Introduction

담당교수 : 신원
대상 : 정보보호학과 3/4학년
과목 : 해킹 및 악성코드 대응
학기 : 2020년 1학기

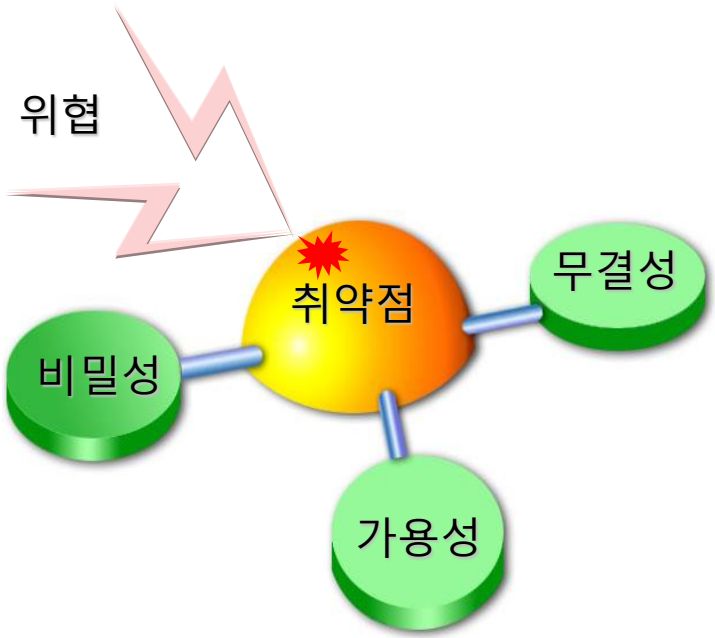
차례

- 정보보호란?
- 주요 위협 동향
  - 다양한 위협 동향을 통계를 통하여 살펴봅시다!

정보보호란?

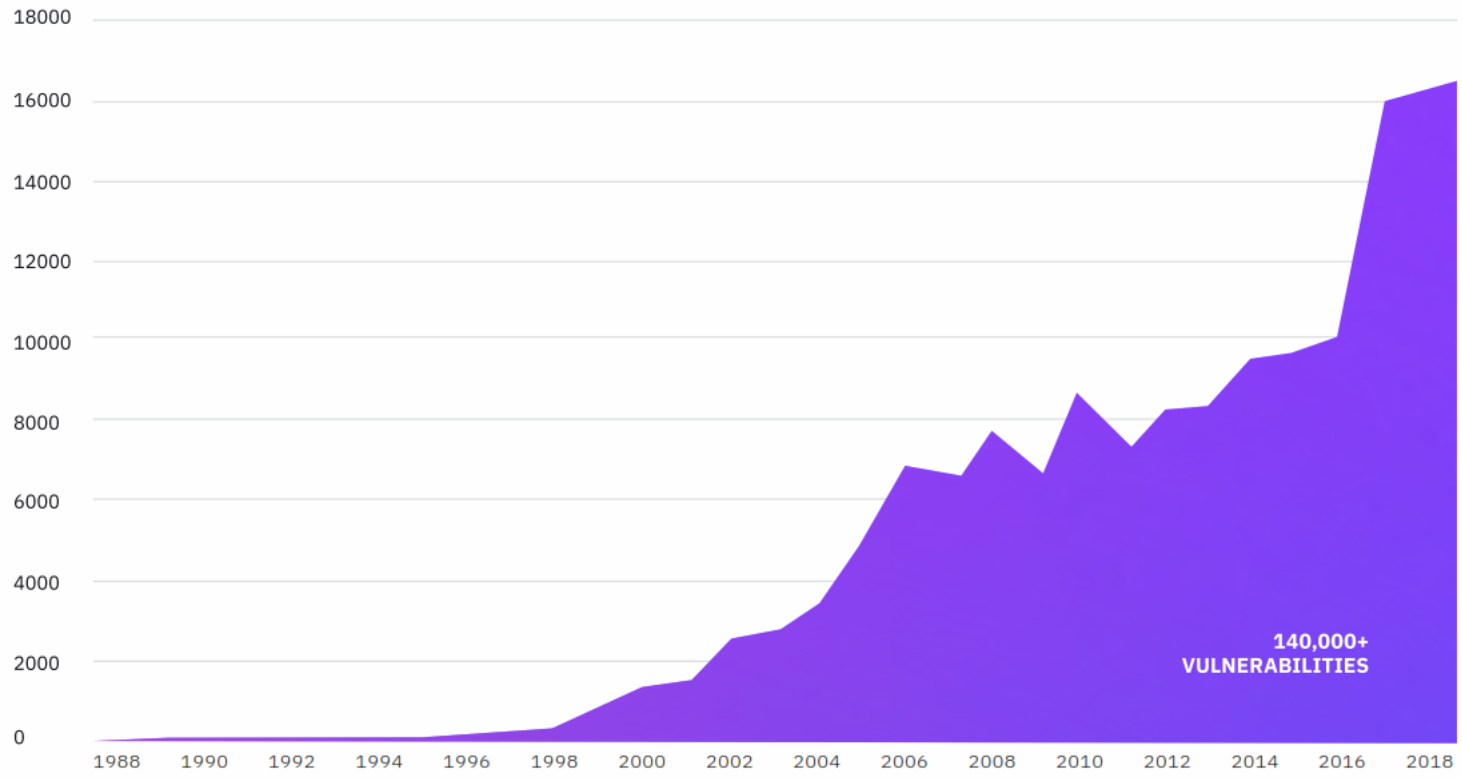
정보보호의 의미

- **정보화 사회의 근간이 되는 “정보”를 보호**
  - 해킹을 통한 정보 누출, 악성 코드를 통한 네트워크의 마비, 인터넷 범죄, 정보전 등 다양한 역기능이 새로운 사회 문제로 등장
  - 이에 대응하여 정보에 대한 비밀성, 무결성, 가용성을 보장하기 위한 기술 및 학문을 연구하는 분야



