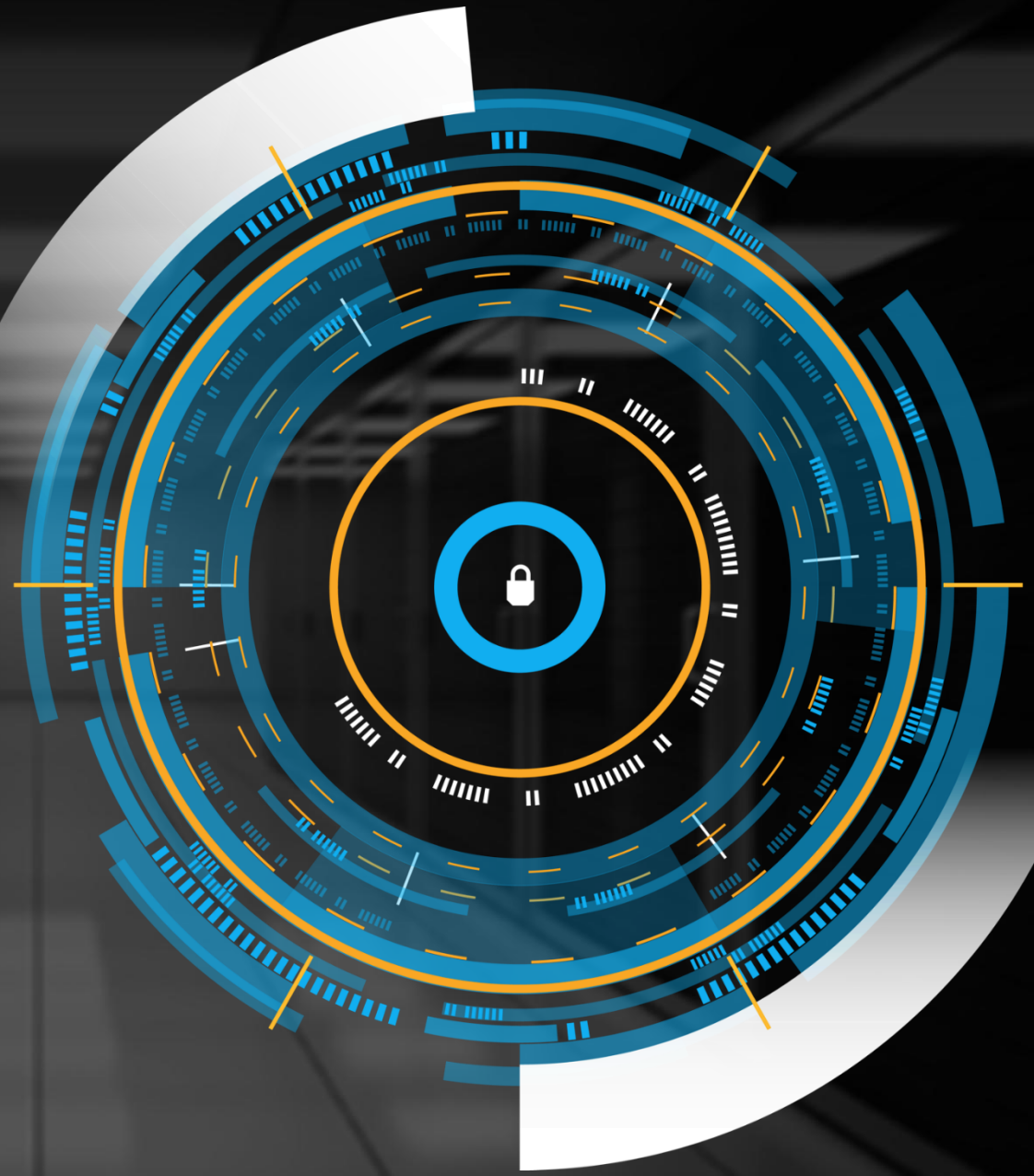
Symantec

ISTR

Internet Security Threat Report



시만텍 코리아

April 21, 2016

2009년

2,361,414개

신규 악성코드 발생

2015년

430,555,582개

2014년

3억 1천 7백만 개 대비

36% 증가

매일

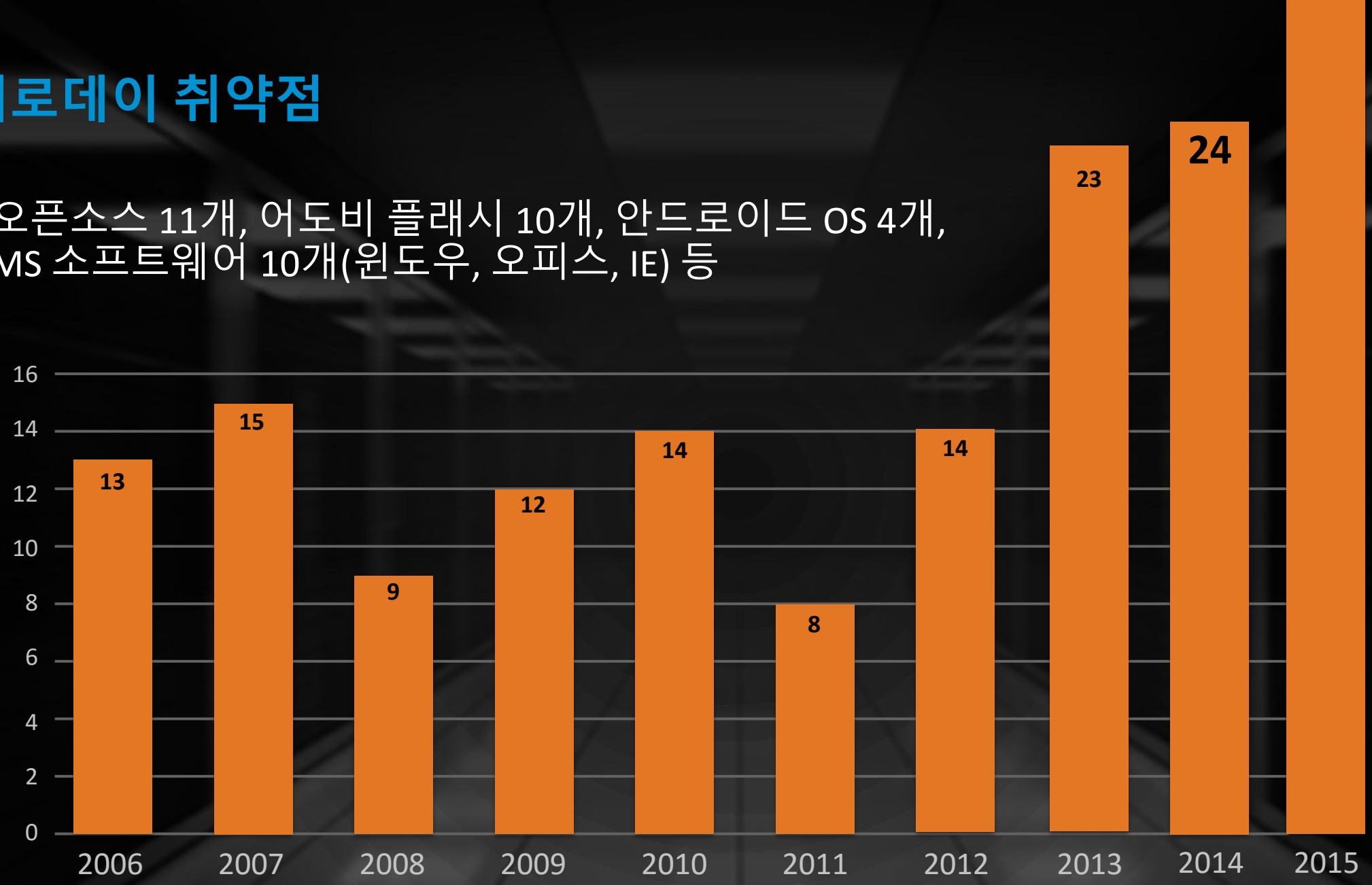
1 ,179,000개

신규 악성코드 발생

제로데이 취약점

제로데이 취약점

- 오픈소스 11개, 어도비 플래시 10개, 안드로이드 OS 4개, MS 소프트웨어 10개(윈도우, 오피스, IE) 등



2014년 대비 125% 증가

해킹팀의 '데이터 보물 창고' 해킹 당해

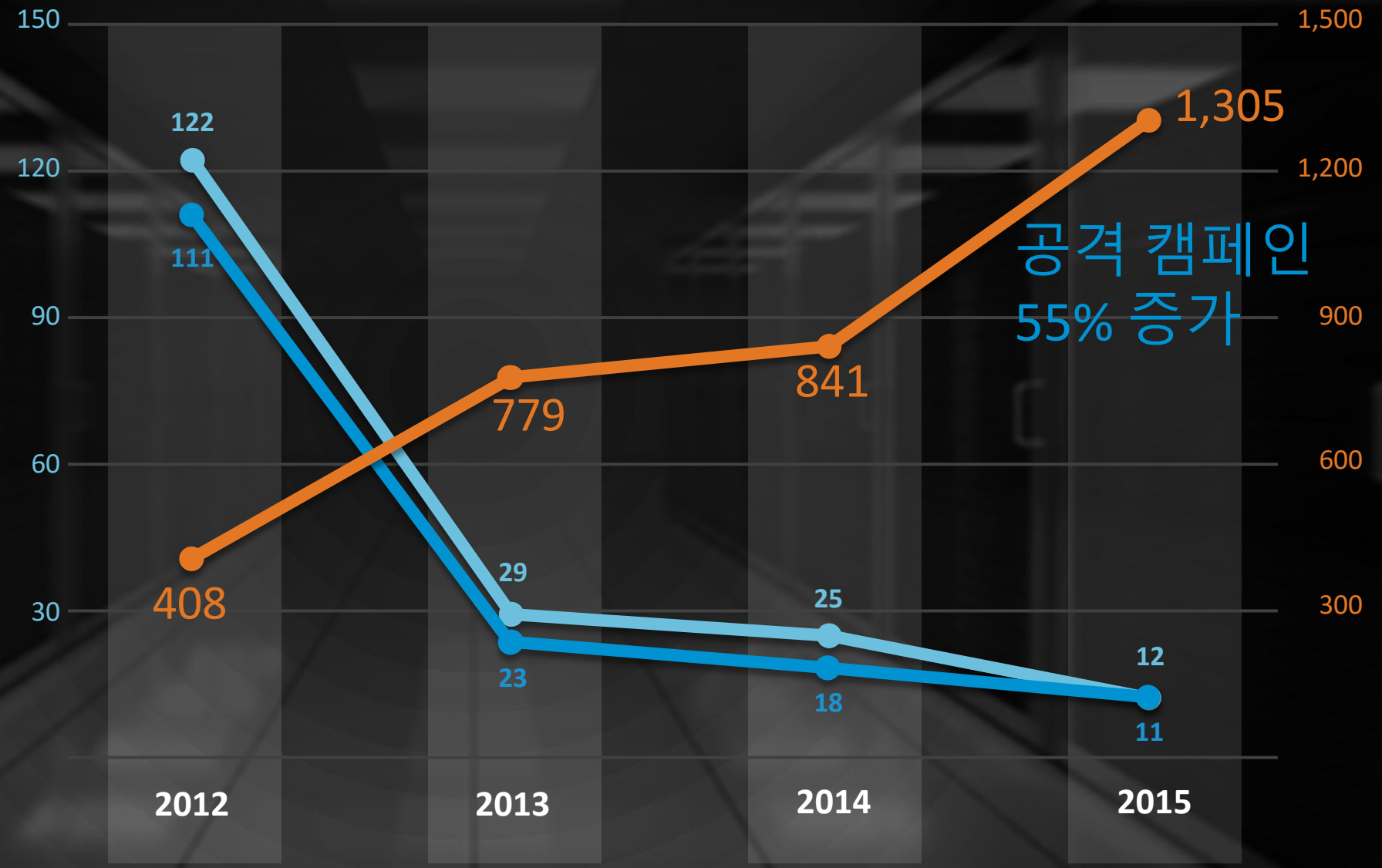
- 해킹팀(Hacking Team 이탈리아 회사)은 어도비 플래시, 인터넷 익스플로러 및 MS 윈도우의 제로데이 취약점 보유

CVE	해당제품	최초 공고일	패치일
CVE-2015-5119	어도비 플래시	7월 7일	7월 8일
CVE-2015-5122	어도비 플래시	7월 10일	7월 14일
CVE-2015-5123	어도비 플래시	7월 10일	7월 14일
CVE-2015-2425	인터넷 익스플로러	7월 14일	7월 14일
