보안, 2013년 최신 동향 리포트
- IBM 보안연구소가 말하다

IBM 소프트웨어 보안 사업부 김형욱 차장

세상은 변화하고 있습니다

변화를 받아들이고 대응하는 기업만이 생존할 수 있습니다

50억 개의 지능화된 디바이스
2016년까지 활용 예정

전세계 67%의 소비자
모바일을 통한 적극적인 거래를 기대

40%의 사람들
대면 대신 소셜을 통해 더 많이 의사소통

300억 개의 컨텐츠
매달 페이스북을 통해 공유

95%의 사용자
클라우드를 사용하지 않는다고 믿고 있지만 알게 모르게 사용 중

30억 명의 iCloud 사용자
소셜, 모바일, 개인 데이터를 활용

스마트한 시대의 비즈니스 경쟁력 확보

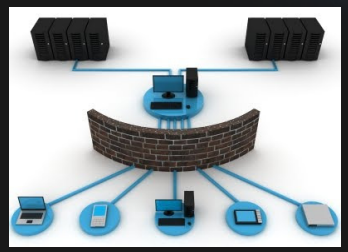
새로운 기술은 신규 비즈니스 기회를 의미합니다

빅 데이터

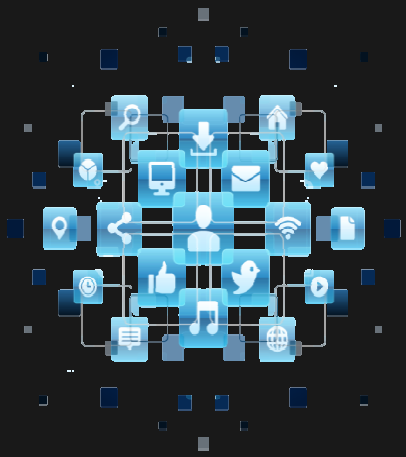
클라우드

비즈니스

고객 • 파트너 • 직원

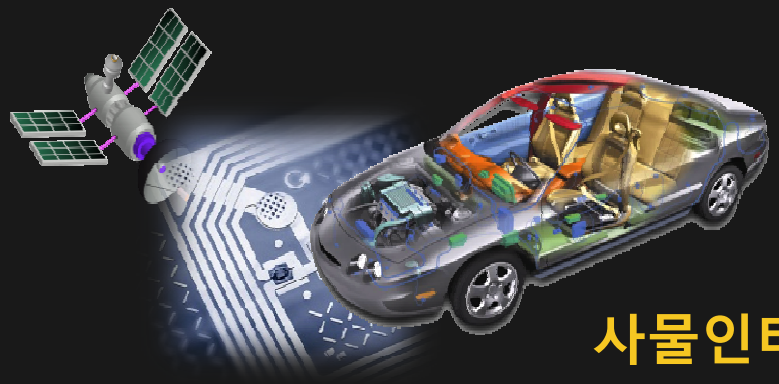


보안



소셜

모바일

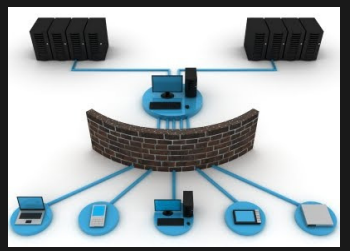


사물인터넷

게임의 판도를 바꾸는 출발점

기업이 살아 숨쉴 수 있는 원동력을 만들어 드립니다

빅 데이터



보안

모바일

IBM X-Force 보안 연구소는 IBM 보안 프레임워크에 보다 향상된 보안과 위협 연구를 제공하는 토대입니다.

X-FORCE

IBM X-Force 연구소의 임무:

- **연구**
  오늘날 보안 도전과제를 위한 새로운 공격 기술과 보호 방법 개발 연구
- **모니터링**
  빠르게 변화하는 위협 동향 평가와 모니터링
- **교육**
  고객과 일반 대중을 위한 보안 교육

변화하는 위협 동향을 모니터링하고 분석하기 위해 IBM의 많은 팀들은 협업하고 있습니다.

범위

20,000+ 관리 계약된 디바이스

3,700+ 전세계 통합보안 관제 고객

150억+ 매일 모니터링되는 이벤트수

133 모니터링되는 국가수 (MSS)

