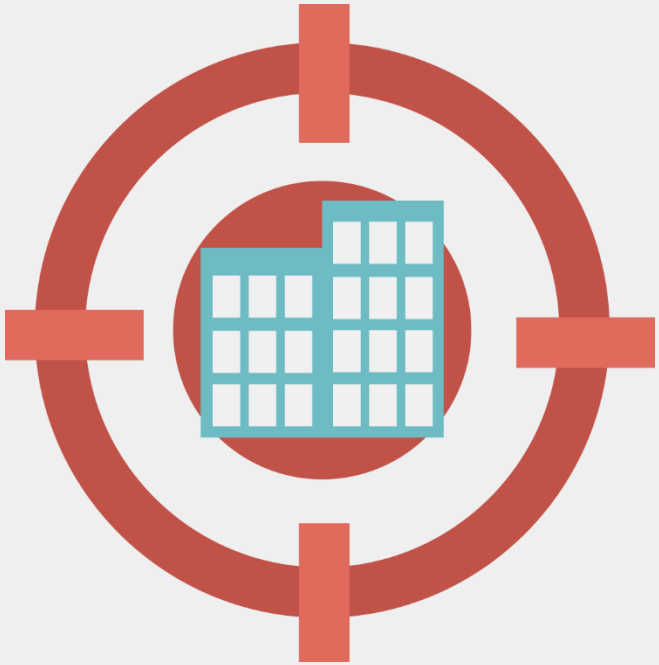
진화하는 표적공격의 #1
진입경로 이메일, 대응방안은 없는가?