주요 위협 동향

매년 X-Force 취약점 DB에 집계되는 취약점 수

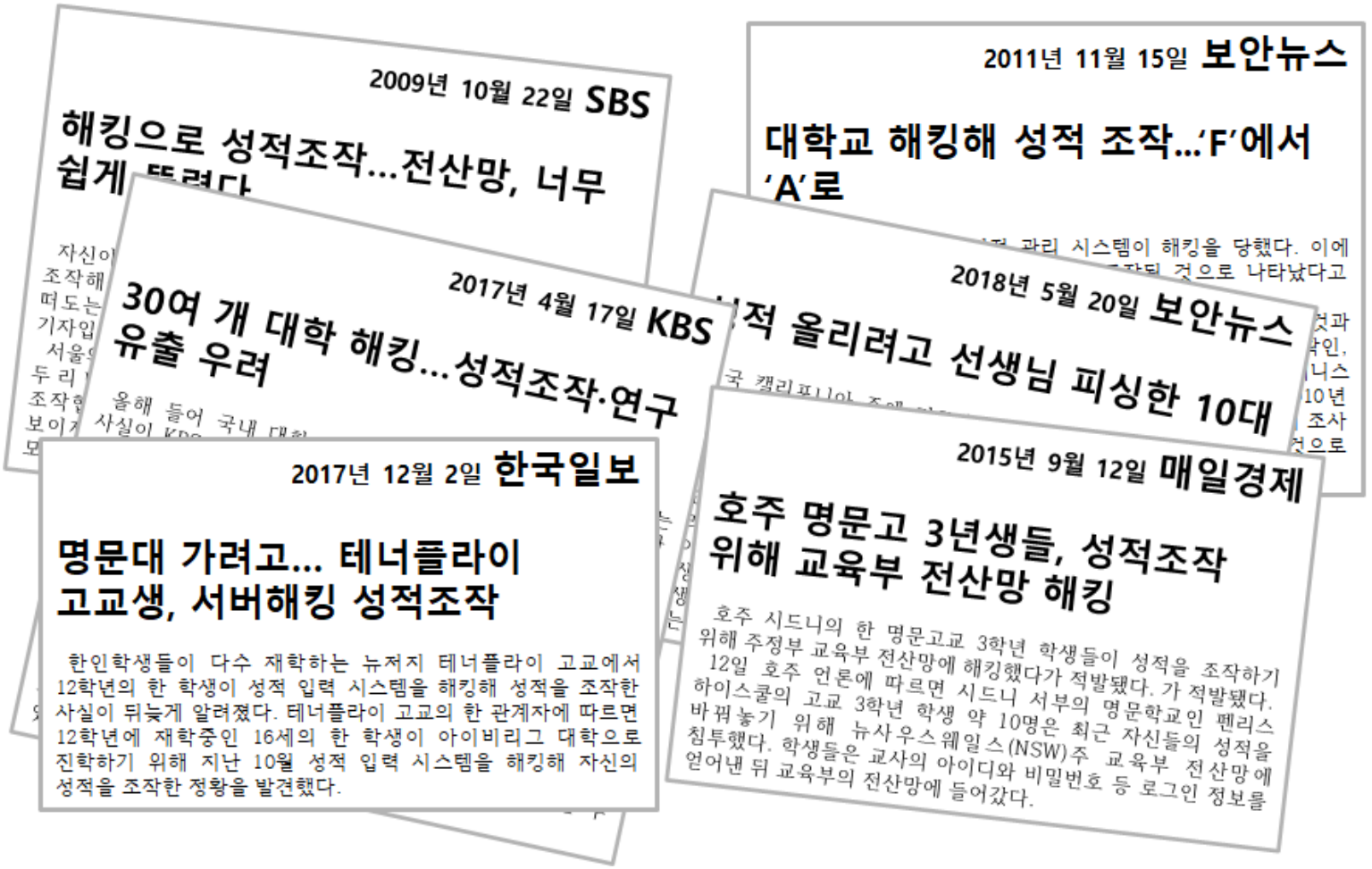


IBM X-Force Threat Intelligence Index 2019

개인정보 유출 & 가상화폐 탈취

연도	사건	피해
2014	국민카드, NH농협카드, 롯데카드 카드 3사 개인정보 유출	1억 400만 건
2014	KT, 개인정보 유출	1,200만 건
2014	이베이, 회원 정보 유출 추정	1억 4,500만명
2015	아이핀, 부정 발급	75만 건
2015	애슐리 메디슨, 이메일과 회원정보 등의 개인정보 유출	3천6백여만 건
2016	인터파크, 개인정보 유출	1,030만 건
2017	이스트소프트, 사용자 아이디&패스워드 해킹	13만 건
2018	페이스북, SW버그로 개인정보 유출	7,000만명 이상
2018	코인레일, 가상화폐 탈취	400억원 상당
2018	빗썸, 가상화폐 탈취	350억원 상당
2018	테크뷰로, 가상화폐 탈취	67억엔 상당

