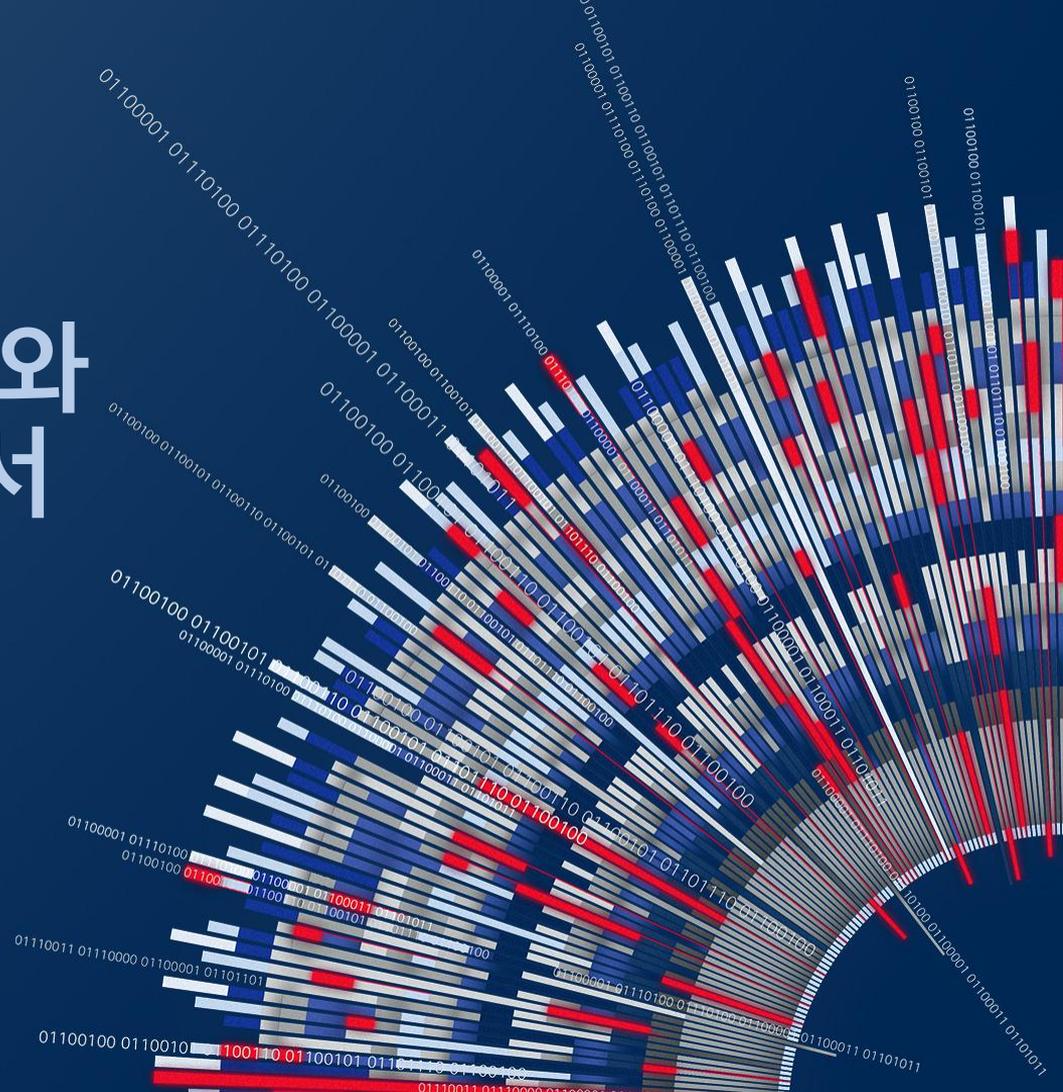


# 최근 보안 트렌드와 오픈소스를 찾아서

정관진 부장

시스코 GSSO APJ Security - Korea

September, 2015



# 뉴스 헤드라인을 장식하는 보안 뉴스

**MOBILE CUSTOMER  
DATA LEAKED ONLINE**

Source: Naked Security

**DATA BREACHES ON  
TRACK TO COST  
COMPANIES \$2.1  
TRILLION**

Source: Corporate Counsel

**HEALTH CARE  
ORGANIZATIONS  
REPORT DATA BREACHES  
AFFECTING THOUSANDS**

Source: iHealthBeat

**WIKILEAKS POSTS  
STOLEN DATA FROM  
ENTERTAINMENT GIANT**

Source: The New York Times

**UNNAMED FINANCIAL  
INSTITUTION RECEIVED  
ALERT THAT CONTAINED  
9,000 CUSTOMER CARDS  
FOR A BREACH**

Source: Network World

**UNDER ATTACK:  
WHAT BANKS CAN  
LEARN FROM RECENT  
DATA BREACHES**

Source: Forbes

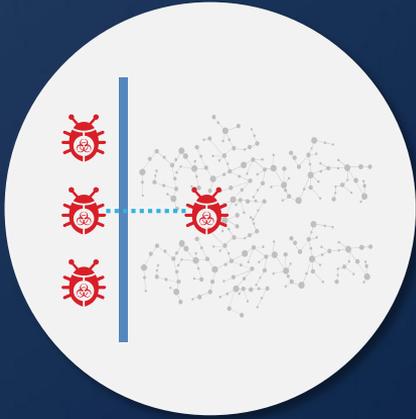
**LARGE ELECTRONICS  
RETAILER EMAIL  
ADDRESSES EXPOSED**

Source: Engadget

**BIG BOX STORE  
ANNOUNCES \$19  
MILLION DATA BREACH  
SETTLEMENT WITH  
CREDIT CARD COMPANY**

Source: CNBC

# 지금 여러분의 환경에는 무슨 일이 ?



여러분의 환경에  
침해사고가 발생할  
수 있습니다.

