Security

□ 최근 랜섬웨어, 가상통화 취급업소 및 IP 카메라 해킹 등 사이버 사고가 빈번히 발생하여 국민 불안감 확산

○ 국내 가상통화 취급업소 해킹사고로 약 1,000억원('18)의 손실이 발생하는 등 사이버 사고에 따른 글로벌 피해 규모는 약 6천억 달러(676조원)에 달하는 것으로 추산(맥아피, '17)

□ 드론, 자율차 등 ICT 기술이 발전·확산되면서 사이버위협이 정보통신 서비스의 안전과 디지털 경제 발전의 걸림돌로 작용

○ 기존 PC·네트워크 중심의 사이버보안 대응체계로는 신기술을 기반으로 새롭게 발생하는 사이버위협 대응에 한계 발생

블록체인	• 블록체인 거래기록이 조작되어 가상통화 유출사고 발생('18, 일본)
드론	• 제14회 해킹방어대회(HDCON)에서 드론 해킹 시연('17, 한국)
자율차	• 전파 송신기를 활용한 자동차 해킹으로 차량 도난 사고 발생('17, 영국) • 루벤대(KU Leuven), 스마트카 테슬라 모델S 해킹 취약점 발견('18, 벨기에)

❑ 사이버위협 및 대응 현황

○ 인터넷에 연결되는 기기가 폭발적으로 증가함에 따라, 신종 악성코드, 보안취약점 등 사이버위협 또한 급격히 증가

※ 일 평균 약 4만3천개의 신규 악성코드 등장 (출처: 카스퍼스키, '17년)

※ IoT 취약점 대응 건 수 3년간 456% 증가('15년 : 156건→ '17년 : 867건) (출처 : KISA)

- 특히, IP카메라 사생활 침해, 가상통화 취급업소 등 사회적 파급효과가 큰 사이버 침해사고 및 피해 증가

※ IP카메라 4,912대를 해킹하여 개인 사생활 몰래 촬영한 일당 검거('18.10)

※ 코인레일, 빗썸('18.6) 등 가상통화취급업소에 최근 3년간 7건(1,000여억원의 해킹피해 발생

○ 미·영·중·일 등 세계 각 국은 각종 사이버보안 전략을 마련하며 보안 투자를 확대, 글로벌 보안시장 규모는 연평균('18~'21) 약 7.9% 성장 전망

* '18년 약 960억 달러(약 107조원)에서 '21년 약 1,215억 달러(약 136조원)('18.3, Gartner)

1)

암호, 범용 인증,
보안 취약성 분석, 디바이스
보안, 시스템 보안, 악성코드 등

2)

CTI(Cyber Threat Intelligence),
DDoS 대응, 경계 보안, 통신망
보안, 보안 관제 등

3)

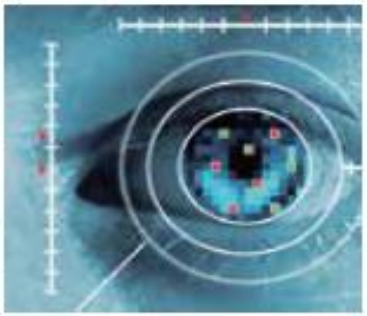
클라우드 보안, 웹·이메일 보안,
프라이버시 보호, 저작권 보호,
핀테크 보안, 디지털 포렌식 등

〈 정보보안 〉

4)

지능형 영상감시,
VMS/통합관제,
CCTV 인프라 보호 등

5)



바이오 인식 센서,
휴먼 인식 및 검색, 보안 검색
및 무인전자경비 등

6)

7)

8)

스마트 홈·빌딩 보안, 자동차 보안,
선박·해양 보안, 비행체·항공 보안,
헬스케어 보안, 인공지능 및 로봇 보안 등

〈 물리보안 〉

〈 융합보안 〉

2. 기술분류(Technology Tree)

중분류	소분류	요소기술
정보보안	암호	암호 설계/분석, 암호 부채널 분석
	인증/인가	범용 인증, ID 관리 및 접근제어, 바이오 인증
	보안 취약성	SW 취약점 분석, HW 취약점 분석
	디바이스 보안	디바이스 보안 관리, 디바이스 펌웨어 보안, 디바이스 하드웨어 보안
	시스템 보안	운영체제 보안, 가상화 보안, 시스템 접근통제
	악성코드	악성코드 대응, 랜섬웨어 대응
	유선네트워크 보안	경계 보안, 보안 연결, DDoS 대응
	무선네트워크 보안	이동 통신망 보안, 무선 근거리 통신망 보안
	위협 분석 및 관제	지능형 사이버위협 분석, 보안정보 분석 및 로그 관리, 보안 관제
	클라우드 보안	가상화 플랫폼 보안, 클라우드 보안 서비스, 소프트웨어 정의 보안
	응용 보안	웹 보안, 이메일 보안, 데이터베이스 보안
	데이터 보안	프라이버시 보호, 데이터 유출 방지, 디지털저작물 침해/권리 보호
	전자화폐·핀테크 보안	전자화폐 보안, 블록체인 보안, 전자거래 이상행위 탐지, 거래·사기 방지
	디지털 포렌식	디지털 증거 수집 및 분석, 안티 포렌식 대응
물리보안	휴먼/바이오인식	바이오인식 센서, 바이오인식 엔진, 휴먼인식 및 검색, 휴먼/바이오인식 응용
	CCTV 감시/관제	카메라 및 저장장치, VMS/통합관제, 지능형 영상감시, CCTV 인프라 보호
	보안검색 및 무인전자경비	수화물/화물 검색기, 알람 모니터링, 무인전자경비 서비스
융합보안	홈·빌딩 보안	홈·빌딩 디바이스 보안 및 제어, 홈·빌딩 데이터 프라이버시
	산업제어시스템 보안	스마트공장 보안, 기반시설 보안
	자동차 보안	자동차 내·외부 통신 보안, 자동차 내·외부 접근제어, 자동차 침입탐지, 자동차 보안취약점 진단
	선박·해양 보안	자율운항 선박 해킹 방지, 해운항만 통신 보안, 해양 인프라 보안 관제
	비행체·항공 보안	무인비행체 보안, 항공 인프라 보안 관제
	헬스케어 보안	헬스케어 디바이스·센서 보안, 의료 데이터 보안 및 공유
	기타 ICT 융합보안	인공지능 및 로봇 보안, 스마트 에너지 보안

