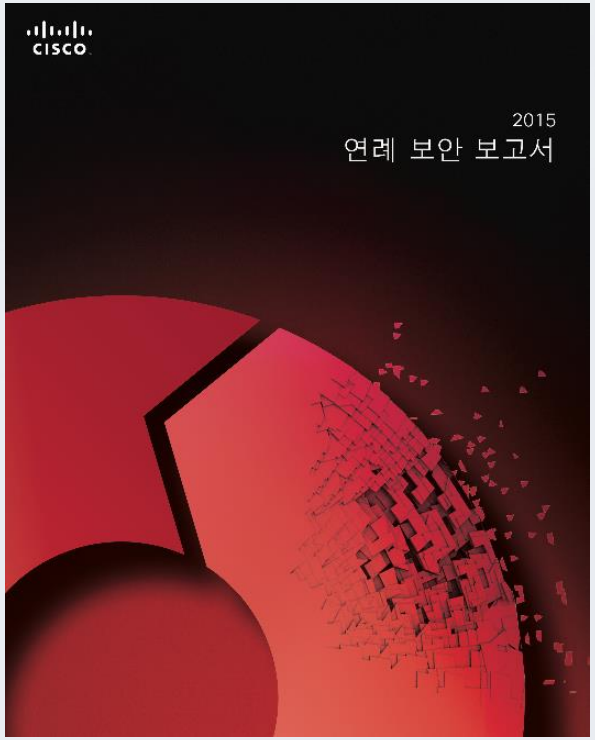
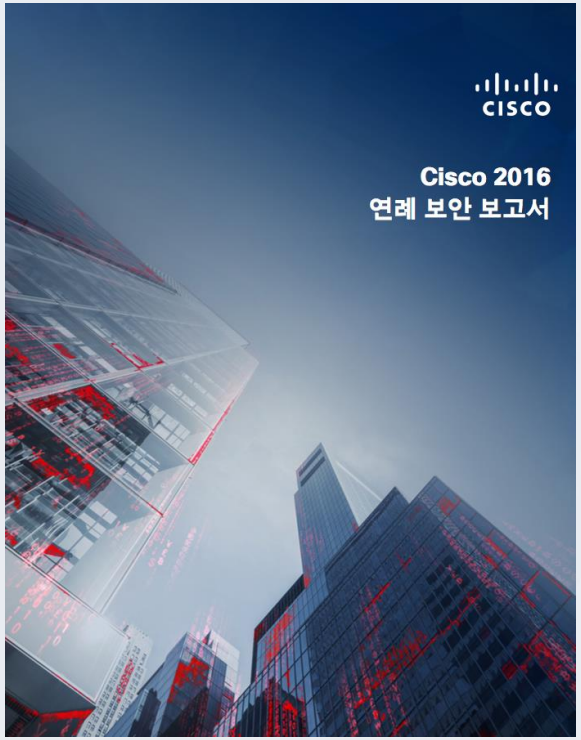
2017 시스코 사이버 중기 보안 보고서를 통해 본 위협 전망