조윤진 보안컨설턴트

Symantec Korea

표적 공격의 증가

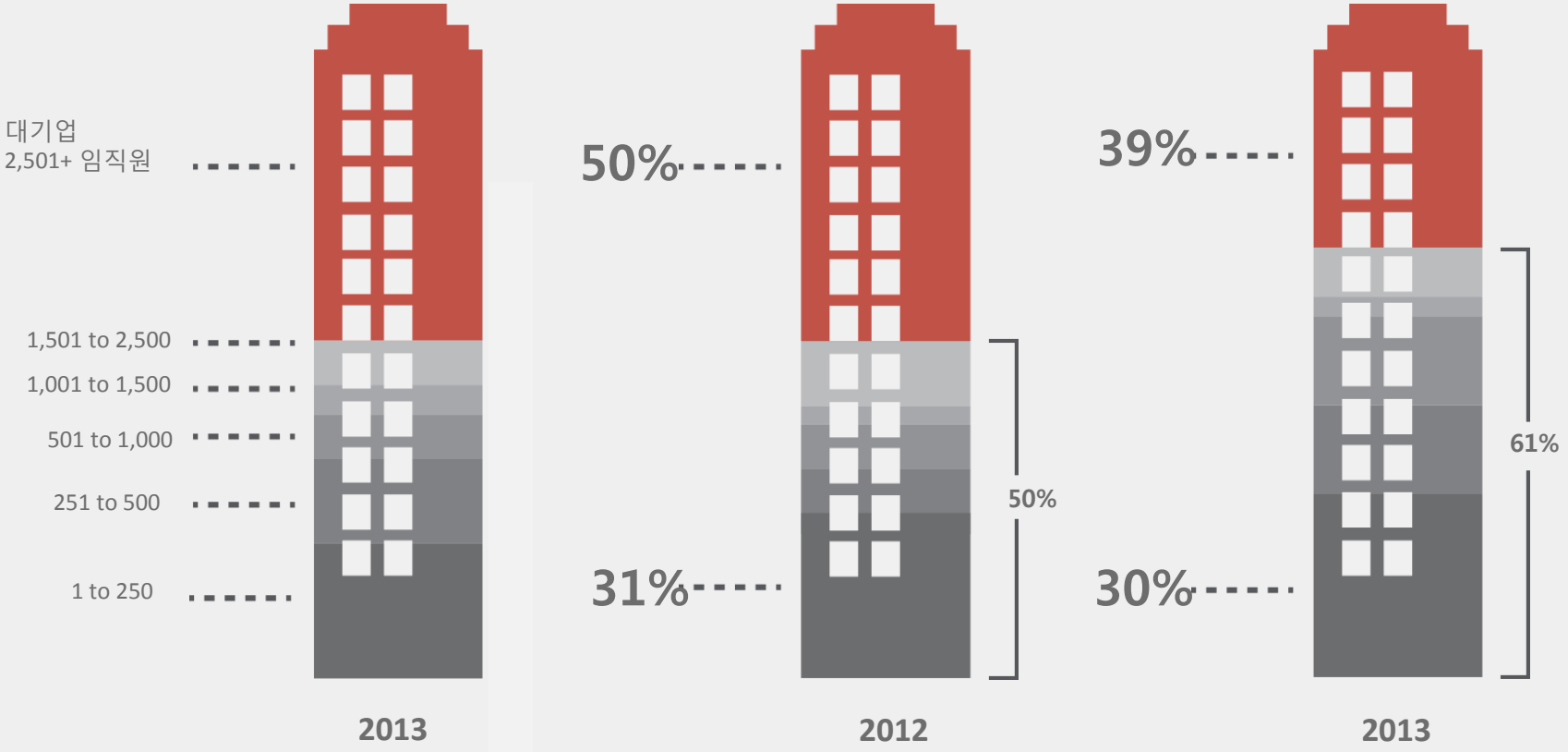


91%

전년 대비
표적공격 증가율
2013 vs. 2012

*ISTR 19 (Symantec, 2014)

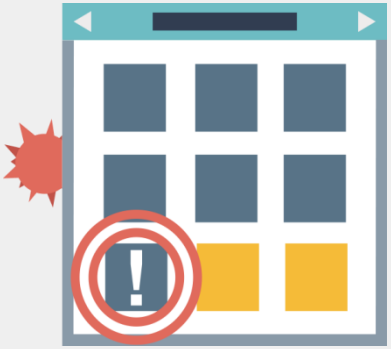
규모별 표적공격



*ISTR 19 (Symantec, 2014)

기업은 표적공격 대응이 점점 어려워짐

사고발생 기업의
66%는, 약 30일 이상
사고발생 사실을
인지하지 못함



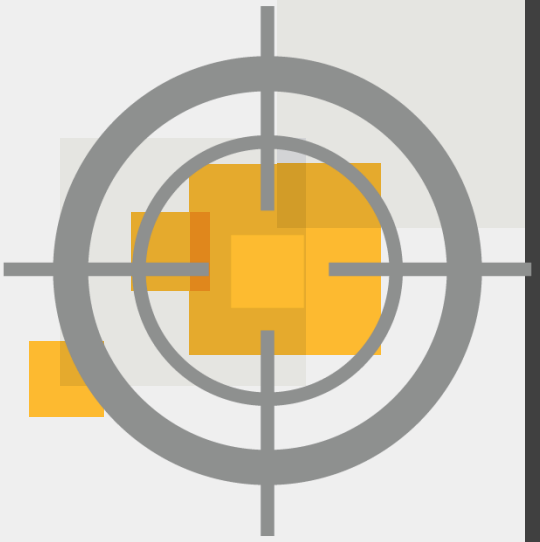
탐지가 되기까지
약 243일 소요

제거에 약 4개월 소요

단계별 분석의 필요성

성공적인 도둑질 단계

단계	성공적인 도둑의 흐름
1단계	표적하는 대상에 대한 정보 수집
2단계	수집된 내용을 기반으로 침투
3단계	침투 완료후, 집안의 구조및 주요 자산에 대한 탐색
4단계	다양한 형태의 물건을 수집
5단계	수집된 물건을 안전하게 밖으로 가지고 나옴



