Cisco 2016

중기 사이버 보안 보고서

Robert Paek

GSSO

2016년 9월

비대칭 공격에 대응할 수 있는 역량 부족

- 혁신적인 방법
- 지속적 공격
- 달라지는 전술
- 글로벌 운영

cisco

보안 실무자는 공격자의 공격 공간을 파악하고 이를 차단해야 합니다.

주제

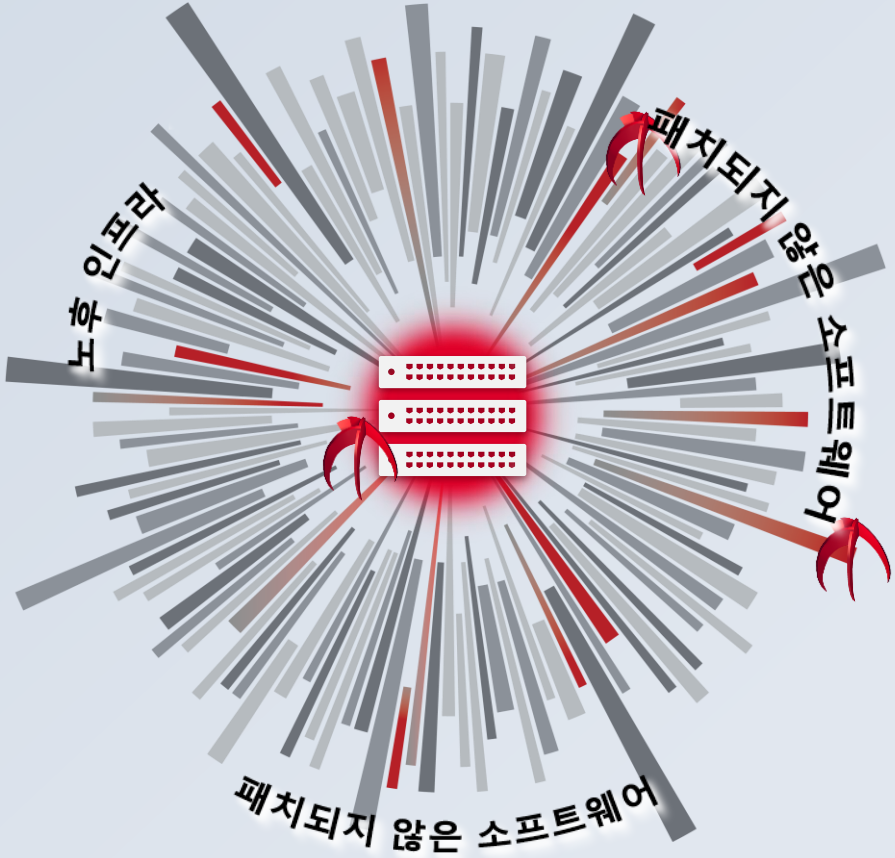
- 현재 위협 환경
- 공격 준비 시간 연장
- 보호까지 걸리는 시간 단축
- 글로벌 관점

Cisco의 포괄적인 텔레메트리 데이터 분석 결과

- 매일 160억 건의 웹 요청
- 매일 6,000억 개의 이메일
- 총 200억 개에 달하는 위협을 매일 차단
  - 매일 150만 개 이상의 고유 악성코드 샘플(17/초)
- 185억 건의 AMP 쿼리
  - 214k AMP 쿼리/초

현재 위협 환경

- 랜섬웨어의 발전
- 악의적인 해킹 기술의 발전
- 의심스러운 네트워크 상태
- 상충된 지정학적 관점



랜섬웨어

암호화 기술을 통해 대상별 맞춤화 가능

익명 지불에 비트코인 사용

이미 암호화된 마케팅 시스템과 파일

이중 기한:
1. 비용 증가
2. 데이터 삭제

Ransomware 2.0

자체 전파

- 광범위하게 구축된 제품의 취약성 활용
- 사용 가능한 모든 드라이브에 복제
- 파일 감염
- 제한적인 무차별 대입 공격
- 복원력 있는 C&C(command and control)
- 다른 백도어 사용

모듈형

- Autorun.Inf/USB 대용량 스토리지 전파
- 인증 인프라 익스플로잇
- C&C(command and control)/보고 감염
- 레이트 리미터: 시스템 리소스를 한정적으로 사용하도록 제한
- RFC 1918 대상 주소 리미터

- "방어자는 프로세스를 개선하고 혁신하여 취약점 공개와 패치 적용 간의 격차를 좁히고 있으나, 공격자는 자신들이 보유한 기술을 사용하여 이러한 격차를 다시 벌리려고 합니다. 다시 말해, 더욱 다양하고 복잡하게 방어자가 대응할 역량을 약화시키는 공격을 만들어냅니다."

- 연결 사이에 존재하는 VPN 게이트웨이와 같은 디바이스는 안전할 수도 있지만 그렇지 않을 수도 있습니다. 또한 안전한 보안 연결 상태라고 표시된 웹 사이트가 감염되었을 가능성도 있습니다. 중요한 것은 이러한 URL에도 "자물쇠" 아이콘이 있고 일반적인 사용자는 이를 안전한 활동을 나타내는 것으로 생각하지만, 이러한 URL을 결코 안전한 것으로 간주할 수 없다는 점입니다.