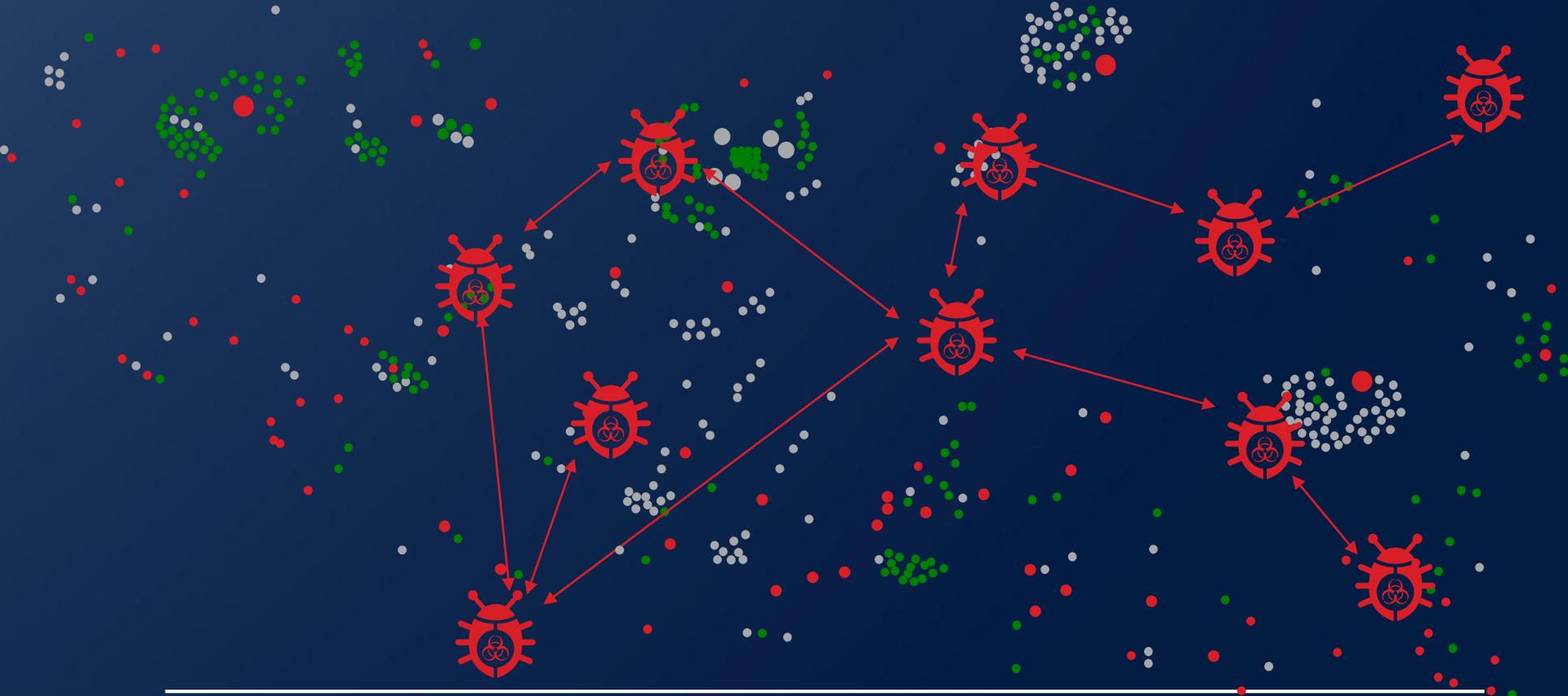


이메일을 통해서  
새로운 위협이  
유입 될 수도 있는  
것이죠