APT 단계별 표적 공격 분석

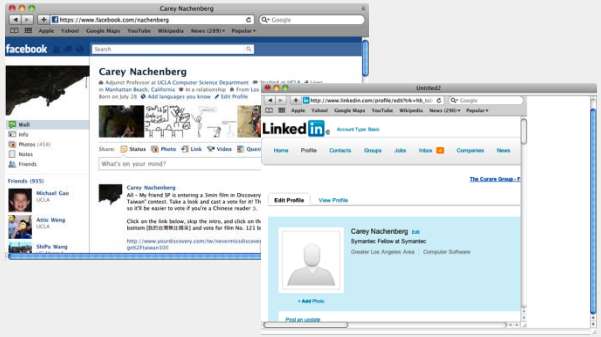
Symantec

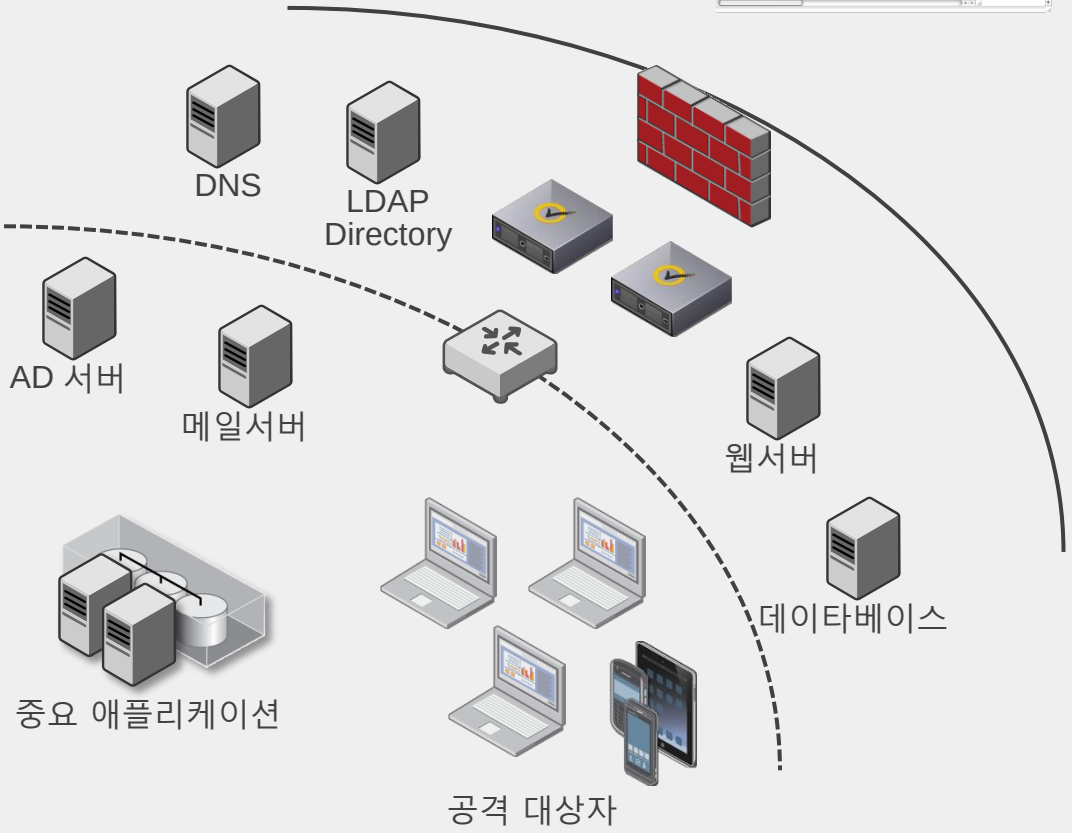
1단계: 사전조사

사전조사

공격자가 표적으로 삼은 기업과 기관의 취약한 시스템, 네트워크, 직원에 대해 파악하고 공개된 정보 출처를 활용하여 해당 표적에 대해 조사