공격 준비 시간 연장

공격자는 제한이 없는 공격 준비 시간을 활용합니다.

공격 벡터: 주변의 서버

공격자가 클라이언트 측 공격에서 서버 측 공격으로 주력 분야를 확장

여전히 Adobe Flash의 취약점이 익스플로잇 킷에 이용되고 있습니다.

Cisco에서는 4월에 전 세계에 있는 모든 Jboss 서버 중 10%가 손상된 것으로 추산하고 있습니다.

- 보통 익스플로잇 킷이 악성 파일을 유포하면 모니터링에 의해 탐지됩니다. 악성코드가 "홈을 호출"할 때C&C(command-and-control) 트래픽으로 간주하고 탐지가 됩니다. 그러나 Cisco에서 관찰한 Nuclear 익스플로잇 킷 페이로드 유포의 경우, 맨 처음에는 Tor 실행 파일이 유포되었고 그다음에는 Tor를 통해 통신 요청이 이루어졌습니다. Tor는 엔드 투 엑시트(end-to-exit) 암호화 라우팅 프로토콜이므로, 보안 전문가는 이 브라우저 내에서 악성코드가 어떤 작업을 수행하는지 확인할 수 없습니다.

그림 7. 스팸에 자주 사용되는 소셜 엔지니어링 항목

버전 수	URL	메시지 요약	언어	최종 발행일(GMT)
95	RuleID4626	청구서, 결제	영어, 독일어	3.18.16
82	RuleID4400KVR	구매 발주서	영어	2.1.16
64	RuleID4626(cont)	청구서, 결제, 배송 확인	영어, 독일어, 스페인어	1.28.16
62	RuleID4961KVR	결제, 이체, 주문, 배송	영어	3.25.16
58	RuleID4961KVR	견적 요청, 제품 주문	영어, 독일어, 다국어	1.25.16
52	RuleID5118KVR	제품 주문, 결제	영어, 독일어	3.17.16
49	RuleID858KVR	배송 견적, 결제	영어	3.14.16
47	RuleID4961	이체, 배송, 청구서	영어, 독일어, 스페인어	2.22.16
44	RuleID4627 및 RuleID4627KVR	비행기 E-티켓	영어	3.29.16
30	RuleID8337KVR	주문, 결제, 견적	영어	.21.16

출처: Cisco Security Research

최근 공격자들은 서버를 활용하여 공격을 확장하고 이를 통해 훨씬 높은 수익을 올리고 있습니다. 변종 랜섬웨어인 SamSam은 네트워크에 액세스하기
위해 엔터프라이즈 애플리케이션 플랫폼인 JBoss를 이용하였습니다(**7**페이지 참조). Cisco 연구 팀이 관찰한 의료 기관 사례의 경우, 공격자는 JexBoss를 이용해 JBoss 애플리케이션 서버를 공격하고 네트워크 내에 거점을 확보하였습니다. 네트워크에 진입한 후에는 SamSam을 사용하여 Windows 파일을 암호화할 수 있었습니다.

익스플로잇 킷 활동: Adobe Flash 및 멀버타이징(Malvertising)

Adobe Flash 및 Microsoft Silverlight의 취약성이 대부분의 익스플로잇 킷에 이용

취약점

	Nuclear	Magnitude	Angler	Neutrino	RIG
Flash					
CVE-2015-7645	✓	✓	✓	✓	✓
CVE-2015-8446			✓		
CVE-2015-8651	✓		✓	✓	
CVE-2016-1019	✓	✓			
CVE-2016-1001			✓		
CVE-2016-4117	✓	✓	✓		
Silverlight					
CVE-2016-0034			✓		✓

HTTPS의 악성코드 사용:

HTTPS에서 지난 4개월 동안 광고 인젝터가 300% 증가했습니다.