- **(암호/인증)** 경량·양자내성 암호 등 환경 적합형 다기종·고신뢰 암호 기술 개발이 활발히 추진 중이며, 생체인식기반 인증서비스가 확대되는 추세
  - IBM/Microsoft(동형 암호), NIST(양자내성 암호 공모사업), RSA(멀티팩터인증) 등
- **(디바이스 보안)** SW 개발 생명주기 전체에 걸친 보안 테스트가 진행되고 있으며, 보안 내재화를 위한 SDL 및 Secure Composition 연구가 활발함
- **(악성코드)** Zero-day 악성코드 대응 기술에 집중한 연구개발 진행 및 일부 솔루션 출시됨
  - AI 기반 신종 악성코드 탐지 기술 개발 (카스퍼스키, 트랜드마이크로, IBM, RSA 등)
- **(네트워크 보안)** 정교한 사이버 공격 대응을 위해 머신러닝, 인공지능 기반의 지능형 보안 기술, 능동적 사전예방 MTD 기술, 공격 대상을 숨기기 위한 Deception Security 기술이 연구되고 있음
- **(위협 분석 및 관제)** 네트워크 및 시스템 보안 제품군을 통합한 보안 이벤트 정보관리 기술과 빅데이터 처리 기술을 활용한 지능형 보안 기술에 대한 연구가 본격화되고 있음
- **(클라우드 보안)** 접근 제어, 위협 방지, 데이터 보호 등의 통합된 보안 기능을 클라우드 서비스 형태로 제공하는 SecaaS와 보안 기능 가상화 기술을 사용하여 보안 서비스를 제공
- **(데이터 보안)** GDPR 법령 시행에 따라 기업이 수집해 활용하는 개인 데이터에 대한 프라이버시 강화 기술과 개인이 자신의 데이터를 직접 관리, 활용하는 기술을 개발 중
- **(핀테크 보안)** GDPR, 오픈뱅킹, 인공지능 등 새로운 정책과 신기술이 적용되는 핀테크 서비스 보안을 위한 체계적인 연구를 추진 중
  - 다양한 응용에 블록체인을 활용하기 위해 ID관리, 프라이버시 보안 기술 개발과 전자화폐와 블록체인을 위한 원천 보안 기술 분야의 연구를 활발히 진행 중

- **(휴먼/바이오인식)** AI기반 바이오인식 기술이 지능형 도시감시 영역으로 확대되어 스마트시티 전체의 안전을 위한 통합 프레임워크 형태로 발전하고 있음
  - NGI(미국 FBI)는 미전역 공공장소에서 얼굴, 홍채, 음성, 지문, 걸음걸이 등 바이오인식을 통해서 위험인물을 실시간 인식, 추적, 검거하는 데 활용
- **(CCTV 감시/관제)** 지능형 CCTV를 중심으로 치안정보, 환경/이벤트 정보 등 빅데이터 복합 분석을 통해 가까운 미래의 범죄를 사전 예측하고 선제적으로 대응, 예방
  - DAS(미국 NYPD), 텐왕(중국) 등은 지능형 CCTV를 통해서 도시/국가 전체의 범죄 등 위험상황을 실시간 감지, 대응하는 지능형 도시감시의 트렌드로 부각되고 있음
  - Cortica AI(인도), PredPol, DAS(미국)는 이상행동, 이상상황 및 치안 빅데이터를 수집하고, 복합적으로 분석해서 위험상황을 미리 예측하고 예방하는 사회안전시스템 운용 중

- **(의료/헬스케어 보안)** 착용형/이식형 의료기기 해킹 방지, 생체정보 기반 보안통신 기술 등 활발히 연구되고 있음
  - 의료기기 악성코드 탐지기법 등 60여개 이상의 헬스케어 관련 보안 프로젝트 진행(메사추세츠대학)
- **(산업제어시스템 보안)** 산업제어시스템 네트워크 트래픽 및 행위 정보 기반 이상행위 탐지 및 방화벽 등의 기술을 적용하여 보안성을 강화하는 추세 (Tofino, Indegy 등)
- **(무인 이동체 보안)** 차량 PKI기반 V2X 통신 보안은 실증단계, IMO 해사안전위원회 등 해양선박 예산투자 확대추세, 안티드론, 키관리 기술 연구 활발히 진행
  - 해상 초고속광대역위성통신 서비스 'Fleet Xpress'를 위한 통합위협관리시스템 개발 중 (인말새트)
- **(홈/빌딩 보안)** 내외부 트래픽 분석기반 이상징후 탐지 및 제어 제품 출시 (맥아피, 징박스 등)

나 핵심 이슈

- 현존 암호체계 한계를 극복하기 위한 양자 키 분배, 양자내성 암호(PQC), 경량 암호 원천기술 확보
- 인공지능 기술을 활용한 보안 관제 로봇, 공격그룹 추적, 사이버 위협 예보 등 사이버 위협을 선제적으로 예측하는 기술 및 IoT·모바일 환경에서의 악성코드 등 사이버 공격 대응 및 보안 인텔리전스 기술 확보
- 사이버 공격 침투경로를 자동으로 격리하고 SW·HW 취약점을 자동으로 탐지·패치하여 피해를 입은 시스템의 복원력을 강화하는 기술 확보
- 5G, IoT 네트워크 환경에 특화된 침입 방지 기술, 인공지능을 활용한 LPWAN, LB-IoT 보안 기술 고도화
- 클라우드 환경의 통합 보안위협 인텔리전스 기술 및 시스템, 네트워크, 데이터의 구성을 수시로 변경하여 공격을 스스로 방어·예방하는 기술 확보
- IoT, O2O 등 새로운 핀테크 환경에서 요구되는 편의성과 보안성 제공 및 재화의 디지털화 과정에서 발생하는 금융사고 대응 및 예방 기술 확보
- 개인정보보호 강화를 위한 대용량 정형·비정형 빅데이터(텍스트, 영상, 이미지 등)의 민감 정보 비식별화, 온라인 ID 절도(Identity Theft) 방지 및 프로파일링 기술 확보
- 자율 이동체의 공통핵심 기능에 대한 사이버 위협 대응 기술 고도화 및 해킹이나 오인식·오작동 등 오류로부터 자율 이동체의 안전을 보장하는 기술 확보
- AI 기반의 의료 정보 저장·활용과 스마트 의료기기 신뢰성 강화를 위한 보안위협 대응 및 안전한 헬스케어·의료시스템 구축
- 산업용 사물인터넷 환경으로 진화함에 따라 제조운영 기술(OT)과 정보 기술(IT)을 통합하는 스마트제조 보안 기술 확보

나 기술로드맵

구분		2018	2019	2020	2021	2022	2023
달성 목표	서비스	지능형 전력 AMI서비스 보안	진화형 사이버방어 가시화 서비스	스마트시티 위험 예측	다중 AI 백신	400G급 Anti-DoS	디지털새도우 보안관제
		9) 		10) 		11) 	12) 
		생체인식기반 웹서비스 인증	펌웨어 보안 취약성 분석	비정형데이터 비식별화	의료기기 해킹방지	AI 포렌식	유전체 프라이버시 보존 암호
		13) 	14) 	15) 	16) 	17) 	18) 
	제품	차량 PKI 시스템	IoT 경량 OS 보안	취약점 검증 툴	200G급 모바일보안	디지털 신분증	양자내성 블록체인
		19) 	20) 	21) 		22) 	23) 
		FIDO2	사이버 자가방어 솔루션	AI 위협예측엔진	메디컬 침입탐지시스템	생체암호	협업형 엔드포인트 보안솔루션
		24) 			25) 	26) 	27) 

Top 10 Cyber Security Trends for 2019

01
The Coming Pain of GDPR

General Data Protection Regulation is expected to have a significant effect in 2019.

02
Increase in Sabotage, Espionage and Crime by Rogue Nation-States

The cyber security teams have to rely on techniques of breach detection.

03
Dark Ages of Single Factor Passwords

They are still the main security protection for most organizations in spite of the ease and low cost deployment of the multi-factor authentication solutions.

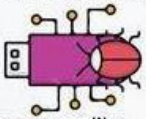
04
Insecure Clouds

Inspite of the continual publicity of repeated breaches, most organizations still fail to deploy and enforce good housekeeping across their entire cloud data estate.

05
Growth of Cyber Hygiene in companies

Response from the organizations will be in the form of cyber education combined with monitoring, measuring, and testing cyber behavior of staff.