성적 조작 위협



2009년 10월 22일 SBS

해킹으로 성적조작...전산망, 너무 쉽게 뚫려다

2011년 11월 15일 보안뉴스

대학교 해킹해 성적 조작...'F'에서 'A'로

2017년 4월 17일 KBS

30여 개 대학 해킹...성적조작·연구 유출 우려

2018년 5월 20일 보안뉴스

적 올리려고 선생님 피싱한 10대

2017년 12월 2일 한국일보

명문대 가려고... 테너플라이 고교생, 서버해킹 성적조작

한인학생들이 다수 재학하는 뉴저지 테너플라이 고교에서 12학년의 한 학생이 성적 입력 시스템을 해킹해 성적을 조작한 사실이 뒤늦게 알려졌다. 테너플라이 고교의 한 관계자에 따르면 12학년에 재학중인 16세의 한 학생이 아이비리그 대학으로 진학하기 위해 지난 10월 성적 입력 시스템을 해킹해 자신의 성적을 조작한 정황을 발견했다.

2015년 9월 12일 매일경제

호주 명문고 3년생들, 성적조작 위해 교육부 전산망 해킹

호주 시드니의 한 명문고교 3학년 학생들이 성적을 조작하기 위해 주정부 교육부 전산망에 해킹했다가 적발됐다. 가 적발됐다. 12일 호주 언론에 따르면 시드니 서부의 명문학교인 펜리스 하이스쿨의 고교 3학년 학생 약 10명은 최근 자신들의 성적을 바꿔놓기 위해 뉴사우스웨일스(NSW)주 교육부 전산망에 침투했다. 학생들은 교사의 아이디와 비밀번호 등 로그인 정보를 얻어낸 뒤 교육부의 전산망에 들어갔다.

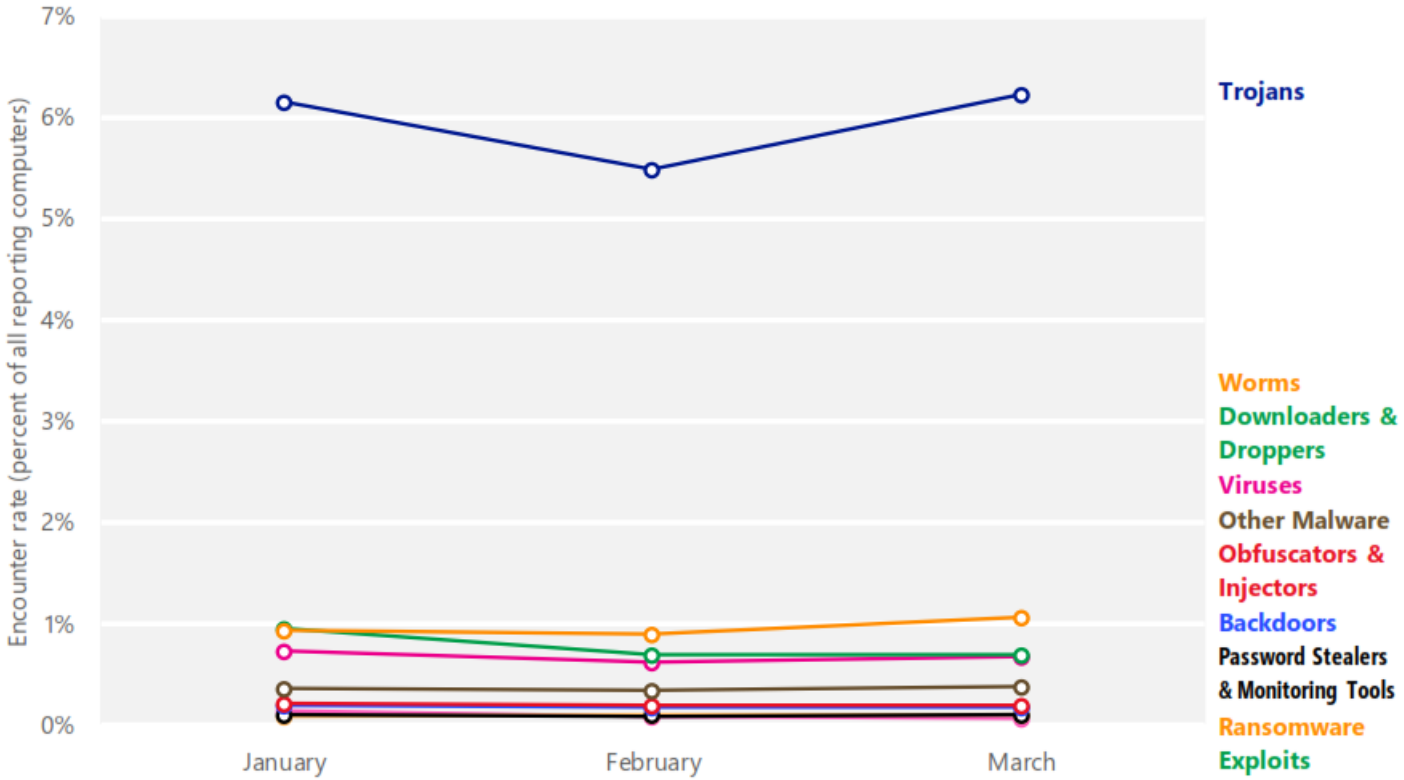
지하경제

ACCOUNTS	
Online retailer gift cards	15~50% of value
Online banking accounts (depending on value & verification)	0.5%~10% of value
Cloud service account	$5~10
Hacked email accounts (2,500)	$1~15
Online payment accounts (depending on value & verification)	$1~100
IDENTITIES	
Stolen or fake identity (name, SSN, and DOB)	$0.1~1.5
Mobile phone online account	$15~25
ID/passport scans or templates	$1~35
Full ID packages (name, address, phone, SSN, email, bank account, etc.)	$30~100
Fake ID, driver license, passport, etc.	$25~5,000