공격자

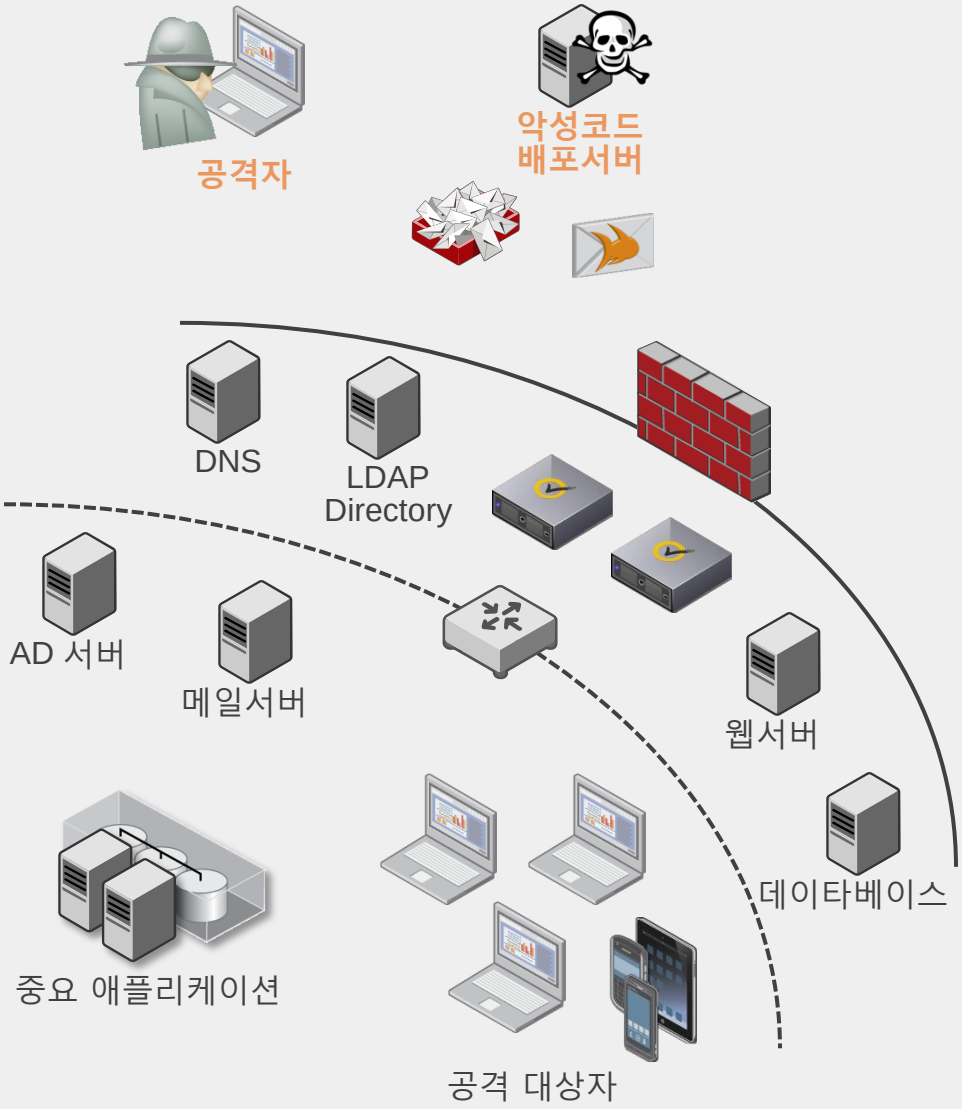




1단계: 사전조사

사전조사

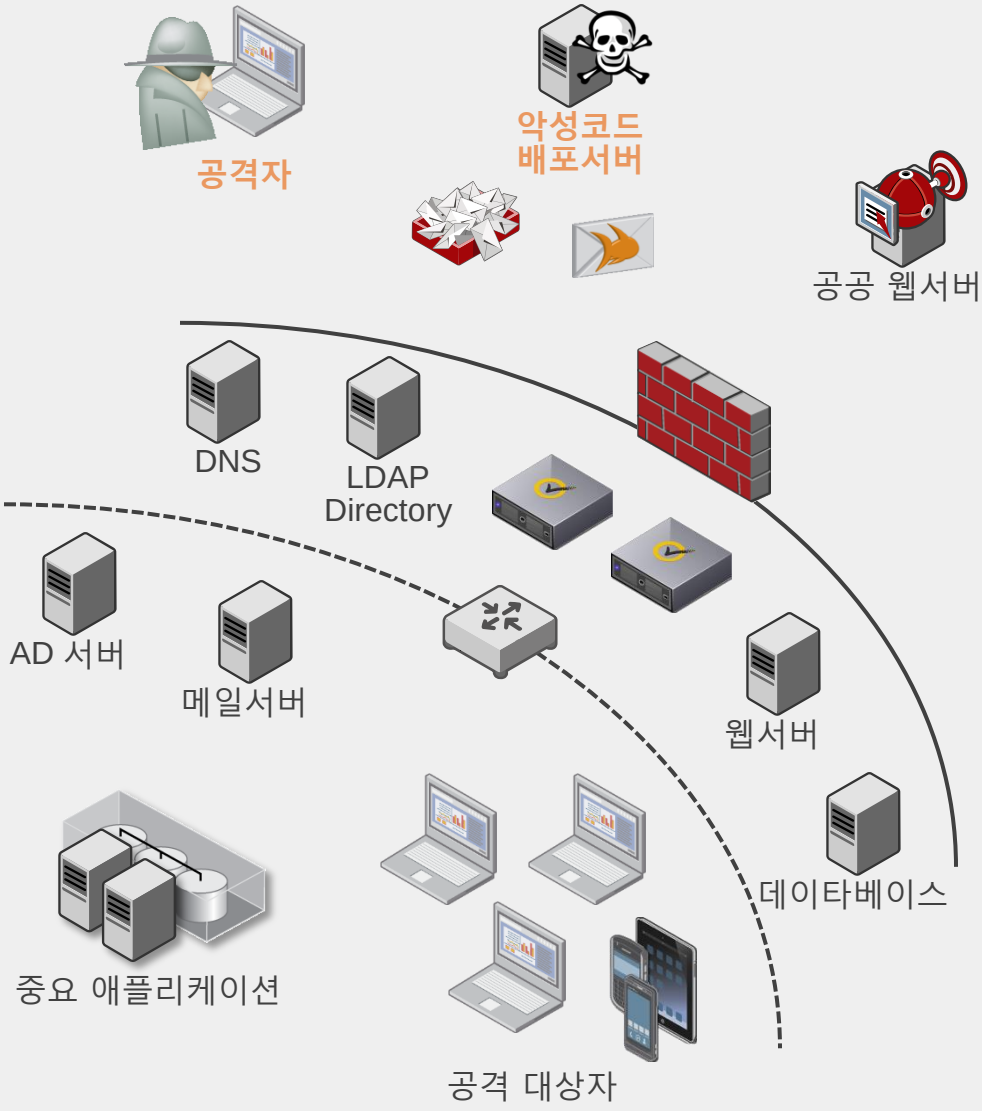
수집된 정보를 통해,
공격자는
공격대상자에
스팸을 발송하거나
피싱공격을 사용함