06
Malware Challenges



Some areas like ransomware will see an increased sophistication together with increased malware volumes in some areas and new malware approaches.

07
Increased Risks with bad Housekeeping & Shadow IT Systems

Both cases are very easy attack surfaces with substantial oversight, budget challenges,internal politics and were seen in the past as a lower resolution priority.

08
More Challenges in IoT

With the lack of standard or perceived security need, IoT is going to be deployed even more and create insecurity in areas which used to be secure.

09
Boardroom Cyber Security

This trend will accelerate this 2019 with boards demanding understanding and clarity in an area which was often delegated as subcomponent of the role of CISOs.

10
Unseen Nightmare of DDoS

DDoS is a dirty secret for most organizations, with attacks continuing to grow in 2019 together with the price of defending against them.

Big Numbers

Web Threats

More than
1 Billion
Web requests analyzed each day
Up 5% from 2016

1 in 13
Web requests lead to malware
Up 3% from 2016

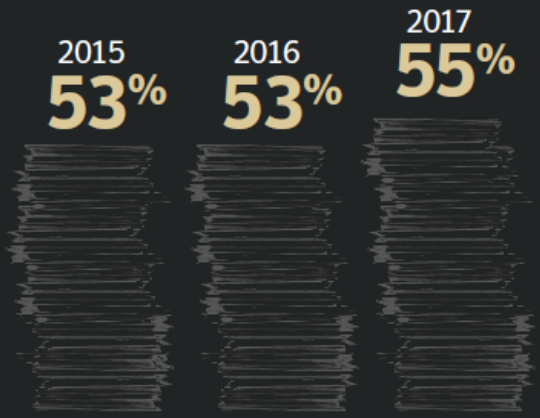
Malware

92%
Increase in new downloader variants

80%
Increase in new malware on Macs

Email

Percentage spam rate

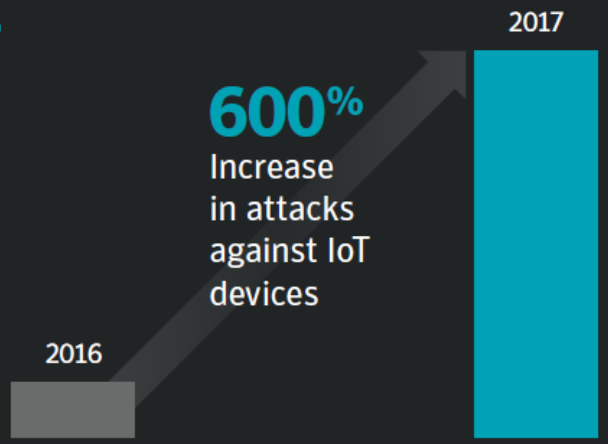


Ransomware

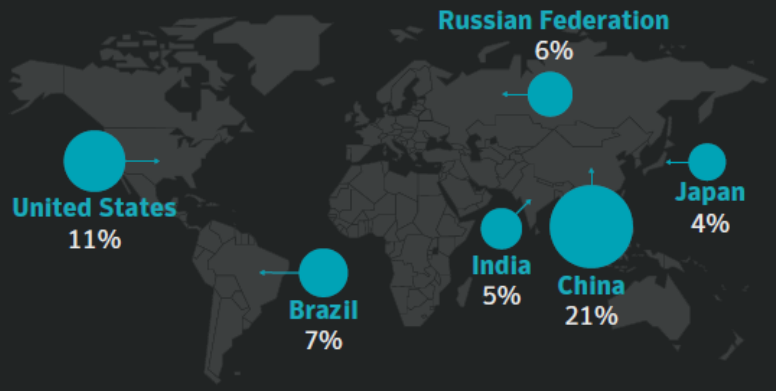
5.4B
WannaCry attacks blocked

46%
Increase in new ransomware variants

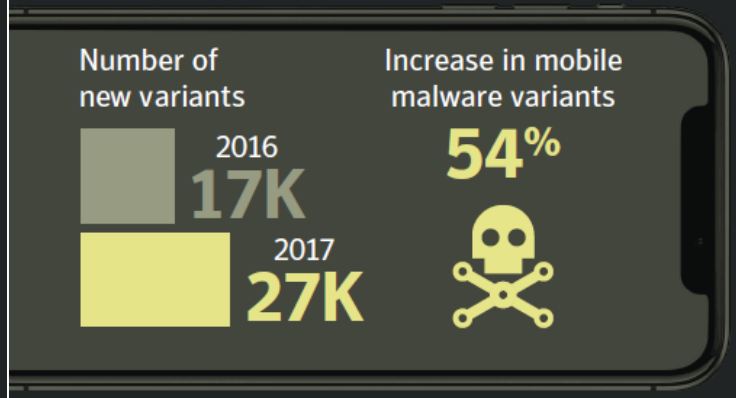
IoT



Attack Origin



Mobile



24,000 Average number of malicious mobile apps blocked each day

App categories that have the most malicious mobile apps are:

- **27%** Lifestyle
- **20%** Music & Audio

Leaky apps – what sensitive information do they most often leak?

- **63%** Phone Number
- **37%** Device Location

Symantec 보안보고서

- **모바일** 보안 위협이 지속적으로 증가하는 추세(2017년, 54% 증가)
- 2017년에는 시장이 조정되면서 평균 몸값이 522달러로 낮아지면서 **랜섬웨어**가 범용화되었음

- **Coin mining**
  - 코인 채굴 공격이 2017년에 8,500% 급증
  - 훔친 처리 능력과 클라우드 CPU 사용량을 이용하여 암호 화폐를 채굴


웹사이트
1
접속
PC감염
2
3
DECRYPT_INSTRUCTIONS.html
DECRYPT_INSTRUCTIONS.txt
DocFiltersRes.kor.encrypted
EquationRes.kor.encrypted
EzSamCtrl.kor.encrypted
EzSAMCtrl.ocx.encrypted
EzSamCtrl.tlb.encrypted
사용자 PC 파일 암호화
익명 웹사이트
4 파일 복호화를 위한
금전요구 안내 페이지
5 파일 복호화 프로그램
구매 페이지
해커

Ransomware

숫자로 보는 2017년 랜섬웨어

약 950,000명

2017년 공격을 받은 카스퍼스키랩 사용자 수
(2016년 약 150만 명)

신종 랜섬웨어 수:

