Case Studies on Cyber Incidents

2016. 2. 21

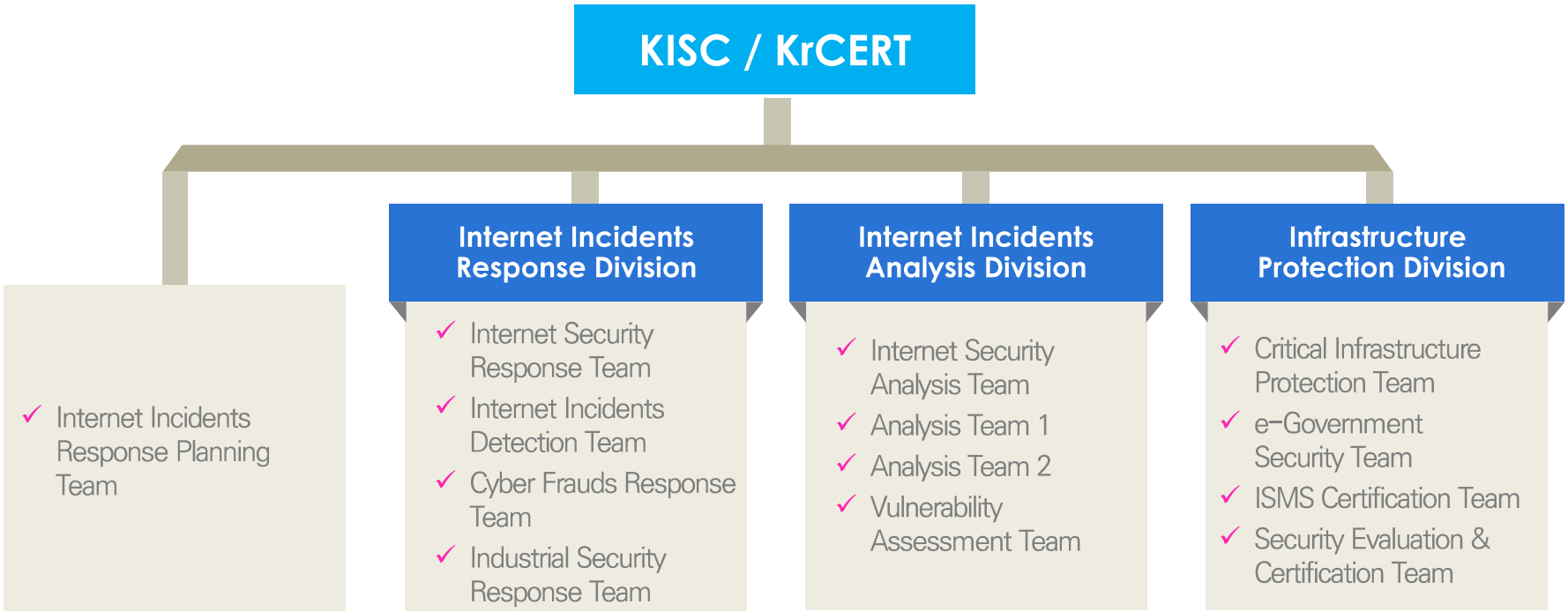
KISA

Contents

1 Introduction of KrCERT/CC

1. Organization of KISC

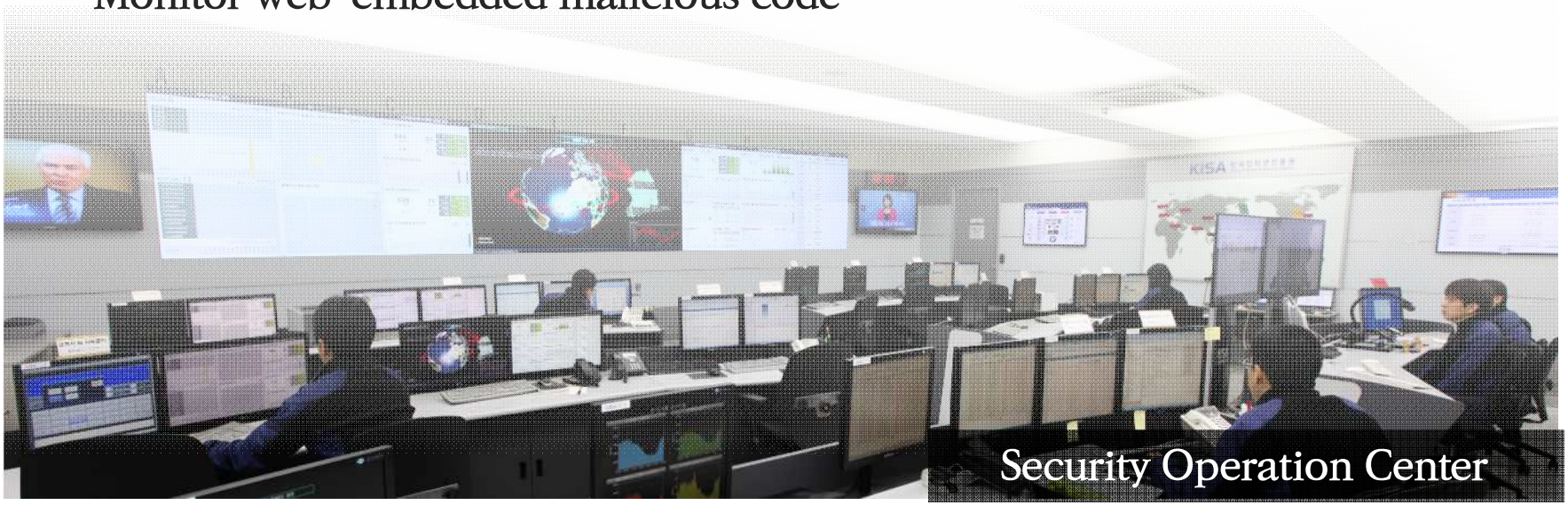
- KISC (Korea Internet Security Center) is a Part of KISA (Korea Internet & Security Agency)
- Mission : Rapid Detection / Response for Cyber Incidents in Private sector



2. Monitoring

Monitor internet network in Korea

- **Traffic** : local Internet Service Provider Traffic, Ports, Protocols, Attacks
- **Web Servers** : 900+ Major Domestic Web servers
- **DNS** : 13 Root DNS, 6 KR DNS, 12 Major Domestic ISP DNS
- **Security Information** : Major Anti-Virus, System/Software/Security Company sites
- **Monitor web-embedded malicious code**