1단계: 사전조사

사전조사

공격자는
공격 대상자가 자주
방문하는 사이트를
공격하여 워터링 홀
공격을 통해
악성코드를
감염시킴

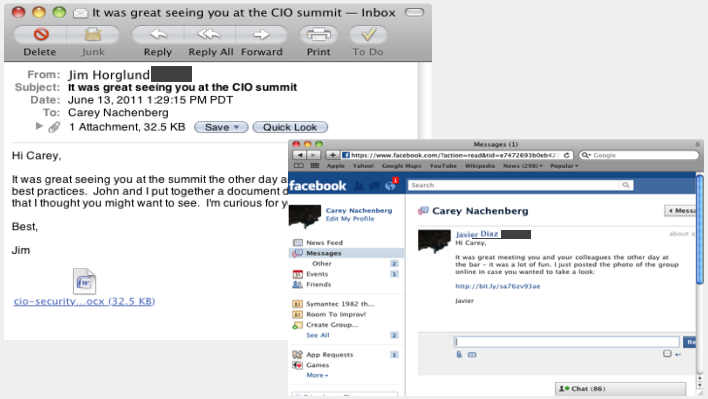


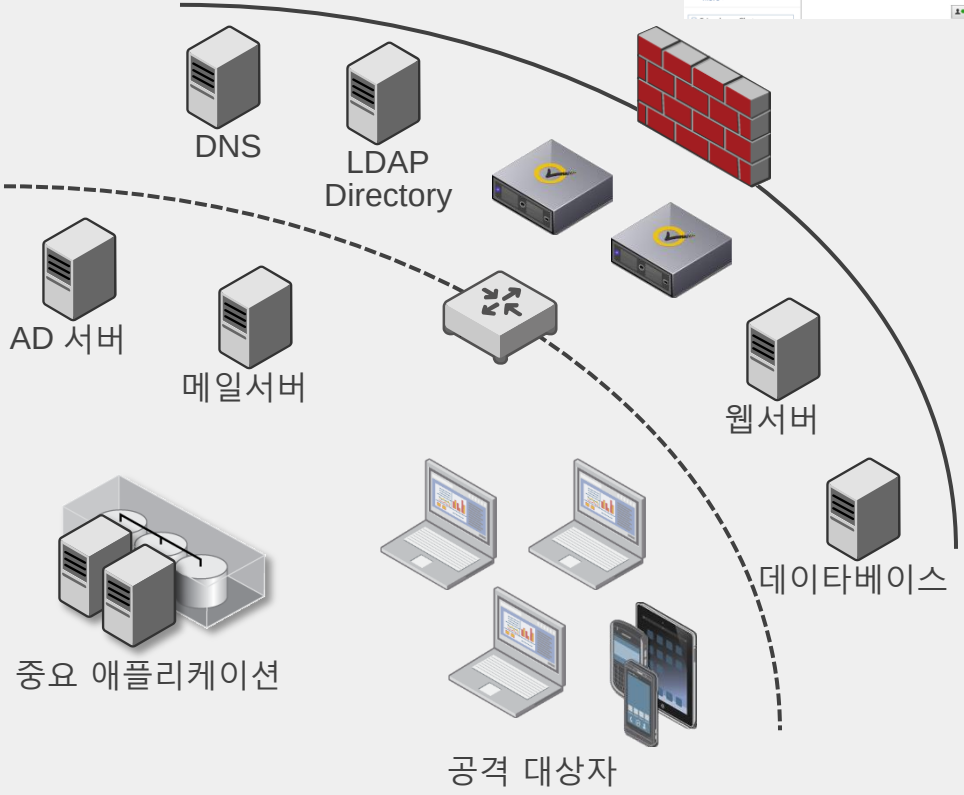
2단계: 침투