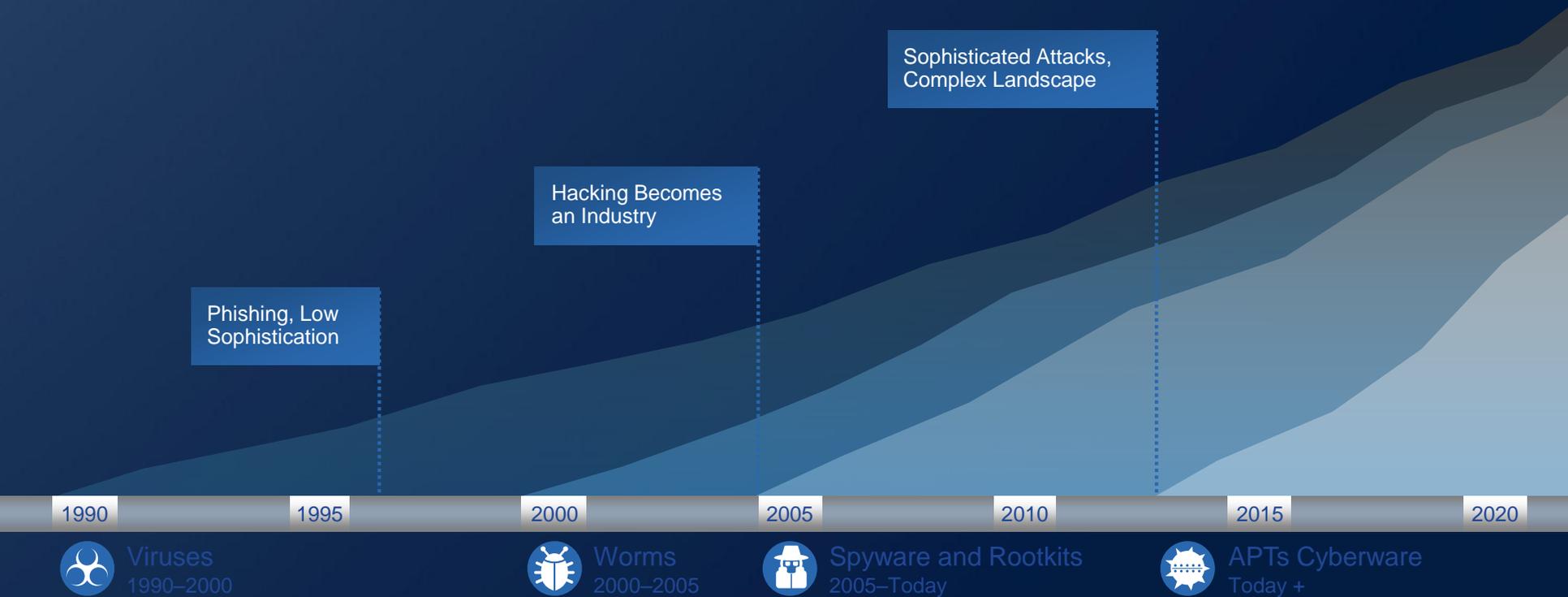


해커는 웹을 통해  
명령어를 통해 제어를 할  
수도 있게 됩니다.

위협은 더욱 지능화 복잡화 되고 있습니다.