MALWARE	
DDoS bot software	$1~15
Spyware	$3~50
Cryptocurrency miner (e.g. Monero)	$10~200
Ransomware toolkit	$0~250
Common banking Trojans toolkit with support	$10~1,500
SERVICES	
DDoS service, short duration <1 hour (medium protected targets)	$5~20
DDoS service, duration >24h (medium and strong protected targets)	$10~1,000
SOCIAL MEDIA	
100 likes on social media platforms	$0.1~3
500 social media followers	$2~6
100,000 social media video views	$200~250

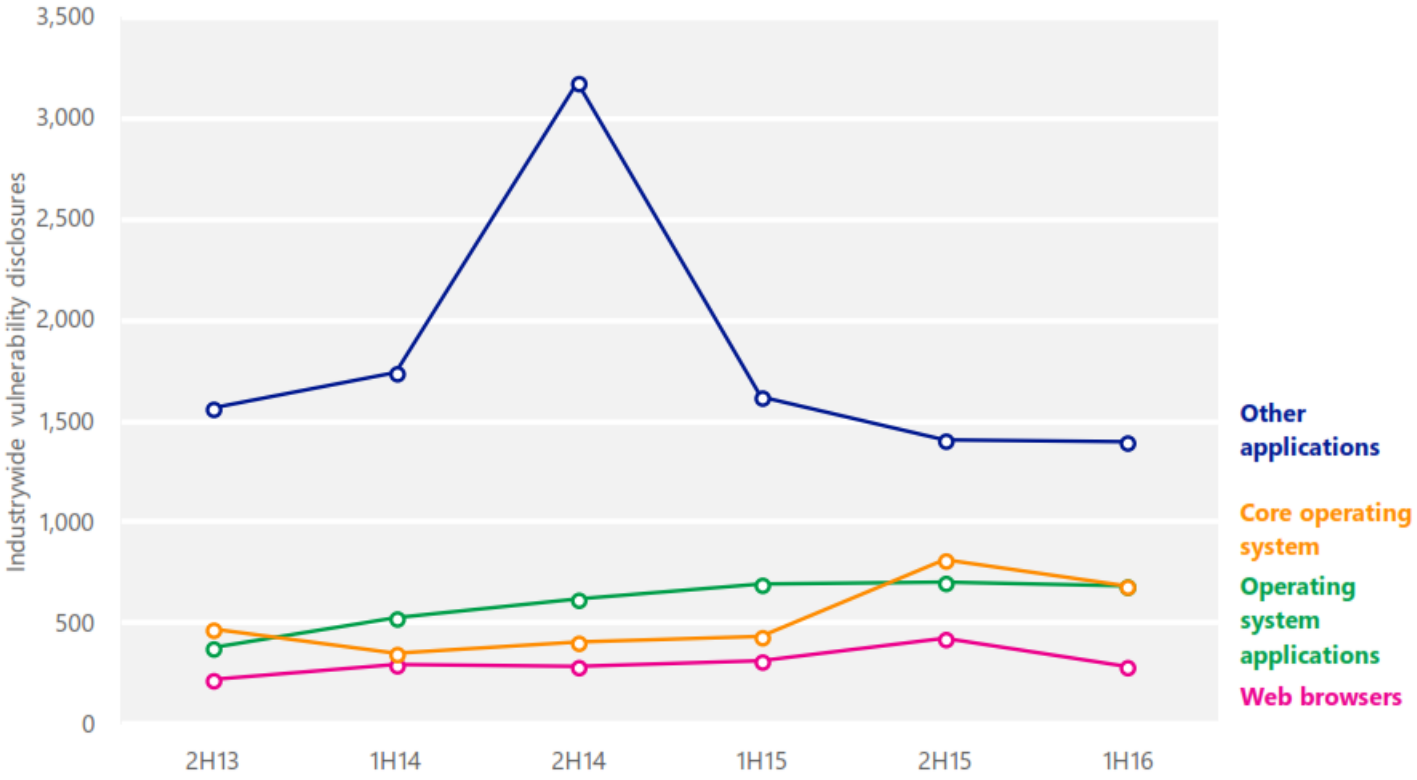
악성코드 분포 비율

Microsoft (2017 1Q)