1,000+ 보안 관련 보유 특허수

IBM Research

깊이

17B 분석된 페이지와 이미지 수

40M 스팸/피싱 공격 수

73K 문서화된 취약점들

수십억 매일 탐지되는 공격 시도 수

수백만 악성코드 샘플 수

2013 상반기 보안 동향 키워드 :
Attackers Optimize Tactics

보고서의 주요 3가지 동향

Targeted Attacks and Data Breaches

- 전략적 정교화
- Watering Hole 공격
- 본사로부터 멀리 떨어진 지역 사이트 침해
- DDoS 엽합작전

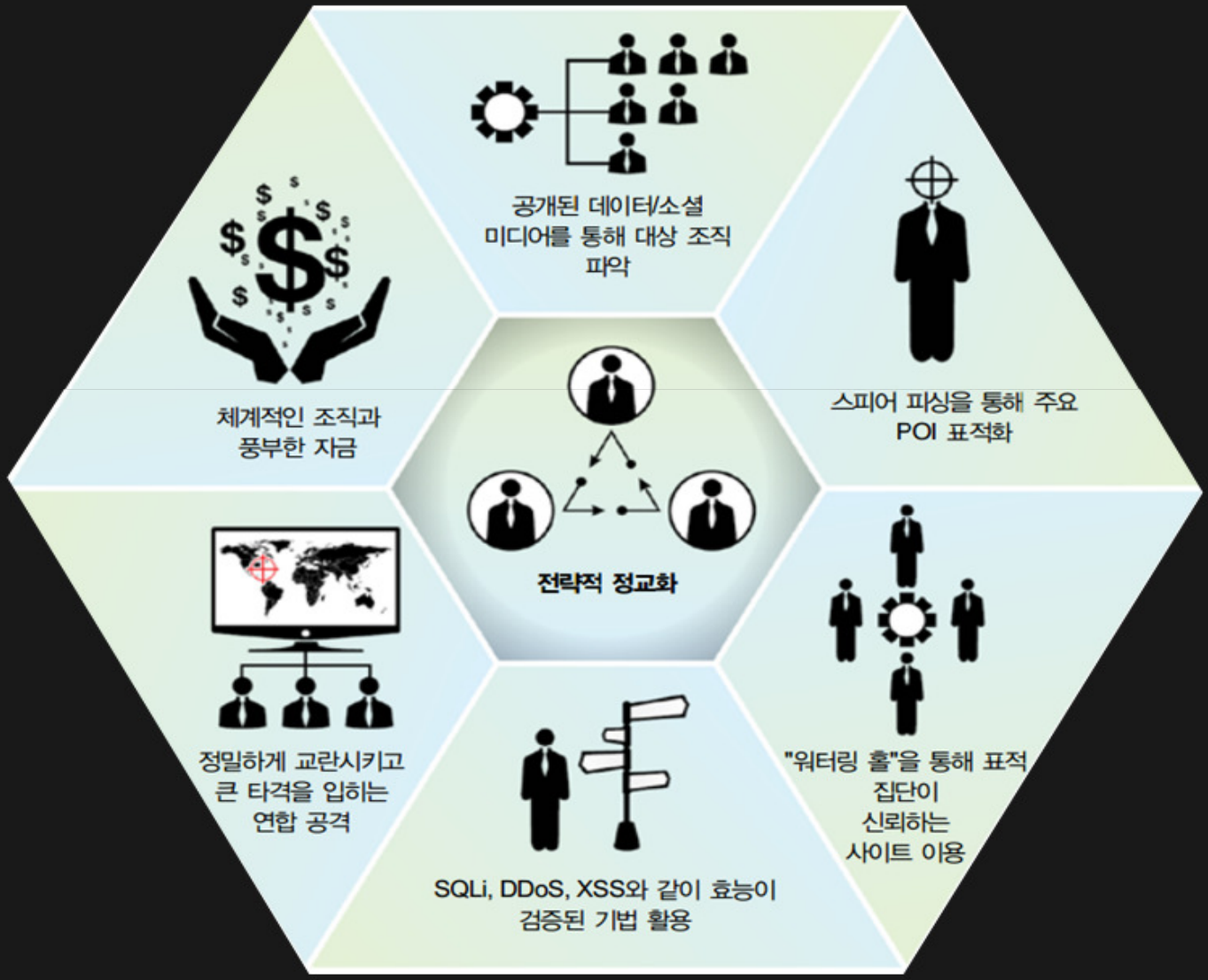
Social and Mobile

X-Force by the Numbers

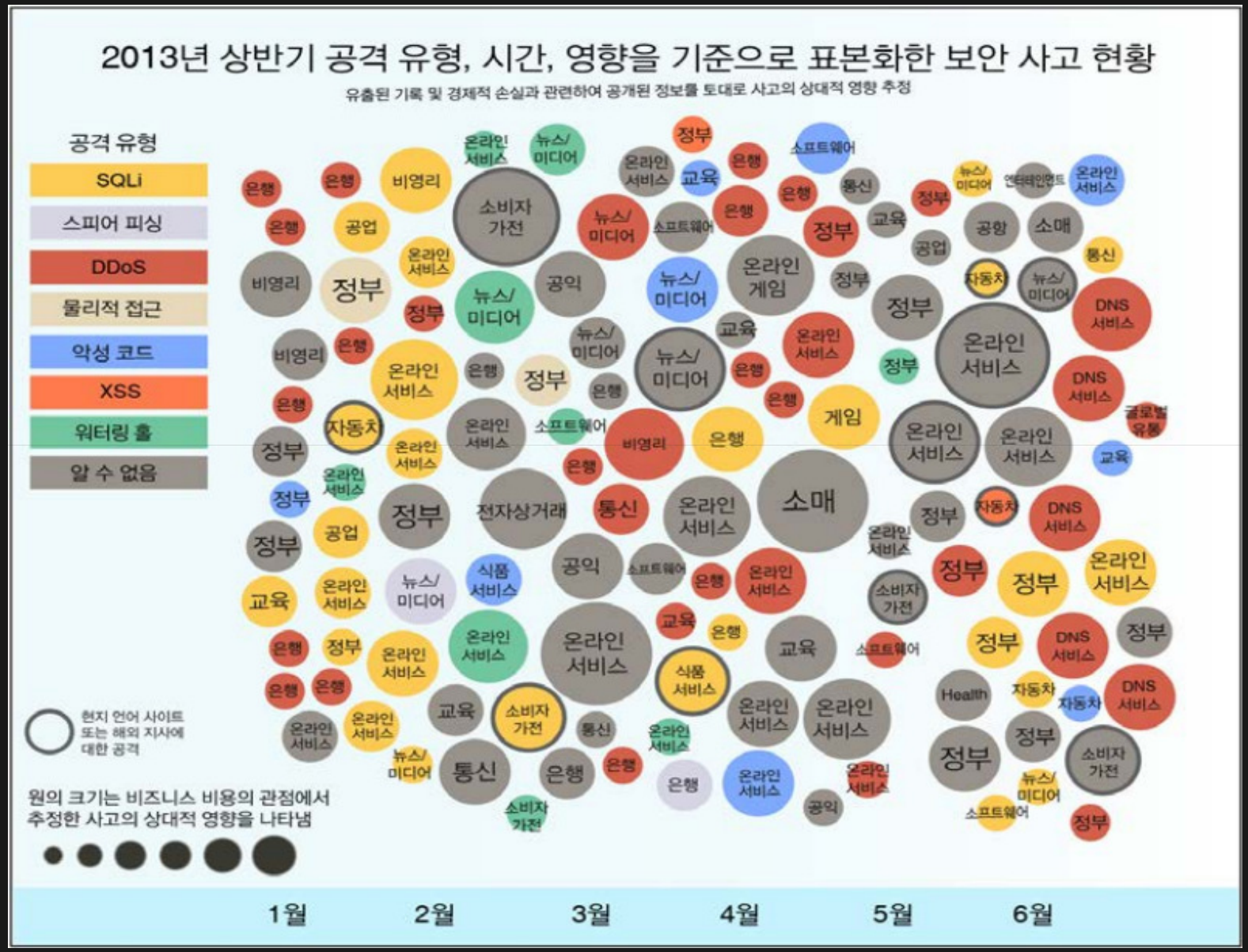
Operational sophistication

신뢰 기반 공격은 공격 대상을 침해하기 위해 좀더 **전략적으로** 정교화되는 공격의 한 예입니다.

많은 유출사고들이 개별 제작된 악성코드와 제로데이 공격의 결과만이 아니라, 가장 저항성이 낮은 경로를 찾는 것도 포함됩니다.