# 위협 변화



Viruses  
1990-2000

Worms  
2000-2005

Spyware and Rootkits  
2005-Today

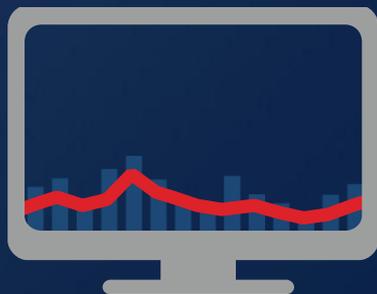
APTs Cyberware  
Today +

# 웹 기반의 공격은 꾸준히 증가

2014년 12월 - 2015년 5월



Java



PDF



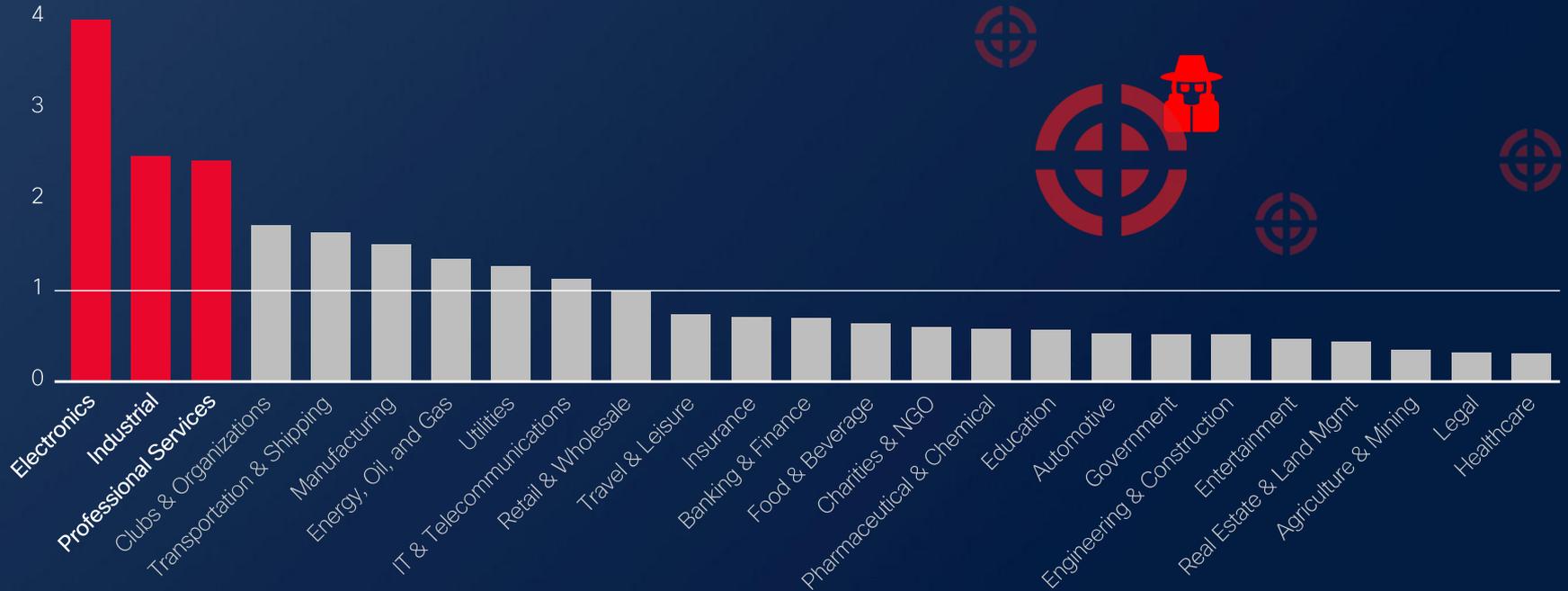
Silverlight



Flash

# 각 산업군에 위협이 되고 있는 악성코드

전자산업쪽에 공격 트래픽 비율이 크게 증가하였지만, 전영역에 공격이 발생되고 있음



# 전세계 곳곳에서 활동중인 악성코드

악성코드의 감염은 특정 국가에 한정되지 않음

악성코드 트래픽



차단 비율이 높은 국가는 취약한 웹 서버 운영이 많았음

# 해킹 경제학

글로벌  
사이버범죄  
시장 :  
4500억-1조  
달러



Social Security  
\$1



DDoS  
as a Service  
~\$7/hour



Medical Record  
>\$50



Credit Card Data  
\$0.25-\$60



Bank Account Info  
>\$1000  
Depending on account  
type and balance



Mobile Malware  
\$150



Spam  
\$50/500K emails



Malware Development  
\$2500  
(commercial malware)