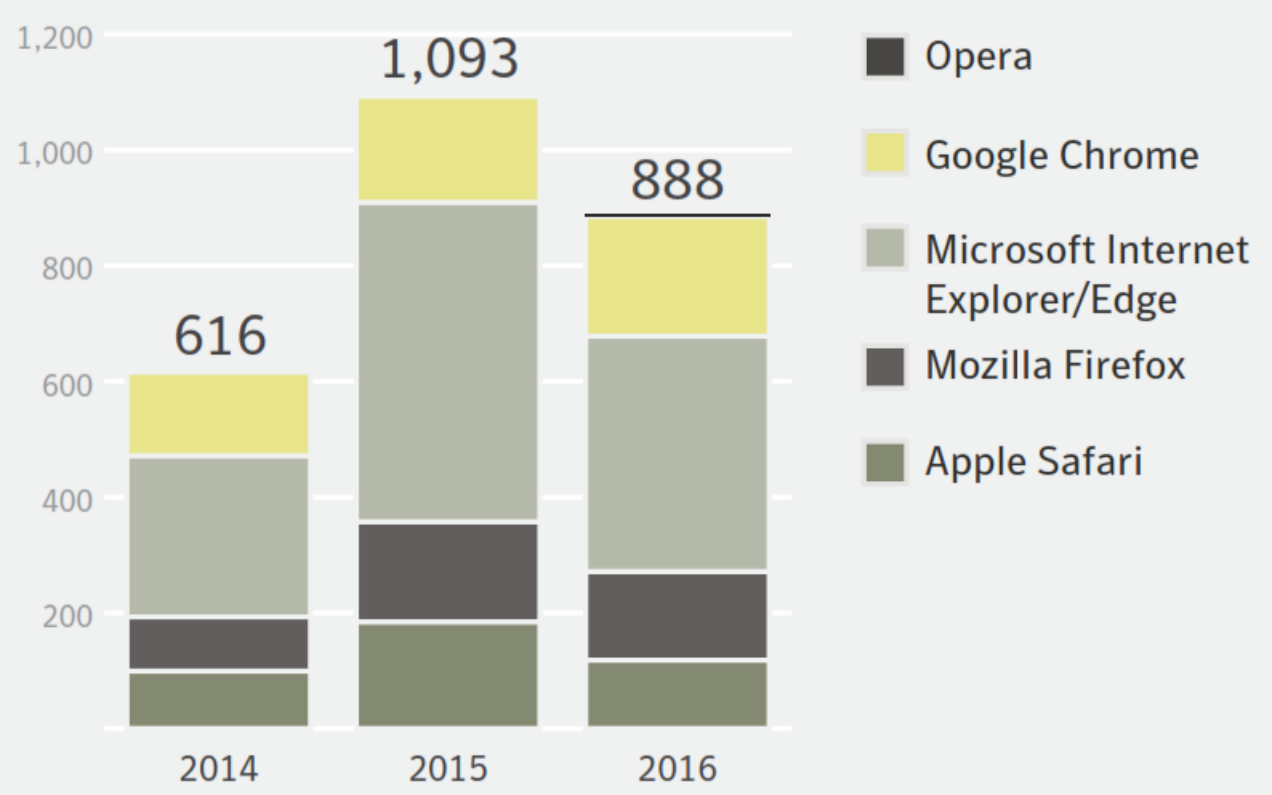
보안 취약점 동향

Microsoft (2013.7~2016.6)



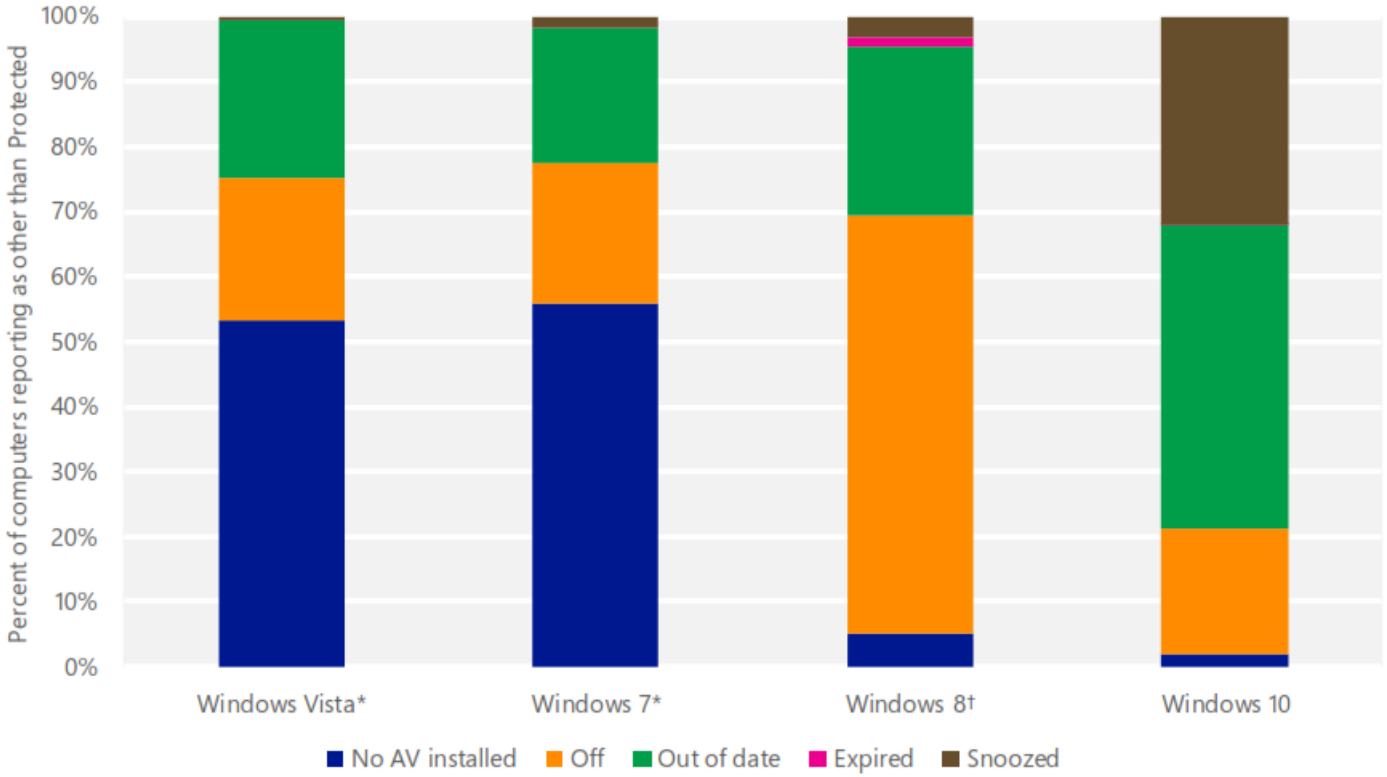
브라우저 보안 취약점 동향

Symantec (2014~2016)