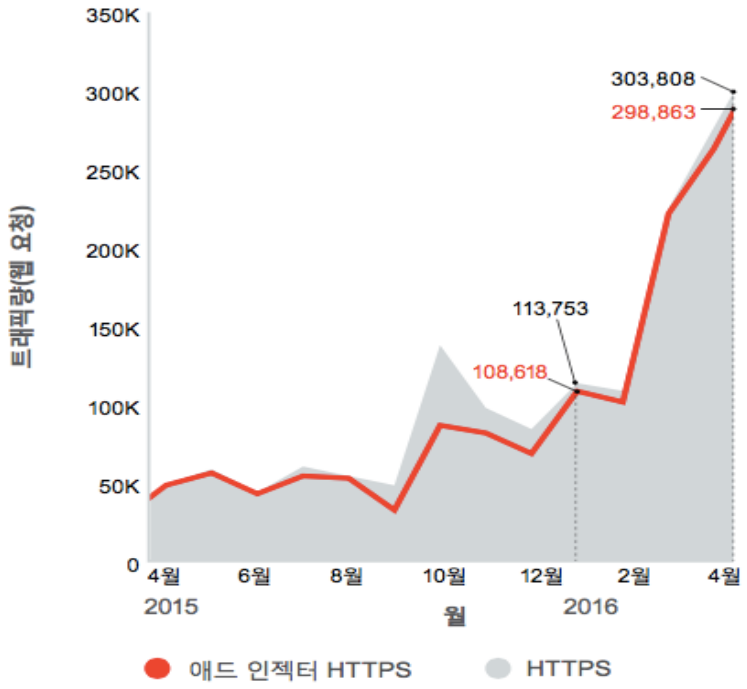
4개월 내

300%

증가됨

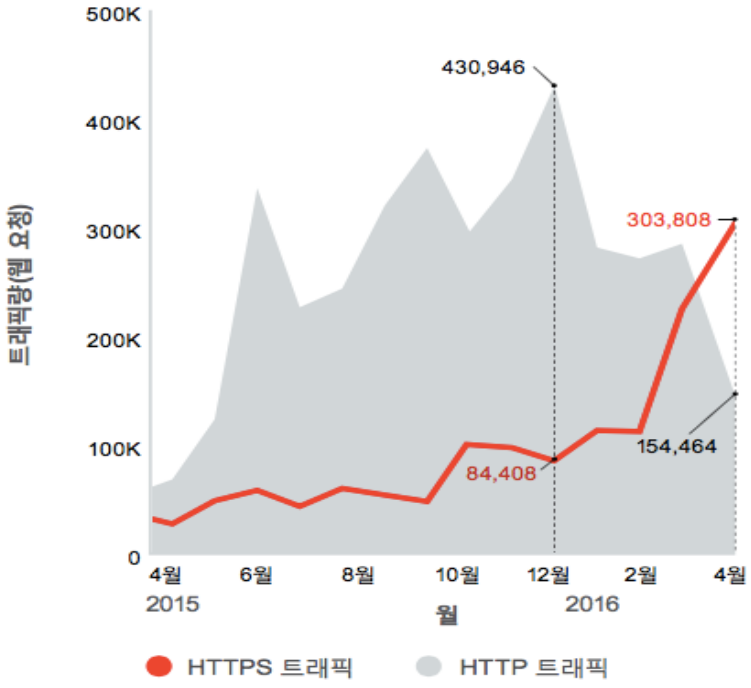
광고 인젝터가 가장 큰 원인입니다. 공격자가 HTTPS 트래픽을 사용하여 공격 준비 시간을 연장하고 있습니다.

그림 8. HTTPS 증가의 주요 원인인 애드 인젝터



출처: Cisco Security Research

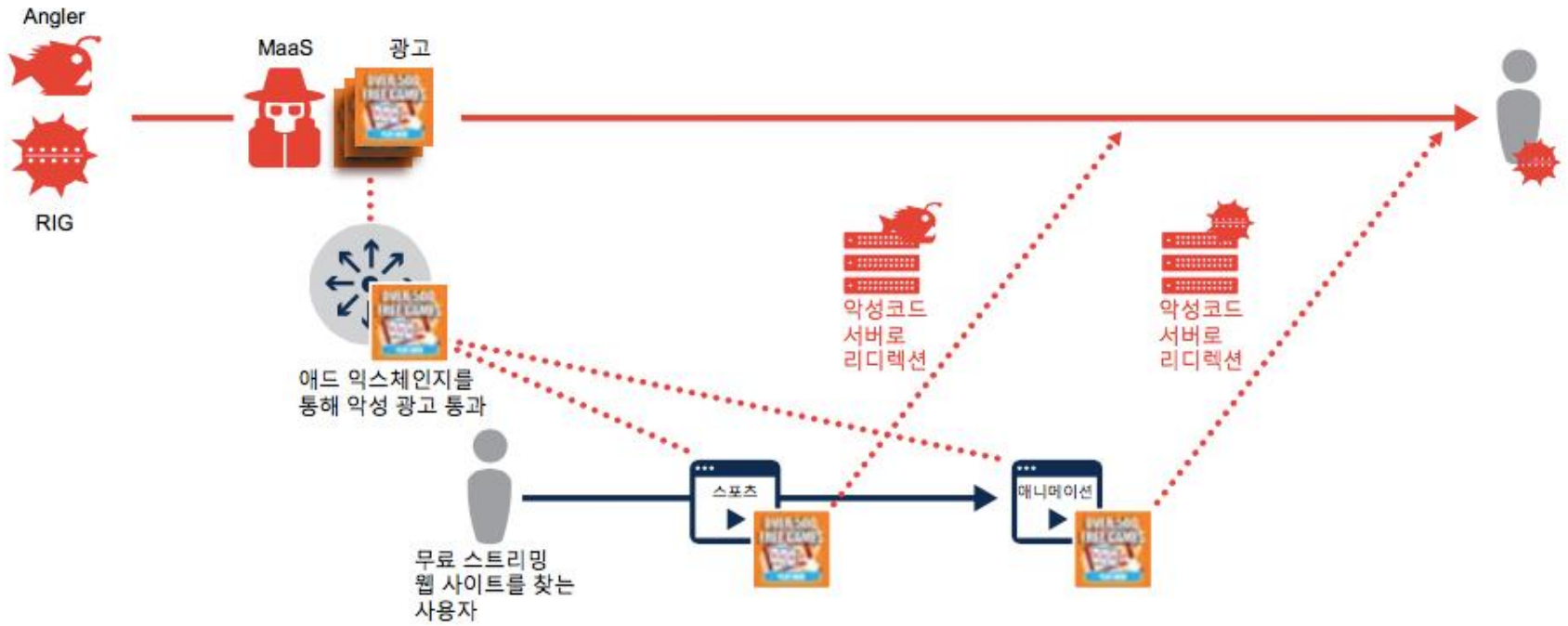
그림 9. 4개월 동안 애드 인젝터에 대한 HTTPS 트래픽이 300% 증가함