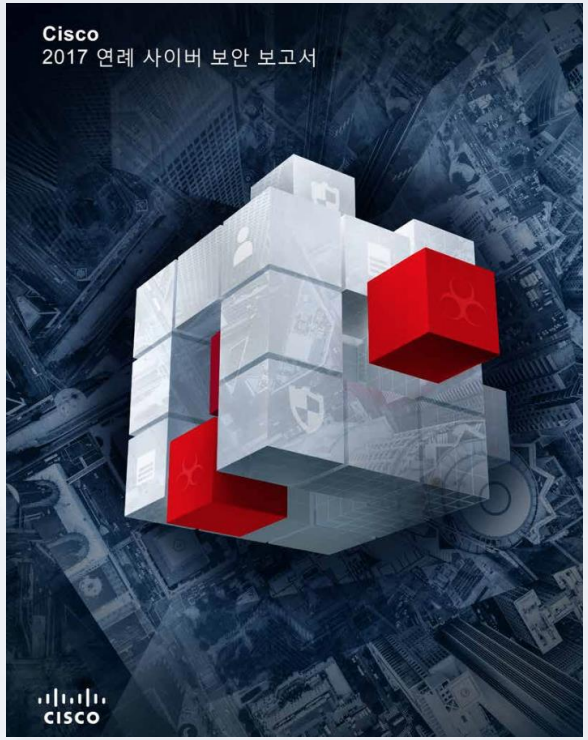
정관진 부장
GSSO APJ Security

2017년 10월 12일

보안 위협 트랜드를 한눈에 파악하는 위협 보고서





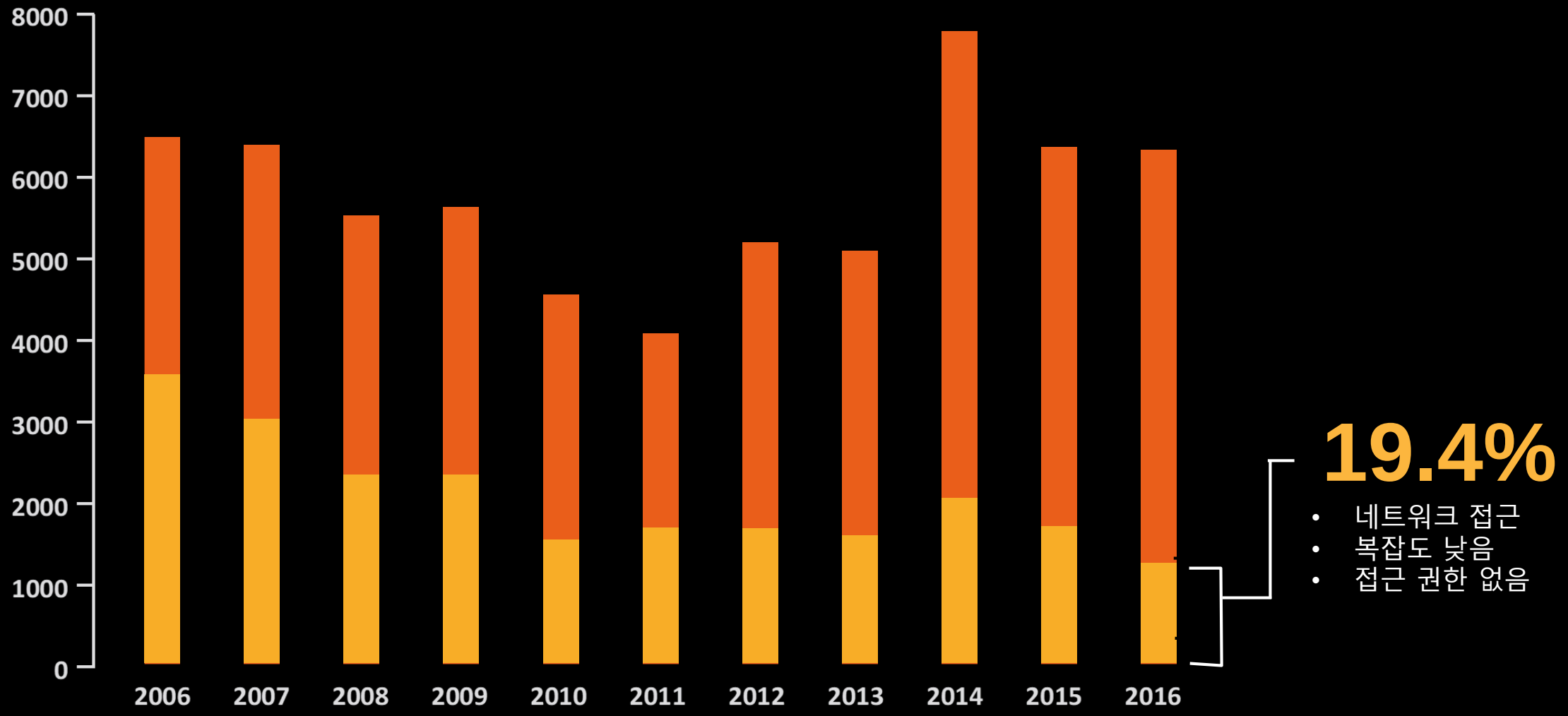


매년 2회 (년간, 중기) 보고서를 통해 보안 위협 동향 요약 및 향후 발전 방향등을 예측해 봄

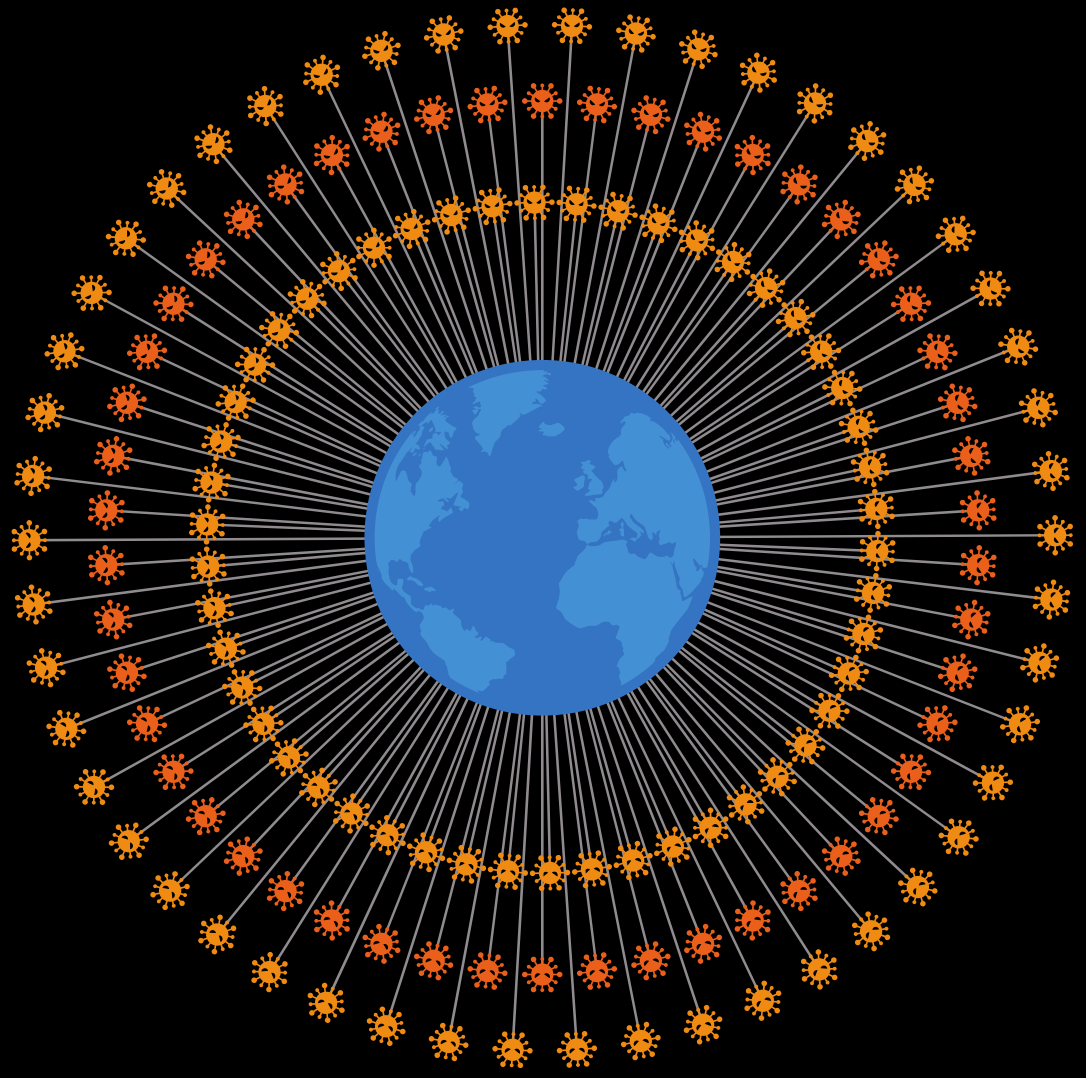
2017 MCR 의 주요 내용

- 익스플로잇 키트 감소, DDoS, 이메일, 랜섬웨어 증가(DDoS, 이메일, 랜섬웨어가 최대 난제로 대두)
  - DDoS: 규모와 공격 위협 증가
  - 이메일: 비즈니스 이메일의 악성 첨부 파일로 침해
  - 랜섬웨어: 진화 – 랜섬웨어화된 사물 인터넷(IoT), RasS(Ransomware-as-a-Service), 랜섬웨어 DDoS
- 취약점(워너크라이 – WannaCry 문제 발생, 인터넷 연결 DevOp 서버까지 가세)
- 사물 인터넷(IoT) 보안 위험
- 업종별 IT/OT 통합 문제 대두
- 간소화, 개방성, 자동화가 더욱 요구됨

현재의 위협 상황 – 취약점


8000
7000
6000
5000
4000
3000
2000
1000
0
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
19.4%
네트워크 접근
복잡도 낮음
접근 권한 없음

현재의 위협 상황 – 악성코드

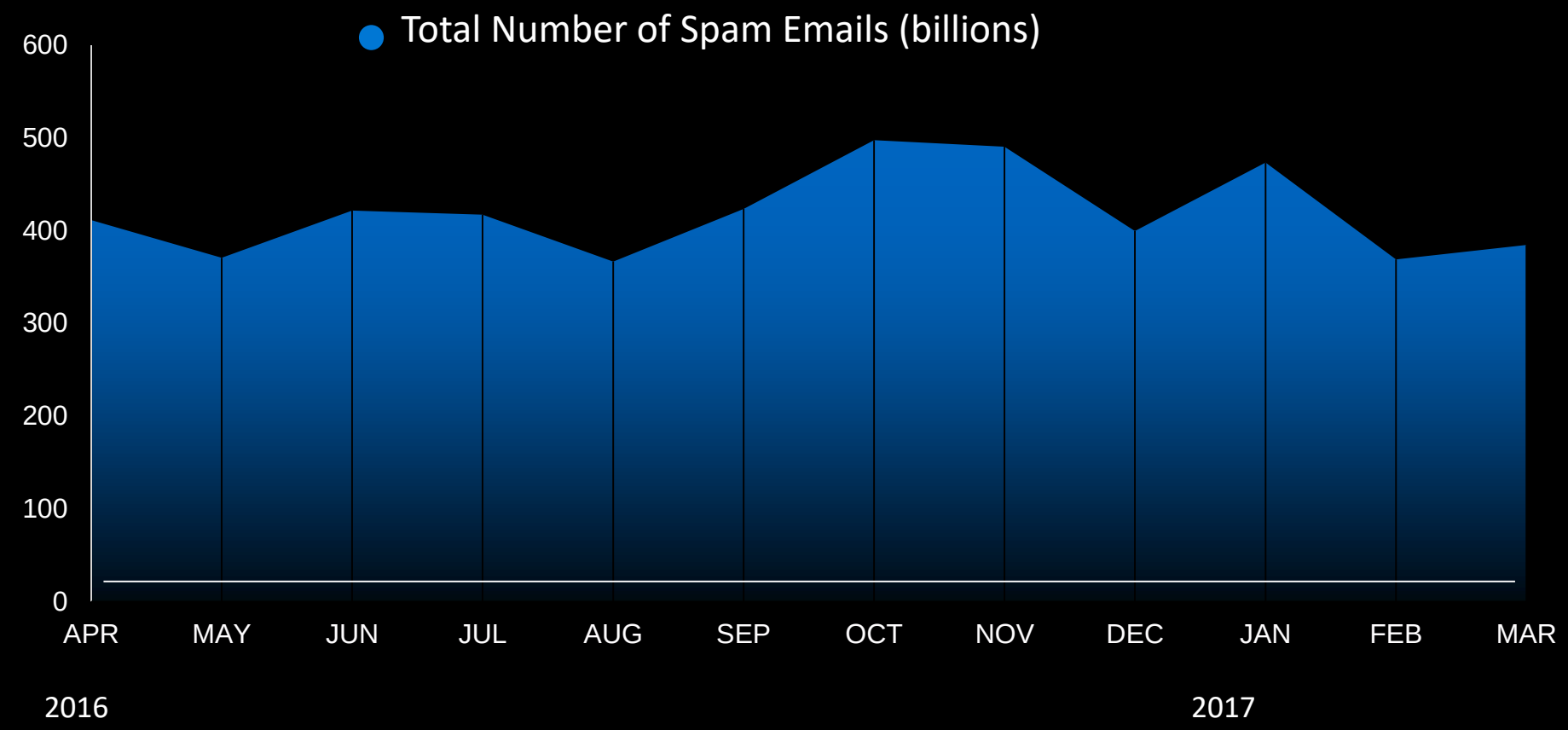


= 10,000

150 만개

매일 악성코드 샘플

현재의 위협 상황 – 스팸


Total Number of Spam Emails (billions)
600
500
400
300
200
100
0
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
JAN
FEB
MAR
2016
2017