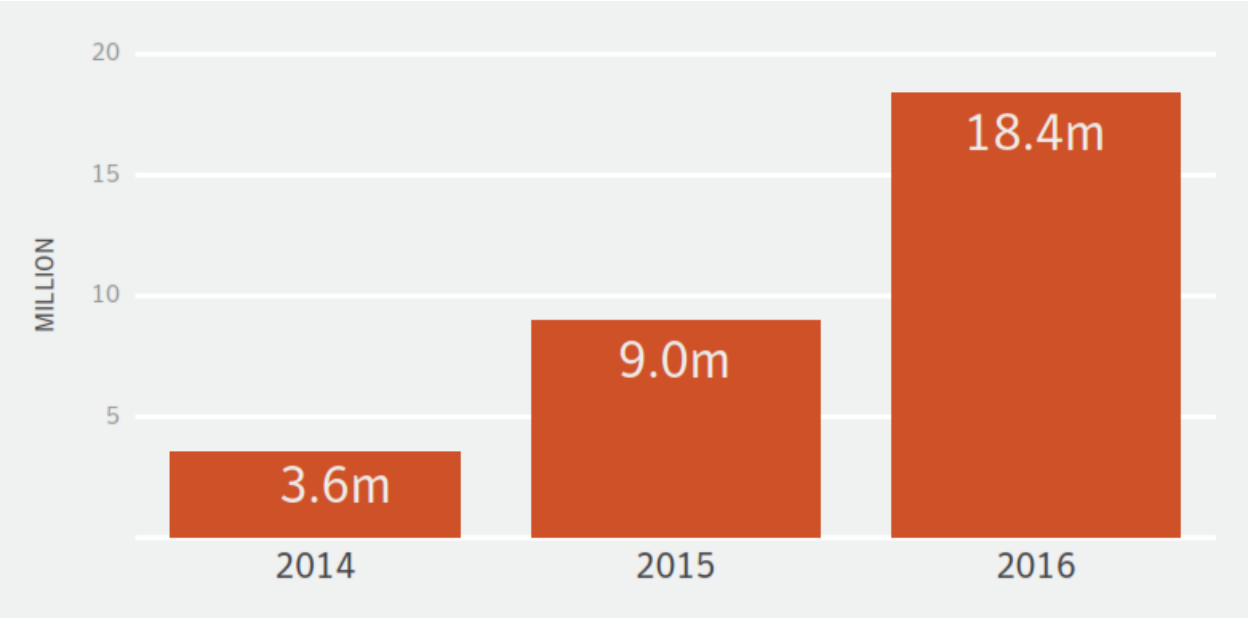
운영체제별 백신 사용 동향

- Microsoft (2017.3)



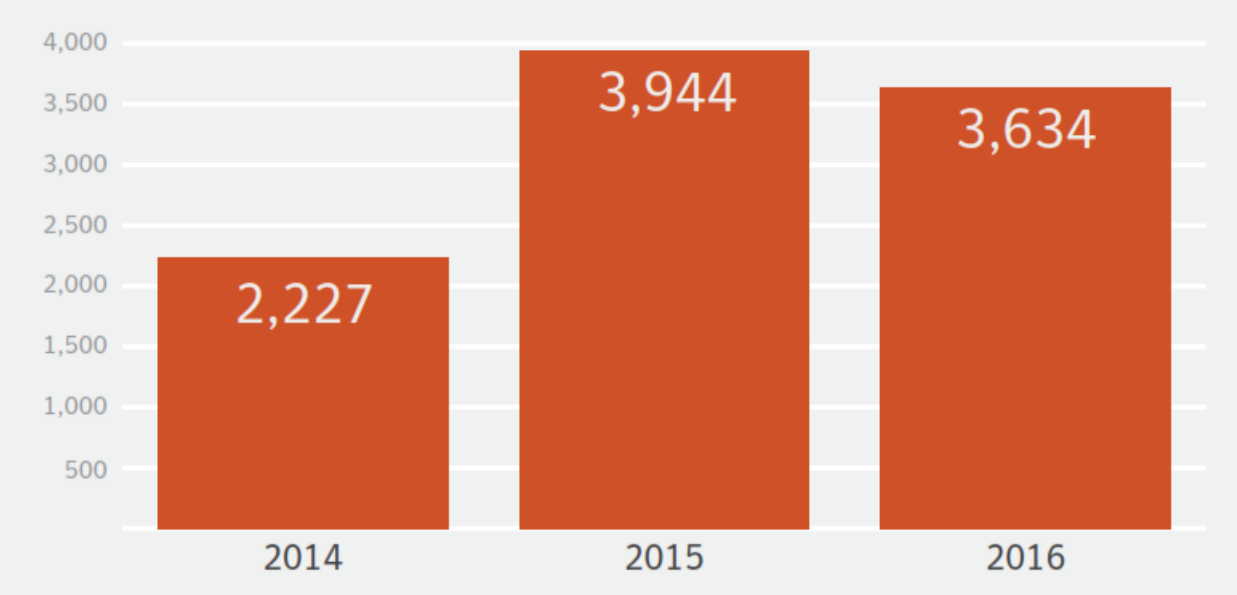
악성코드 탐지 건수

- Symantec (2014 ~ 2016)