출처: Cisco Security Research

- 위협 공격자는 맬버타이징을 진행하기 위해 유명하며 합법적인 웹 사이트에서 광고 영역을 구매하고 있습니다.
- 공격자는 합법적인 광고 영역을 구매함으로써 관련 없는 사이트 전체에 손쉽게 위협을 확산시킬 수 있습니다. 광고 팝업은 아주 잠깐 나타나므로, 방어자에게는 위협의 존재 유무를 파악할 수 있는 시간이 거의 주어지지 않습니다.
- 보안 팀에서는 애드 익스체인지들로부터 광고를 업로드 받아 게재하는 사이트들을 차단할지 여부에 대해 고민해야만 합니다.

그림 11. MaaS(Malvertising as a Service) 작동 방식



출처: Cisco Security Research

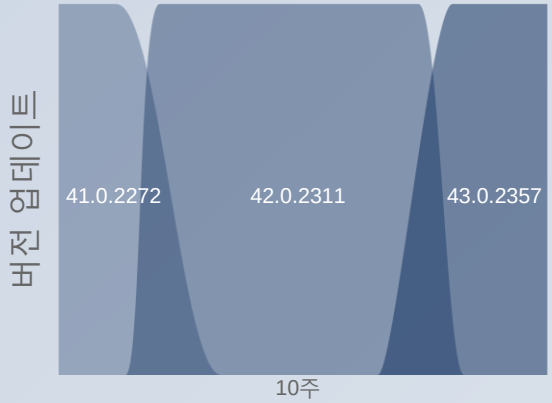
보호까지 걸리는 시간 단축

공격자의 성공을 방해하는 데 핵심적입니다.

패치 시간: 취약한 엔드포인트가 적합한 대상임

브라우저

Chrome

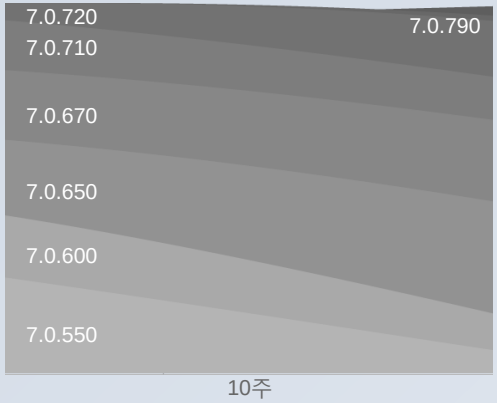


들쭉날쭉한 패턴

사용자가 업데이트하며
도입률이 높습니다. 버전 간
겹치는 부분이 적습니다.

애플리케이션

Java.

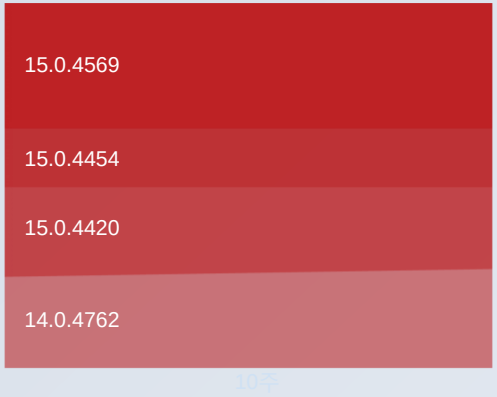


경사진 패턴

사용자와 조직이 모두
업데이트합니다. 수많은 버전이
동시에 실행 되어 마이그레이션
속도가 저하됩니다.

엔터프라이즈 소프트웨어

사무실



박스 패턴

조직에서 업데이트합니다.
버전 간 업데이트에서 움직임이
거의 없습니다. 취약한 상태로 둡니다.

취약한 인프라에 디지털 경제로 만든 인프라

취약하고 안전하지 않은 인프라에서 차세대 경제를 안전하게 지원할 수 없습니다.

디바이스에서 알려진 취약점이 처리되는 기간 평균

5년

문제는 시스템입니다.