Exploits  
\$100k-\$300K



Facebook Account  
\$1 for an account  
with 15 friends

# 시스코 글로벌 위협 현황을 통해 본 숫자

- 위협 차단 : 19,692,200,000 / 매일
- 스팸을 통한 위협 차단 : 2,557,767 차단/ 초
- 웹 요청 / 매일 : 169억 요청 / 매일

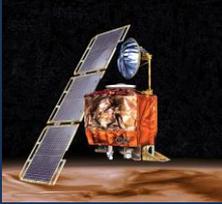
하루에 악성코드는 얼마나 될까요?



왜 보안은 끝이  
없을까요?



# 소프트웨어는 버그에서 자유롭지 않습니다.



## NASA 화성 착륙기

- 소프트웨어 버그로 NASA 화성 착륙기가 화성 표면에서 폭발
- 세금 1조6,500만 달러 사라짐
- 영어와 측정 단위간의 변환 계산의 오류
- 우주선이 화성에 도착할 궤적을 잘못 계산
- 착륙기가 너무 일찍 엔진을 꺼서 표면 충돌



## MV-22 오스프리

- MV-22 오스프리는 고급 군사 항공기
- 항공기와 공기 역학이 복잡하여 고성능 소프트웨어를 통해 비행기 제어
- 소프트웨어가 비적절한 백업 시스템 호출하면서, 항공기 폭발
- 이로 인해 네명의 군인사망



## US 비세네스

- 1988년, 미 해군 함정은 레이더에 나타난 표적을 보고 적기라고 판단 후 미사일을 발사
- US 비세네스 추적 소프트웨어가 잘못 식별함
- 에어버스 A320 에 탑승한 290명이 목숨을 잃음

# 더 많은 코드 수, 더 많은 버그

```
...files: OSError: [Errno 13] Permission denied: '...'
socket.error, (errno, strerror)
print "ncfiles: Socket error (%s) for host %s (%s)" % (
for hs in page.findAll("tr"):
    value = (hs.contents[0])
    if value != "Afdeling":
        print >> txt, value
import codecs
f = codecs.open('...', 'w', encoding='utf-8')
text = f.read()
f.close()
# open the file
f = code
f.write('...')
# write
```

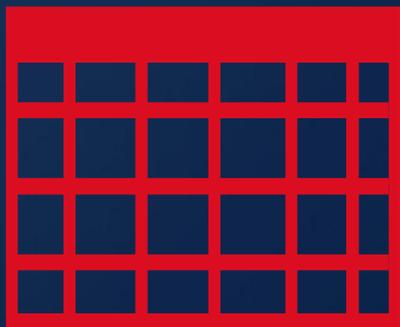
코드 수	시스템
400,000	솔라리스7
40,000,000	우주 스테이션
10,000,000	비행 셔틀
7,000,000	보잉 777
35,000,000	Windows NT5
< 5,000,000	Windows 95
45,000,000	Windows XP
50,000,000	Windows Server 2003
419,000,000	Debian 7.0

- 현대의 소프트웨어는 복잡하고 앞으로 더욱 고도화 될것임
- 천 라인(KLOC)당 버그수는 약 5-50 개 정도
- 코드가 길어지면 버그 가능성 높음
- 이러한 버그나 설계결함으로 인해 악의적인 코드 수행이 더욱 쉬워짐
- 보안 문제에서 자유롭다고 보장하기 어려움

[참고] [https://en.wikipedia.org/wiki/Source\\_lines\\_of\\_code](https://en.wikipedia.org/wiki/Source_lines_of_code)

과연 어떤것이 여러분들에게 필요한 것일 까요 ?