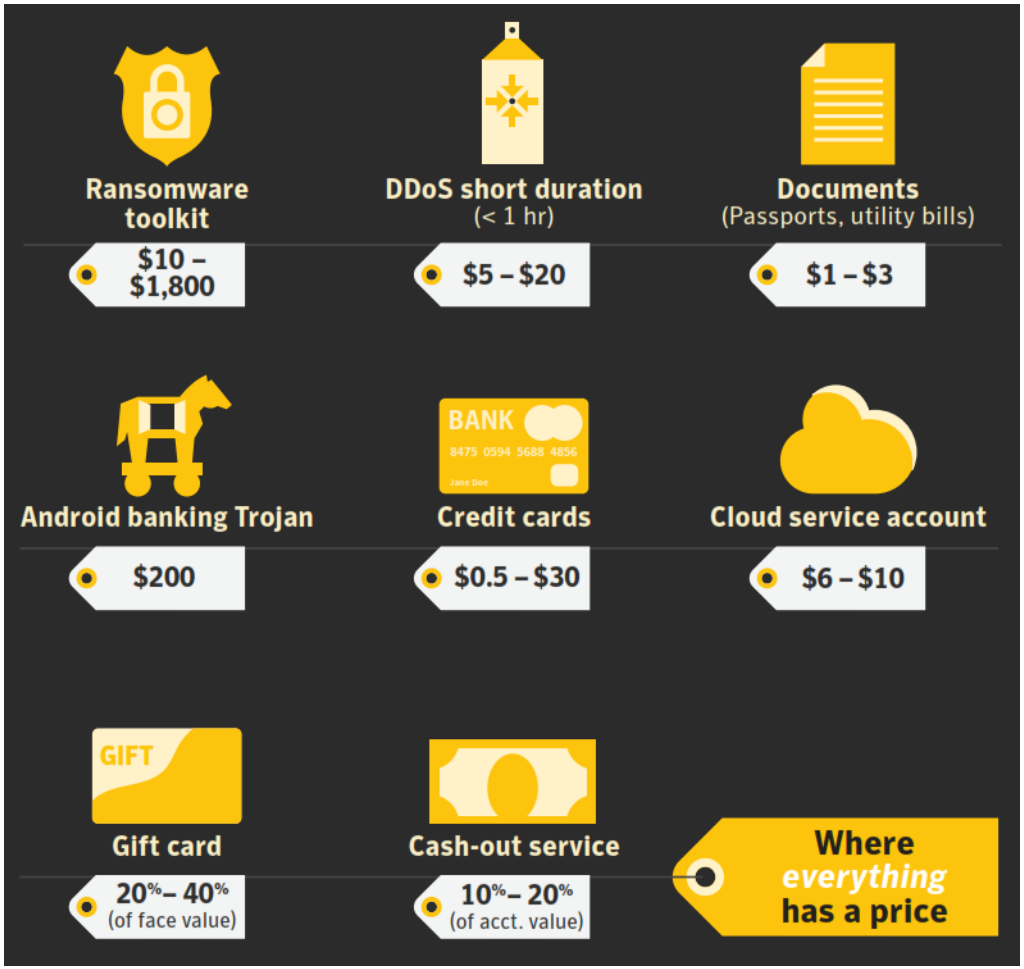


변형 악성코드 건수

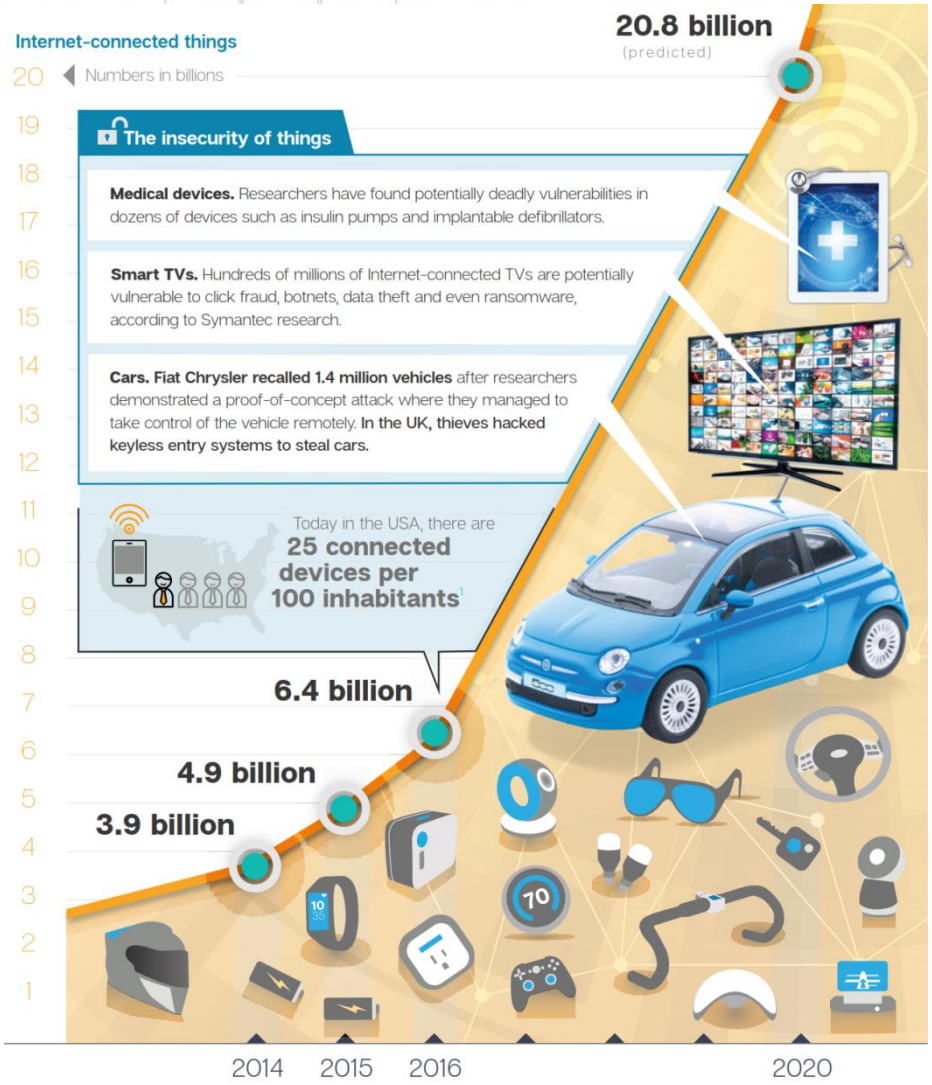
- Symantec (2014 ~ 2016)