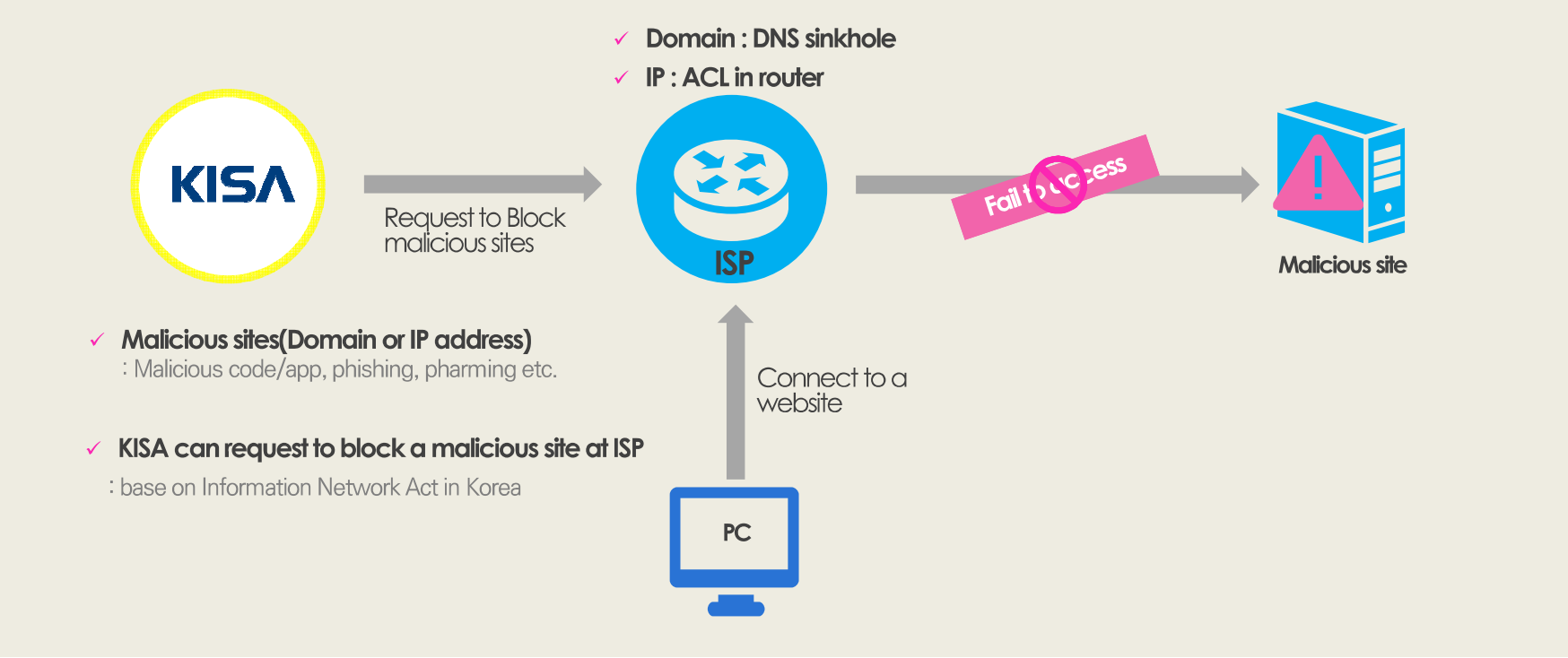


Security Operation Center

3. Blocking

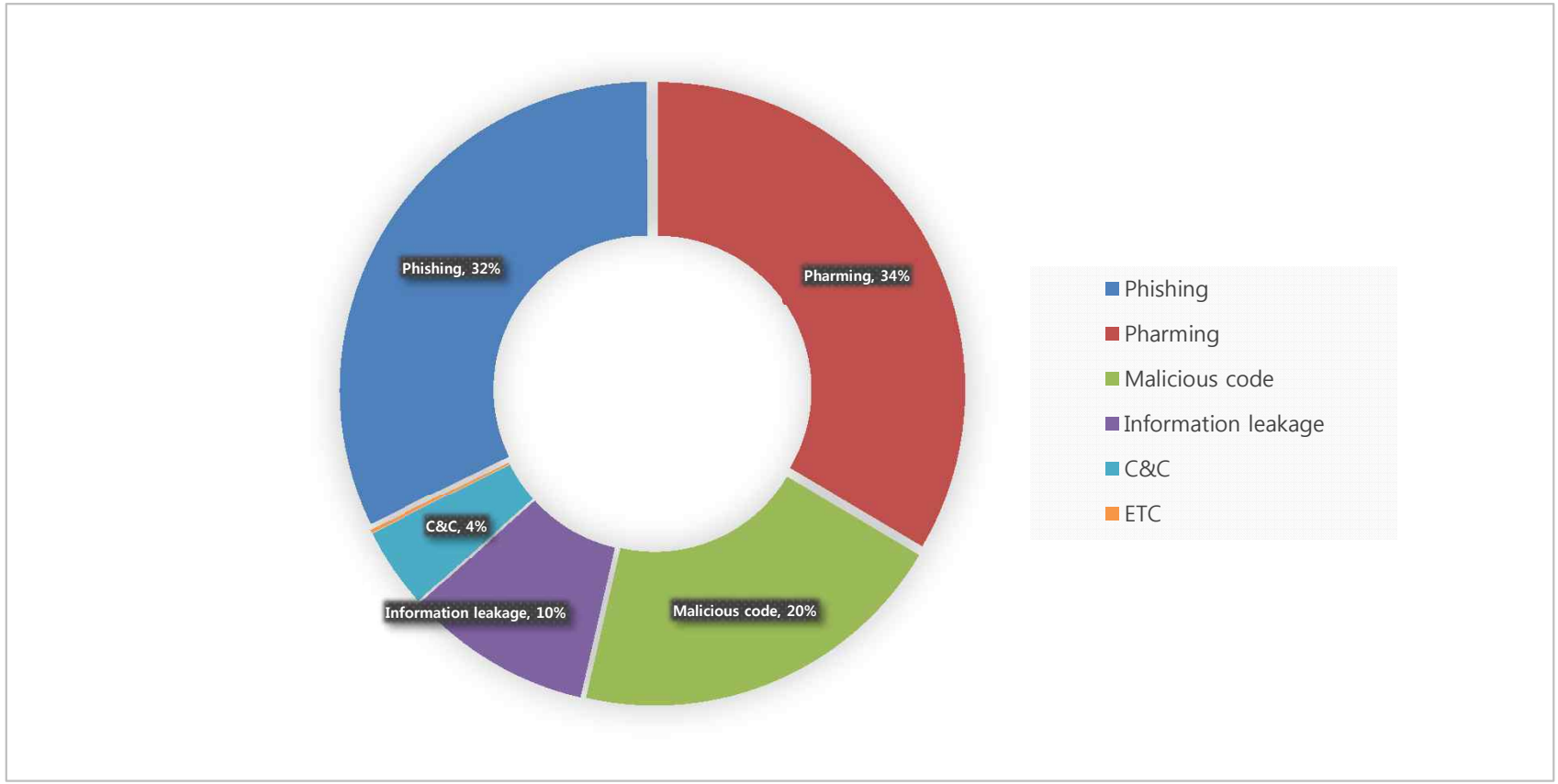
Block access to malicious sites

- Collaboration with ISPs to prevent damage by blocking malicious sites



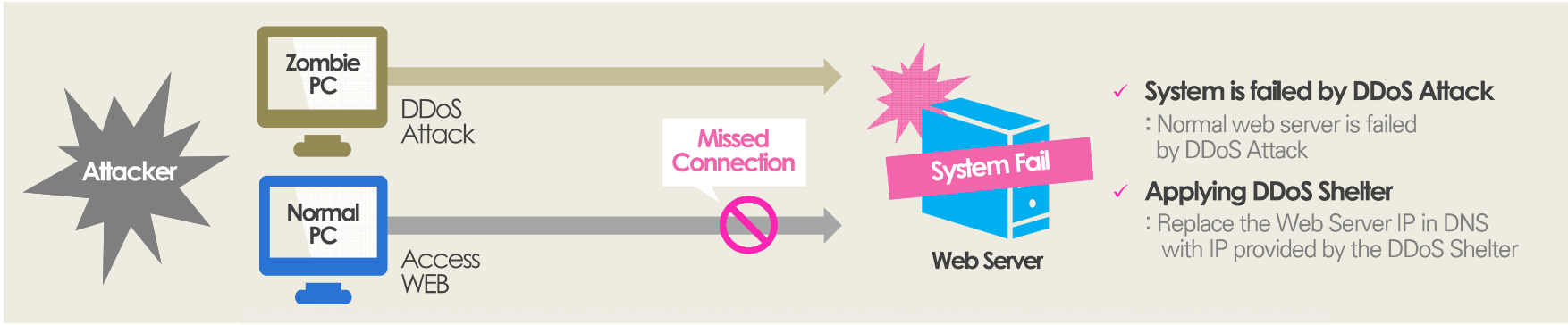