상용

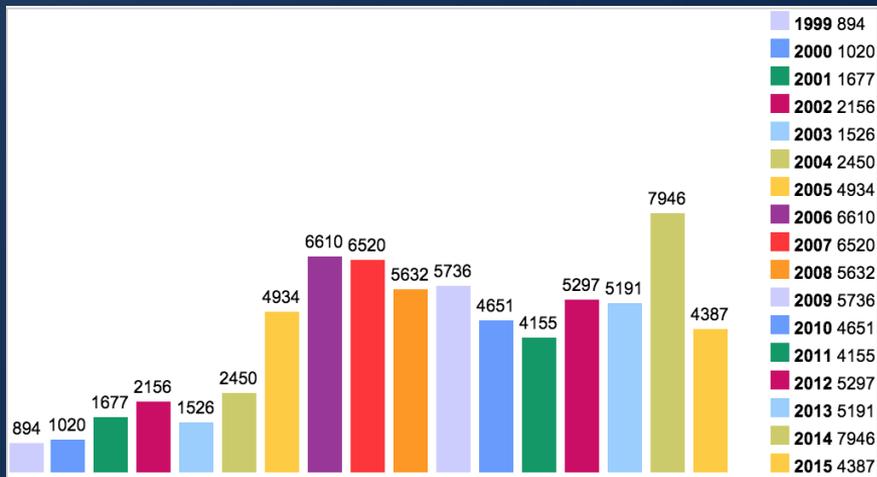


vs



오픈  
소스

# 얼마나 많은 취약점이 ?

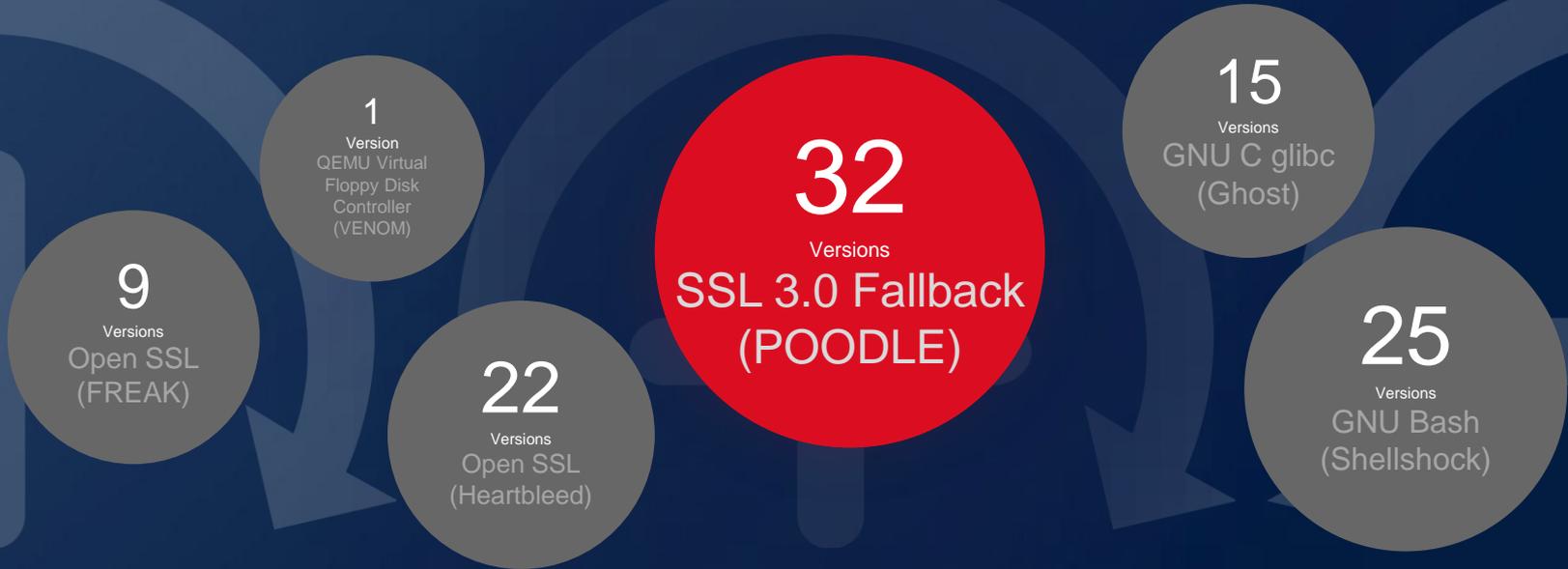


Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	<u>Microsoft</u>	<u>398</u>	<u>4051</u>
2	<u>Oracle</u>	<u>256</u>	<u>2814</u>
3	<u>Apple</u>	<u>100</u>	<u>2801</u>
4	<u>IBM</u>	<u>714</u>	<u>2537</u>
5	<u>Cisco</u>	<u>1284</u>	<u>2305</u>
6	<u>SUN</u>	<u>204</u>	<u>1617</u>
7	<u>Mozilla</u>	<u>21</u>	<u>1496</u>
8	<u>Adobe</u>	<u>97</u>	<u>1359</u>
9	<u>Linux</u>	<u>14</u>	<u>1335</u>
10	<u>Google</u>	<u>44</u>	<u>1312</u>