50% 감소

2016년 62개 → 2017년 38개

랜섬웨어 변종 수

약 2배 증가

2016년 54,000 → 2017년 96,000

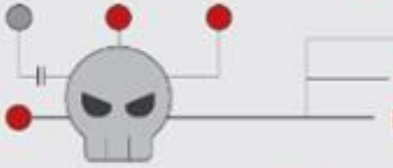
랜섬웨어 공격을
받은 26%가

기업
컴퓨터

2017년 공격을 받은 기업 중 65%가
데이터 전체 또는 상당량에 대한

액세스 권한 유실

3건의 대규모 공격



WANNACRY - 5월 12일
EXPETR - 6월 27일
BADRABBIT - 10월 말

전세계적으로 70만대의 PC가 WANNACRY에 감염

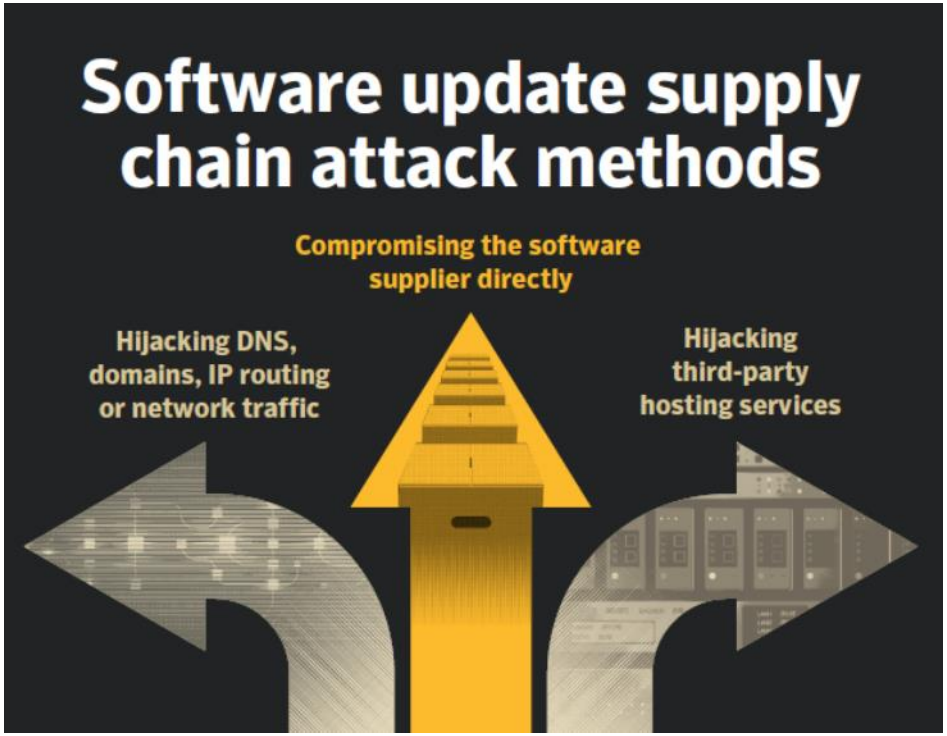
대가를 지불한
기업 6곳 중 1곳이
데이터 복구에

실패

KASPERSKY

Major destructive malware attacks

- 공격의 71%가 **스피어 피싱**으로 시작
- 합법적인 소프트웨어 패키지에 악성 코드를 심는 **소프트웨어업데이트** 공급망 공격은 2017년에 최대 200% 증가
  - **Petya**는 우크라이나의 합법적인 회계 소프트웨어를 진입 지점으로 삼고 기업 네트워크 전반에 확산되면서 공격자의 악성 페이로드를 배포하여 전 세계적으로 심각한 타격을 입혔음



Cybersecurity

- Computer Systems
- Data
- Privacy

- Mobile
- Network Security

- Government
- Industry
- Military

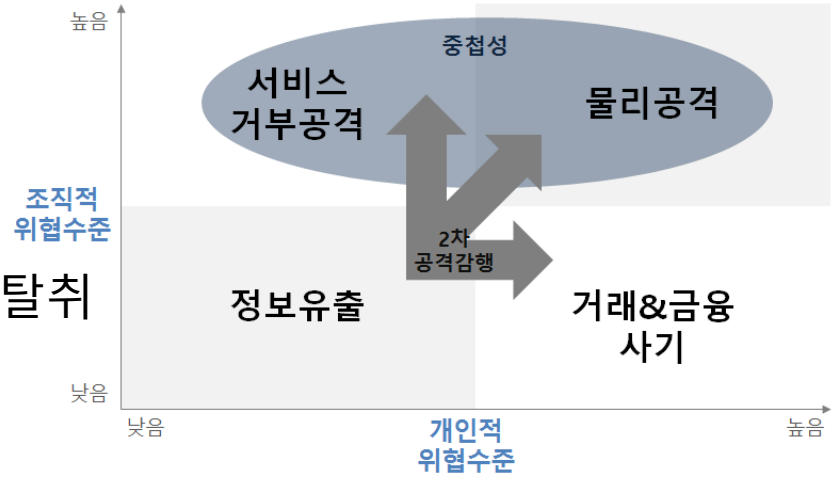
- '기밀성',
- '무결성',
- '가용성',
- '인증',
- '부인방지',
- '접근제어',
- '추적불가능',
- '익명성',
- '확장성',
- '실시간성'

10대 기술

사이버 공격

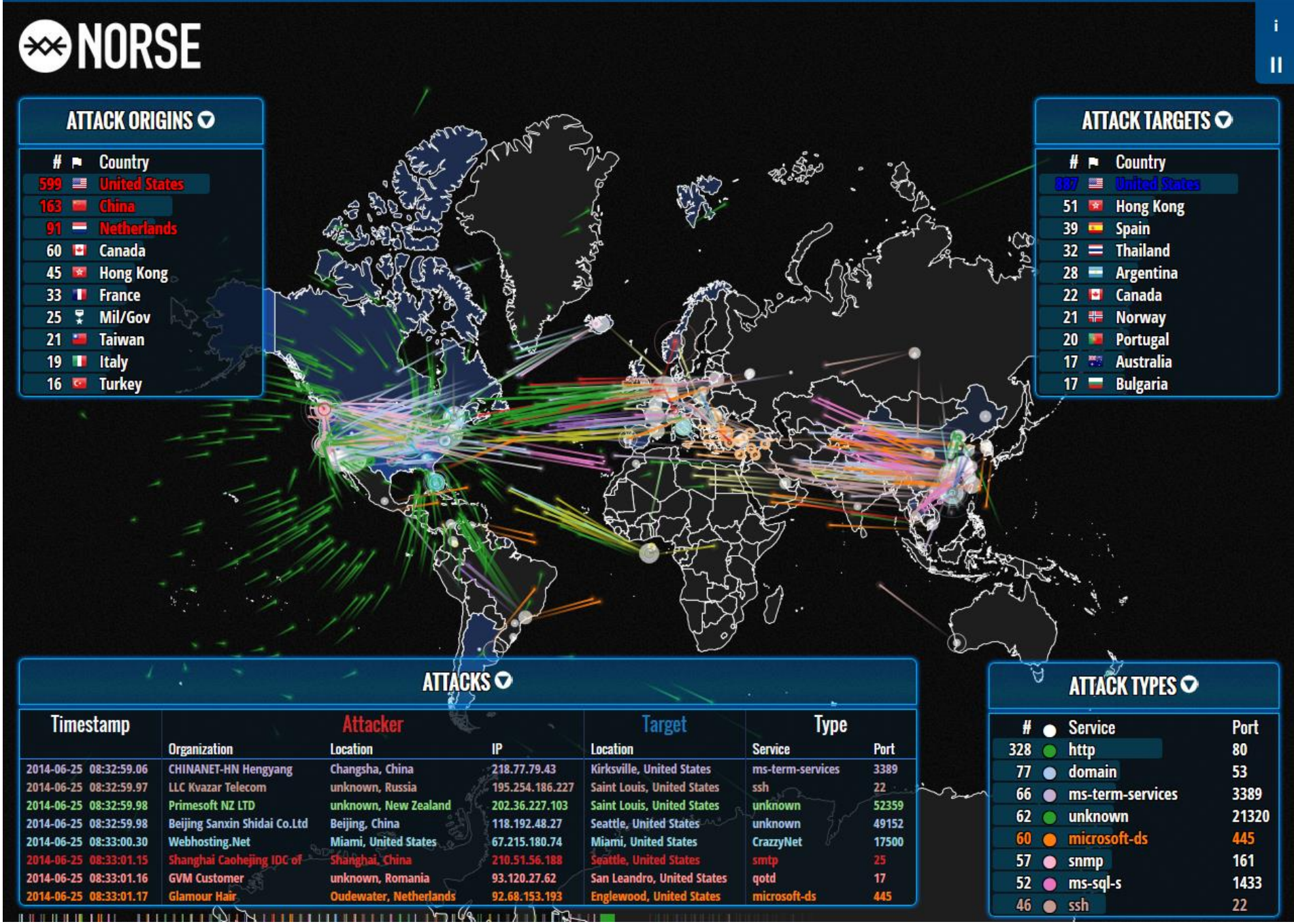
- 정보를 포함한 재산탈취 및 주요 시설 파괴가 **해킹**의 감행 목적