CVE-2015-2426	MS 윈도우	7월 20일	7월 20일
CVE-2015-2387	MS 윈도우	7월 8일	7월 14일

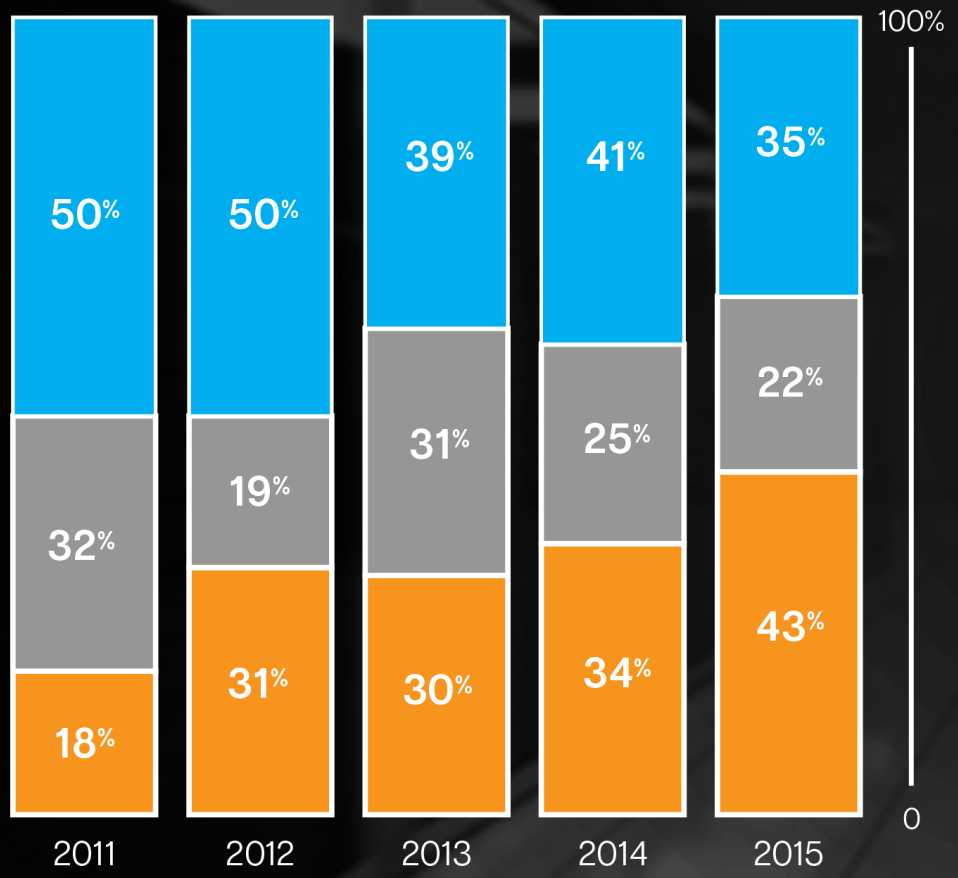
표적 공격

표적 공격 캠페인 분석

- 공격 캠페인 1건 당 발송된 평균 이메일 건수
- 공격 1건 당 이메일 수신자 수
- 공격 캠페인



표적 기업의 규모별 스피어피싱 공격 현황



기업 규모	2015 위험율	2015 %로 환산한 위험율	기업 당 공격건수
종업원 2,500명 이상의 대기업	2.7건 중 1건 꼴	38%	3.6
종업원 251–2,500명 미만 중견기업	6.8건 중 1건 꼴	15%	2.2
종업원 1–250명의 중소기업	40.5건 중 1건 꼴	3%	2.1

스피어피싱에 사용된 첨부 파일 형식

순위	첨부파일 형식	2015년도 분포율	첨부파일 형식	2014년도 분포율
1	.doc	40.4%	.doc	38.7%
2	.exe	16.9%	.exe	22.6%
3	.scr	13.7%	.scr	9.2%
4	.xls	6.2%	.au3	8.2%
5	.bin	5.4%	.jpg	4.6%
6	.js	4.2%	.class	3.4%
7	.class	2.6%	.pdf	3.1%
8	.ace	1.7%	.bin	1.9%
9	.xml	1.6%	.txt	1.4%
10	.rtf	1.4%	.dmp	1.0%