3. Blocking(cont.)

Statistics on 2015

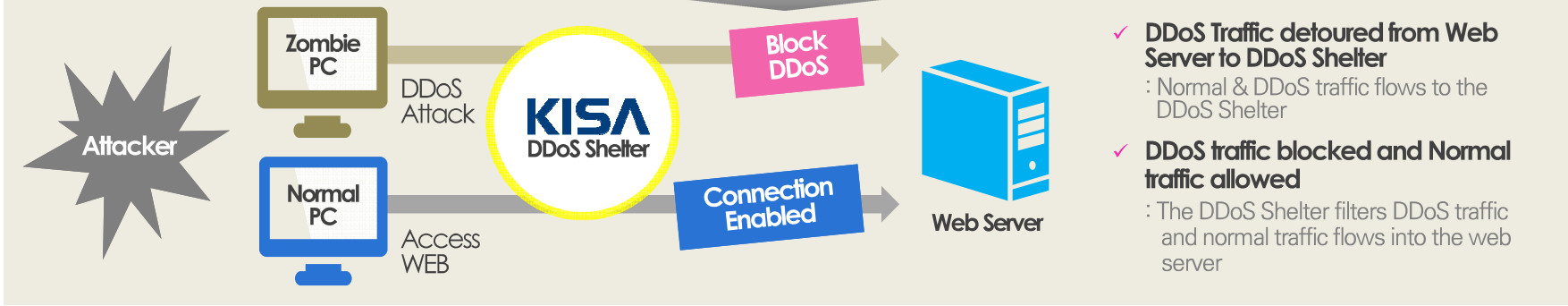


4. DDoS Shelter System

- DDoS defense service at the government level for SMEs
  : It's blocking DDoS attack and supporting normal web service of SMEs