Cisco

5.64

년

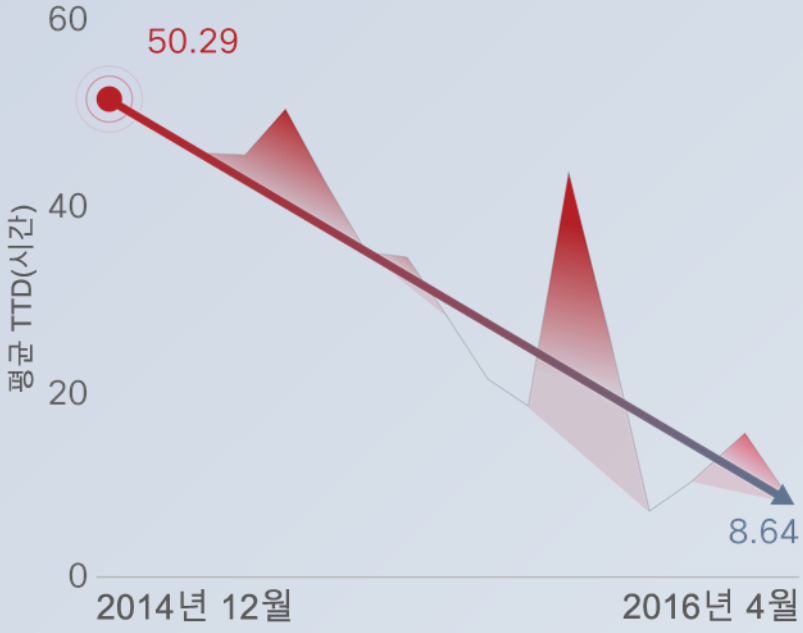
Apache/
Open SSH

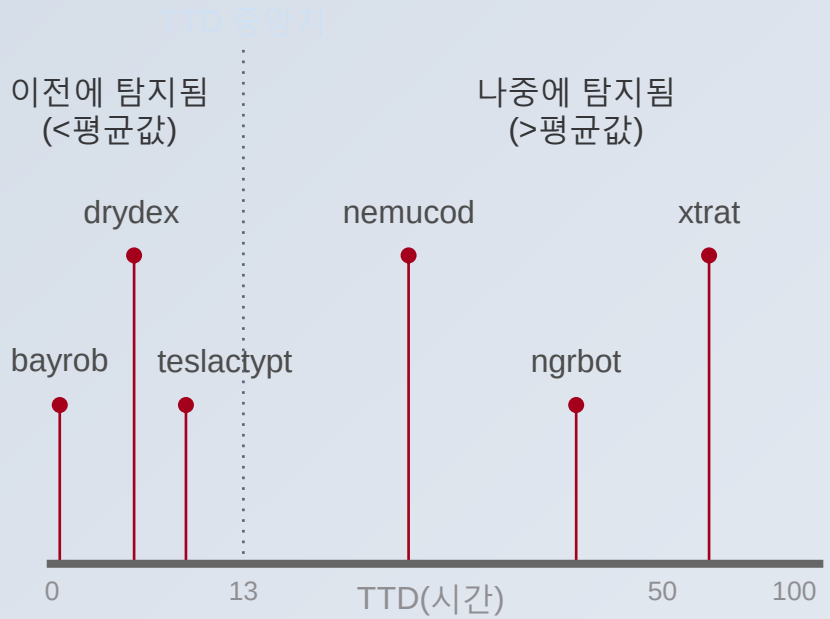
5.05

년

탐지까지 걸리는 시간: 공격자 탐지 향상

지속적인 "군비 경쟁"에서 우위 점유





암호화: 행방 감추기

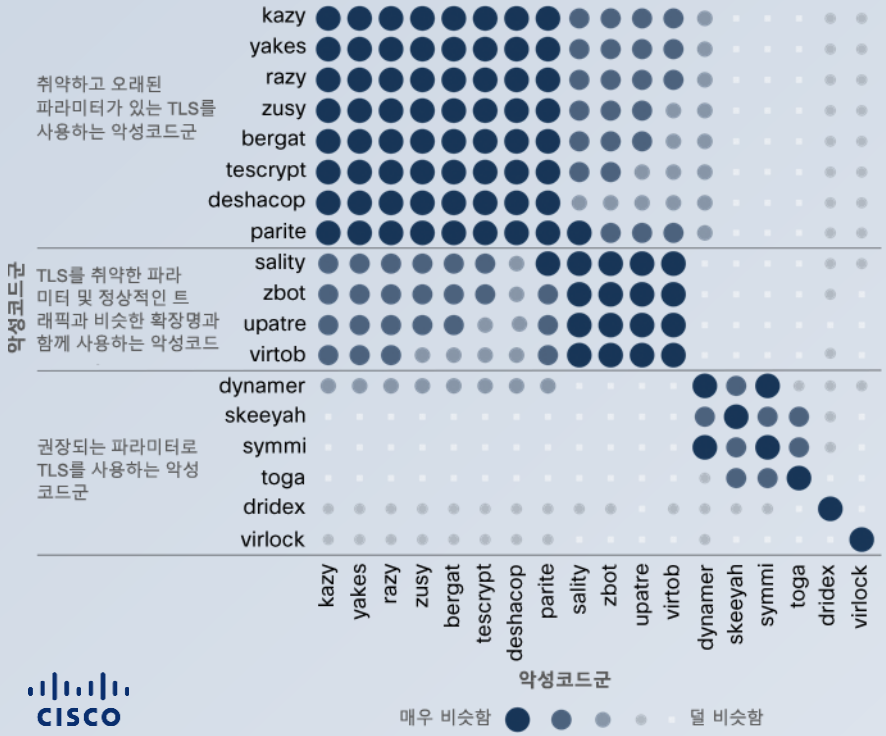
공격자가 탐지를 피하기 위해 암호화된 트래픽으로 진행 경로를 숨깁니다.