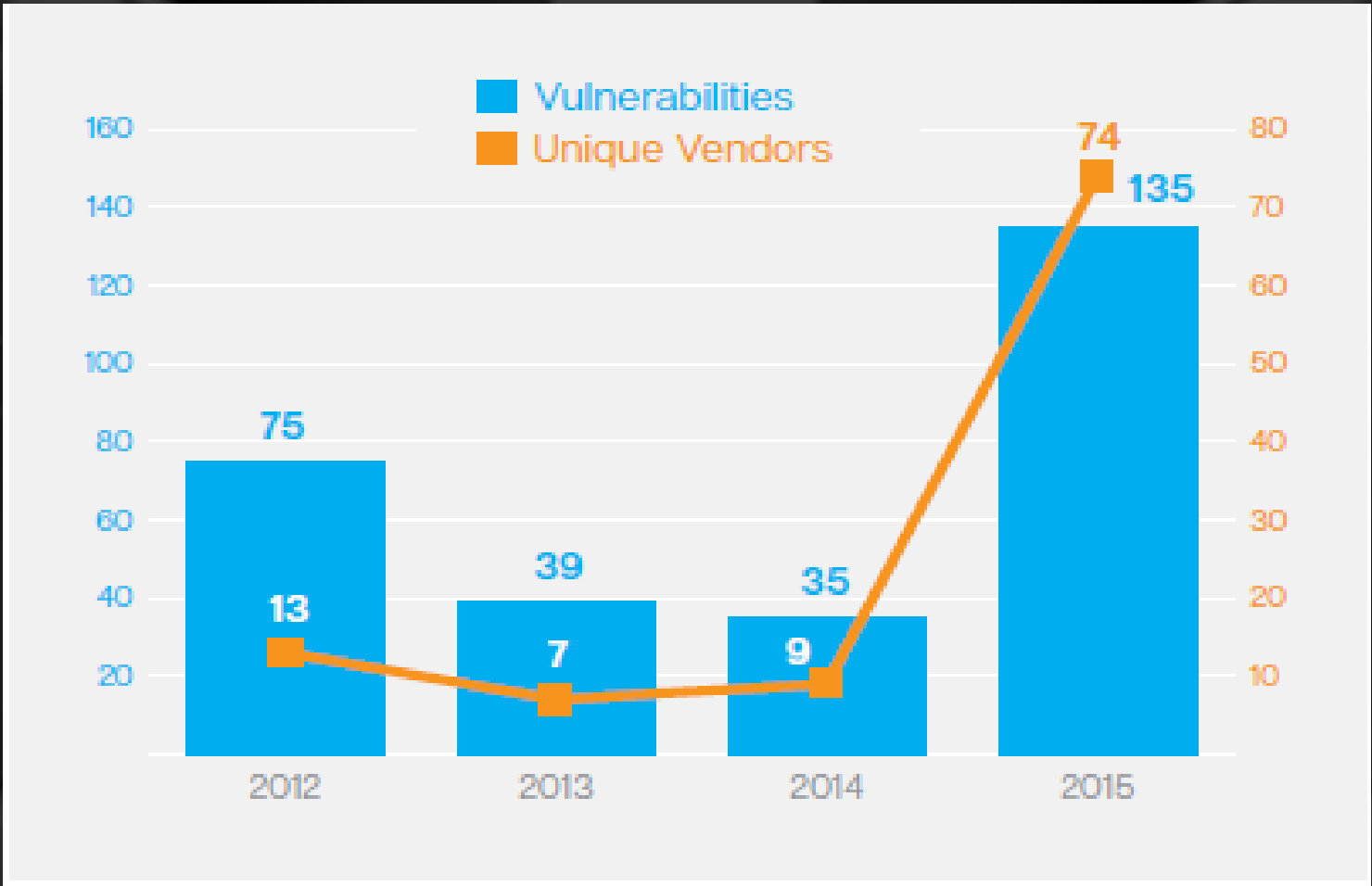
2015년 활동중인 악명 높은 APT 공격 그룹

- **Black Vine**
  - 중국 기반, 항공/의료, 지적재산권 및 신원정보
- **Advanced Threat Group 9**
  - 이란 정부지원, 저널리즘/인권단체 및 과학자
- **Cadelle and Chafer**
  - 이란 기반, 항공/에너지/통신, 주로 중동 대상
- **Duke and Seaduke**
  - 정부지원, 주로 유럽 정부기관 저명인사 대상, 2010년부터 활동
- **Advanced Threat Group 8**
  - 중국 기반, 금융/항공/정보기관/통신/에너지산업, 지적재산권
- **Waterbug and Turla**
  - 러시아 기반, 정부/대사관, 2005년부터 활동
- **Butterfly**
  - Facebook/Apple등과 같은 기업 대상

* APT: Advanced Persistent Threat (지능형지속위협)

산업용 제어 시스템(ICS)의 위험 증가

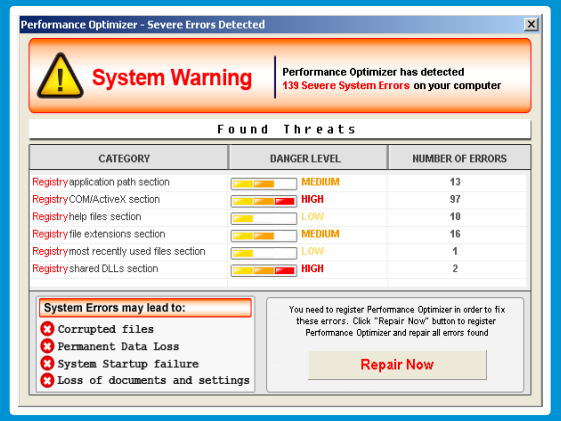
최소 7개의 제로데이 취약점이 악용됨



랜섬웨어

랜섬웨어의 진화 경로

위장 애플리케이션



사기성 안티바이러스

락커 랜섬웨어

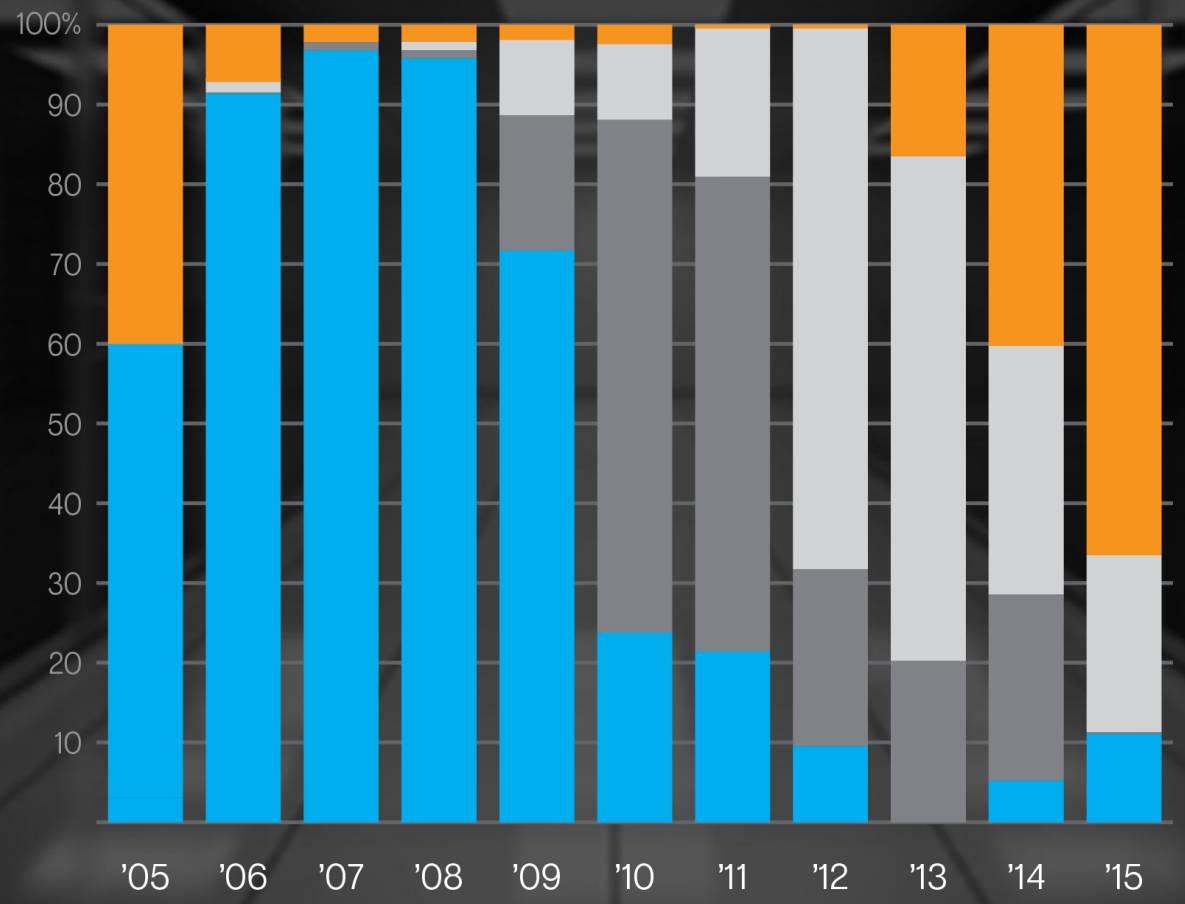
크립토 랜섬웨어

2005-2009 — **2010-2011** — **2012-2013** — **2014-2015**

"문제 해결" | "컴퓨터 청소" | "벌금" | "이용요금"

대세는 크립토 랜섬웨어

위장 애플리케이션 | 사기성 안티바이러스 | 락커 랜섬웨어 | 크립토 랜섬웨어



랜섬웨어 패밀리

- 안드로이드
- Linux
- OSX

2005 – 2012
2013 Q1 Q2 Q3 Q4
2014 Q1 Q2 Q3 Q4
2015 Q1 Q2 Q3 Q4
2016 Q1

Gpcoder
Reveton
Urausy
Nymaim
Cryptowall
Kovter
Browlock
Linkup
Onion
Zerolocker
TorrentLocker
Slocker
CTB-Locker/Citron
Synolocker
Coinvault
TeslaCrypt
Cryptolocker2015
VirLock
BandarChor
Cryptvault
Simplocker
Pacman
Pclock
Threat Finder
Tox
Troldesh
Encryptor RaaS
CryptoApp
LockDroid
Unix.Ransomcrypt
LowLevel404
CryptInfinite
Radamant
VaultCrypt
XRTN
Dumb
Mabouia OSX POC
Power Worm
DMA-Locker
Gomasom
Chimera-Locker
Hidden Tear
ORX-Locker
Locky
Ransom32
KeRanger
PayCrypt
Job Cryptor
Hi Buddy
Vipasana
Hydracrypt
Umbrecrypt
73v3n
CryptoJocker
Nanolocker
LeChiffre
Magic
Ginx

전세계 크립토 랜섬웨어 공격 35% 증가

크립토 랜섬웨어		
2014	2015	
269K	362K	
–	+ 35%	
Average Per Day	Average Per Day	
737	992	
1일 평균	1일 평균	