현재의 위협 상황

사람을 공격하는 것이 소프트웨어 취약점을
이용하는 것보다 더욱 비용 효율적임

현재의 위협 상황

197 억건

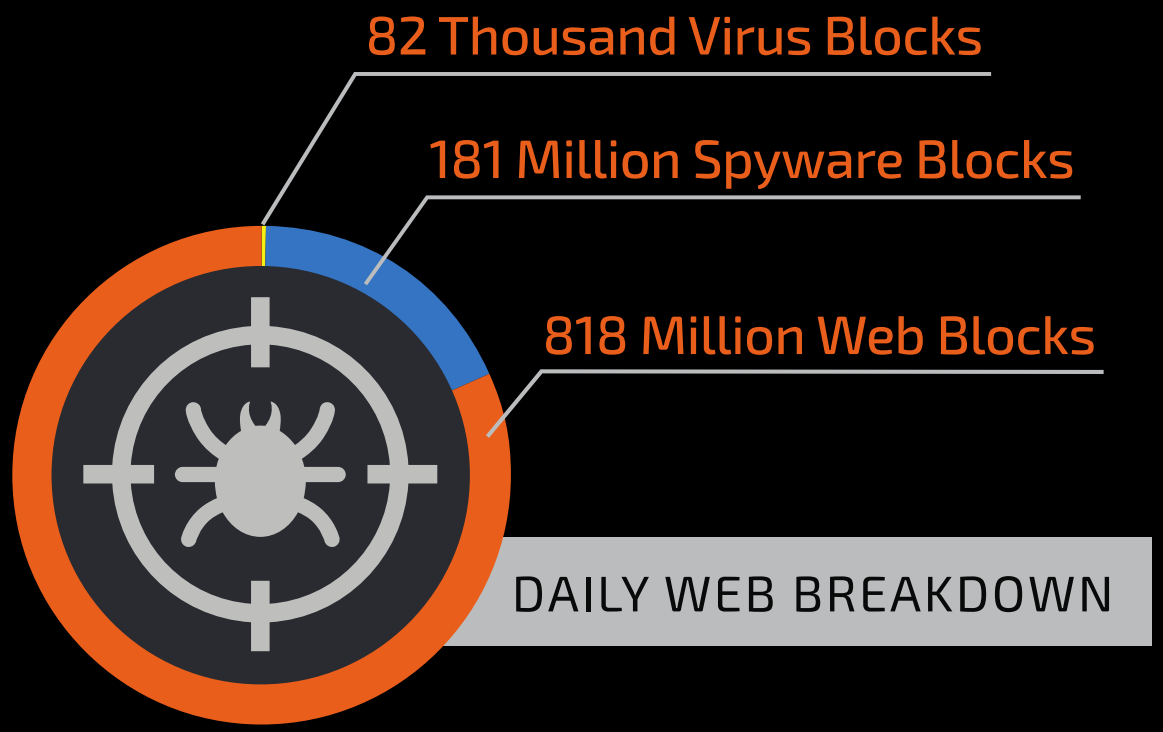
TOTAL THREAT BLOCKS

DAILY

=

72 조

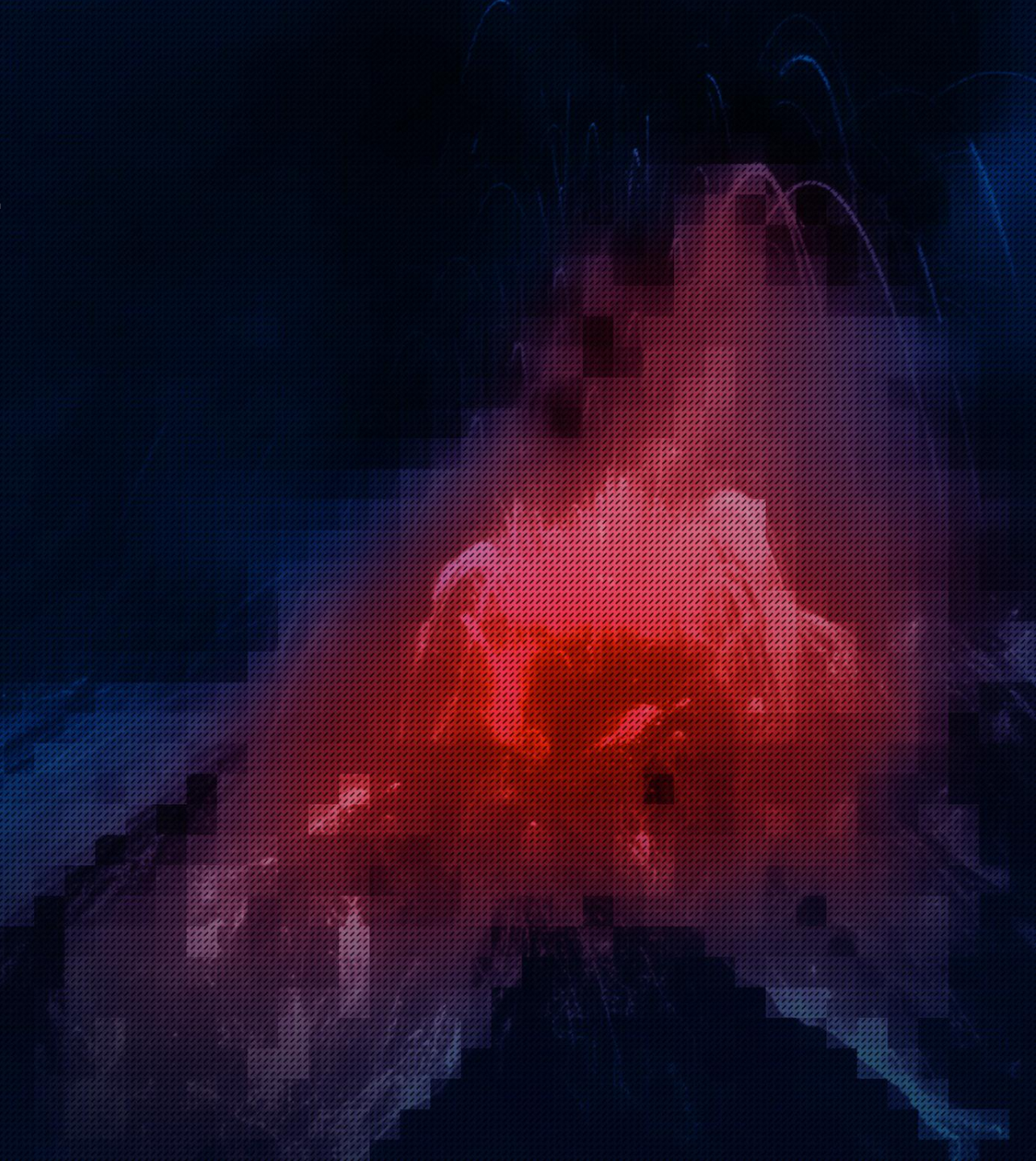
YEARLY



영향력 증가

기술 및 규모에 의해 압도

- 기술 발전으로 인해 엔터프라이즈에서 방어해야 하는 보안 경계 확장 및 침해
- 악의적인 행위자는 계속 증가하는 공격 표면(취약점)을 이용
- 보안 팀의 부족한 리소스로 최근 지능적이고 점점 더 강력해지는 사이버 위협을 해결하기 위한 노력 필요



현재 위협을 해결하기 위해 무엇이 필요할까요?