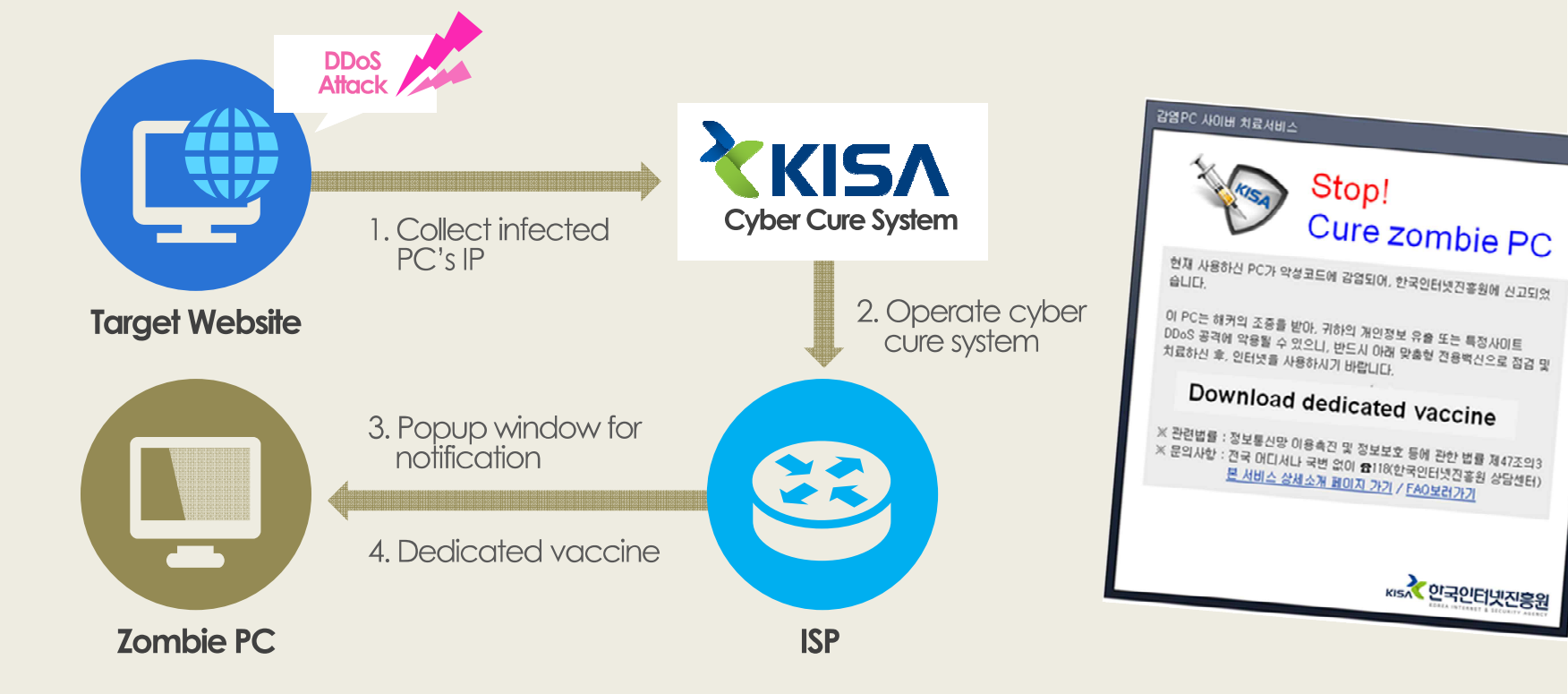


After applying DDoS Shelter



5. Cyber Curing System

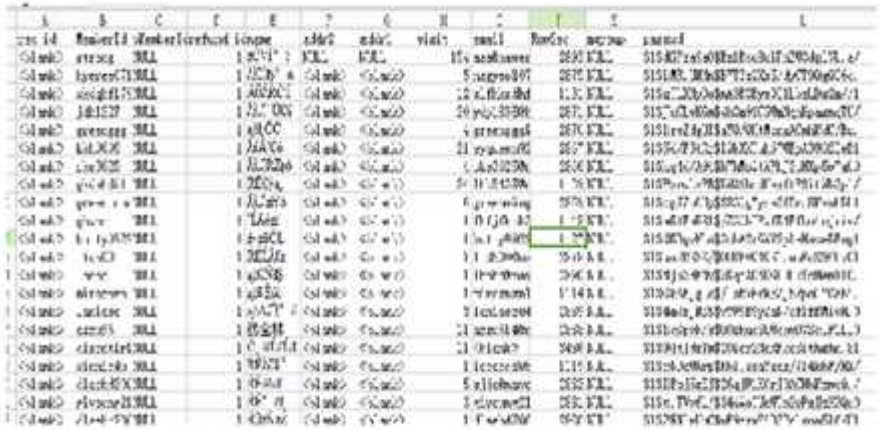
- Provide a notification of malware infection and removal method using popup window
- Effective measure against large-scale DDoS attack



2 Case Studies

Case 1 : Personal Information leakage

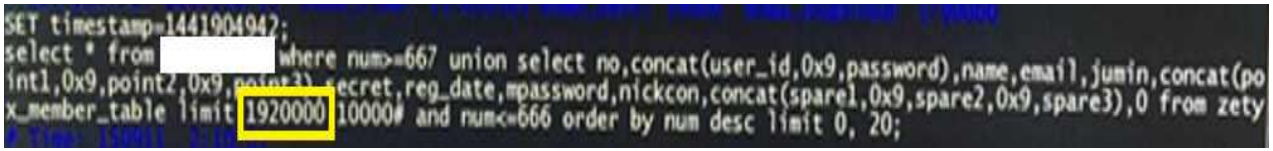
- Data breach(2015.9)
  - Hacked a famous community site and a demand for an apology
  - Threats to disclose around 1.9 million sets information
  - Disclosed some customer's information(ID, Password, e-mail, etc.)