지하경제


Ransomware toolkit
$10 – $1,800
DDoS short duration
(< 1 hr)
$5 – $20
Documents
(Passports, utility bills)
$1 – $3
Android banking Trojan
$200
BANK
8475 0594 5688 4856
Jane Doe
Credit cards
$0.5 – $30
Cloud service account
$6 – $10
GIFT
Gift card
20%– 40%
(of face value)
Cash-out service
10%– 20%
(of acct. value)
Where everything has a price

IoT 보안 위협


Internet-connected things
Numbers in billions
20.8 billion
(predicted)
The insecurity of things
Medical devices. Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.
Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.
Cars. Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. In the UK, thieves hacked keyless entry systems to steal cars.
Today in the USA, there are
25 connected devices per 100 inhabitants
6.4 billion
4.9 billion
3.9 billion
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
2014
2015
2016
2020

2020 보안 위협 동향 (AhnLab)

1. 무한한 공간, 저 너머로! (To Infinity and Beyond!) - 랜섬웨어
   - 2019년 5월 말 대표적인 서비스형 랜섬웨어(RaaS)인 갠드크랩의 제작자가 운영 중단을 선언했지만 랜섬웨어 시장은 위축되지 않았다. 오히려 개인에서 기업 또는 국가 기관으로 시장의 변화를 꾀함으로써 더 큰 수익을 올릴 것으로 예상된다.
2. 보이지 않는 위협(The Phantom Menace) – 클라우드 보안 위협
   - 이미 여러 차례 경험했던 것처럼 사람들의 관심과 데이터가 모이는 곳에 공격자의 관심도 집중되기 마련. 기업 및 기관의 클라우드 이용이 증가함에 따라 클라우드 인프라에 대한 공격이 증가할 것으로 관측된다.
3. 잊고 있는, 또는 숨겨진 세상을 향해 (Into The Unknown) - 특수목적시스템 및 OT 보안 위협
   - ICS는 폐쇄망이라는 숨겨진 세상에 존재할 때도 있지만 네트워크에 연결되어 관리 및 운용된다. ICS 등 OT(Operational Technology) 환경은 오랫동안 축적된 운영 노하우와 다양한 보안 기술로 보이지 않는 곳에서 보호되고 있다. 그럼에도 불구하고 랜섬웨어를 비롯한 악성코드의 타깃이 되고 있다.
4. 당신이 한 일을 알고 있다(I Know What You Did Last Summer) – 정보 수집 및 탈취
   - 고전적이지만 지금도 변함없는 사이버 공격의 대표적인 목적 중 하나는 시스템에 침입해 사용자나 조직의 중요 정보를 수집, 탈취하는 것이다.
5. "계획이 있구나" – 모바일 보안 위협
   - 기존의 모바일 위협은 사용자를 속여 불법적인 방법으로 금전적인 이득을 취하는 방식이 대다수였다. 이제 더욱 교묘해진 공격자들은 모바일 앱 개발 업체도 파악하기 어려운 형태의 소프트웨어 개발 키트(SDK)를 제작, 유포하는 방식으로 비즈니스 모델의 변화를 꾀하고 있다.

- **2020년 7대 사이버 공격 전망**
  - 1. 일상 속으로 파고든 보안 취약점, 보이지 않는 위협 - KISA
  - 2. 랜섬웨어, 개인에서 공공기관·기업으로 피해 확대 - 안랩
  - 3. 취약한 가상통화 거래소, 반복되는 해킹 사고 - 잉카인터넷
  - 4. 문자 메시지, 이메일 안으로 숨어드는 악성코드 - 하우리
  - 5. 은밀하게 정교하게, 진화하는 지능형 표적 공격 - 이스트시큐리티
  - 6. 모바일까지 확대되는 소프트웨어 공급망 공격 - NSHC
  - 7. 융합 서비스를 노리는 새로운 보안 위협의 등장 - 빛스캔