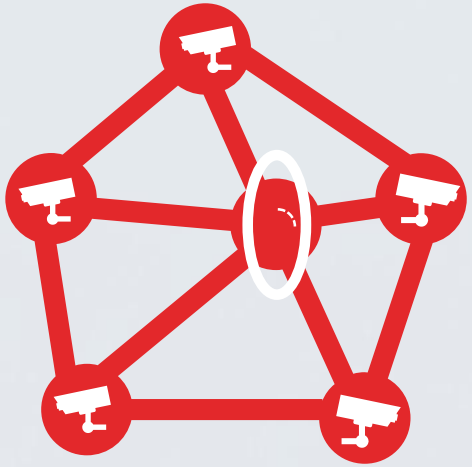
공격에 대한 이해

cisco

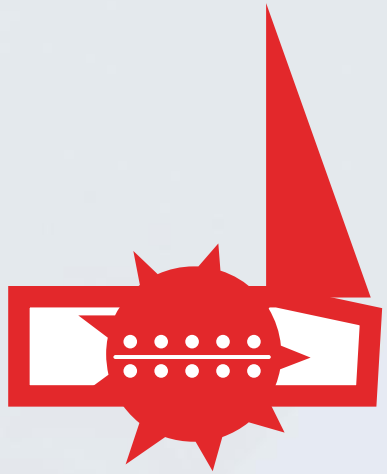
익스플로잇 키트 사용 감소

공격자가 다른 공격에 주력

익스플로잇 키트



DDoS



이메일

랜섬웨어

익스플로잇 키트

DDoS

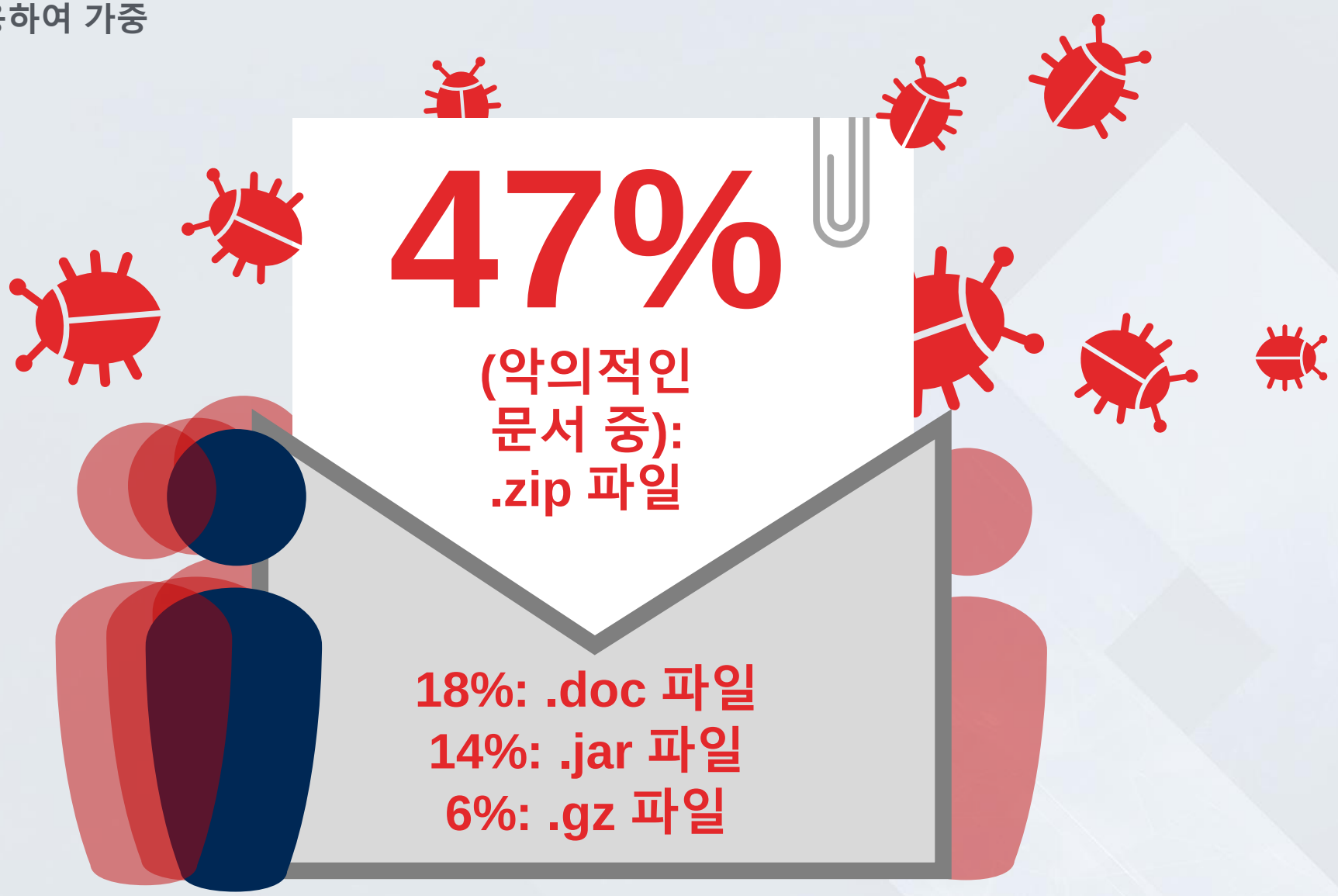
봇넷이 사물 인터넷(IoT) 제어를 위해 경쟁 및 정상적인 인터넷 운영 방해

- 사물 인터넷(IoT) DDoS 공격으로 인해 1TBps DDoS 현실화
- 1시간 내에 설정 완료 가능
- 신속한 배포 공격자가 24시간 내에 10만 개 이상의 감염된 디바이스 봇넷 구축 가능
- 악성코드의 낮은 탐지율. 악성코드가 디바이스의 메모리에 상주하고 디바이스를 다시 시작하면 초기화되므로 샘플 검색이 어려움

출처: Radware

악의적인 이메일

악의적인 문서를 사용하여 가중



비즈니스 이메일 침해

랜섬웨어보다 문제가 커질 수 있음

랜섬웨어

비즈니스 이메일 침해

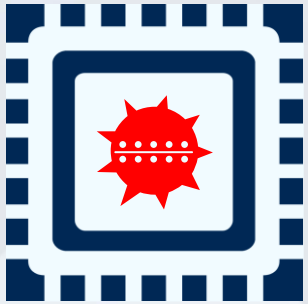
출처: Flashpoint

새롭게 등장하는 악성코드 전술

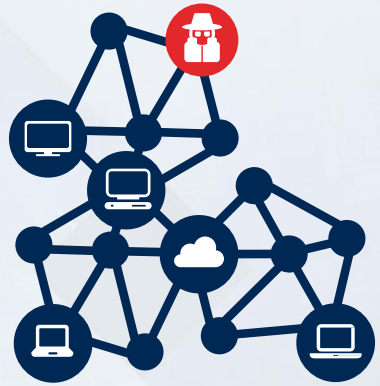
새로운 전술을 통해 악성코드가 계속 진화함

사용자 클릭이 활성화에 이용됨

RaaS(Ransomware-as-a-Service) 증가



파일을 이용하지 않는 악성코드가 대세임



익명의 분산된 인프라가 C&C에 사용됨

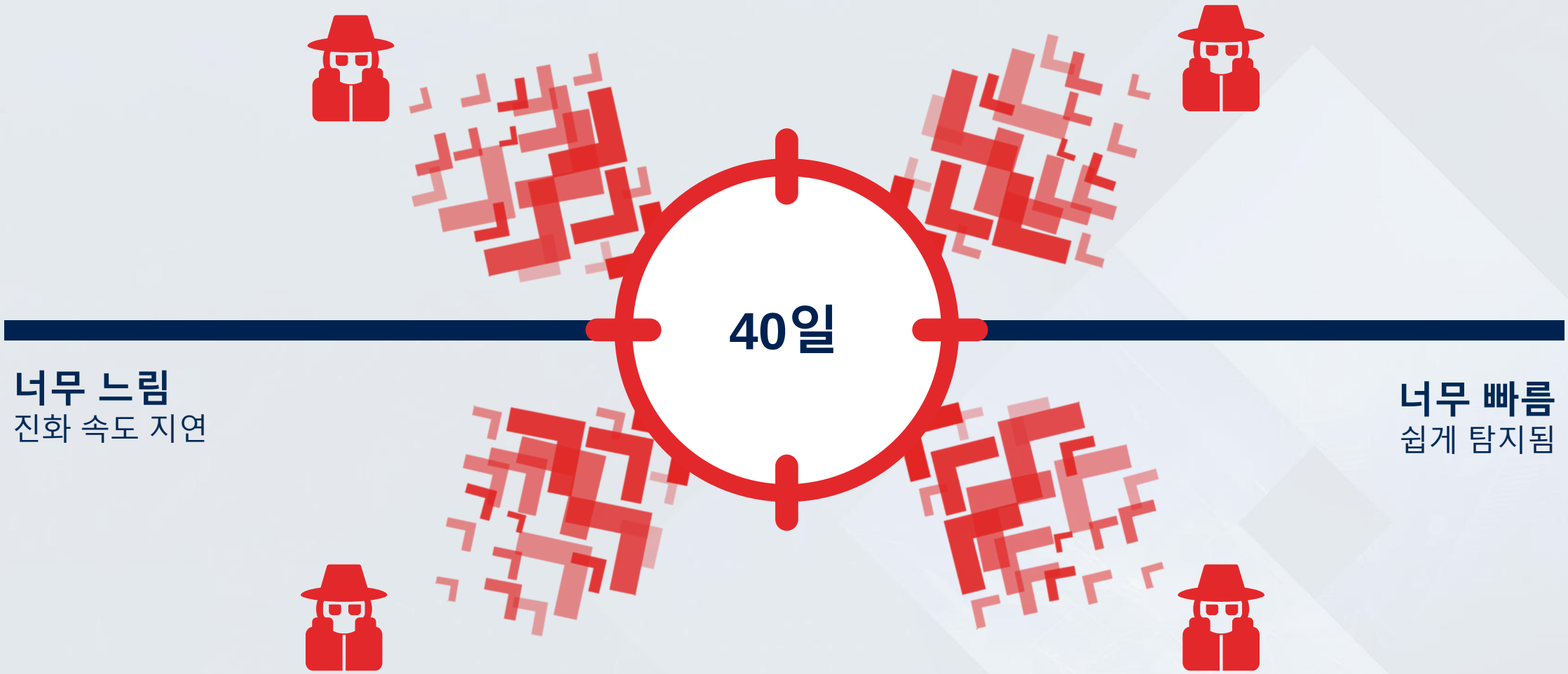
스파이웨어를 애드웨어로 위장

분류되지 않은 스파이웨어를 통해 조직 깊숙히 침투

- **Hola VPN:** 가장 범위가 넓음 - 표본 기업 중 60% 이상에 영향을 미침
- **RelevantKnowledge:** 직접적인 사용자 동의 없이 대량의 정보 수집
- **DNS Unlocker:** 표본 기업의 월간 스파이웨어 감염 40% 이상 차지

