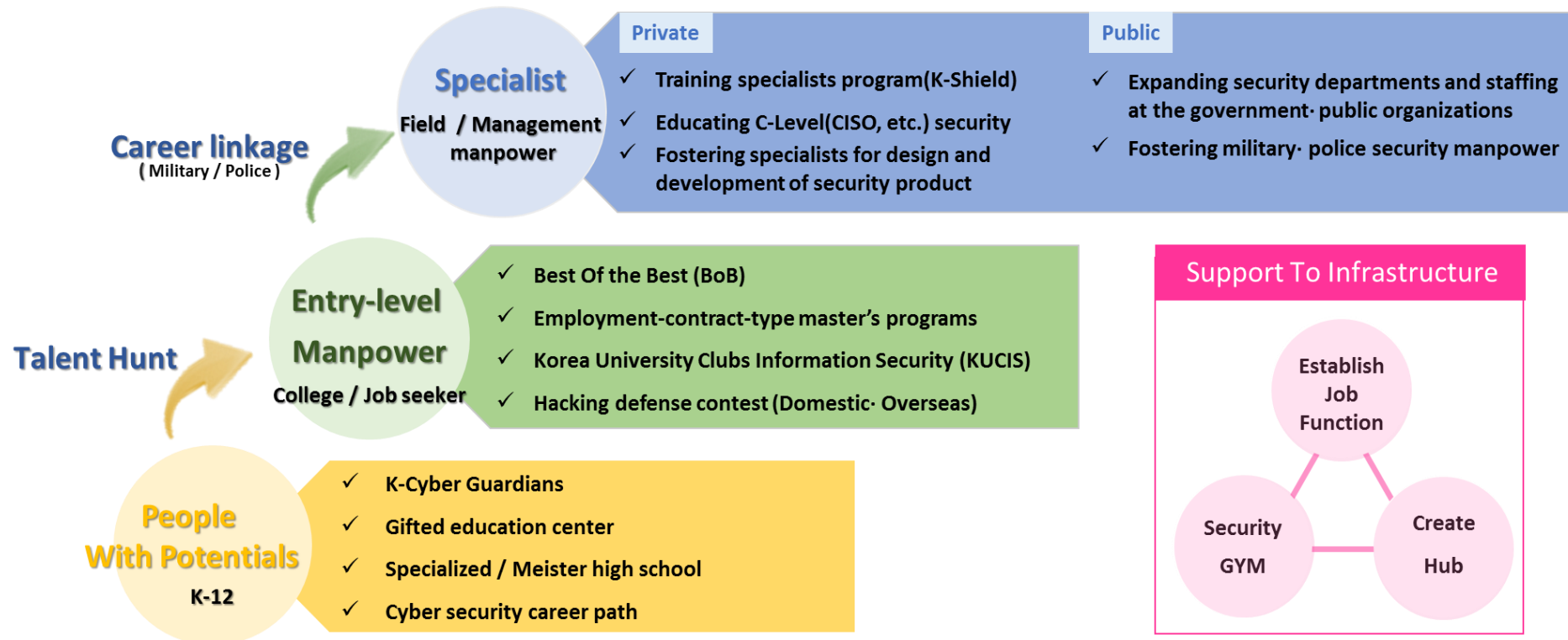


Fostering Cyber Security Manpower

STRATEGY – Lifecycle-based Manpower Fostering

The goal is to bring up the best and brightest 7,000 specialists to 2020

Enhance national cyber security and Information security industry

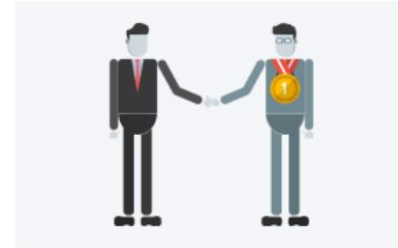
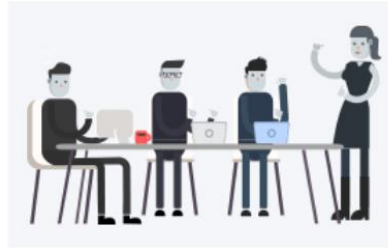


BOB/K-SHIELD



BOB(Best of the Best) / K-SHIELD

Mission and Vision : Developing the next generation of top security leaders and white hackers



BOB

Security Specific
Training

Project
Advancement

The Final Stage
Contest

Certification

K-SHIELD

Security training
(Theory, practical)

1st Assessment +
Training
(based on Scenario)

2nd Assessment

Certification

BOB Security Program

Vulnerability Analysis(Zero-day, CVE), Product Security, Digital Forensics, Security Consulting, Information Protection, Specialty Soldiers, Mobile Security, Cloud Security, Finance & Fusion Security, CC Certification and Other

K-SHIELD Security Program

Buffer Overflow practice, Injection practice, Web security, OS security, DoS scenario based practice, CTF(capture the flag), Security assessment, Penetration practice, Detection, Code analysis



Question & Answer

Furthermore Question

Please contact : jhkim330@kisa.or.kr

jkim@krcert.or.kr

+82-2-405-5565

+82-10-3556-8489



**Keeps Safety
of the Cyber World**

THANK YOU