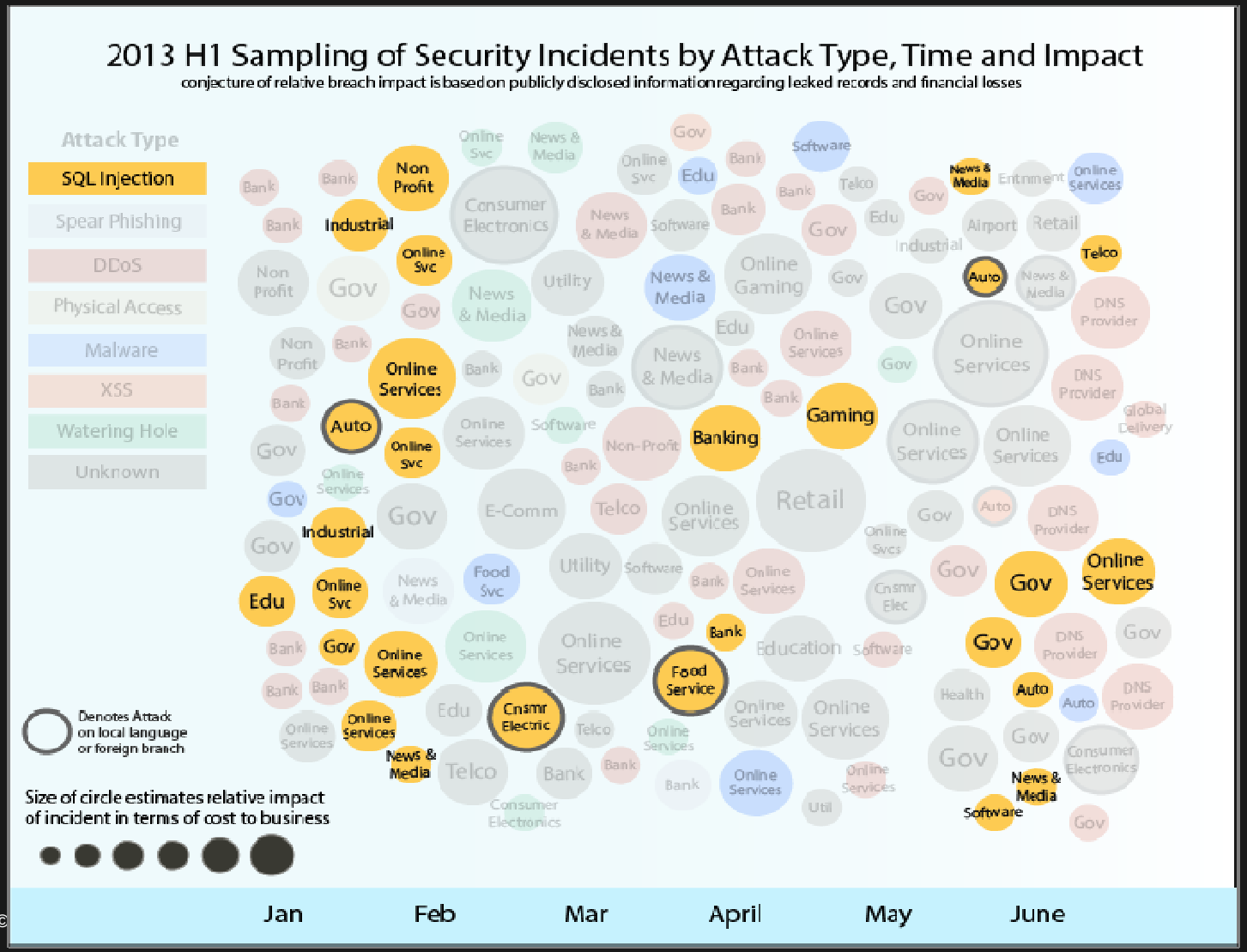


2013 상반기 보안 사고



SQL Injection

데이터베이스 침해를 위한 여전히 높이 사용되는 취약점



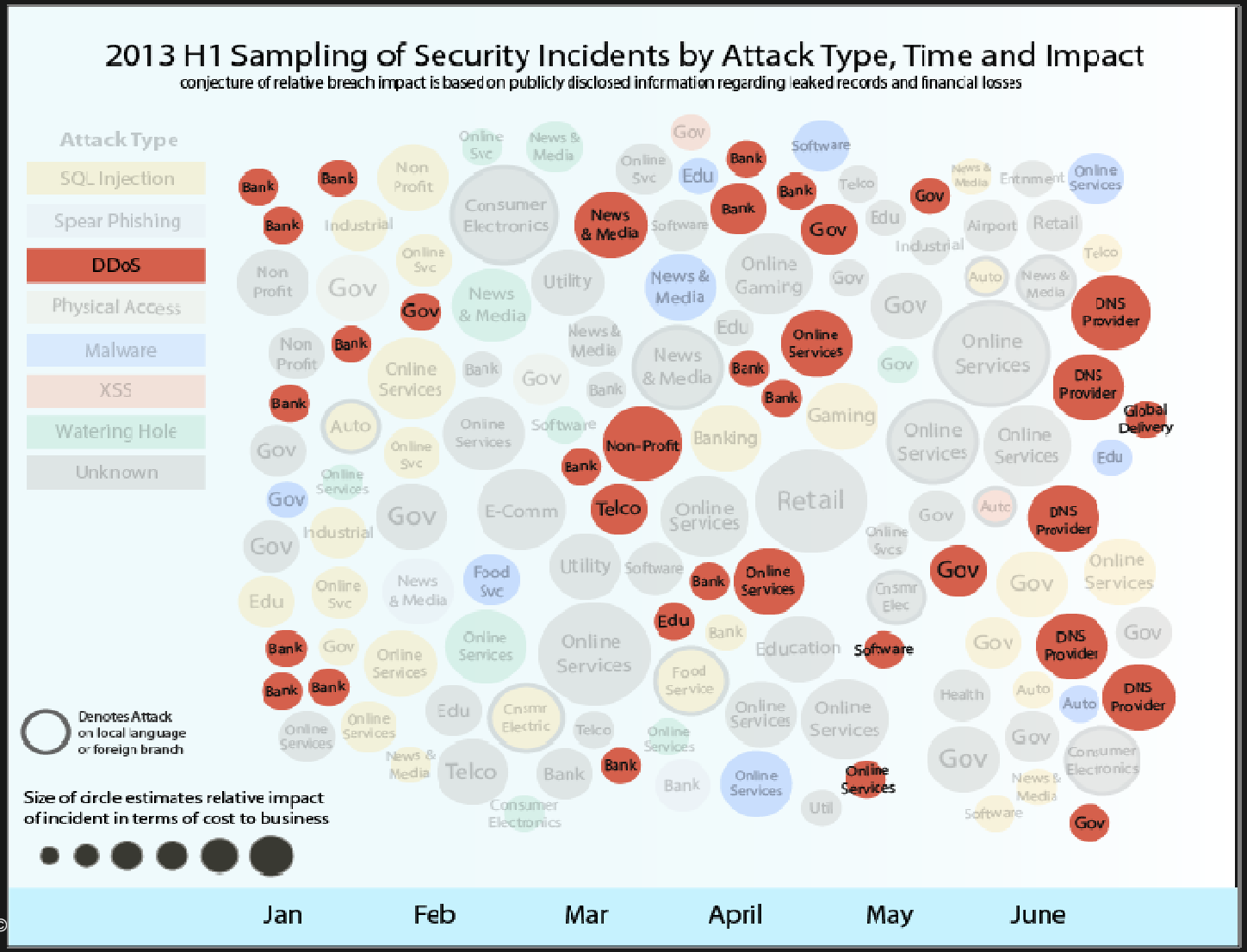
22% 추적되고 공개된 보안사고 중

낮은 위험 / 낮은 보상