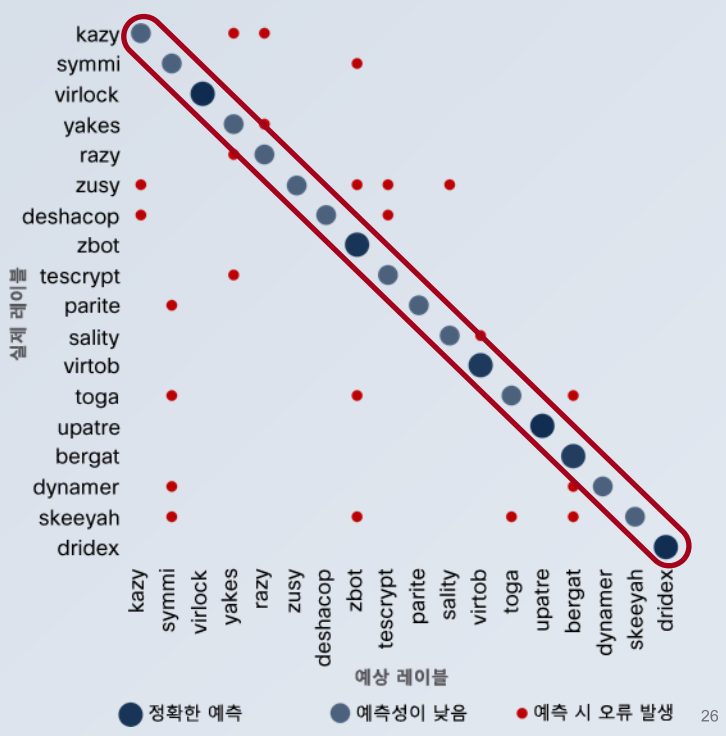
HTTP 악성코드 트래픽 증가	% 증가	평균 % HTTPS
광고	+9.27%	34.06%
검색 엔진 및 포털	+8.58%	64.27%
채팅 및 인스턴트 메시징	+8.23%	96.83%

카테고리 1월~4월	평균 % HTTPS
조직 이메일	97.88%
채팅 및 인스턴트 메시징	96.83%
웹 기반 이메일	96.31%
온라인 스토리지 및 백업	95.70%
인터넷 전화	95.07%

TLS의 악성코드 사용: 탐지할 수 없는 사항 탐지

머신 러닝을 통해 비슷한 속성을 가진 악성코드를 정확하게 탐지하고 식별할 수 있습니다.