사이버공격은 사이버를 활용해서 행하는 **공격**



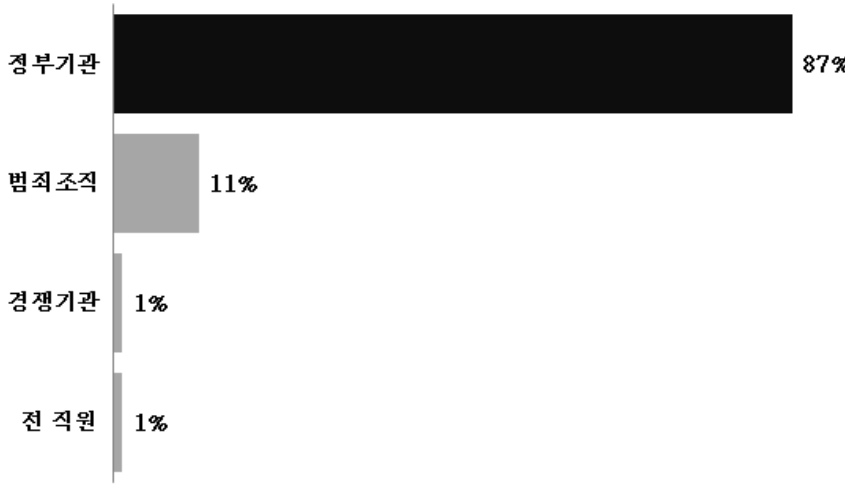
국가 및 개인정보를 해킹 탈취

자율주행자동차
스마트그리드
홈네트워크


NORSE
ATTACK ORIGINS
Country
599 United States
163 China
91 Netherlands
60 Canada
45 Hong Kong
33 France
25 Mil/Gov
21 Taiwan
19 Italy
16 Turkey
ATTACK TARGETS
Country
887 United States
51 Hong Kong
39 Spain
32 Thailand
28 Argentina
22 Canada
21 Norway
20 Portugal
17 Australia
17 Bulgaria
ATTACKS
Timestamp
Attacker
Target
Type
Organization
Location
IP
Location
Service
Port
2014-06-25 08:32:59.06 CHINANET-HN Hengyang Changsha, China 218.77.79.43 Kirksville, United States ms-term-services 3389
2014-06-25 08:32:59.97 LLC Kvazar Telecom unknown, Russia 195.254.186.227 Saint Louis, United States ssh 22
2014-06-25 08:32:59.98 Primesoft NZ LTD unknown, New Zealand 202.36.227.103 Saint Louis, United States unknown 52359
2014-06-25 08:32:59.98 Beijing Sanxin Shidai Co.Ltd Beijing, China 118.192.48.27 Seattle, United States unknown 49152
2014-06-25 08:33:00.30 Webhosting.Net Miami, United States 67.215.180.74 Miami, United States CrazzyNet 17500
2014-06-25 08:33:01.15 Shanghai Caohejing IDC of Shanghai, China 210.51.56.188 Seattle, United States smtp 25
2014-06-25 08:33:01.16 GVM Customer unknown, Romania 93.120.27.62 San Leandro, United States qotd 17
2014-06-25 08:33:01.17 Glamour Hair Oudewater, Netherlands 92.68.153.193 Englewood, United States microsoft-ds 445
ATTACK TYPES
Service Port
328 http 80
77 domain 53
66 ms-term-services 3389
62 unknown 21320
60 microsoft-ds 445
57 snmp 161
52 ms-sql-s 1433
46 ssh 22

Stuxnet

사이버공격 경로의 비중
(출처 : Verizon, June 2016)



- 2010년 7월 이란의 원자력발전소 해킹사건
  - 1,000개의 **원심분리기 파괴**
  - USB를 통하여 지멘스사의 SCADA 해킹
- 500kb사이즈의 웜바이러스
- 미국, 이스라엘 개발 추정

2011년 4월 농협 금융전산 마비

- 농협 서버 절반 손실, 약 550여대의 서버 하드디스크 파괴됨
- 복구하는 데 일주일
- 2010년 9월 하청업체 직원의 노트북에 잠입한 멀웨어가 원인

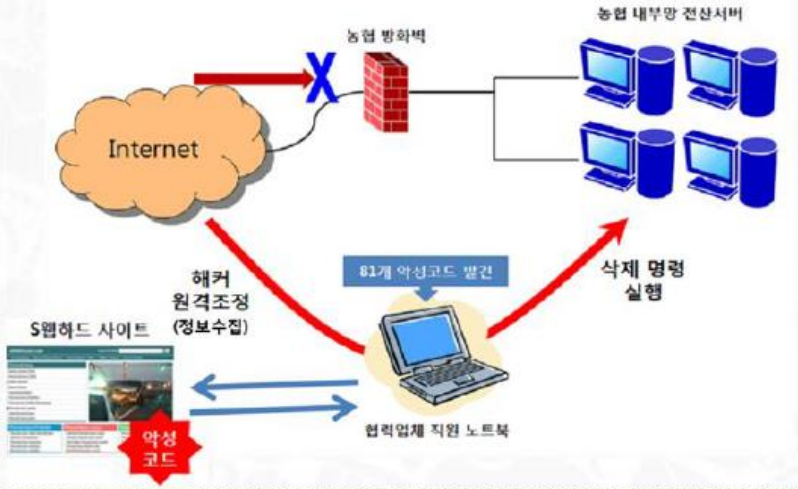
일반 카페에 있는 웹하드 P2P무료쿠폰을 이용해 무료영화를 다운로드 받음

- **APT**(Advanced Persistent Threat)
- APT공격은 지속적으로 특정 기관을 반복해서 공격을 가하는 기법으로 정의

	기존 공격방식	APT 공격방식
공격자	개인해커, 소규모 해커집단	정부, 대형기관, 대규모 해커집단처럼 해킹 기술이 우수하고 자금력이 많은 조직
공격대상	불특정 다수	정부, 금융과 같은 대형 기관
목적	금전적인 이득, 해킹실력 자랑	경쟁 조직에 피해를 주거나 전략적 우위확보
침입방법	단기간, 일회성 공격	느린 속도로 장기간 공격, 공격이 성공할 때 까지 제로데이 공격감행