도메인 생성 알고리즘

공격자가 DGA의 수명을 늘려 탐지 회피 능력 극대화



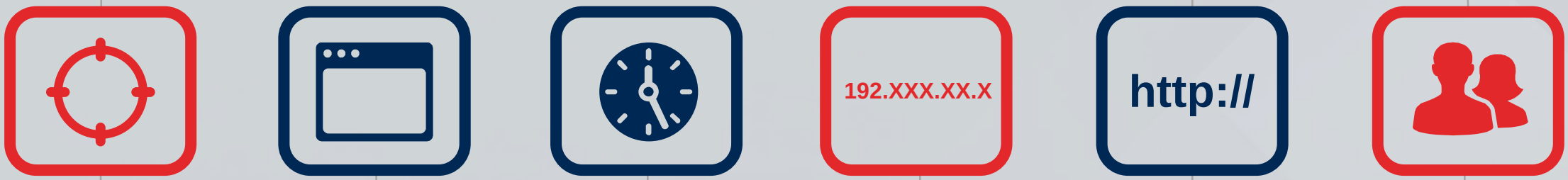
출처: Anomali

인프라 분석을 통한 위협 추적

필요한 입력: 도메인 또는 하위 도메인

공동 도메인

등록자 도메인



1단계

입력 도메인의 생성 날짜 및 등록자 파악

2단계

생성 날짜(도메인 등록) 직후 도메인을 호스팅하는 IP 주소 및 해당 호스팅 기간 파악

3단계

입력 도메인과 동일한 기간 동안 n개 이하의 도메인을 호스팅한 IP 주소 파악

4단계

해당 IP 주소 중 싱크홀 또는 공용 인프라가 아닌 IP 주소 파악

5단계

지정된 도메인과 동일한 기간 동안 해당 IP에서 호스팅된 다른 도메인 파악

6단계

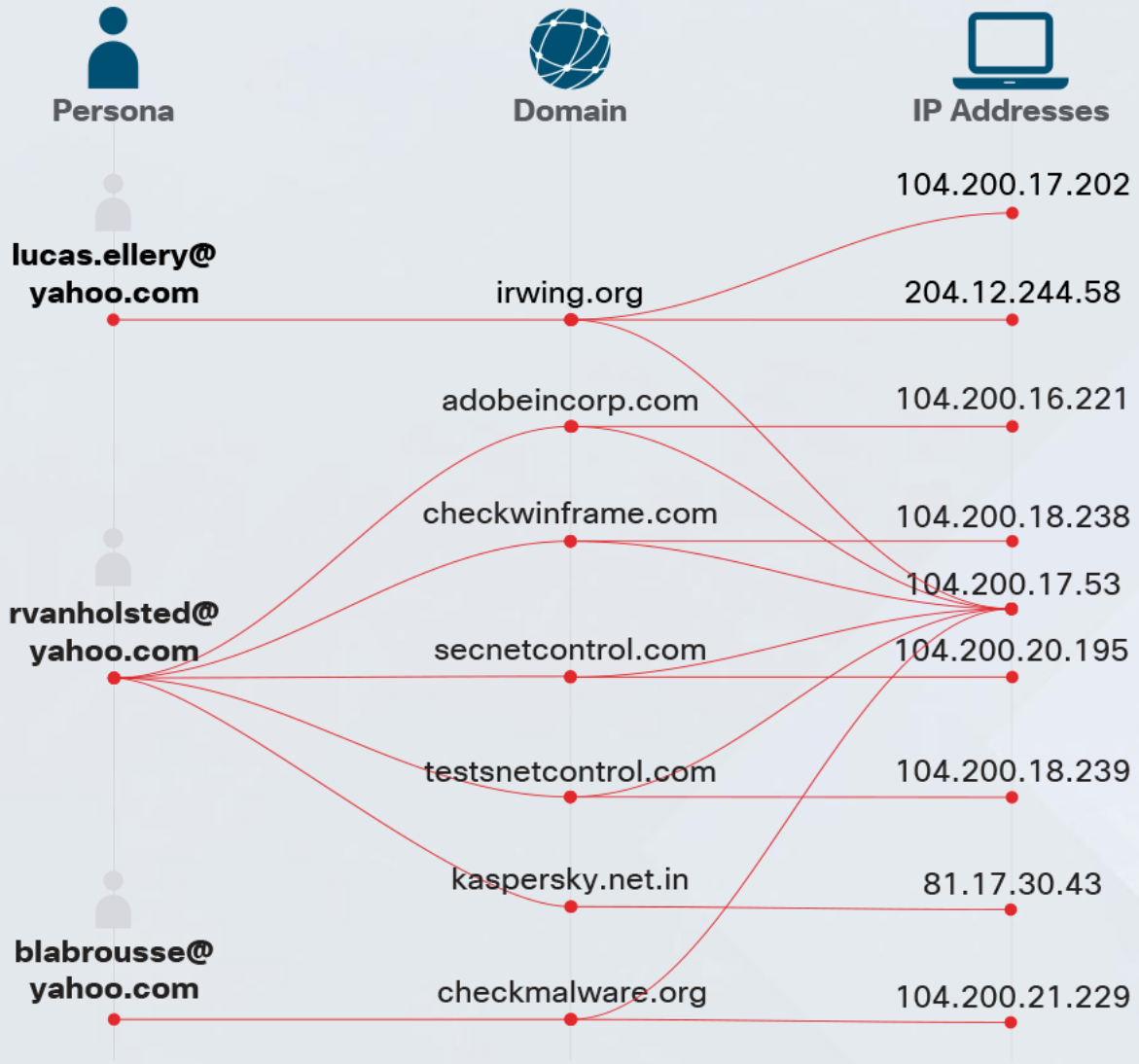
입력 도메인과 공동 도메인의 등록자 파악

CISCO

WHOIS 패시브 DNS

출처: ThreatConnect

인프라 분석을 통한 위협 추적 – 사례



- 위협과 관련이 있거나 의심스러워 보이는 이메일주소, IP 주소, 도메인 그룹 기반 추적
- 좌측의 Case 는 (Fancy Bear APT) Bellingcat 에서 제보한 이메일 헤더를 통해 6개의 도메인,5개의 IP주소, 3개의 이메일 등록자 파악
- 최종적으로 32개 이메일 주소, 180개 이상의 도메인, 50개 이상의 IP 주소 파악

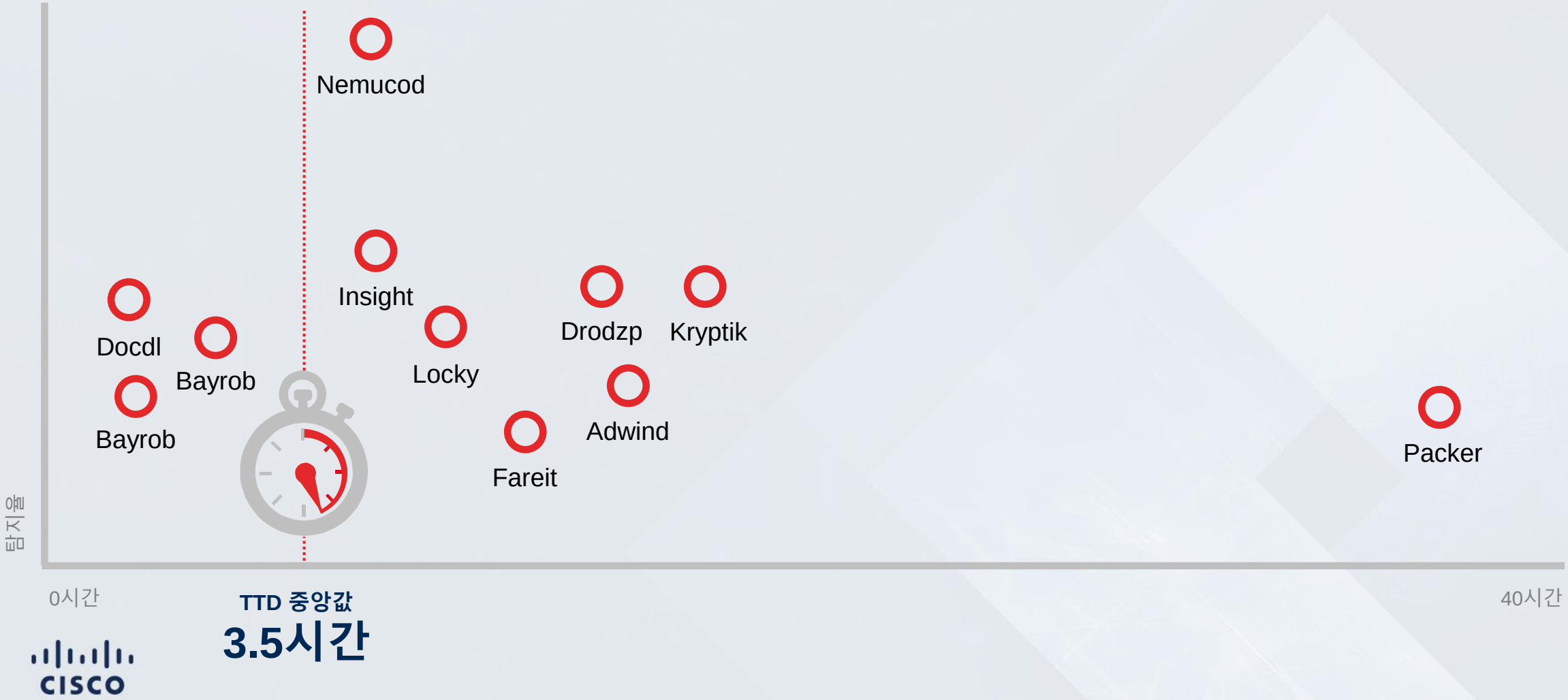
출처: ThreatConnect

새롭게 등장하는 랜섬웨어 전술

- 랜섬웨어 코드베이스 활용
- RDoS(Ransom Denial of Service, 랜섬 서비스 거부)
- RaaS(Ransomware-as-a-Service) 플랫폼이 빠르게 증가