사고 대응: 내막

오래된 인프라로 인해 방어자를 당황하게 만드는 취약성 발생

오래된 인프라

프로세스 부족

예산 제약

패치 안 함

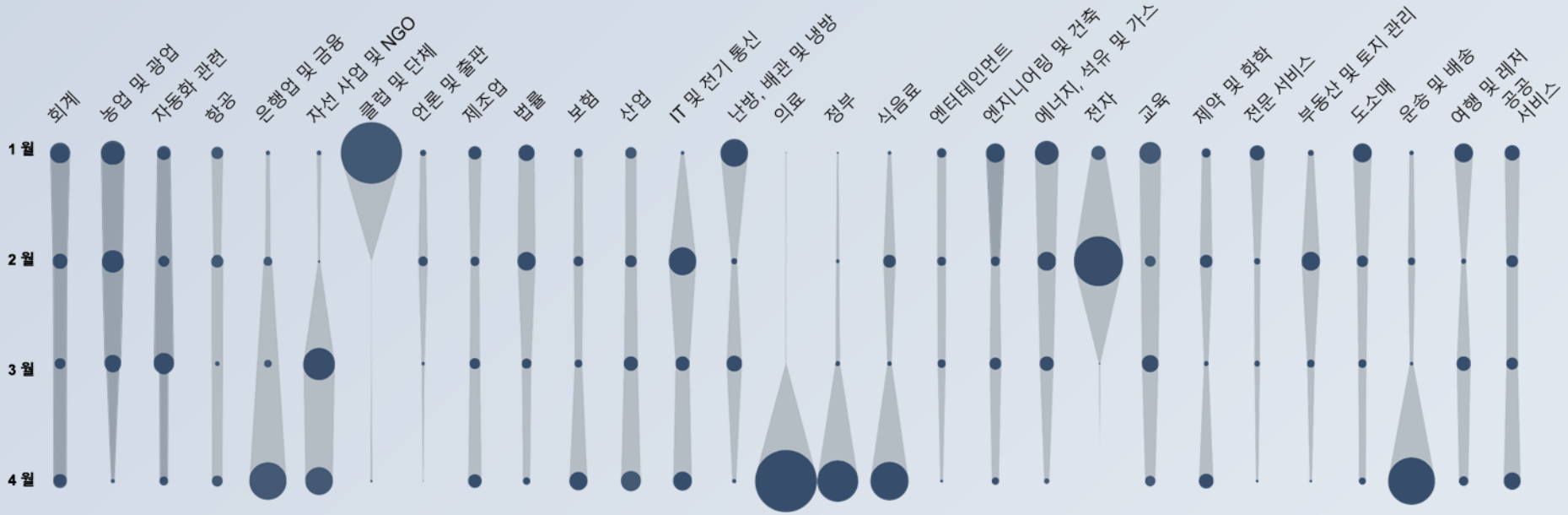
사용 가능한 툴을 사용하지 않음

글로벌 관점

공격자는 이익을 극대화하고 탐지를 피하기 위해 전 세계적인 규모로 운영

산업별 악성코드 발생 위험

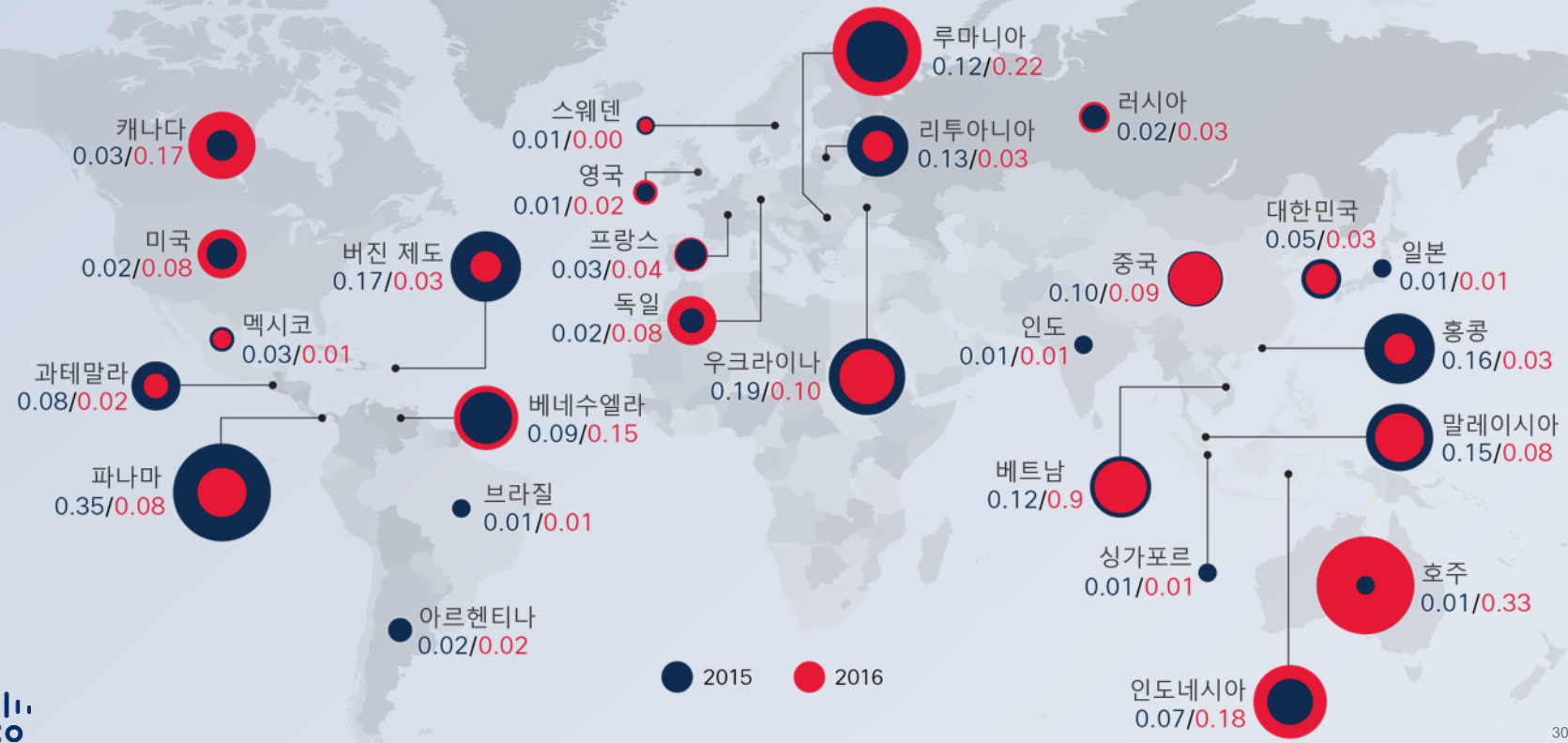
어떤 업계도 안전하지 않습니다. 공격자는 산업을 바꿔가며 공격합니다.



발생률과 기준선 비교

국가별 웹 차단

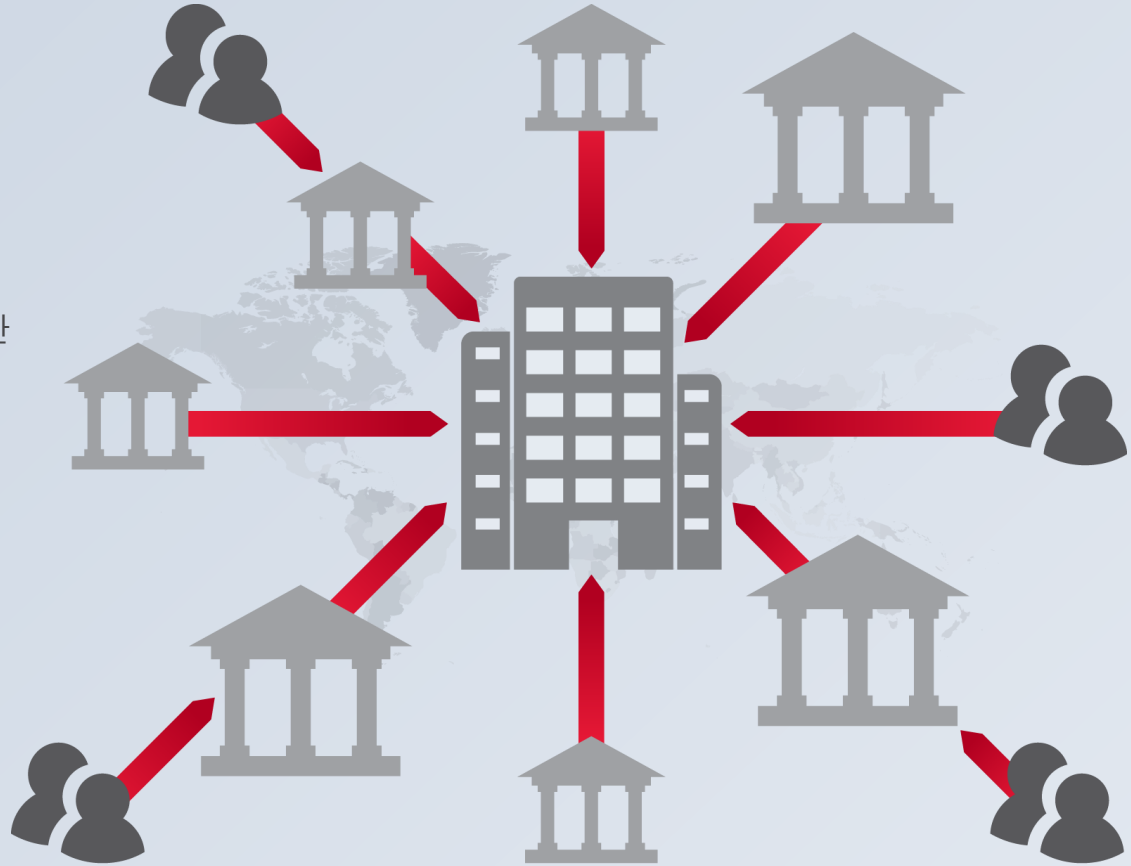
공격자는 경계를 무시하며 공격 기반을 옮깁니다.