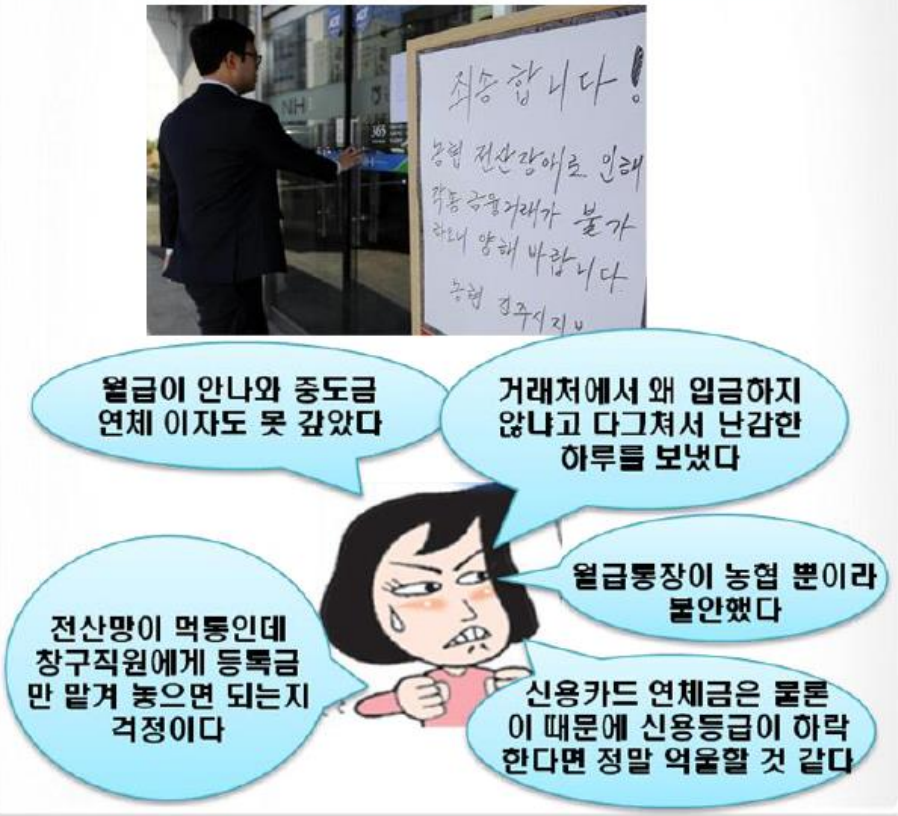
표 2-1. 기존공격방식과 APT 공격방식 (출처 : Ping Chen, etc., 2014)

사건 발생 및 대응



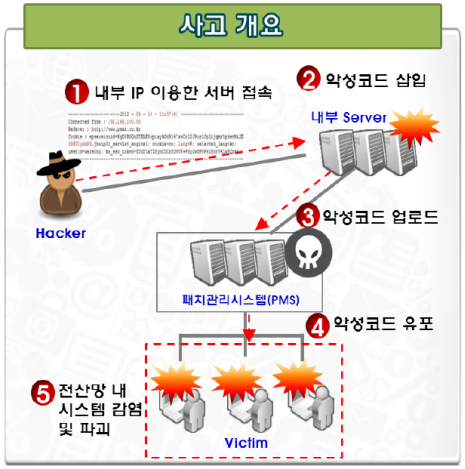
- '10.9.4 – 유지보수업체 직원 노트북 악성코드 감염
  - ※ 7개월 이상 집중모니터링으로 각종 정보 유출
- '11.4.12. – 노트북에 공격파일 설치 → 공격 실행 → 공격 증거 삭제
- '11.5. 3 – 검찰 수사결과 발표

사건 피해 사례



3.20 대란

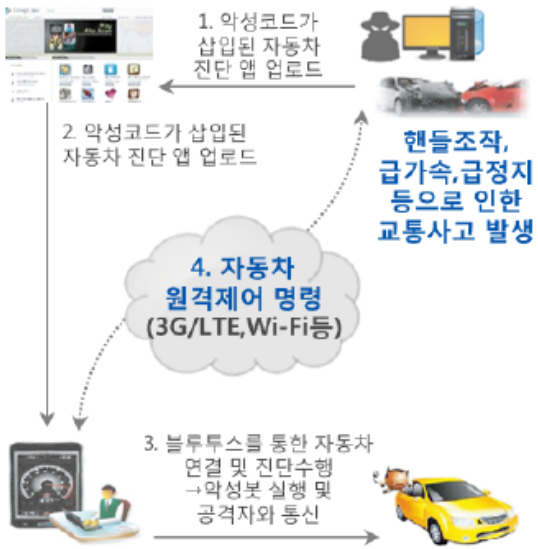
- 7개 기관에서 사이버공격으로 전산망이 마비
- 2012년 6월부터 시스템에 침투 해서 2013년 3월까지 10개월간 1,560회나 해킹
- 총 4만 8천여 대의 PC와 서버가 피해
- 8,672억원 피해 추정
- 공격방식은 APT
- 공격유형은 DDoS



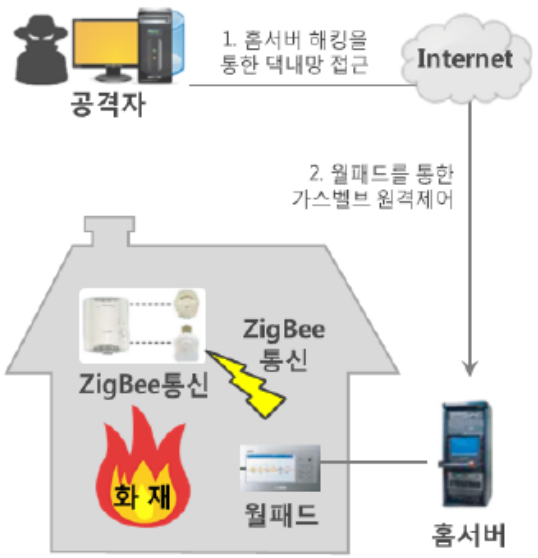
원인 및 영향

1. 내부 IP를 이용한 서버 접속
2. '트로이 목마' 방식의 악성코드 감염
3. 개별 PC의 소프트웨어 업데이트와 운영체제 패치 등을 관리하는 서버에 악성코드 업로드
4. 계획된 시간에 업로드 된 악성코드 유포
5. 전산망 내 시스템이 감염되어 부팅영역(MBR) 파괴

악성코드가 감염된 차량진단 앱을 통한 자동차 원격제어



홈 서버 해킹을 통한 댁내 가스밸브 원격개방



심박기 신호정보 위·변조를 통한 전류량 과잉공급

자율주행자동차 보안

- ECU(Electronic Control Unit)를 조작하여 자동차를 원격으로 조종
- GPS 통신을 해킹해 정보를 탈취
- DDoS 공격 등을 통해 교통신호를 방해

드론 보안

- 현재 드론의 보안수준은 간단한 해킹 공격만으로도 쉽게 뚫릴 수 있을 정도
- 2008년 이라크 무장단체들이 미국의 최신 무인항공기 Predator 해킹
  - 해킹 프로그램이 당시 가격으로 28달러
- GPS신호를 위변조하여 드론을 해킹
  - 2011년 12월, 록히드마틴과 이스라엘이 공동으로 제작한 무인 스텔스 RQ-170가 이란 영내를 정찰하다가 이란의 스푸핑 공격으로 포획됨
- 재밍공격으로 드론을 해킹
  - 2012년 5월 10일 한국 해군 무인기 추락 (북한 소행)

스마트그리드 보안

- Stuxnet
- Night Dragon
  - 미국, 대만, 그리스, 카자흐스탄에 위치한 글로벌 에너지 기업을 대상
  - 중국 소행 추정
  - 고급정보 탈취
- 스마트미터를 활용한 사이버공격
- 서비스거부공격으로 전력망을 마비시켜 버릴 수도
- 송배전망 공격