랜섬웨어 (전체)	2015
	약 4,440

2015년 연간 362,000건, 1일 평균 992개

소비자 대상 사기

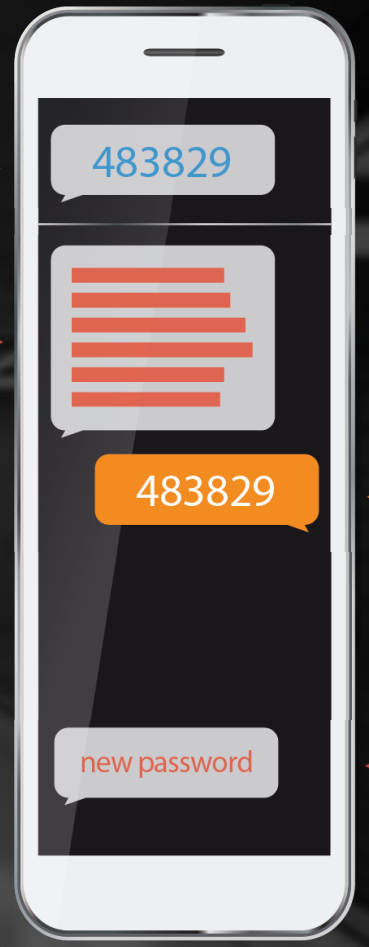
지메일(Gmail) 사기 스캠 과정

공격자가
일반에 공개되어 있는
피해자의 이메일 주소와
전화번호 입수

피해자 행세를 하며
구글에 비밀번호
재설정 요청

3 Google

구글이 피해자에게
인증 코드 발송



4

공격자가 피해자에게
다음과 같은
문자 메시지 전송

"구글이 귀하의 계정에서 비정상적인 활동을 감지했습니다. 승인되지 않은 활동을 차단하기 위해 귀하의 모바일 기기로 발송한 코드를 회신해 주세요."