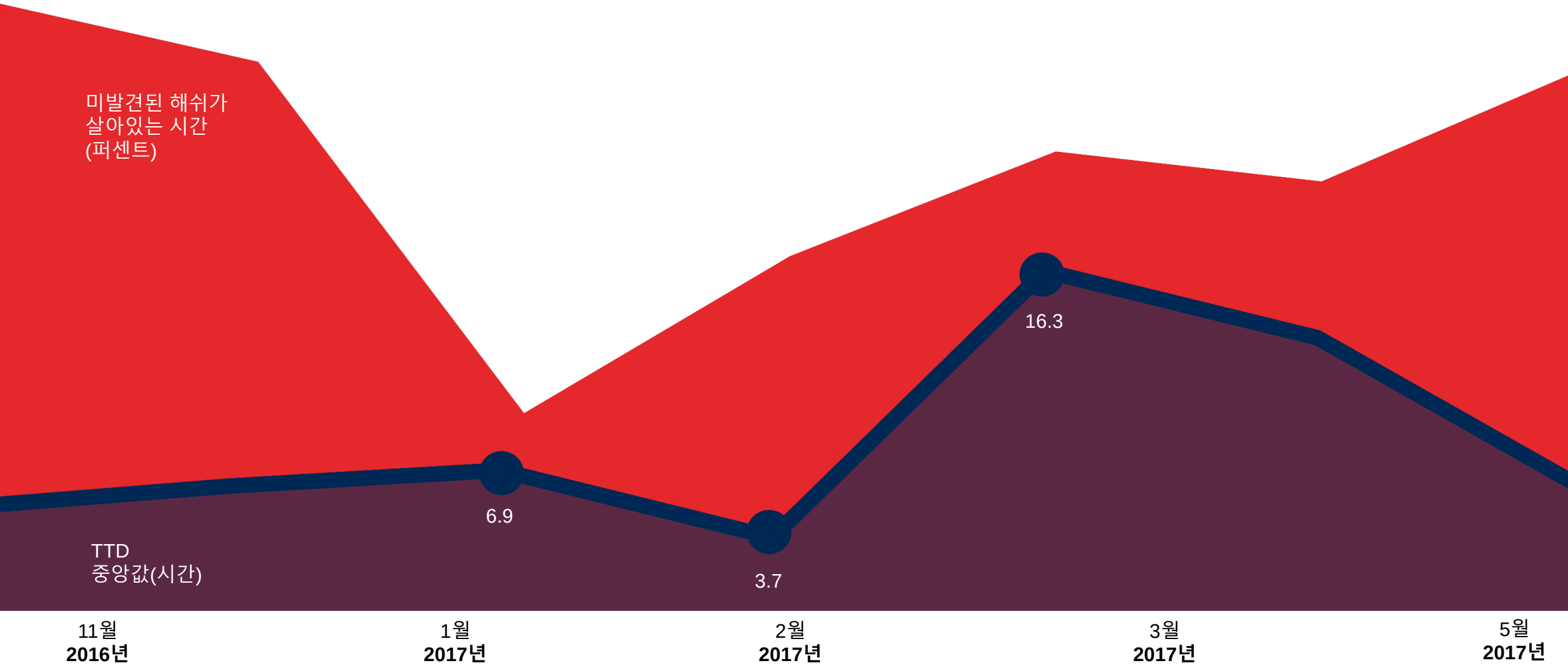
TTD(Time To Detection) 감소

탐지시간 중앙값이 2016년 10월부터 2017년 5월까지 3.5시간으로 단축



TTE: 새로운 조사 결과(Nemucod)

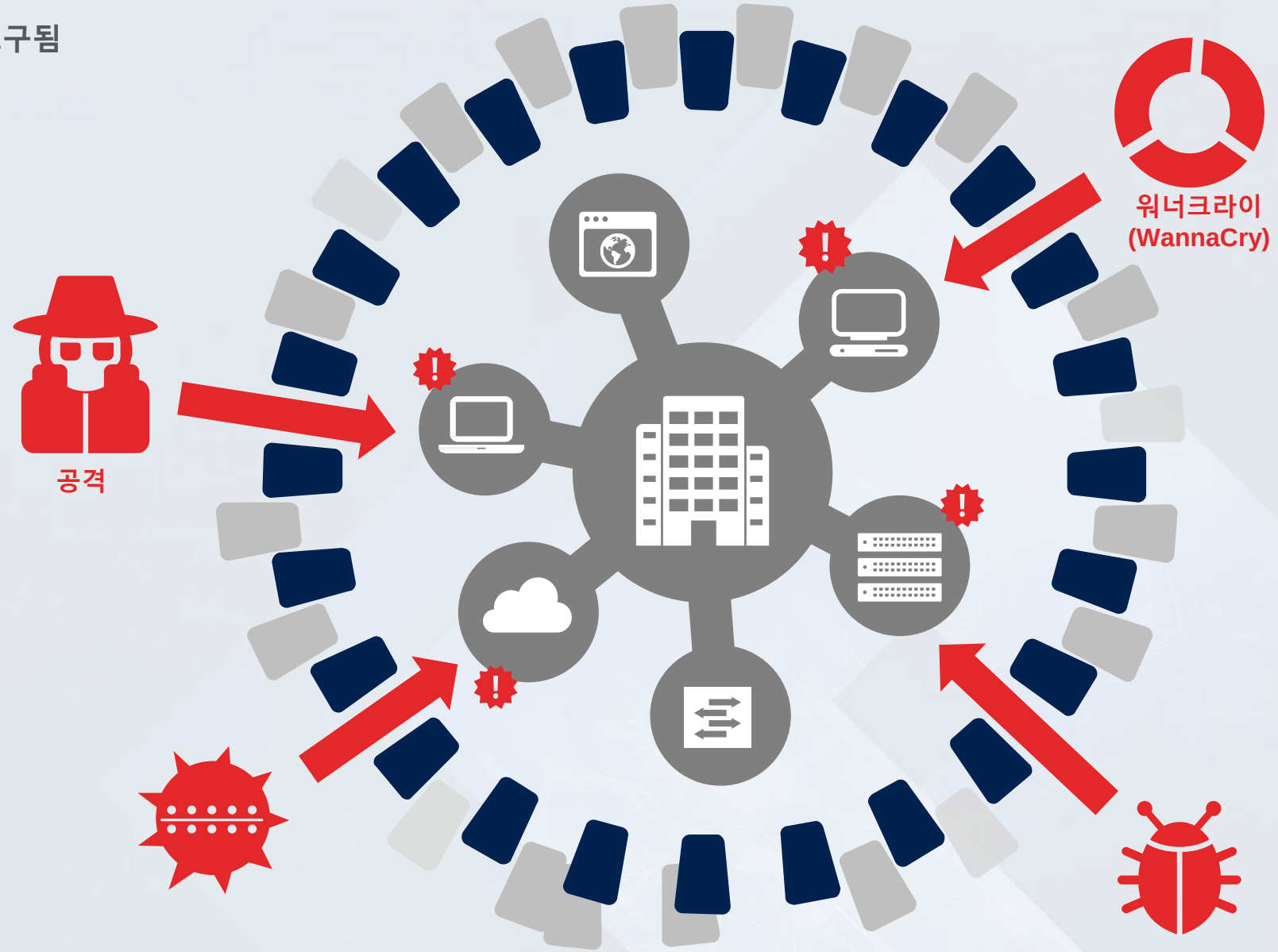
악성코드 탐지 속도가 빨라질수록 진화 속도도 빨라짐



취약점

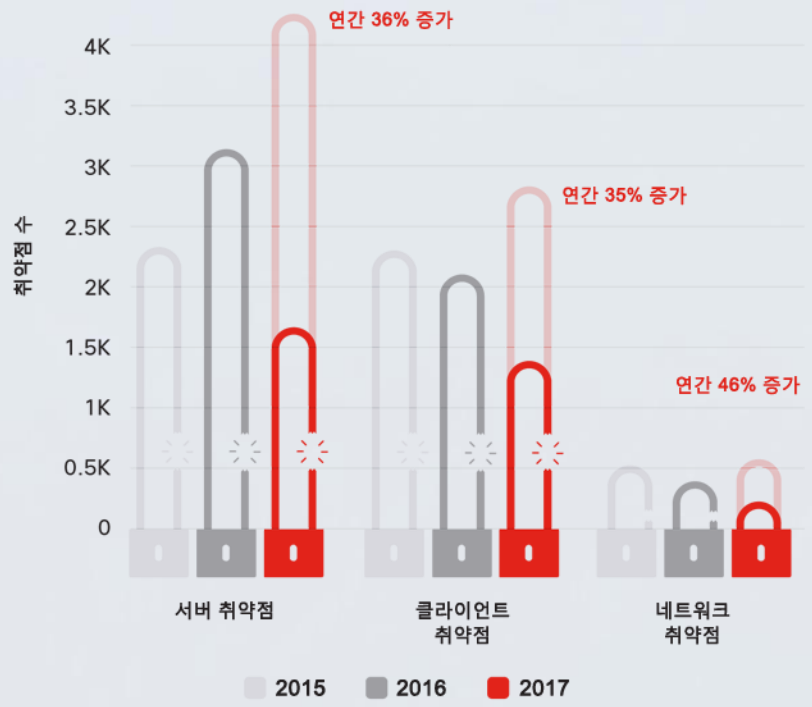
위험을 최소화 하려면 관련자 모두의 주의가 요구됨

- 벤더는 사이버 범죄와의 전쟁에서 리더가 될 수 있음
- 경영진에서 사이버 보안을 최우선 과제로 선정해야 함
- 벤더는 공격자가 계속해서 익스플로잇을 만들어 갈 것이라는 사실을 인정해야 함