- 이전 버전 CMS 설치
- CMS 플러그인
- 포럼 소프트웨어
- 다른 유명한 제3자 스크립트

DDoS Attacks

비즈니스 파괴 유지



높은 트래픽 양

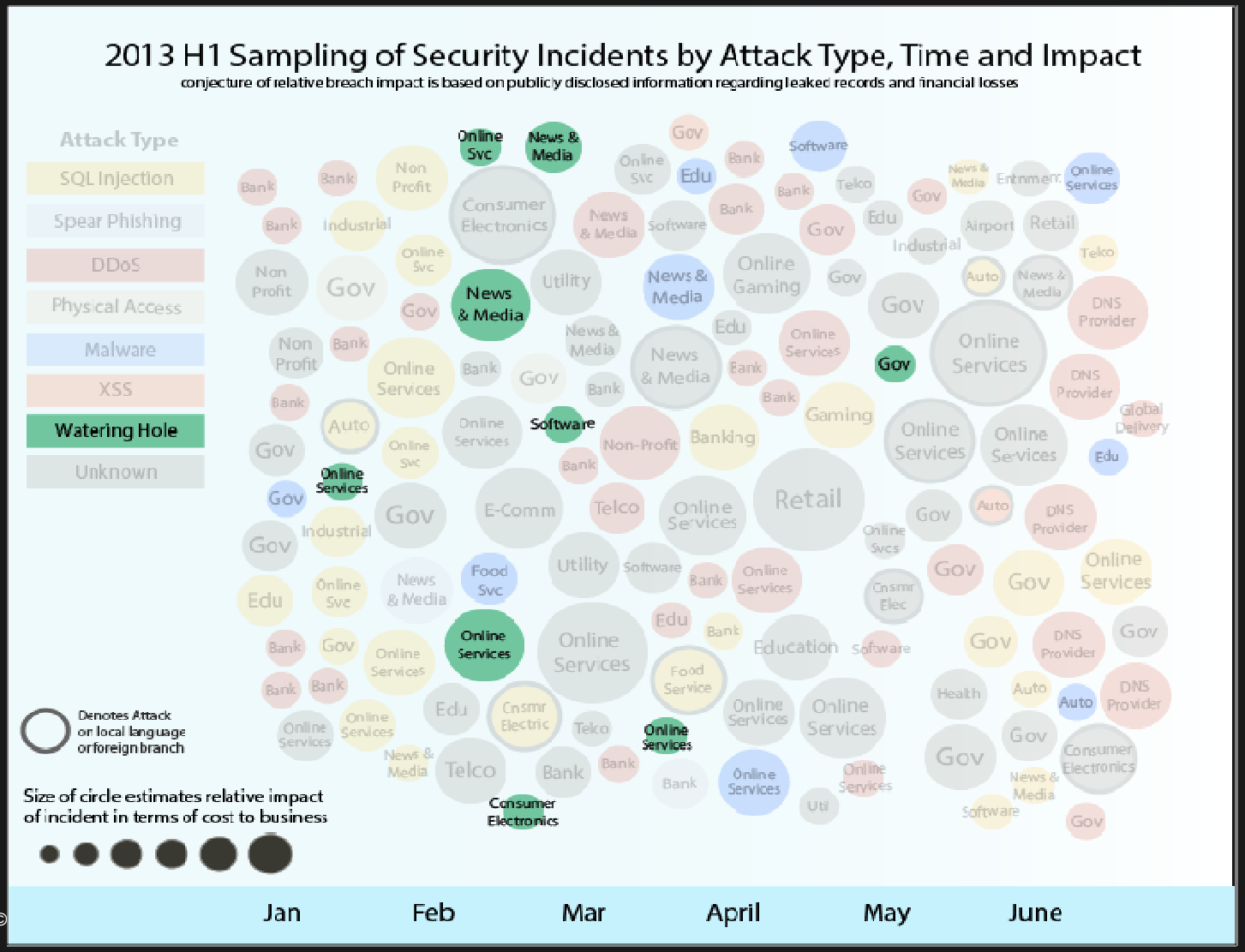
300Gbps

영향받는 산업군:

- 은행
- 정부
- DNS 서비스 회사

"Watering Hole"