노후된 인프라가 전 세계적으로 문제임

지정학적: 모순된 신호로 인해 제한된 보안

정부의 고유한 규칙 실행, 하지만 서로 모순된 규칙

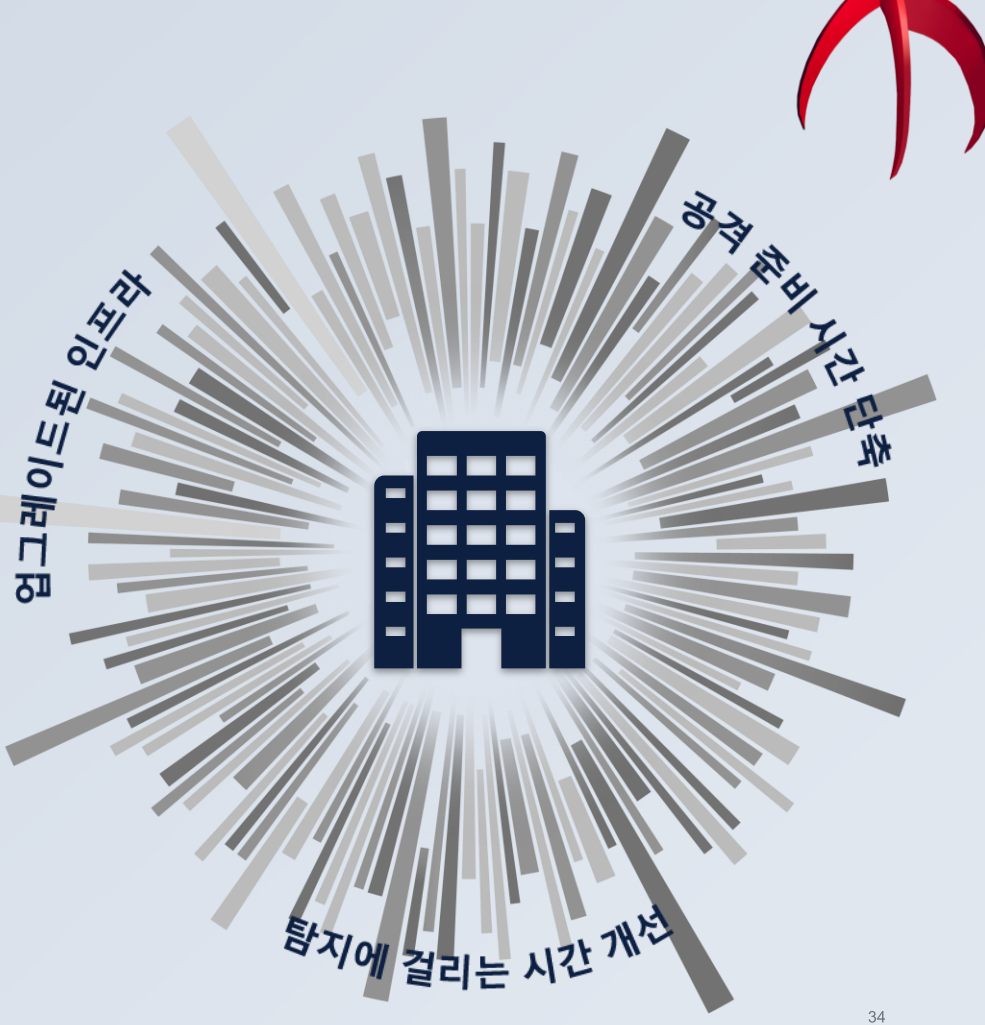


개인정보를 우려하는 대중

보안 실무자는 공격자의 공격 공간을 파악하고 차단해야 함

결론

- 널리 퍼져있고 강력한 랜섬웨어
- 일반 데이터 백업
- 네트워크 상태 향상
- 방어 통합
- 탐지 소요 시간 측정



2016 중기 사이버 보안 보고서

www.cisco.com/go/mcr2016