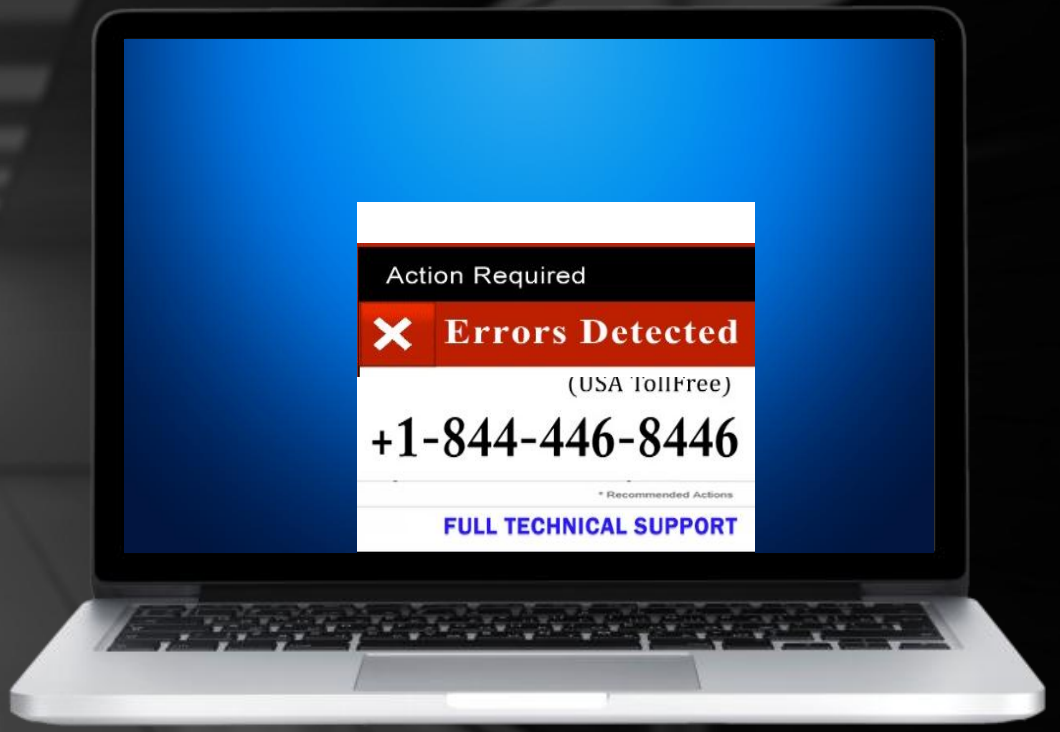
5

피해자는 구글이
비밀번호 재설정을 위해
보낸 인증코드를
공격자에게 전달

6

공격자는
비밀번호를 재설정하고
원하는 정보를 탈취한 뒤에
피해자의 의심을 피하기
위해 구글 행세를 하며
새로운 임시 비밀번호를
피해자에게 전달

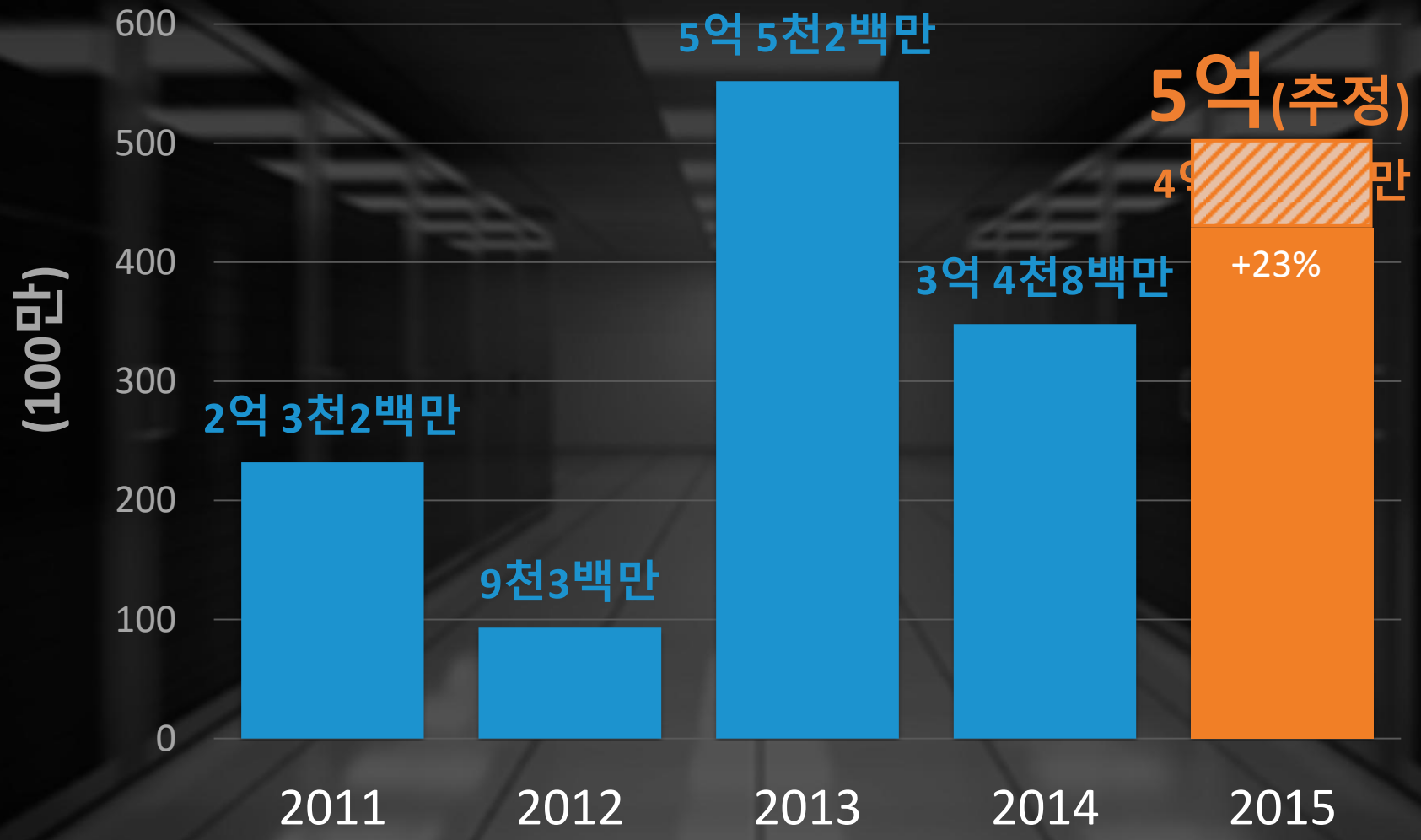
‘기술 지원 위장 사기’ 스캠



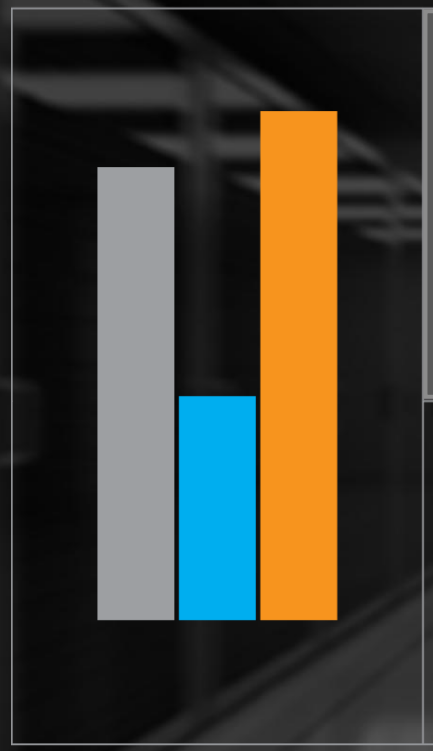
‘기술 지원 위장 사기’ 스캠 차단

정보 유출

유출된 개인정보 전체 건수



2015년 대형 정보유출사고



1천만 건 이상의
개인정보 유출사고

2013	2014	2015
8	4	9
–	-50%	+125%

취약점

합법적인 웹사이트 여전히 위험

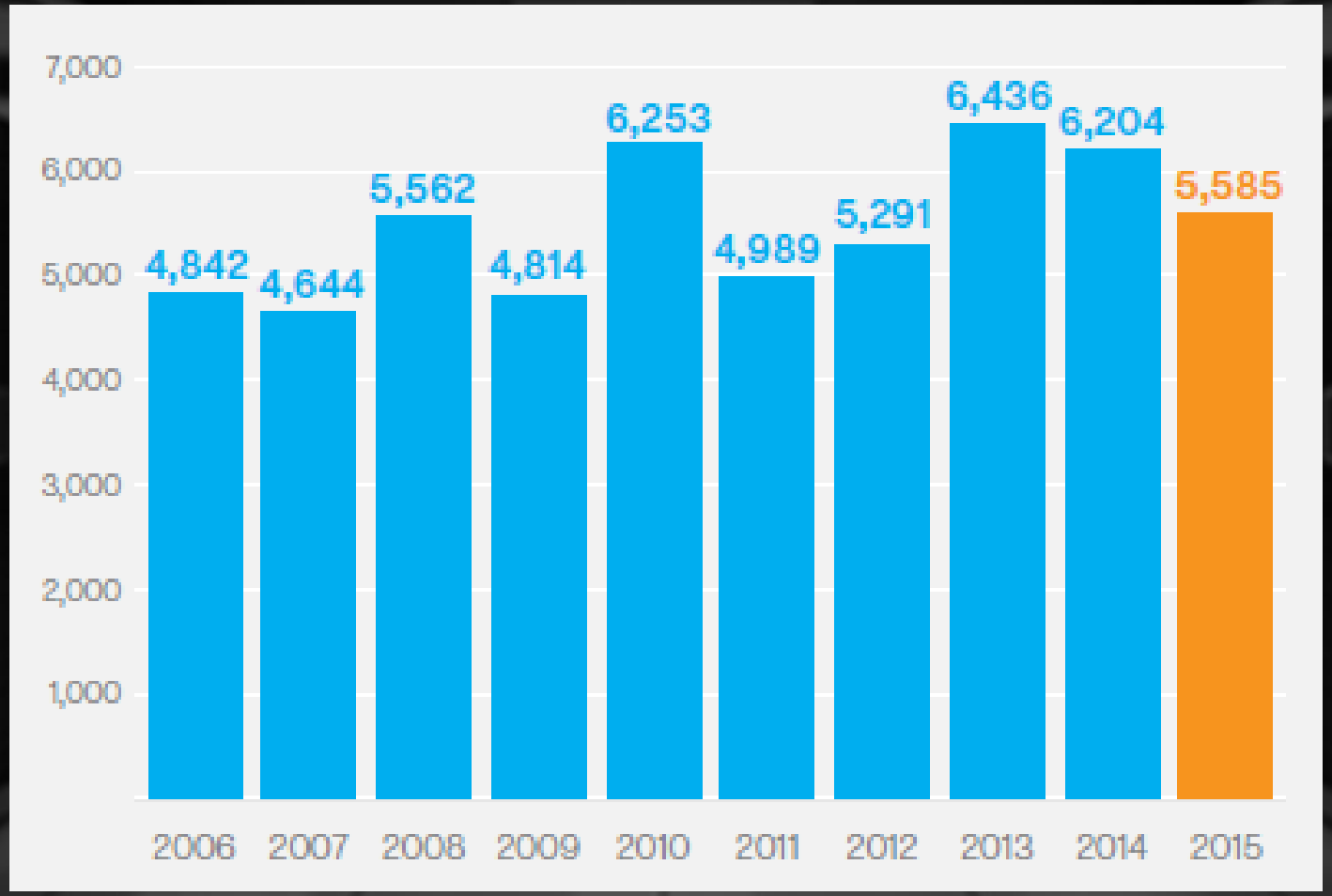
취약점이 발견된 웹사이트 비율

2013	2014	2015	
77%	76%	78%	
–	-1% pts	+2% pts	

중대한 취약점이 발견된 웹사이트의 비율

2013	2014	2015	
16%	20%	15%	
–	+4% pts	-5% pts	

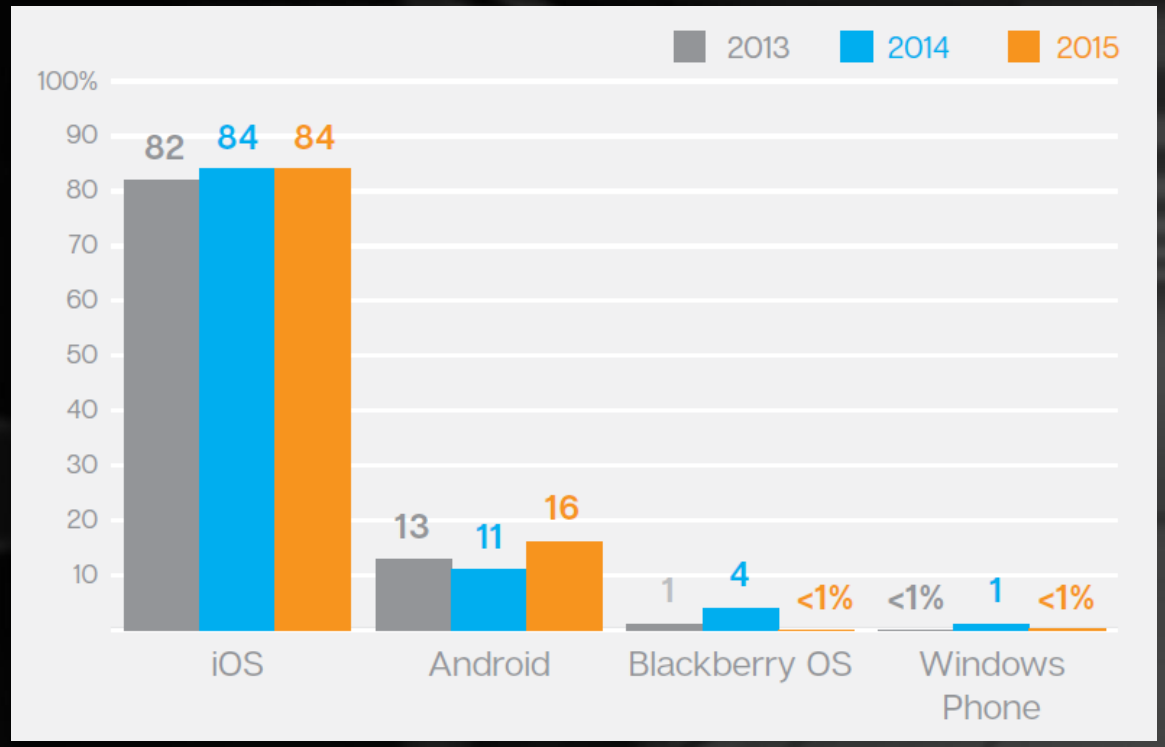
새롭게 발견된 취약점 수



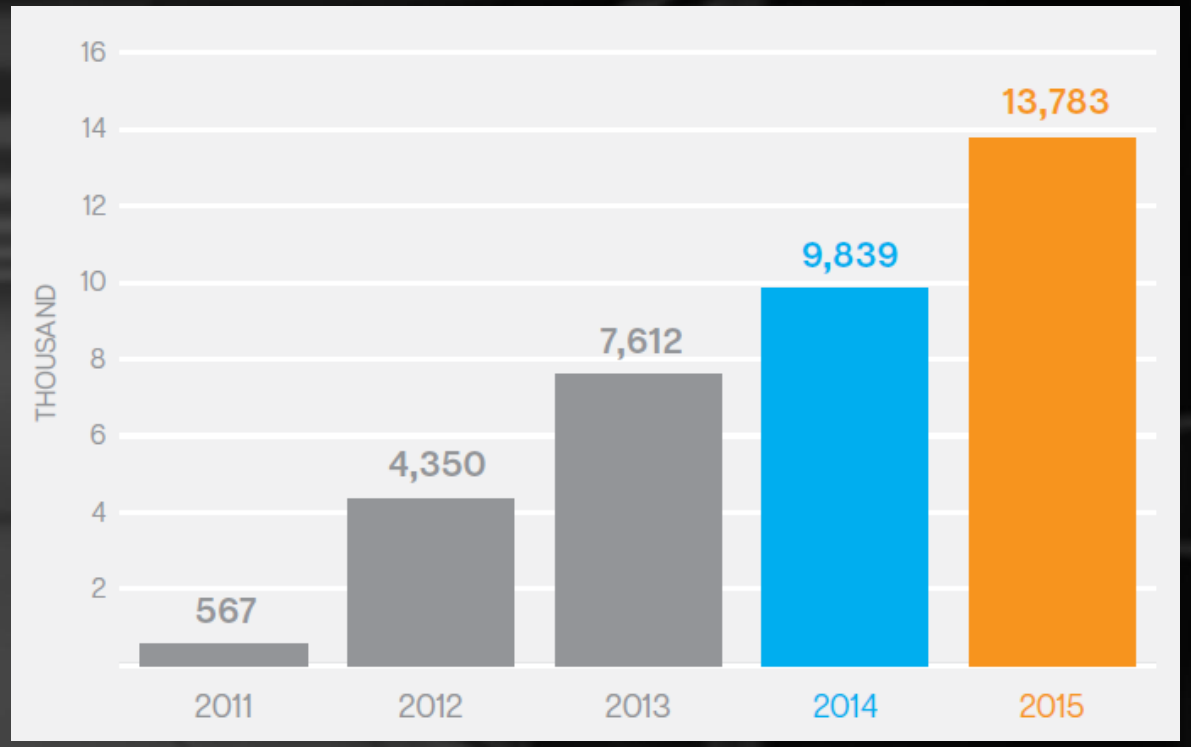
2014년 대비

15% 감소

모바일 취약점



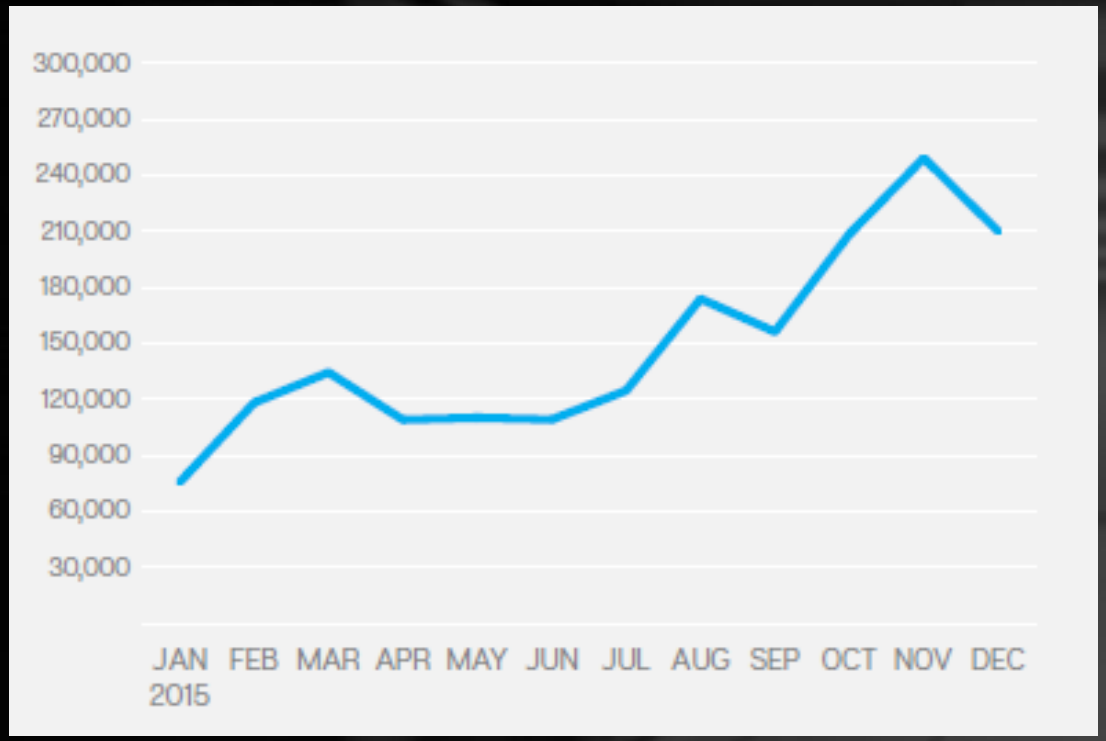
<모바일 OS별 취약점 수>



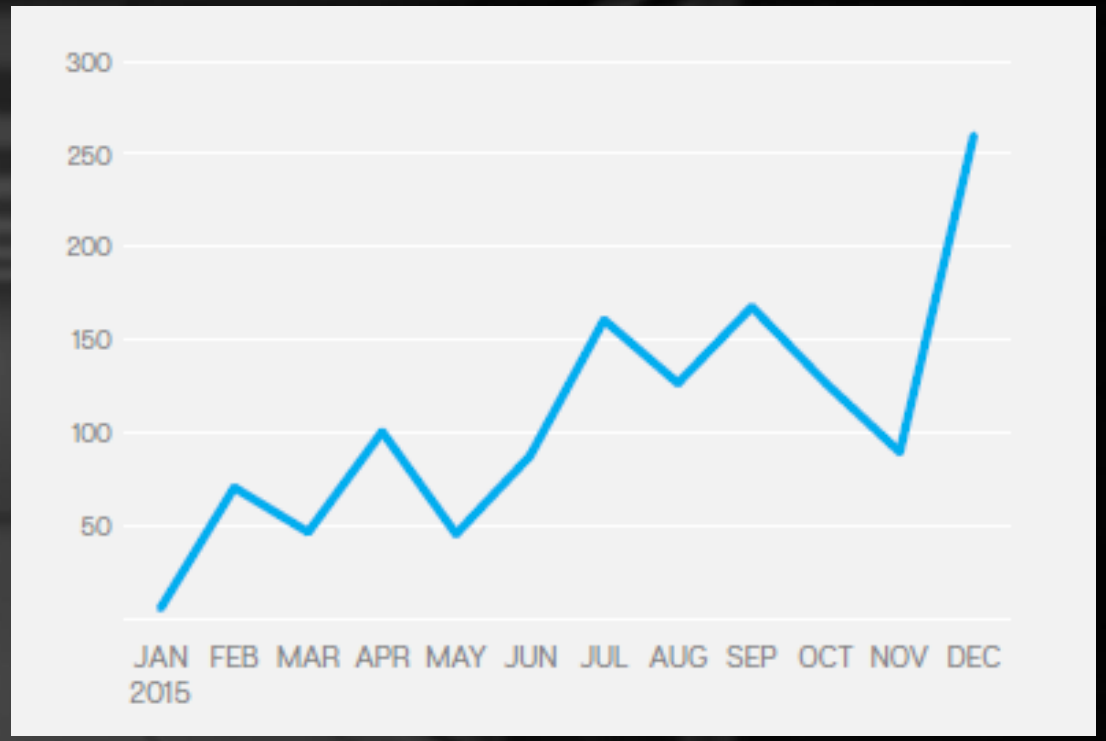
<누적 안드로이드 악성코드 수>