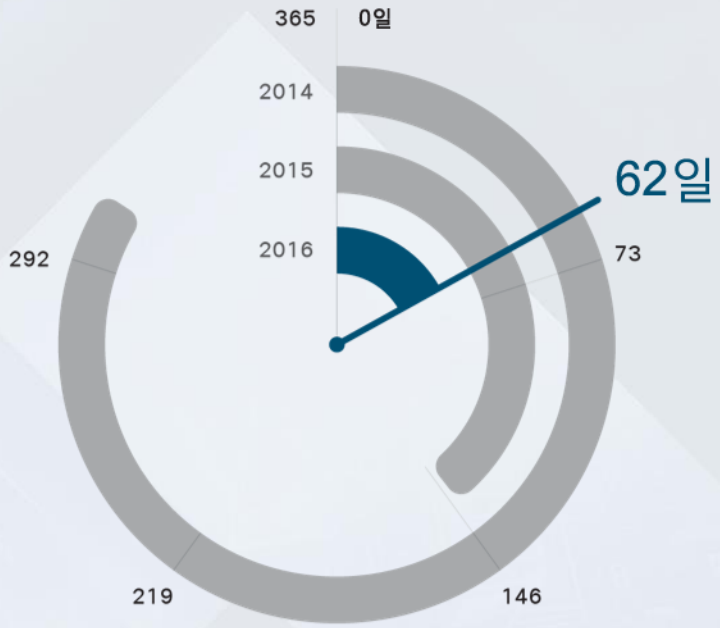
취약점

취약점이 빠르게 증가하여 방어하기 어려움



상위 취약점

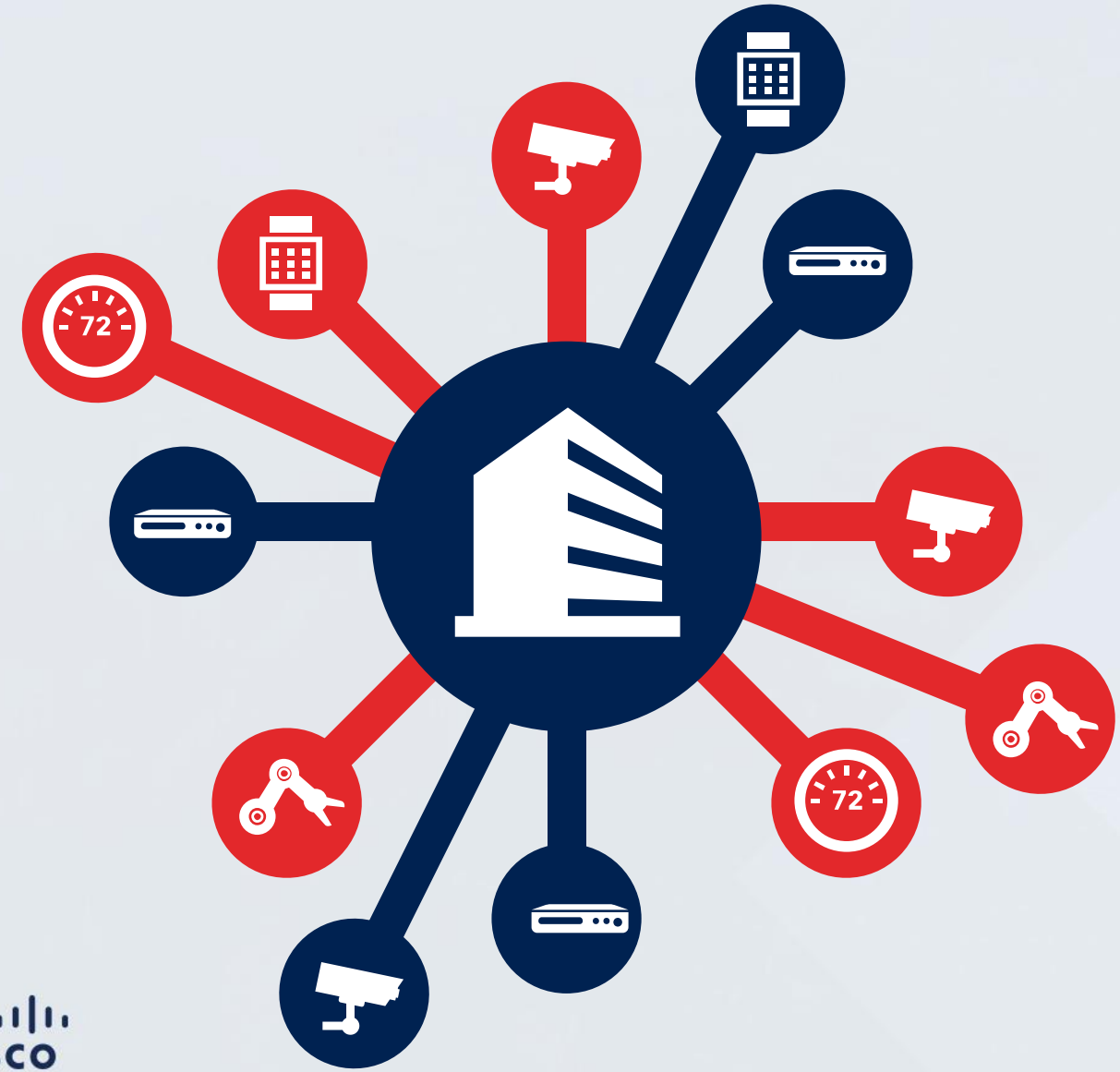
상위 위협 카테고리



플래시 취약점 중 80%를 패치하는 데 필요한 기간(일)

플래시 취약점 출처: Qualys

사물 인터넷(IoT)

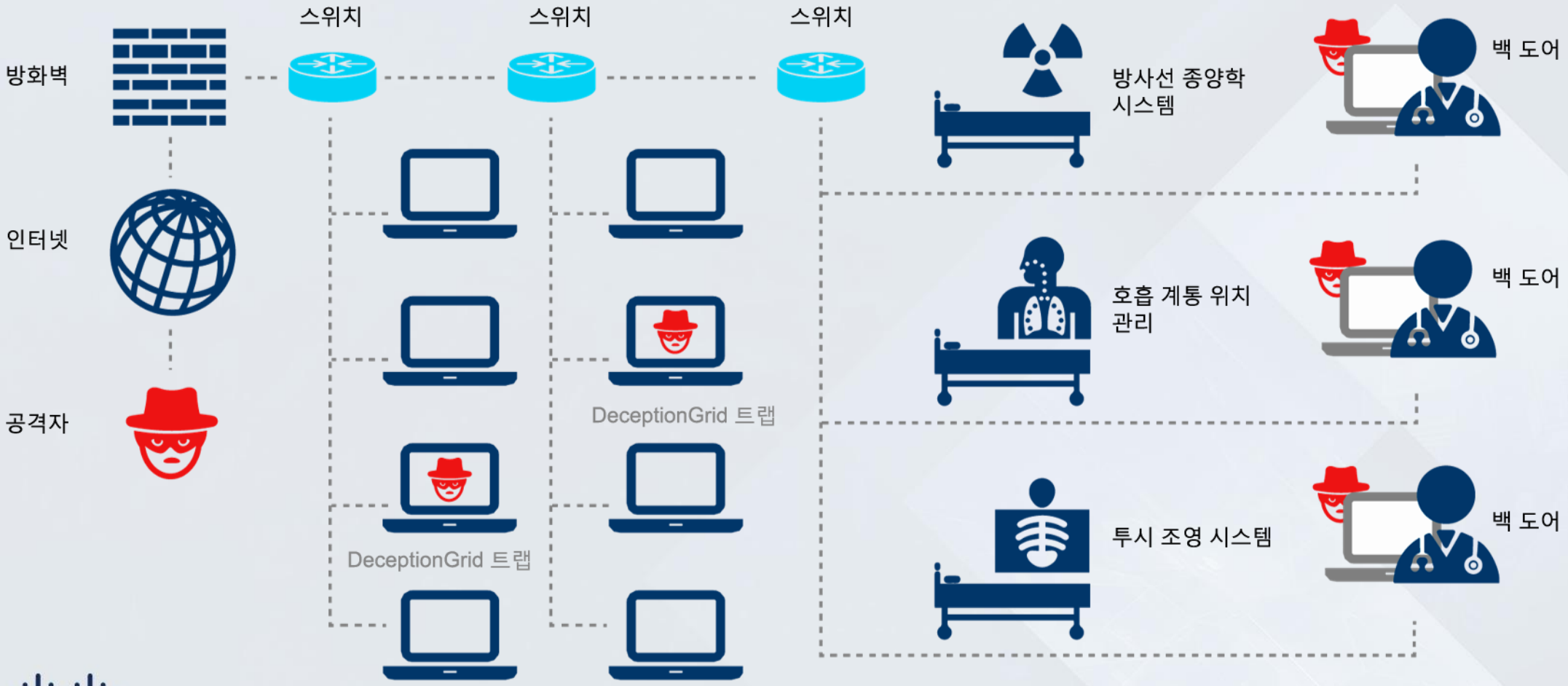


- IT에서 OT로 이동
- 가시성 문제
- 손쉬운 공격 대상
- 데스크톱 보안보다 훨씬 뒤처짐
- 안전하지 않은 애플리케이션 실행

cisco

공격의 측면 확산

취약한 보안 방식에 의해 조직과 환자가 위험에 노출됨



출처: TrapX

방어자

다이나믹 네트워크 가시성

40%

알 수 없거나 관리되지 않는
디바이스가 네트워크에서 누락됨

다음 영역의 강화 필요:

상황화(Contextualization)
통합
전문 지식

출처: Lumeta

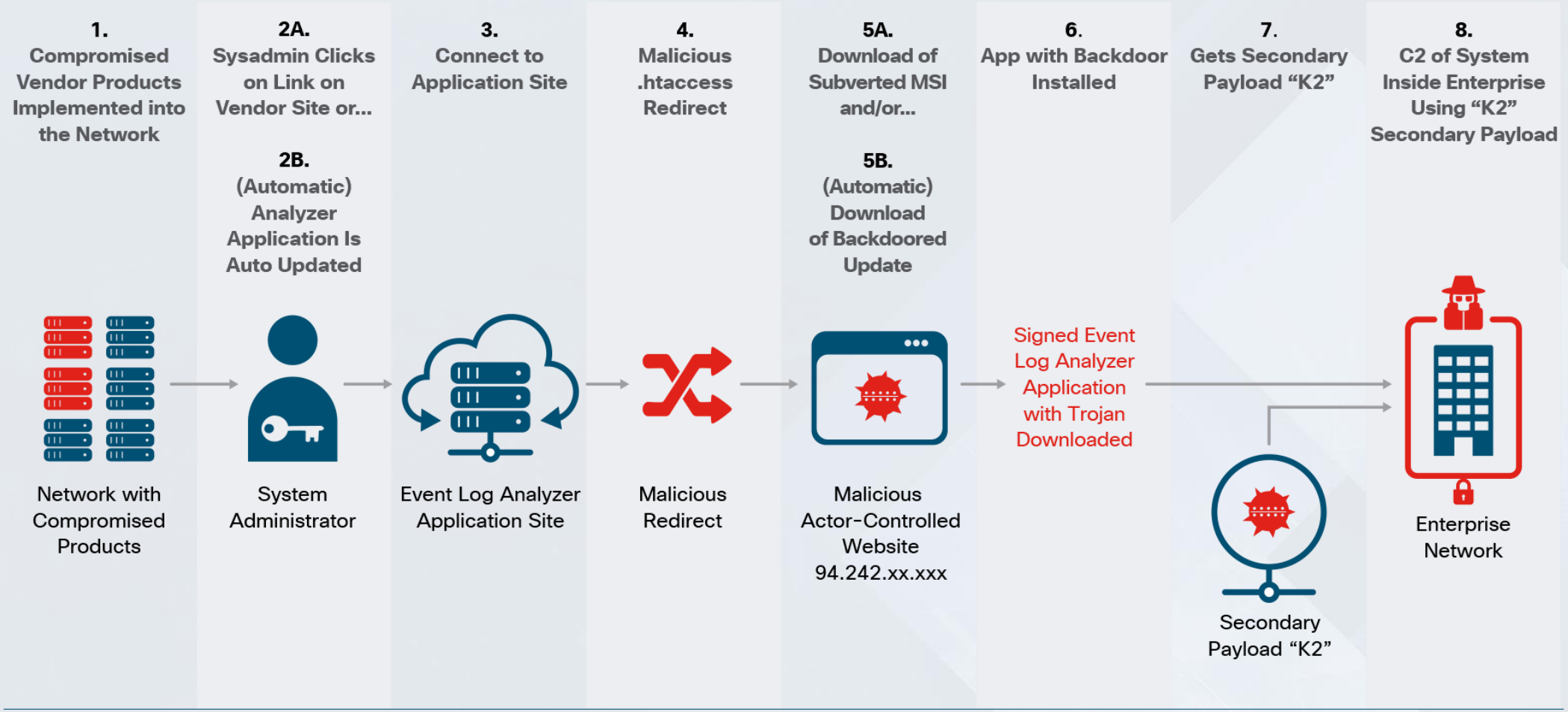
노출된 개발 시스템

무방비 상태의 개발 운영(DevOps) 서버의 높은 비율이 심각한 랜섬웨어 위험을 초래함

출처: Rapid7(일부)

공급망 공격: 한 곳만 뚫려도 전체가 위험

Kingslayer



출처: RSA

위험한 클라우드

조직의 클라우드 시스템 활용이 증가함에 따라 보안 팀이 해결해야 하는 위험 레벨도 높아짐

조직

- 조직에서 클라우드 애플리케이션이 빠르게 확장됨
- 수백만 명의 직원이 클라우드 애플리케이션 이용
- 애플리케이션 위험 레벨 상승
- OAuth에서 조직 백본에 대한 액세스 권한 부여
- 권한 있는 사용자 수가 너무 많음

공격자

- 권한 있는 사용자를 타게팅하여 자격 증명 도용
- 전체 네트워크 액세스
- 이전에 보안 침해된 자격 증명 활용

cisco

보안 운영 과제


온프레미스와 클라우드 로그 간의 포렌식 과제
적절한 구조 제어 부재
예산과 인력 부족
알림 피로
프로세스가 아닌 제품에 너무 치중

산업별 동향

업종별 요약

- 보안 침해 완화에 대한 우려
- 고객 데이터 보호, 규정 제약 처리, 최신 커넥티드 시스템과 레거시 소프트웨어 통합이 당면 과제임
- IT 및 OT 통합 필요

업종별 요약 (통신, 공공, 제조)

- 자체 IT 및 생산 인프라 보호가 당면 과제임
- 59% 사이트가 해당 데이터 센터 및 코어 생산 네트워크 보호를 최우선 과제로 선정
- 대규모 비즈니스
- 71%가 관리되는 보안 서비스 제공
- 오케스트레이션이 당면 과제임

- 46%가 보안 침해로 인해 보안이 개선된다고 대답
- 27%가 보안 인력 부족이 주요 장애물이라고 대답
- 30%가 침투 테스트와 엔드포인트 또는 네트워크 포렌식 툴 사용
- 40%가 서비스를 아웃소싱하지만 아웃소싱 시 사내 전문 지식이 증가하지 않음

- 미국 공장 중 80%가 20년 이상 오래됨
- 계획되지 않은 다운타임 방지가 당면 과제임
- 디지털 대격변
- IT/OT 통합
- 40%가 공식적인 보안 전략이 없음

cisco

업종별 요약 (의료, 운송, 금융)

- 환자 안전 우선
- 보안으로 인한 서비스 속도 저하에 대한 우려
- 통합된 IT/OT 시스템
- 37%가 표적 공격을 우려함
- 34%가 상당한 보안 예외를 적용하고 있고, 이들 중 47%는 보완 방안이 있음

- 폐쇄형 전용 시스템에 구축
- 커넥티드 IP 시스템으로 전환
- 새로운 안전 및 모빌리티 시스템 요구
- 데이터가 에지에 설치되어 공격 영역 증가
- 27%가 SOC를 보유하고 있고, 14%는 새로 구축할 예정임
- 거의 90%가 표준 기관에 참여

- 수익성 높은 표적
- 핀테크와의 파트너 관계로 인해 취약점 증가
- 37%가 벤더의 정보 보안 정책 사용 요구
- 컴플라이언스 및 보안
- 40%가 보안에 미치는 디지털 비즈니스의 영향이 매우 크다고 대답(핀테크, 개발 운영 DevOps, bimodal IT)

CISCO

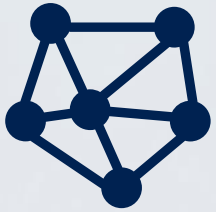
보안 발전을 가장 저해하는 요소

제약

- 예산
- 호환성
- 보안 인력 부족
- 인증 요건

당면 과제

벤더 수



제품 수

삭제된 경보

영향

시스템

다운타임

운영

금융

손실

CISCO

대응 전략 필요

결론

- 보안 침해의 영향력 증가
- 지능화된 위협으로 인한 보안팀의 어려움 커짐
- 경영진의 관심
- 간소화, 개방성, 자동화 필요

Cisco 2017 중기 사이버 보안
보고서 다운로드

www.cisco.com/go/mcr2017