헬스케어 보안

- 세 가지 유형
  - 정보유출,
  - 정보 위변조,
  - 랜섬웨어
- 웨어러블 기기, 네트워크 통신, 병원 해킹
- 병원을 대상으로 하는 랜섬웨어는 특히 치명적 (생명 담보)
  - (예)수술로봇을 해킹해 제어권을 획득

사건	일시	이유	상세
인공 심장박동기/ 인공심장해킹 취약성	2008. 05	해킹에 의한 인공심장 오작동	인공심장박동기/인공심장을 해킹해 기기 오작동 유발이 가능하다는 연구발표
보스턴 BIDMC 병원 데이터 유출 - (1)	2011. 07	악성코드 감염	2,021명 환자기록이 인터넷으로 유출
일리노이주 해킹 및 데이터 인질극	2012. 06	데이터 랜섬웨어	일리노이주 의료기관 시스템에 해커 침입 후 데이터를 암호화한 후 금액요구
보스턴 BIDMC 병원 데이터 유출 - (2)	2012. 07	전문의 노트북 도난	노트북 내 데이터 암호화 부재와 도난으로 인해 3,900명 환자기록 탈취
생화학 자동분석장치 소프트웨어	2013. 01	생화학 자동 분석장치에 연결된 데이터 해킹	COBAS ITEGRA400 plus 분석기에서 사용하는 오라클의 데이터베이스 취약점을 이용해 원격으로 잘못된 데이터 저장

사물 인터넷(IoT) 디바이스 70%가 보안 취약점에 노출

Insecure Web Interface

60% 디바이스/모바일 앱/클라우드 웹 XSS 공격에 취약, 부적절한 세션 관리, 기본 사용자 ID 사용

Insufficient Authentication/Authorization

80% 디바이스/모바일 앱/클라우드 부적절한 패스워드 관리(복잡도, 길이)

70% 디바이스/모바일 앱/클라우드 유효 사용자 ID 확보 가능(User enumeration)

Lack of Transport Encryption

70% 디바이스 인터넷 통신 시 안전한 암호화 통신 미사용

Privacy Concerns

80% 디바이스/모바일 앱/클라우드 이름, 주소, 생년월일, 건강정보, 신용카드번호 등의 개인정보 관리소홀, 통신 시 암호화 미사용

90% 이상의 디바이스 최소 한가지 이상의 개인정보 요구

Insecure Software/Firmware

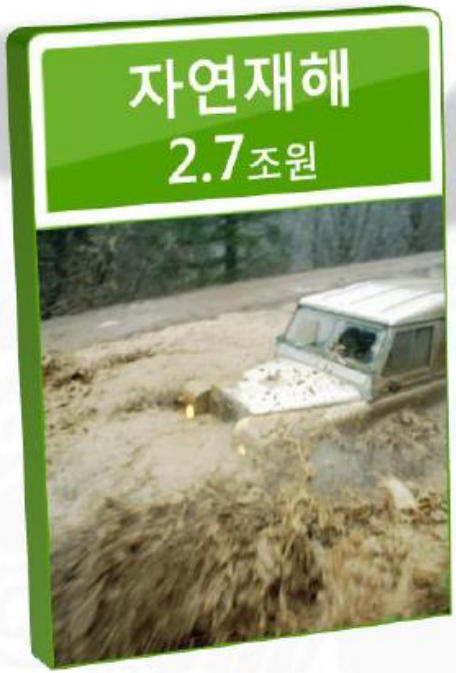
60% 클라우드로부터 디바이스 소프트웨어 / 펌웨어 업데이트 다운로드 시 암호화 채널 미사용으로 이를 중간 가로채기 후 리눅스 파일 시스템에 마운트 후 소프트웨어 / 펌웨어 조작 가능

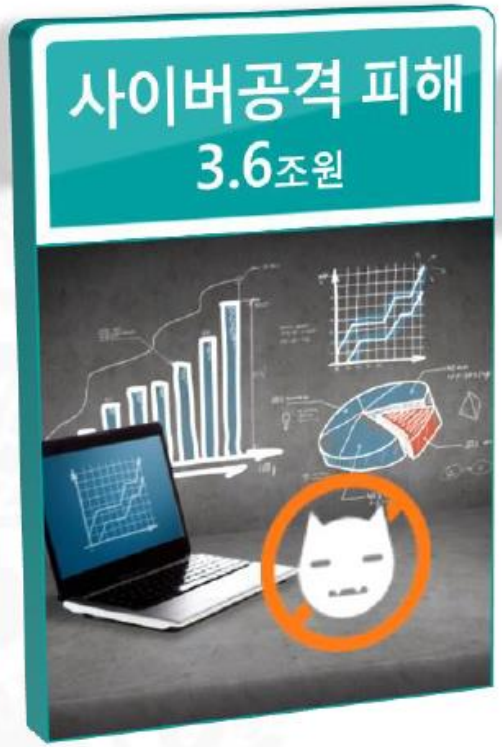
출 처 : http://www.dailysecu.com/news_view.php?article_id=8799

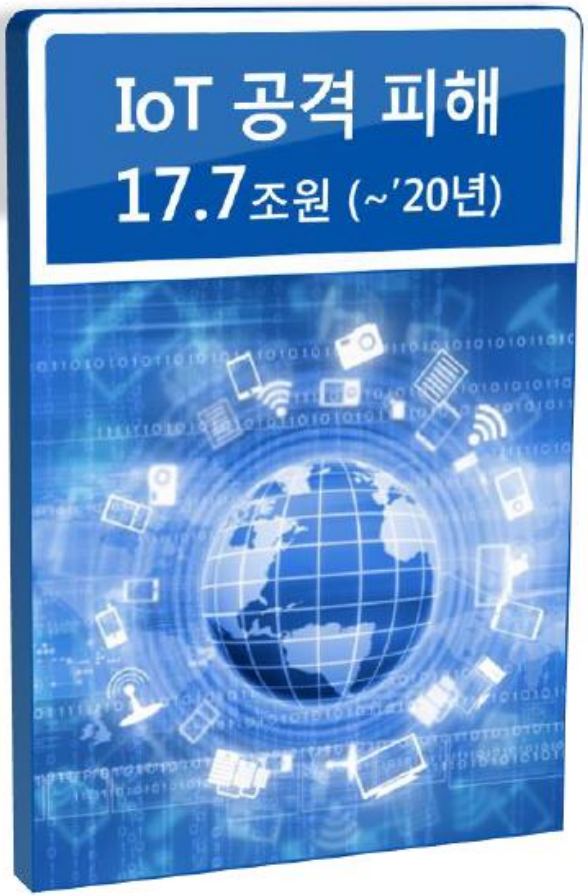
1.07건의 사고 / 100만 번의 공격

사고 유형	봇넷 활동	네트워크 손상	맬웨어 감염	이메일 손상	데이터 유출
평균적인 대응 비용	$120,000	$92,156	$61,875	$33,000	$23,062

IoT 공격으로 인한 경제적 피해 (추정)







KISA (2014), 산업연구원(2014)

GDPR (유럽 일반 개인정보보호법)

The Big Picture

Key changes of the GDPR

Fines of up to 4% of annual global turnover

€'000 → **€'000,000**

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.