Case 1 : Personal Information leakage

- Analysis & Response
  - Korea IP(X.X.161.67) in web log.

  - SQL-injection attack and 1920,000 information leakage



  - Additional attack using CMS vulnerability
  - Noticed a guideline for prevention of further hacking

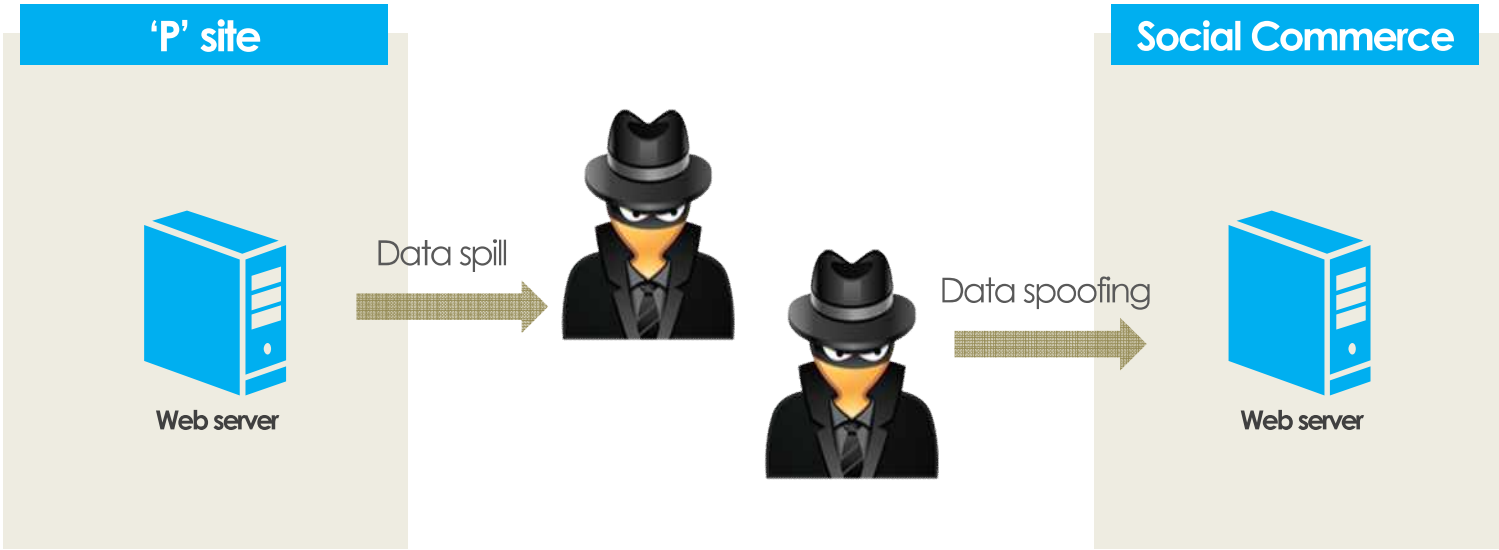
Case 1 : Personal Information leakage

- Violation(According to Information Network Act in Korea)
  - §28-①-2(Access Control) : must have access control devices.
  - §28-①-3(Access Log) : must have a web log over 6 months
  - §28-①-4(Encryption) : must use a proper encryption algorithm

- Fine(According to Information Network Act in Korea)
  - Below 3% of the total sales & Below 30 Million won
  - 120 Million won(≒ 110 thousand dollars)