iOS의 경우 2015년 9개 악성코드 발견

Mac과 Linux, 보안 안전지대는 옛말



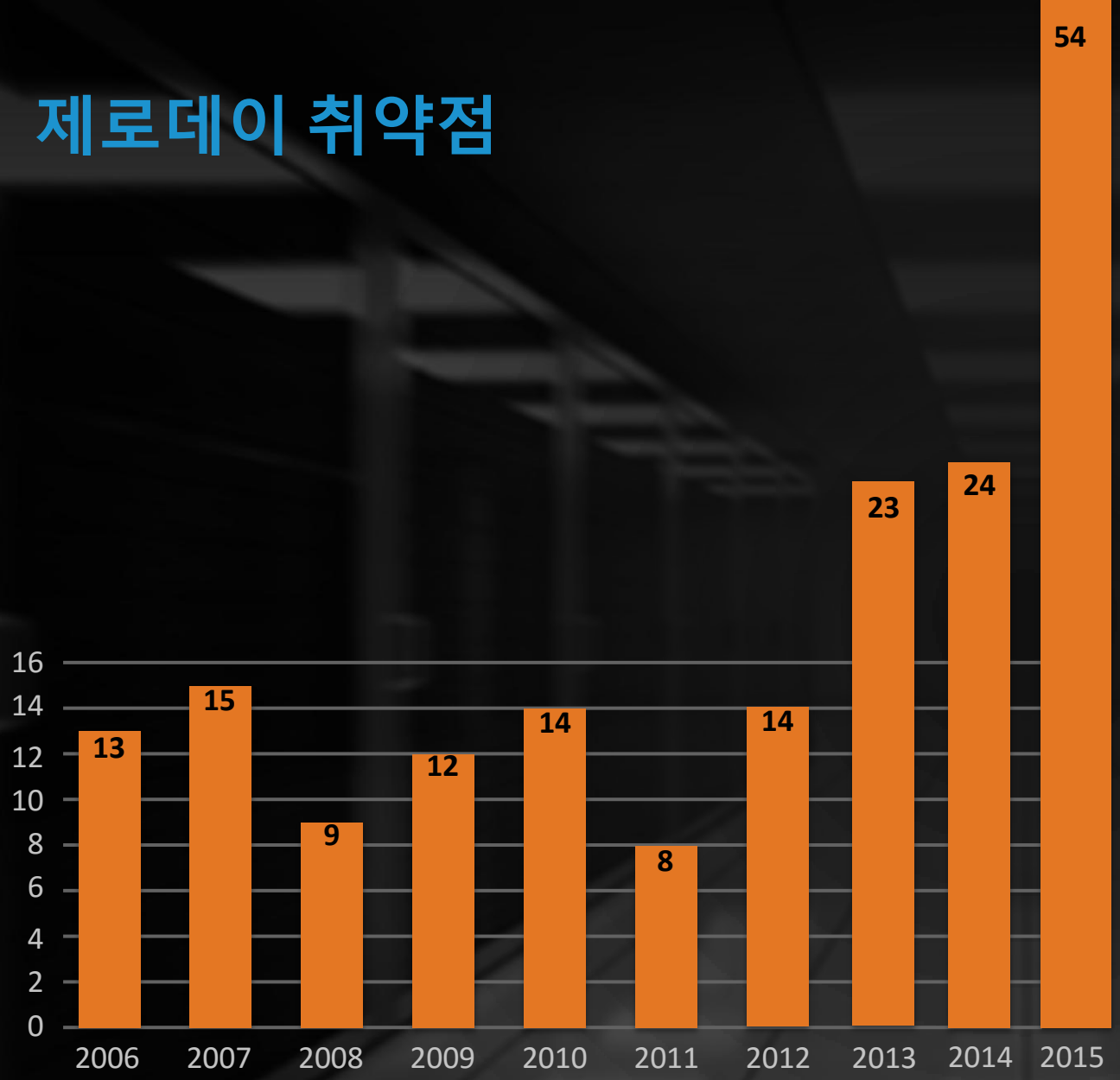
<Mac OS X 악성코드 증가 추이>



<Linux 악성코드 증가 추이>

사이버범죄의 전문화

제로데이 취약점



가장 많이 공격에 이용되는
Top 5 제로데이 취약점

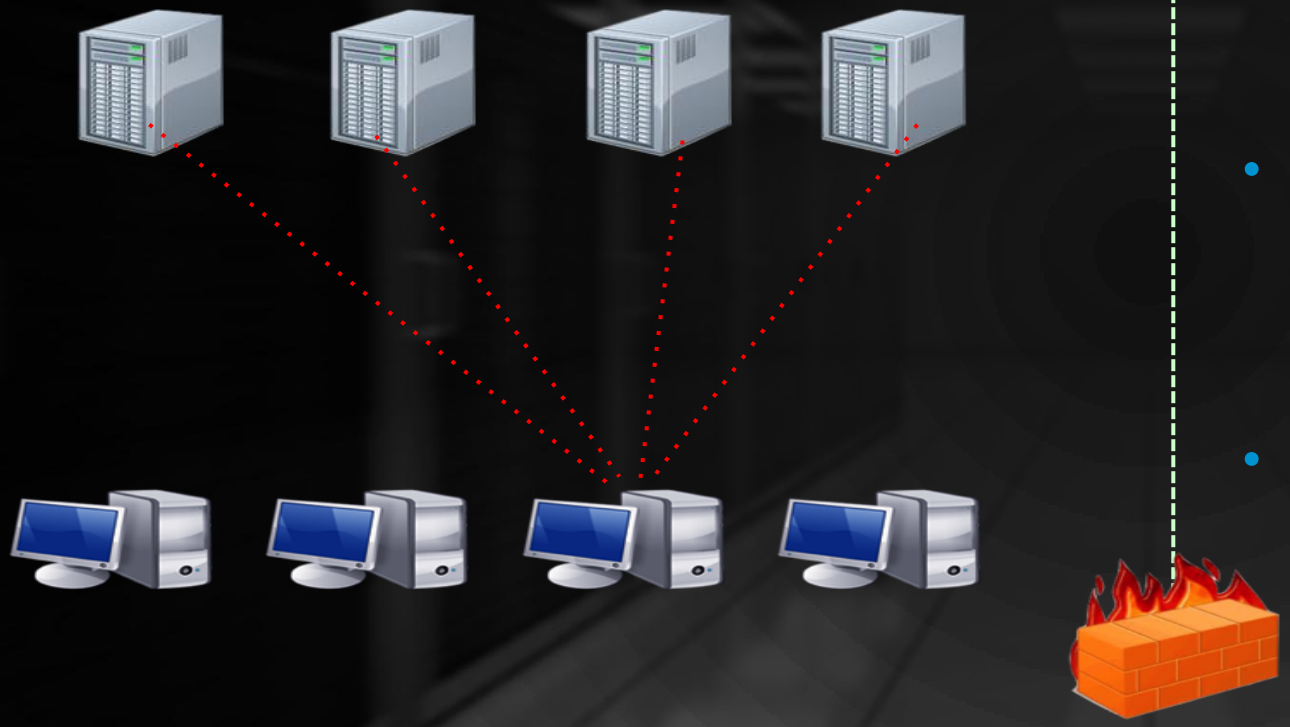
순위	취약점 이름	2015년 비율
1	어도비 플래시 플레이어 CVE-2015-0313	81%
2	어도비 플래시 플레이어 CVE-2015-5119	14%
3	어도비 플래시 플레이어 CVE-2015-5122	5%
4	힙(Heap) 기반 버퍼 오버플로우 ('고스트') CVE-2015-0235	<1%
5	어도비 플래시 플레이어 CVE-2015-3113	<1%

어도비, 플래시 취약점에 대한 긴급 패치 배포

- 6월 23일 어도비는 중대 제로데이 취약점(CVE-2015-3113)에 대한 긴급 패치 배포
- 그 후 일주일 내로 가장 유명한 5개 익스플로잇 키트(exploit kit)에 패치된 이 취약점들 추가

익스플로잇 키트	최초 발견
매그니튜드(Magnitude)	2015년 6월 27일
앵글러(Angler)	2015년 6월 29일
뉴클리어(Nuclear)	2015년 7월 1일
리그(RIG)	2015년 7월 1일
뉴트리노(Neutrino)	2015년 7월 1일

버터플라이(내부정보 탈취후 증시 차액) – 공격자 툴



- **Hacktool.Bannerjack:** 로컬 네트워크에서 취약 서버의 위치를 파악하는데 이용
- **Hacktool.Multipurpose:** 기본적인 네트워크 검색(network enumeration) 수행, 로그 수정, 파일 삭제 등을 통한 활동 은닉
- **Hacktool.Eventlog:** 이벤트 로그 분석, 콘텐츠 복사(dump), 입력 정보 삭제

Hacktool.MultiPurpose, 제3자를 위한 도움말 페이지 제공

```
General options
---------------
 --install: install server on local host and load it
 --host <host>: hostname or IP (local host if not set)
 --password <password>: server password connection (mandatory)
 --forceload: load server on local host without test

Server options
--------------
 --cmd: server command:
    dump: dump stuffz
      --sam: fetch LM/NTLM hashes
      --machines: fetch machines hashes
      --history: fetch history for LM/NTLM hashes
      --sh: fetch logon sessions hashes
      --sp: fetch security packages cleartext passwords
      --accounts: <account list>: with --sam, specify accounts to dump
(comma separated)
      --lsa: fetch LSA secrets
```