Increased territorial scope

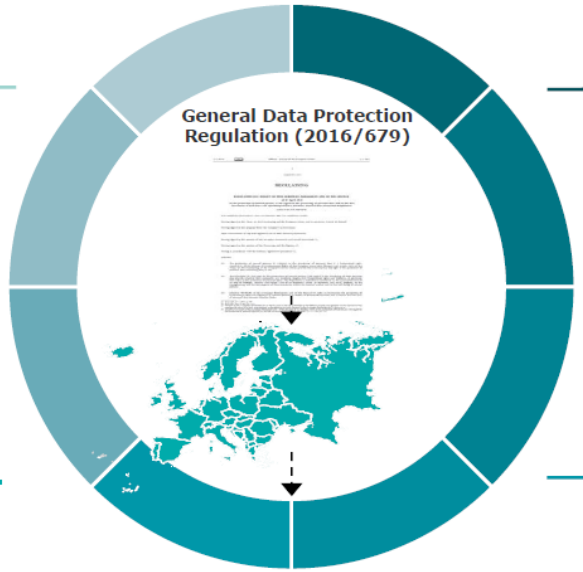
GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Explicit and retractable consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.



Breach notification within 72 hours

Now mandatory that breaches, which are likely to "result in a risk for the rights and freedoms of individuals", are reported within 72 hours of first having become aware of the breach.

Privacy By Design

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

Right to be forgotten

Entitles the data subject to have the data controller erase his/ her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Mandatory Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a company to demonstrate their compliance to the GDPR and compensate for GDPR no longer requiring the bureaucratic submission of notifications/ registrations of data processing activities or transfers based on Model Contract Clauses.

1	**넓은 영토적 적용 범위** EU 내에 설립된 기관의 개인정보 처리 활동 외에 1) EU 밖에서 EU에 있는 정보주체에게 재화나 용역을 제공하거나, 2) EU내에 있는 정보주체가 수행하는 활동을 감시(monitoring)하는 기관에 적용됩니다. ※ 위의 경우 제27조에 의거, EU 회원국에 대리인을 지정하여야 합니다.
2	**강력한 제재** '사업체 그룹' 매출 기반으로 과징금(Fines imposed by reference to the revenues of an undertaking)을 부과하며 1) GDPR 규정의 심각한 위반의 경우 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 가운데 더 큰 금액, 2) GDPR 규정의 일반적 위반의 경우 직전 회계연도의 전 세계 매출액 2% 또는 1천만 유로 가운데 더 큰 금액으로 정합니다. ※ 사업체 그룹은 동일한 사업(same undertaking)을 수행하는 것으로 봅니다.
3	**확대된 개인정보의 정의** IP 주소, 쿠키, RFID 등을 개인정보인 '온라인 식별자'의 예시로 들고 있습니다(전문 제30조). 위치정보는 개인정보의 한 유형으로 소개됩니다. 또한, 민감한 성격의 개인정보를 "특별한 유형(special categories)"의 개인정보라고 정의하면서, 유전정보(generic data)와 바이오 정보(biometric data)를 포함했습니다. 개인정보의 가명처리(pseudonymisation) 개념을 도입하였고, 이를 적용하는 경우 Data Protection by Design and Default 의 이행 등 다양한 실익을 거둘 수 있게 하였습니다. ※ 가명화 = 추가정보 없이는 정보주체 식별 곤란 & 추가정보는 기술적·조직적 조치
4	**프로세서에게도 다수의 규정이 직접 적용** Data Protection Directive 95/46/EC 와는 달리 프로세서를 직접 규제하는 내용을 다수 포함하고 있습니다. 프로세서는 적절한 문서화 의무(제30조), 적절한 보안 기준 적용(제32조), 정기 개인정보영향평가 수행(제32조), 개인정보 국외전송 기준 준수(제5장), 국가 감독기구 협조의무(제31조) 등의 의무를 부담합니다. 또한, 프로세서는 제재의 직접적 적용대상이 되며(제83조), GDPR 요구사항을 충족하지 못할 경우 정보주체로부터 배상을 요구 받을 수 있습니다(제79조).
5	**개인정보 처리 원칙의 확립** 개인정보를 처리하는 경우 1) (처리) 적법성, 공정성, 투명성 원칙, 2) (수집) 목적 제한의 원칙, 3) 개인정보 최소화 원칙, 4) 정확성 원칙, 5) 저장 제한 원칙, 6) 무결성 및 기밀성 원칙 (이상 제5조) 등 6가지 원칙을 모두 준수하여야 합니다. 컨트롤러는 이와 같은 원칙을 준수함을 증명(demonstrate compliance)해야 하는 의무(소위 "책임성 원칙(accountability principle)")를 부담합니다.
6	**적법 처리 기준의 상향** 개인정보의 (처리) 적법성, 공정성, 투명성 원칙에 따라 개인정보의 처리는 법률에서 허용한 어느 하나 이상의 요건에 해당해야 적법 처리로 인정됩니다.
7	**개인정보 국외이전 메커니즘 확립** 국외이전 = 적정성 평가(Adequacy Decision) 또는 ["적절한 보호조치(appropriate safeguards)" 제공 + 정보주체 권리 행사 가능 + 효과적인 법적 구제수단 존재]의 경우에만 가능합니다. 적절한 보호조치에는 구속력 있는 기업 규칙(Binding Corporate Rules), 표준계약서(Standard Contractual Clauses) 등이 있습니다. 기타, 1) 승인된 행동강령, 2) 인증 제도가 새롭게 추가되었습니다. Derogations(명시적 동의, 계약 이행 등)에 의한 국외이전도 가능합니다.
8	**개인정보 유출통지 제도의 도입** 컨트롤러는 개인정보 유출 사실을 알게 된 때로부터 가능한 경우 72시간 내에 감독 당국에 신고해야 하며, 정보주체의 자유와 권리에 고 위험(high risk)이 예상될 때에는 부당한 지체 없이(without undue delay) 유출 사실을 정보주체에게 통지해야 합니다. 프로세서는 개인정보 유출 사실을 알게 된 때엔 컨트롤러에게 그 사실을 부당한 지체 없이 알려야합니다.
9	**정보주체의 권리 확대** 컨트롤러의 투명성 의무 부담에 더하여, 정보주체는 열람권(제15조), 정정권(제16조), 삭제권(제17조), 처리제한권(제18조), 개인정보 이동권(제20조), 반대권(제21조), 프로파일링을 포함한 자동화된 처리의 결과를 적용받지 않을 권리(제22조) 등의 권리를 갖습니다.
10	**DPO의 의무 지정** 공공기관(public authorities)이거나, 컨트롤러나 프로세서의 핵심 활동이 1) 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링에 해당하거나, 2) 민감정보나 범죄경력 및 범죄 행위에 대한 대규모 처리인 경우 DPO를 의무적으로 지정해야합니다.
11	**책임성과 거버넌스 강화** 1) 처리 활동의 세부 기록 유지(제30조), 2) 고 위험 처리에 대한 개인정보영향평가 수행(제35조), 3) DPO 지정(제37조), 4) 개인정보 유출 통지 및 종합적 기록 유지(제33~34조), 5) Data Protection by Design and Default이행(제25조) 등 개인정보 처리에 대한 책임성 및 거버넌스를 강화했습니다.
12	**One Stop Shop의 도입** 컨트롤러, 프로세서는 주 사업장 또는 단일 사업장에 대한 선임 감독기구에 의해 규율됩니다.(제56조). 그러나 선임 감독기구는 다른 연관된 기관과 협력해야 하며, 다른 기관이 특정 사안에 관여할 수도 있습니다.