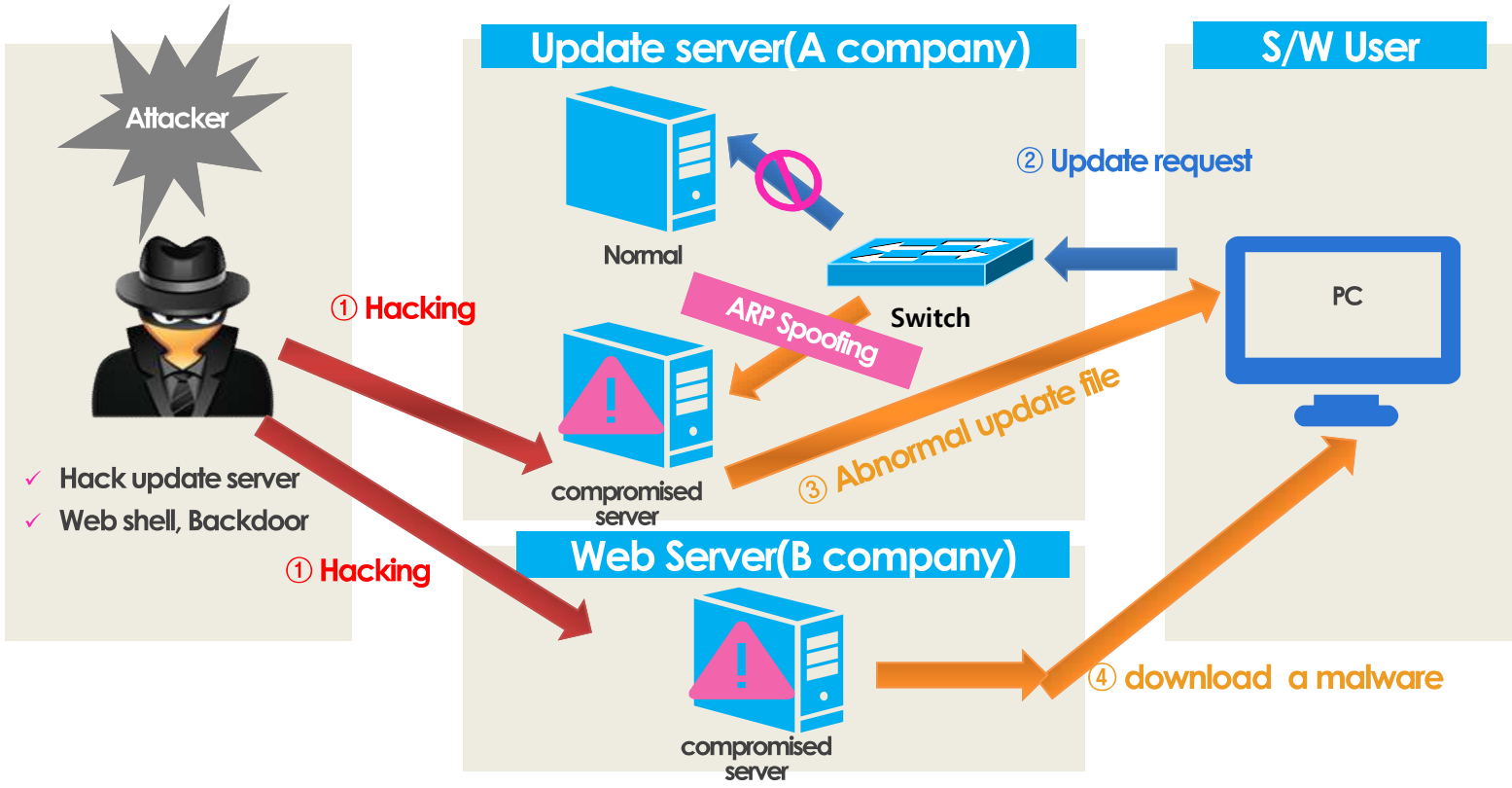
Case 1 : Personal Information leakage

- Data spoofing(2015.12)
  - Customers' accumulated money is being paid without approval
  - Targeted users who used the same account information for both sites T and P



Case 2 : Update Server Hacking

- Summary
  - Developing a fake update server and sending malicious update file
  - Hacking a server for spread of malware



Case 2 : Update Server Hacking

- Analysis(A company)
  - Upload a webshell on web server
  - Acquisition of ROOT using the local privilege escalation vulnerability

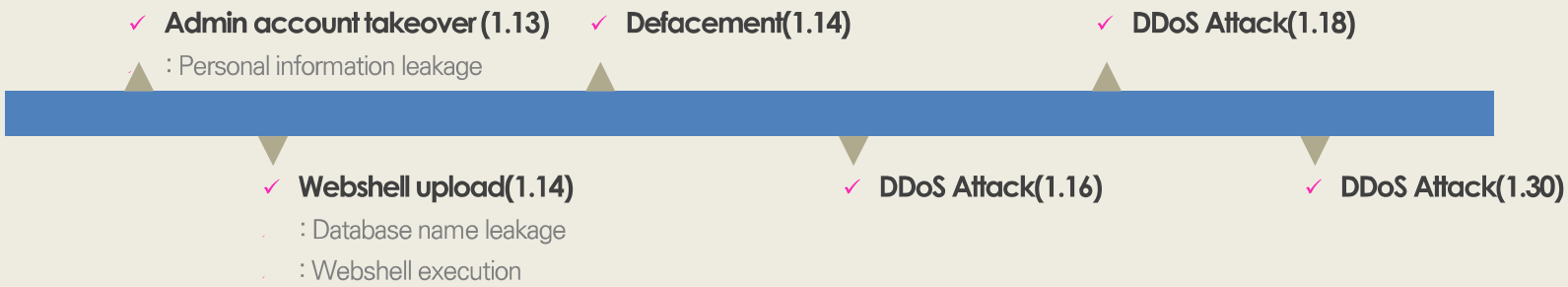
  - Rerouting of the request traffic to the fake update server via ARP spoofing
  - Transmission of malicious update file containing falsified field to user