침해된 최종 사용자의 신뢰 기반 공격



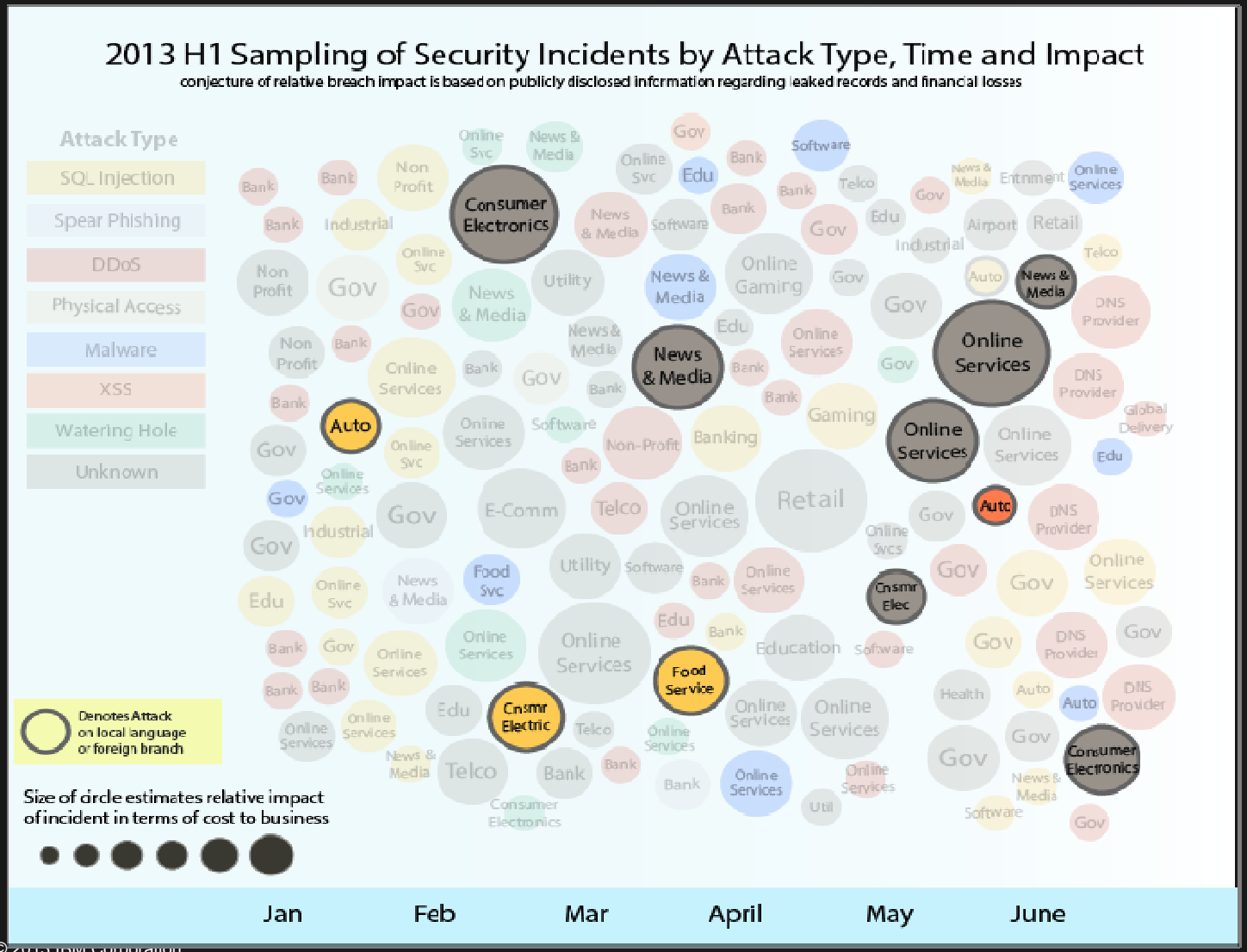
제로데이 공격 기반 합법적 사이트 침해

숙련된 사용자를 공격 목표

- 핵심 개발자
- 정부 직원
- 신뢰 사이트의 의심할 수 없는 접속자

Disenfranchised

브랜드를 침해를 위해 해외 지사 사이트 공격



본사 밖의 해외 국가 내 글로벌 브랜드를 목표로 함

공격자의 탐색

- 외국어 사이트 상의 더 낮은 보안 수준
- 사용자 정보를 수집하는 일시적인 마이크로 사이트
- 최소의 저항성을 갖는 브랜드 침해

보고서의 주요 3가지 동향

Targeted Attacks
and Data Breaches

Social and Mobile

- 사용자들을 목표로 신뢰 관계 남용
- 경제적, 명성에 있어 영향
- 소셜 미디어 블랙마켓
- 안드로이드 악성코드의 최근 발전

X-Force by the Numbers

Social Media

공격자의 새로운 활동무대

공격자의 최우선 목표가 된 소셜 미디어는 모바일 디바이스로 그 대상 영역 확대

- 공격 전 정보 수집
- 계정 판매 범죄 (블랙마켓)
- 악성 링크를 사용자가 클릭하도록 유혹하는 캠페인

경제적, 명성에 있어 영향

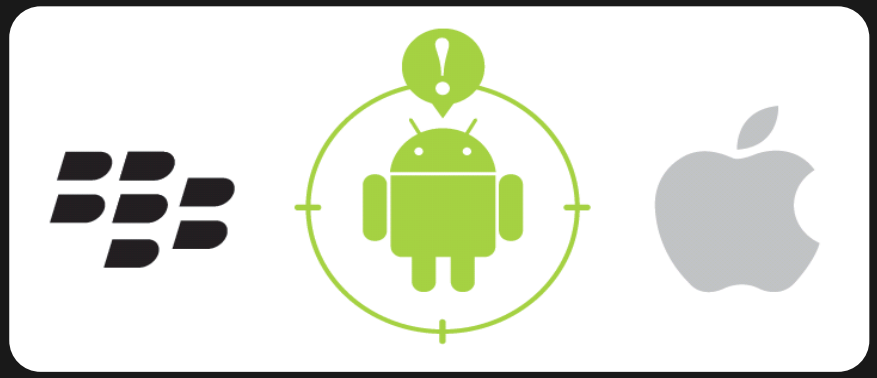
사생활과 업무 영역에 광범위하게 사용

서비스를 차단하는 대신, 조직이 소셜 미디어 플랫폼을 어떻게 모니터링하고 남용을 완화할 것인지 결정해야만 한다.

- 소셜 미디어 공격은 브랜드 이미지와 경제적 손실에 모두 영향을 줄 수 있다.
- 효과적인 방어는 교육 및 모든 것을 의심하고 모니터링하는 것이다.

Mobile Threats

당신이 어디로 가든, 공격자는 따라갑니다.



안드로이드 시장의 급격한 성장은 악성코드 제작자의 관심을 끌고 있다.

모바일 악성코드의 고도화는 데스크톱 악성코드에서 발견되는 수준이상으로 발전

모바일 운영체제(OS)의 파편화 문제

악성코드 제작자들은 보다 견고하고 위험한 악성코드 제작에 좀더 많은 노력을 투자하고 있다.