[출처] <https://www.cvedetails.com/top-50-vendors.php>

- 매년 취약점 발견 건수는 크게 증가하고 있음
- 상업용 소프트웨어에서 발견되는 취약점 또한 큰 비중을 차지
- 제로데이 취약점 증가

# 주요 오픈소스 취약점 및 대응



# CaseStudy : OpenSSL - Heartbleed



조직에서 애플리케이션에  
효과적으로 패치를  
적용하는 것은 여전히  
매우 힘들

56%

OpenSSL 버전이 50개월  
이상 됨

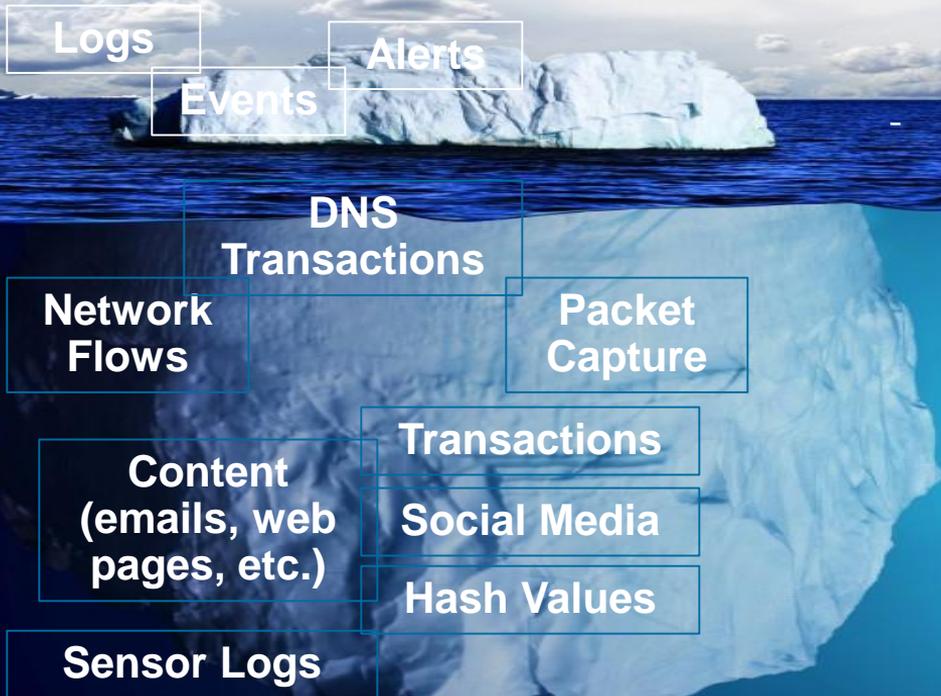
예: Heartbleed

# 군 관련 오픈소스 활용 사례



- DSC(Distributed Common Ground System-Army Standard Cloud)
  - 228 대 서버 (1,800 CPU, Dual 6 코어 2.8GHz )
  - 13.92 테라 램, 1.032TB 스토리지
  - Hadoop, Hadoop Core, Accumulo, Condor, SolrCloud
- ARL(The U.S. Army Research Laboratory)
  - 사이버 공격 탐지를 위한 프레임워크 Dshell 오픈소스 공개
  - 포렌식 분석용으로 미 국방 네트워크에서 발생하는 이벤트 분석으로 5년여 정도 사용한 프레임

# 위협데이터 분석 오픈소스 - OpenSOC



- Cisco 에서 공개한 OpenSOC
  - 오픈소스 기반의 대용량 패킷 분석 시스템
  - 패킷캡처, 인덱싱 저장, 데이터 스트리밍 처리, 배치처리, 실시간 검색 및 집계/통계
  - <https://github.com/OpenSOC>

## Applications + Analyst Tools

Log Mining and Analytics

Network Packet Mining and PCAP Reconstruction

Big Data Exploration, Predictive Modelling







Thank you