Case 2 : Update Server Hacking

- Analysis(B company)
  - Hijacking of user account through brute-force attack
  - Pharming type malware that leaks certificate and financial data
  - KISA, Blocking of information-leaking site, pharming and C&C IP access

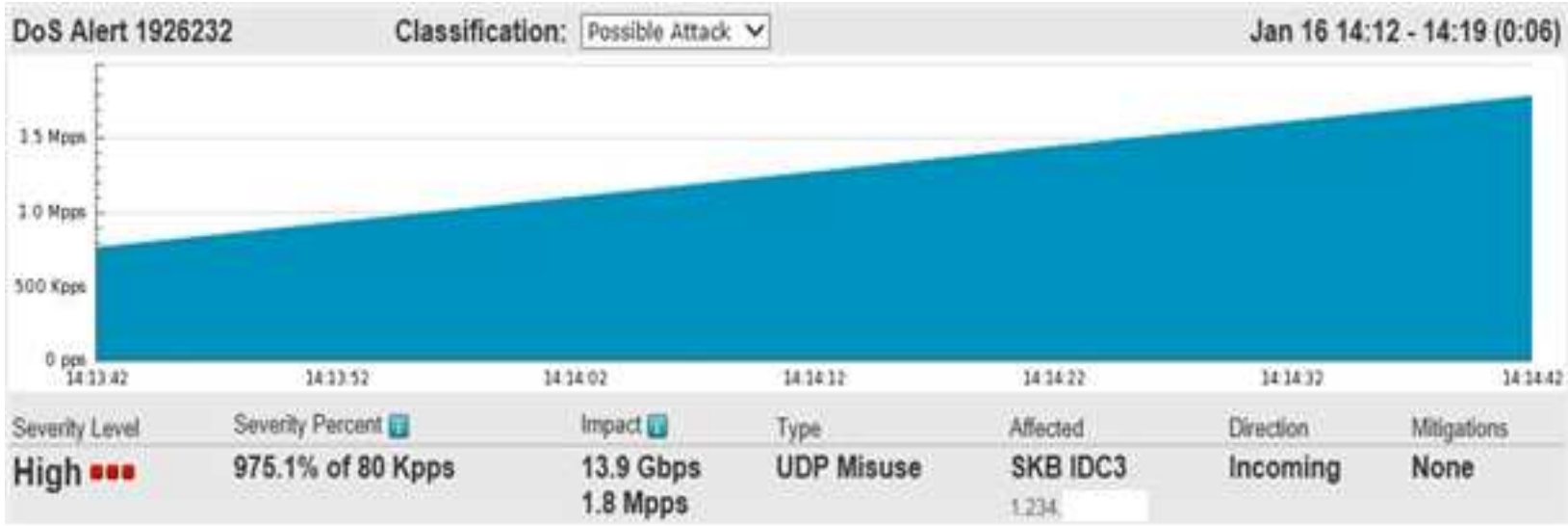
Case 3 : Anonymous

- Entertainment agency DDoS attack(2016. 1)
  - Cyber attack as the result of an international and political issue
  - Server hacking, Defacement, Information leakage, DDoS



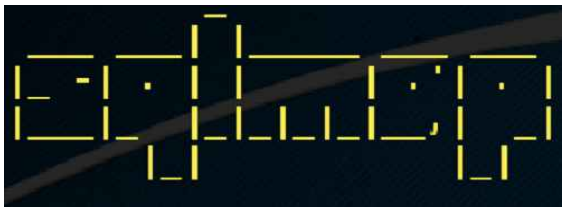
Case 3 : Anonymous

- Analysis & Response(DDoS)
  - DNS DrDoS(Distributed Reflect Denial of Service)
  - Defense against DDoS attack by using the DDoS Shelter system



Case 3 : Anonymous

- Analysis & Response(Hacking)
  - (Account takeover) SQL-Injection automation tool



Pangolin

  - (Information leakage) Database structure & Personal Infomation leakage

Thank you

lsw1@kisa.or.kr