침투

공격자가 시스템 또는 네트워크에 침투하거나 사용자를 속여 이메일이나 웹 사이트를 통해 악성 컨텐트에 액세스하도록 유도

공격자

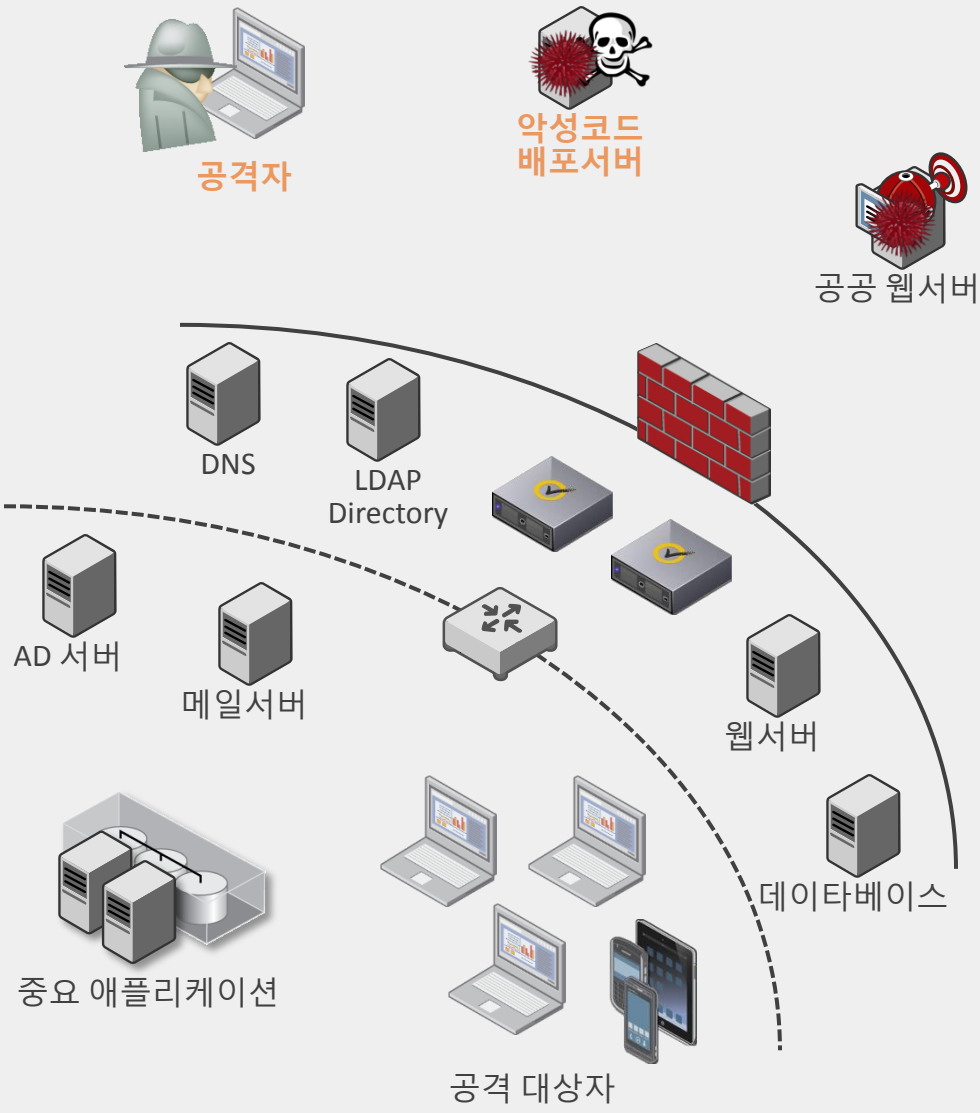




2단계: 침투

침투

사용자는 첨부파일을
다운로드 받거나 또는