버터플라이 – C&C(명령 및 제어) 서버 운영

메일 서버

콘텐츠 관리 시스템

C&C 서버

C&C 서버

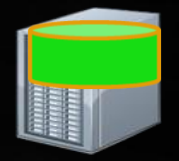
C&C 서버

버터플라이 – C&C(명령 및 제어) 서버 운영

메일 서버

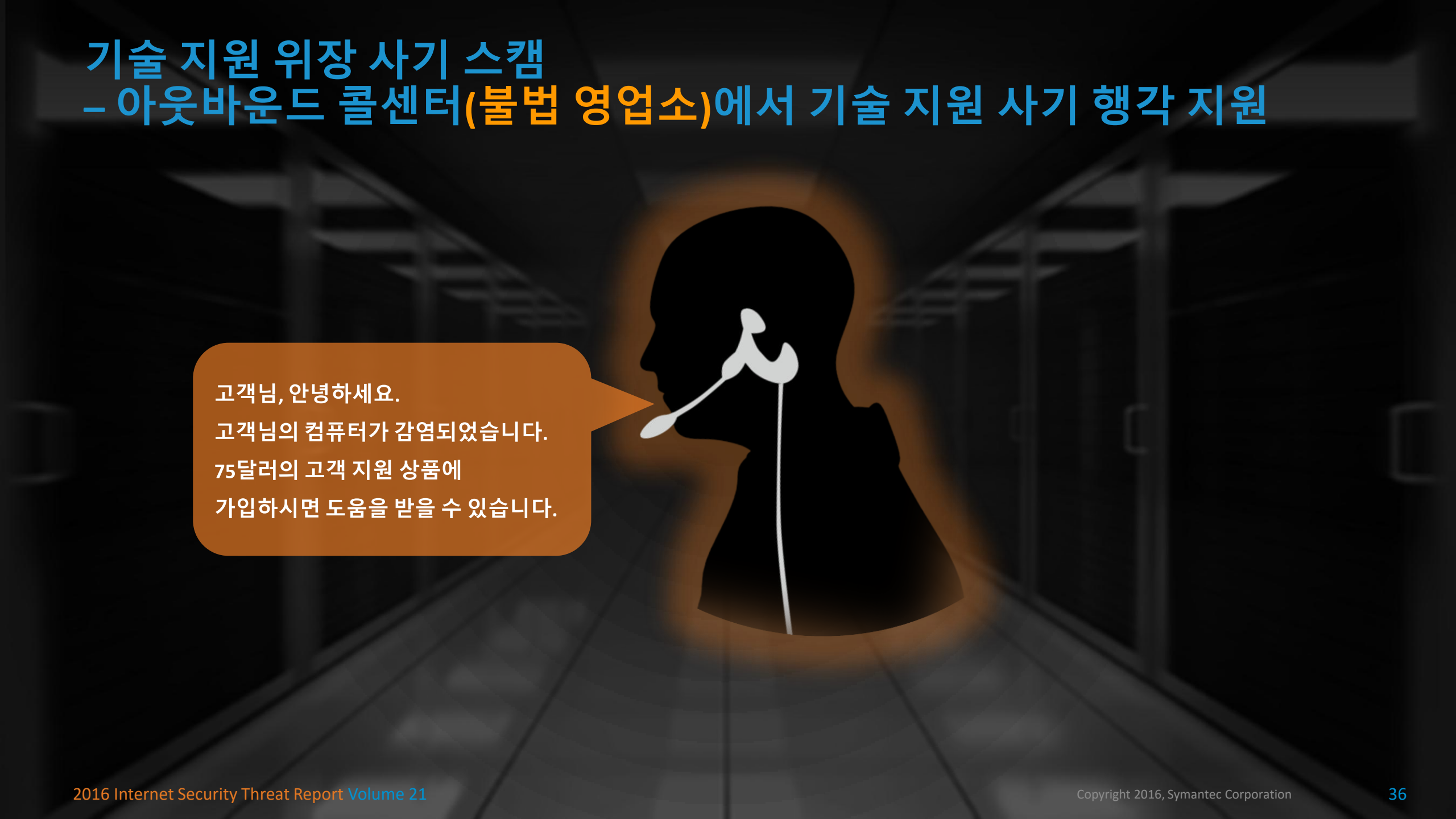
콘텐츠 관리 시스템

- 가상 OS에서 C&C 운영
- 가상 OS 암호화
- 서버 로그 삭제



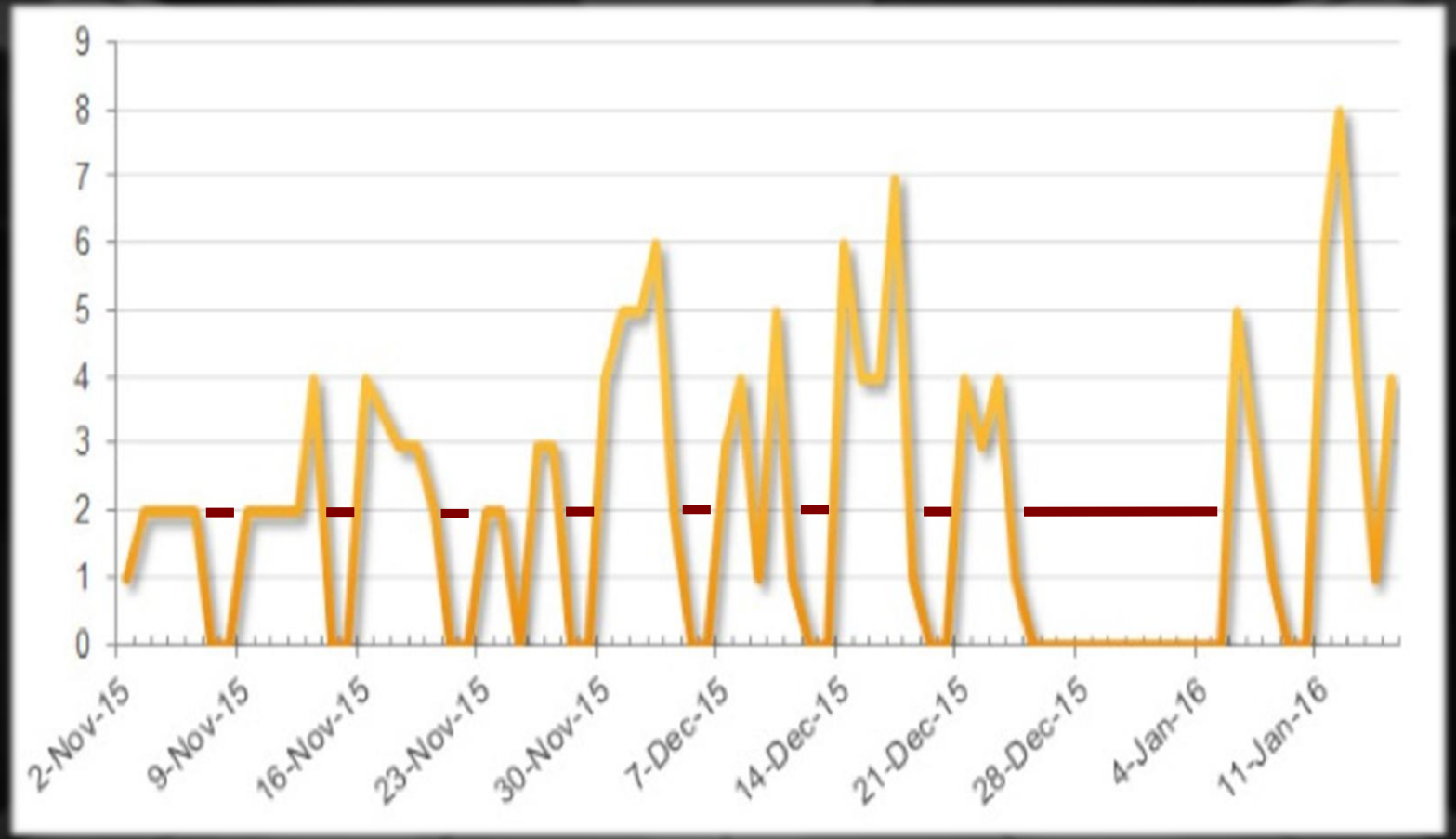
C&C
서버

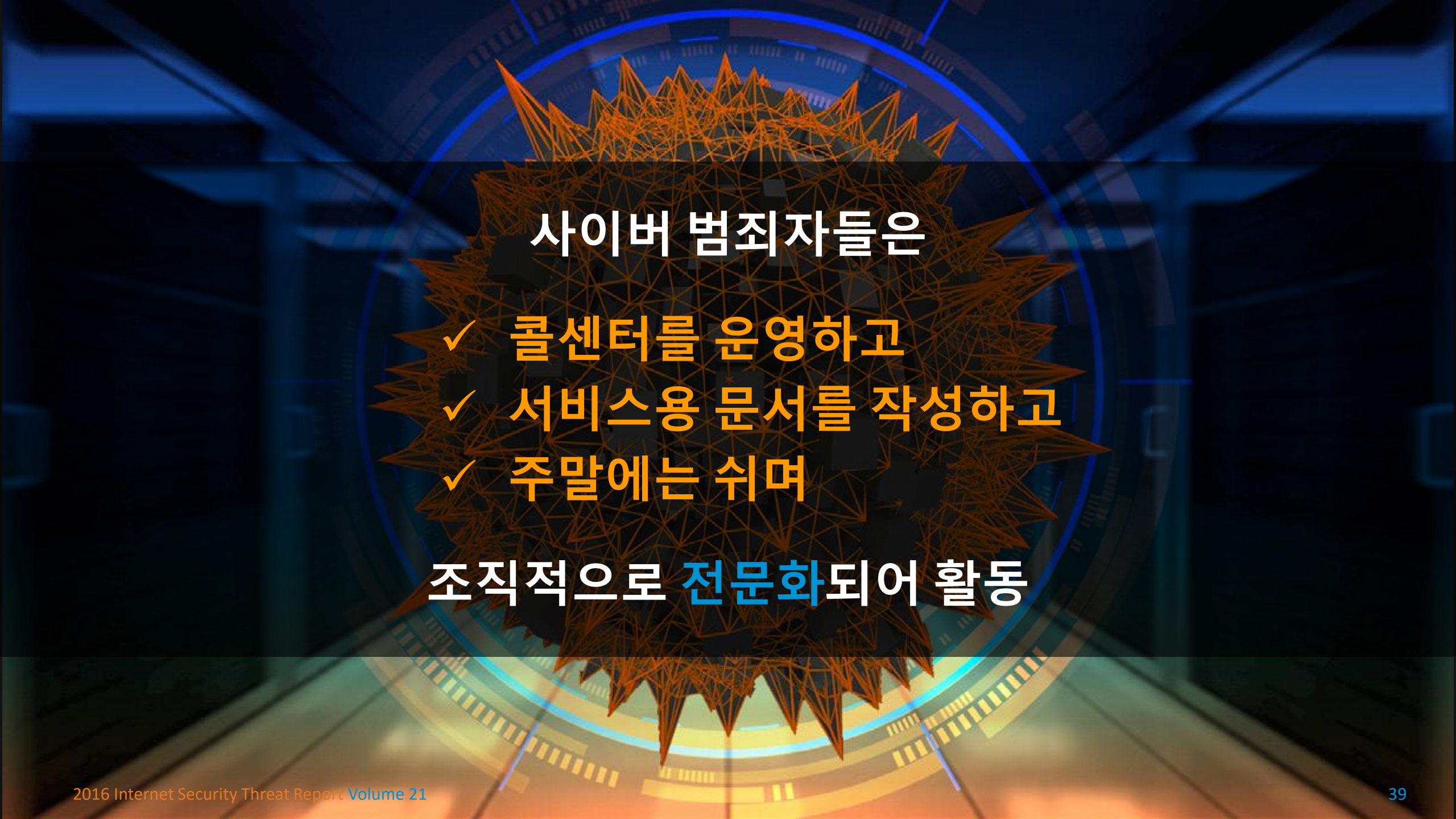
기술 지원 위장 사기 스캠
– 아웃바운드 콜센터(불법 영업소)에서 기술 지원 사기 행각 지원



테슬라크립트(TeslaCrypt) 랜섬웨어 – 콜센터 제공

드라이덱스 갱 – 주중에만 활동(주말/연휴 휴무)




사이버 범죄자들은
✓ 콜센터를 운영하고
✓ 서비스용 문서를 작성하고
✓ 주말에는 쉬며
조직적으로 전문화되어 활동

주요 조사 결과

- 제로데이 취약점 전년 대비 **125% 증가**, **54개**로 사상 최다
- 스피어피싱 표적 공격 캠페인 **55% 증가**
- 정보 유출 사고의 대형화… 전세계 개인 정보 **유출 5억 건**
- 크립토 랜섬웨어 **35% 증가**
- 합법적인 웹사이트 **4개 중 3개**가 위험
- **1억 건**의 기술 지원 위장 사기 스캠 차단
- **iOS** 등 모바일 보안 위협 증가
- 사이버 범죄 집단의 **전문화**

시만텍 코리아

Thank you!