보고서의 주요 3가지 동향

Targeted Attacks
and Data Breaches

Social and Mobile

X-Force by the Numbers

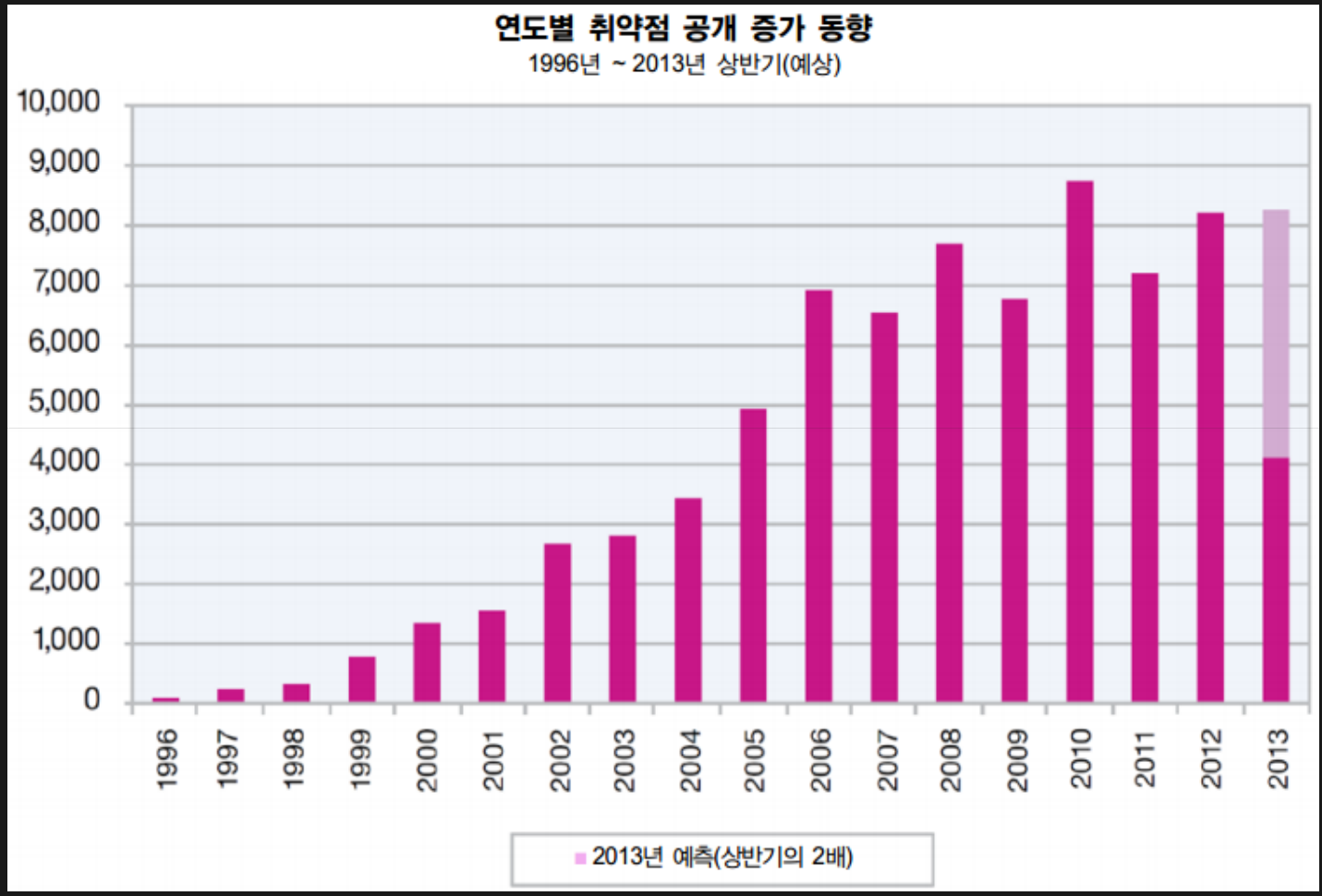
취약점공격
웹 동향
스팸과 피싱

취약점 공개

4,100

공개적으로 발표된 취약점 개수

이러한 경향이 유지된다면, 거의 2012년 수준과 동일

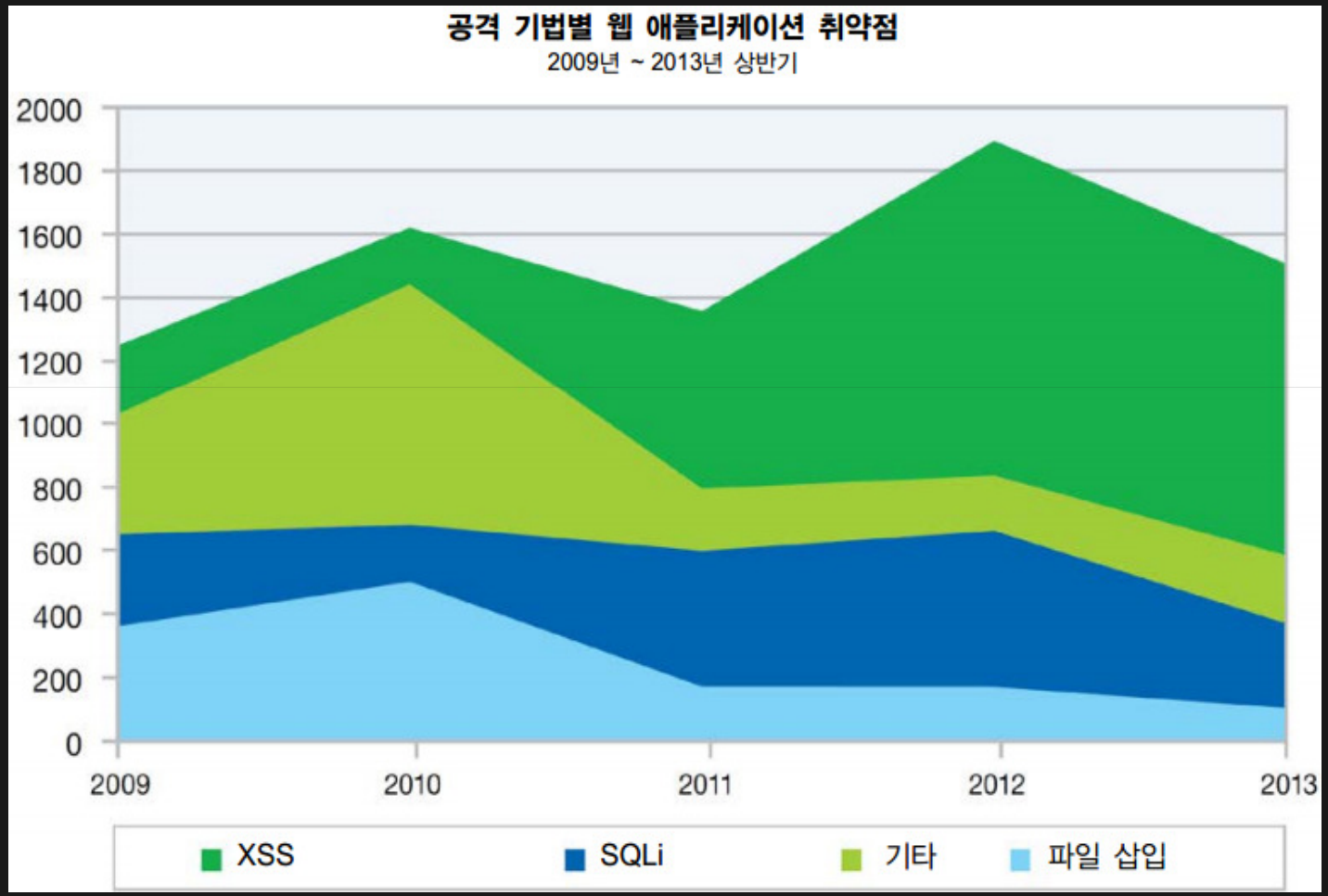


웹 어플리케이션 취약점

50%

모든 웹 어플리케이션의 취약점의 50%는 XSS

2012년과 비교하여 전체적으로 약간 줄어듦

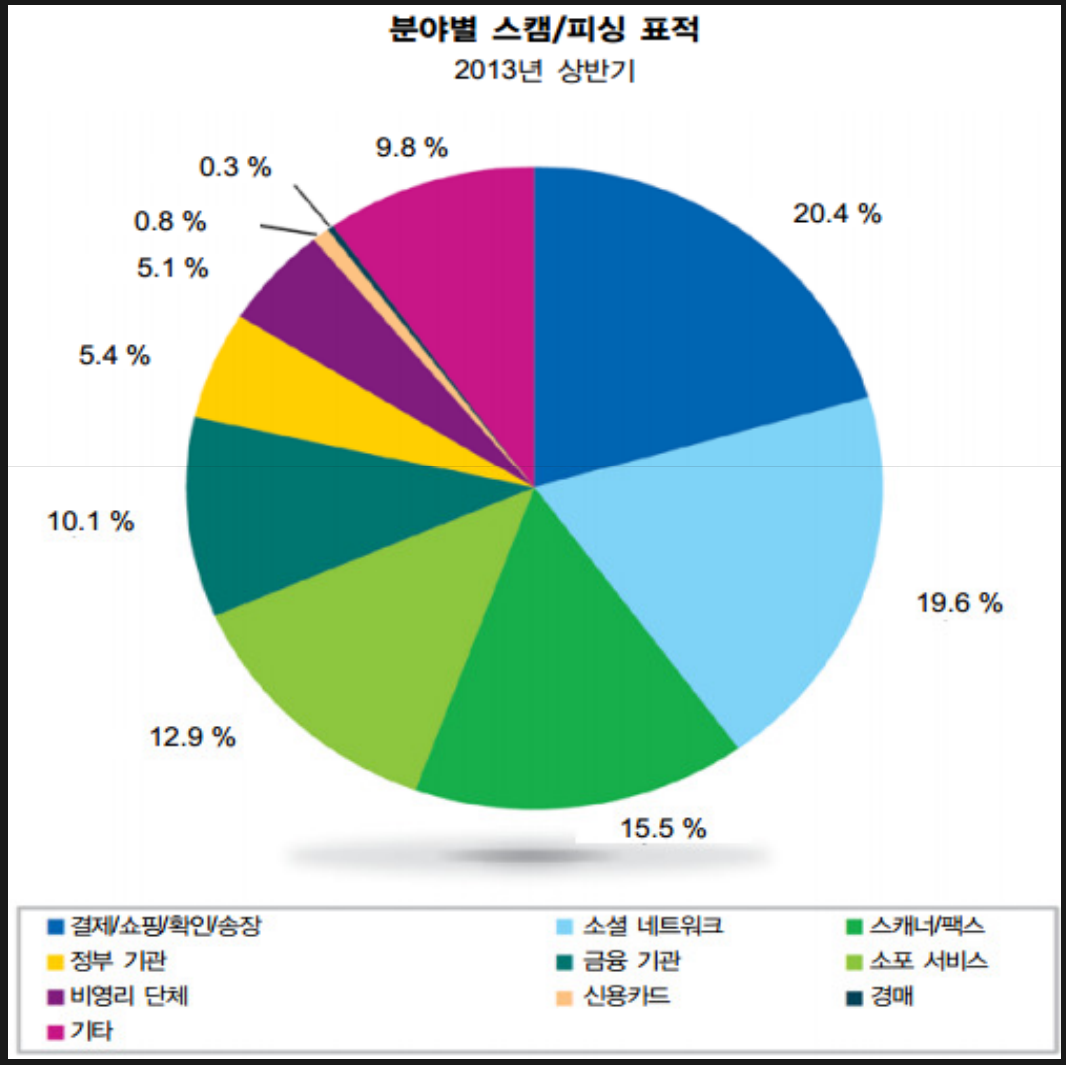


스캠과 피싱 표적

55%

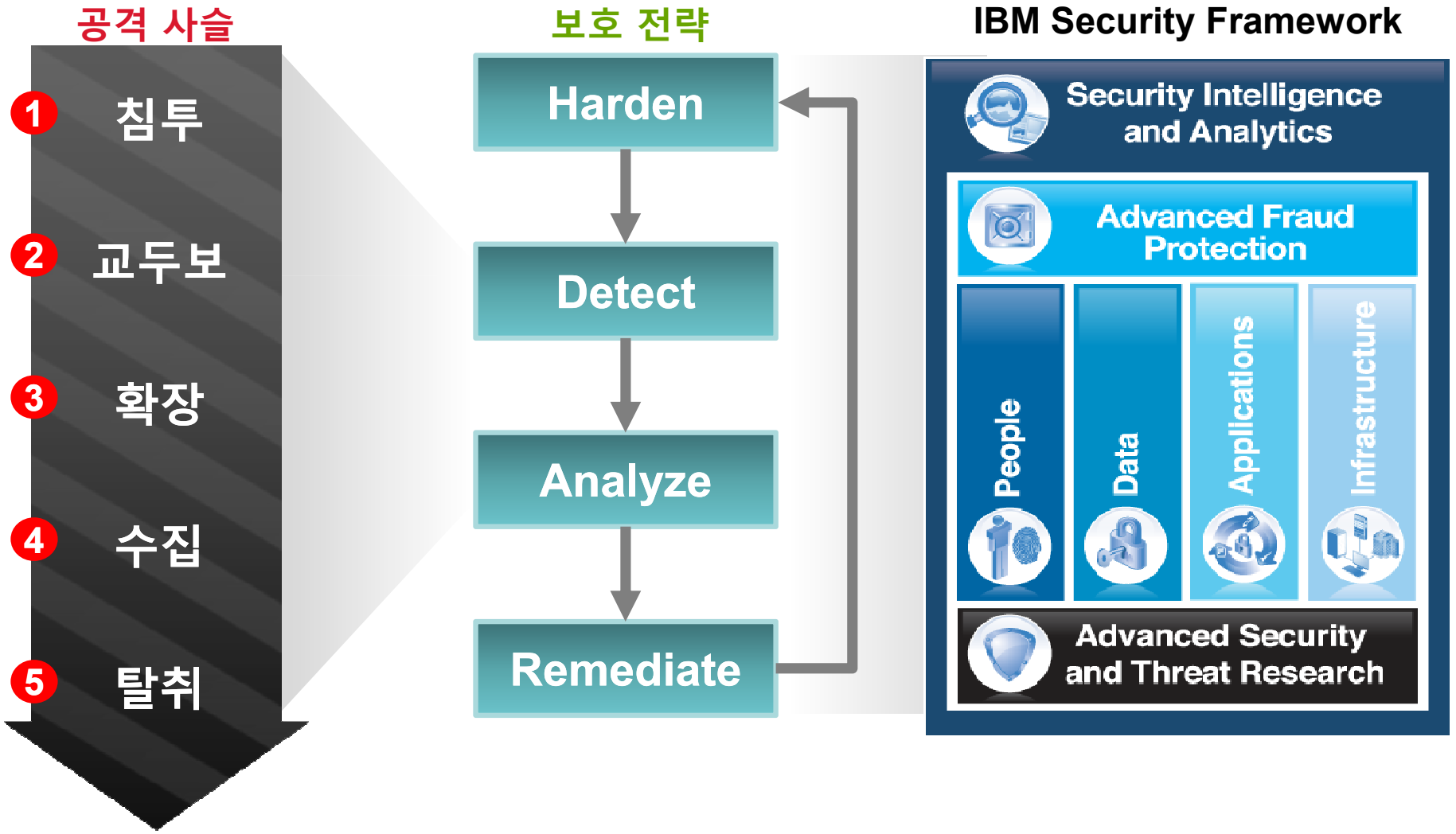
악의적인 링크와 첨부파일

- 결제/인터넷 쇼핑몰
- 소셜 네트워크
- 문서 스캐너/팩스



보호전략에 따른 동향 보고

보호전략은 상호작용 기반의 접근을 따라야 한다



Harden

What the X-Force Trend Report is telling us:

여전히 패치 관리의 문제점 지속됨	*"브라우저, 브라우저 플러그인의 취약점은 기업의 임직원 또는 일반 사용자에게 악성코드를 유포하는 가장 효과적인 방법*
웹 어플리케이션은 아킬레스건	*"2013년 상반기에 가장 일반적인 침해 공격은 SQL 인젝션(SQLi)으로 여전히 건재함"*
취약점이 여전히 증가하고 있는 추세	*"2013년 상반기, X-FORCE 연구소는 취약점 데이터베이스에 4,100개의 새로운 보고된 취약점 정보를 업데이트함"*