악성유도 링크를
클릭하여
원격조정되는
좀비PC가 됨

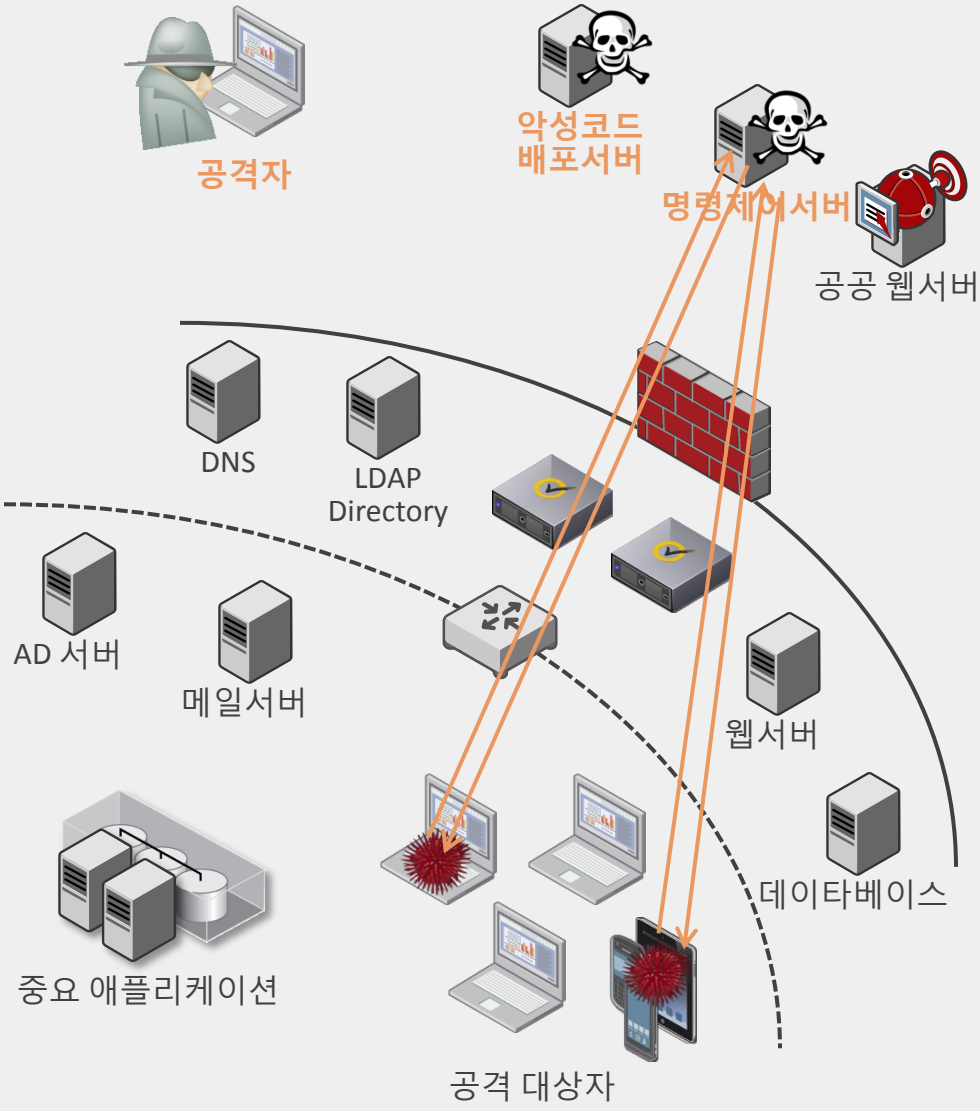


3단계: 탐색

탐색

공격자는 명령제어 서버를 세팅함

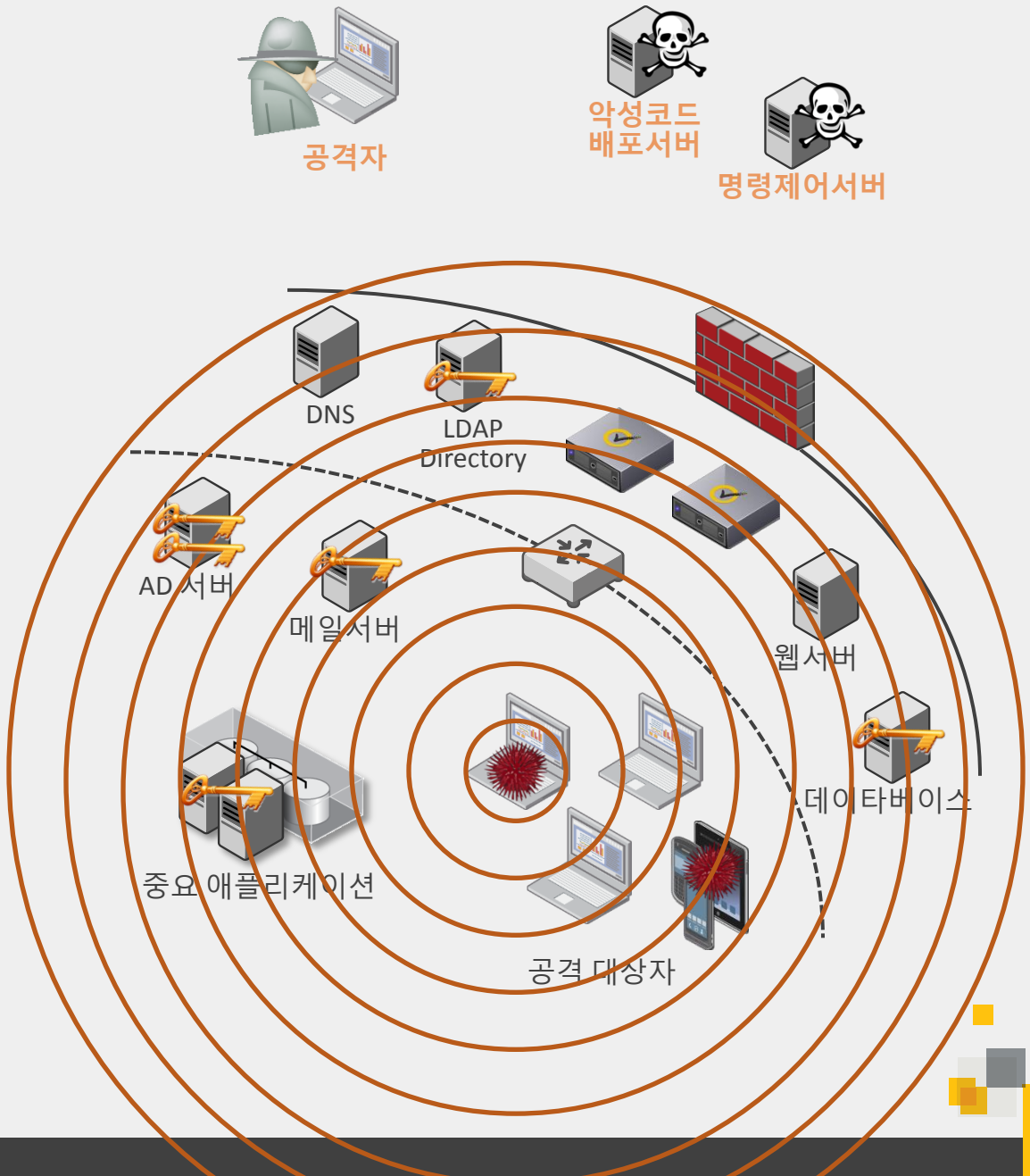
백도어 악성코드는 명령제어 채널에 연결함