Harden

Example Best Practices:

1. 엔드포인트에 대한 적절한 구성 및 패치
2. 네트워크 구성을 모니터링하고 분석
3. 웹 어플리케이션에 대한 안전한 개발 및 감사
4. 특권 및 공유 계정 활동에 대한 통제
5. 인텔리전트한 취약점 스캔 및 우선순위화

Detect

What the X-Force Trend Report is telling us:

소셜미디가 신뢰를 오용하는데 사용됨	*"더 인간적이고 개인화된 소셜 공격은 분명한 관심과 현재 사건을 기반으로 조작될 수 있음"*
상반기 동안에 몇 개의 제로데이 공격 발생	*"상반기에 대중적으로 사용하는 소프트웨어에 영향을 주는 몇 개의 제로데이 공격이 출현함을 발견"*
데이터 탈취는 목표	*"2012년이 데이터 침해사고의 원년이었다면, 2013년은 2012년을 능가할 위치에 있다"*

Detect

Example Best Practices:

1. 소셜 미디어 및 웹 사용의 위험을 관리
2. Unknown, 제로데이 취약점에 대한 방어
3. 의심스러운 접근에 대한 데이터 활동 모니터링
4. 위협인지 기반의 계정 및 접근 정책

Analyze

What the X-Force Trend Report is telling us:

글로벌 가시성 유지	*"기업의 지사, 자회사를 목표로한 데이터 침해 사고가 증가, 또한 모기업에 비해 덜 안전한 해외 지사 웹사이트에 대한 공격 증가"*
심지어 ADVANCED USERS조차 취약	*"신뢰할 수 있는 중앙 사이트를 공격하여, 악성코드를 심음으로 공격자는 더 기술적 지식을 지닌 사용자에게 도달할 수 있음"*
분산된 관심에서 미묘함을 찾아라	*"DDoS공격은 관심을 분산시키는데 사용되고 공격자가 기업내의 다른 시스템을 침해하도록 허용함"*

Analyze

Example Best Practices:

1. 전사적, 통합적 IT 보안의 접근방식
2. 알려지지 않은 위협과 보편적이지 않은 행위 분석

Remediate

What the X-Force Trend Report is telling us:

글로벌 브랜드 이미지에 빠르게 영향 받을 수 있음	*운영관점에서 최신 공격은 기업의 좋은 브랜드 이미지를 퇴색 시킴. "고객 데이터가 유출"되었다면 법적 이슈를 만들 수 있고 브랜드 명성에 영향을 줄 수 있음*
진화하는 기술에 대한 계획	*"공격자는 기술적으로 더 위험하고, 복원력을 가진 최신 모바일 악성코드에 투자 중"*

Remediate

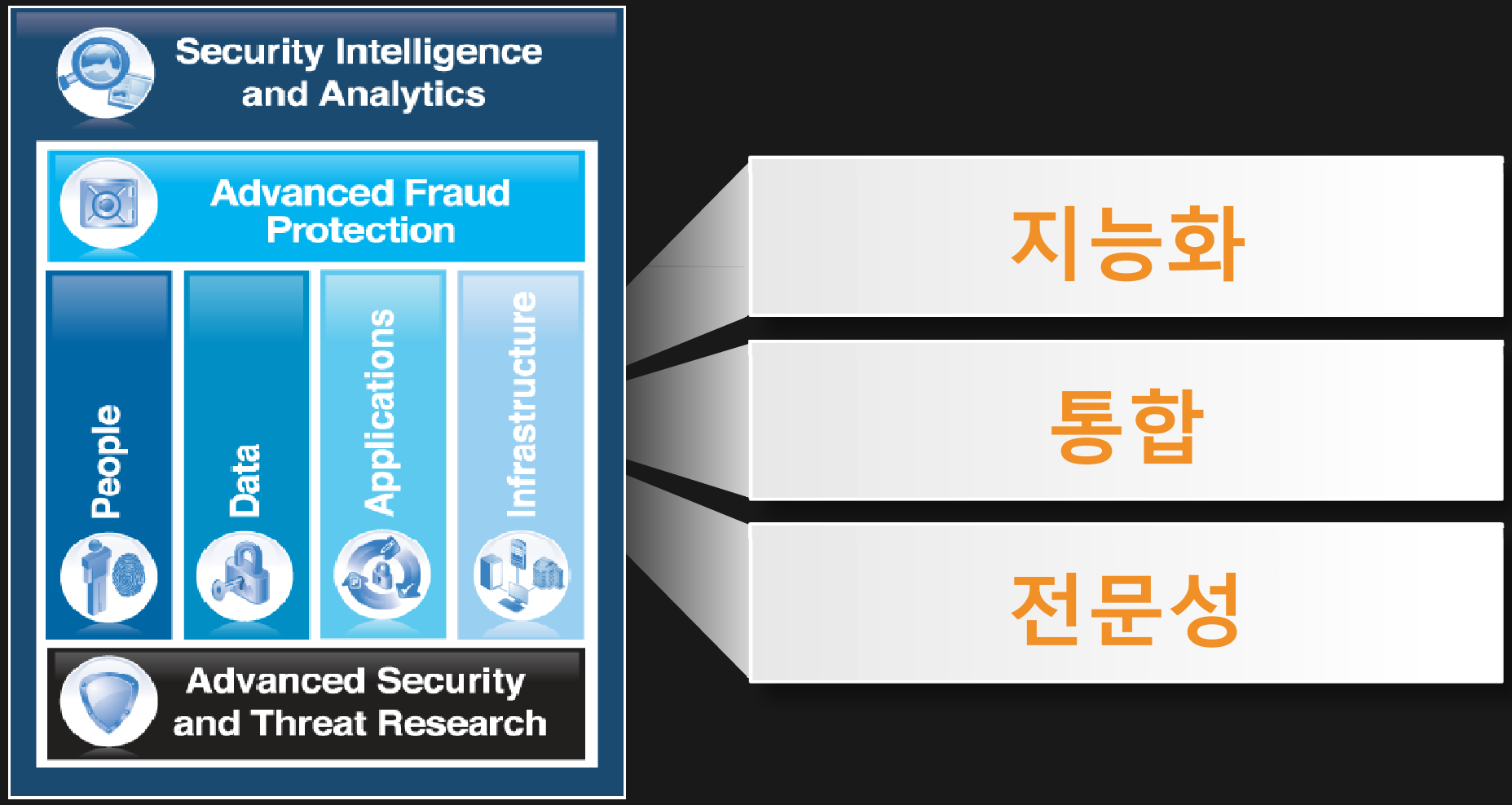
Example Best Practices:

1. 침해사고 발견 시 실행 가능한 절차 및 계획 수립

2. 빠르게 조치 가능한 그리고 더욱 강화된 보안 환경을 조성할 수 있는 보안 투자

지능화,통합,전문성에 기반한 IBM 보안 프레임워크

IBM 보안 프레임워크




IBM