3단계: 탐색

탐색

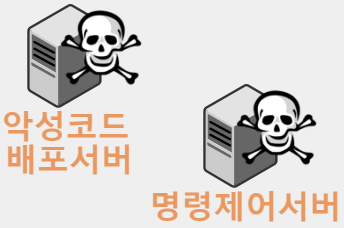
백도어 악성코드는 공격자의 지시에 따라 로긴 정보를 수집하여 기업의 중요서버에 로긴함

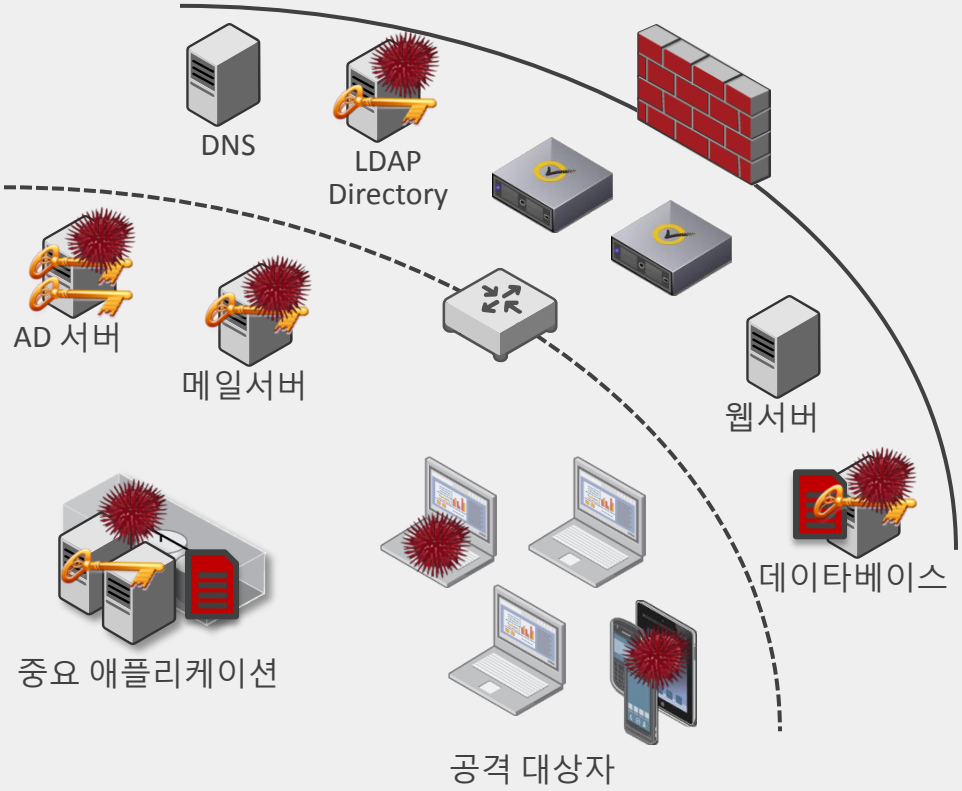


3단계: 탐색

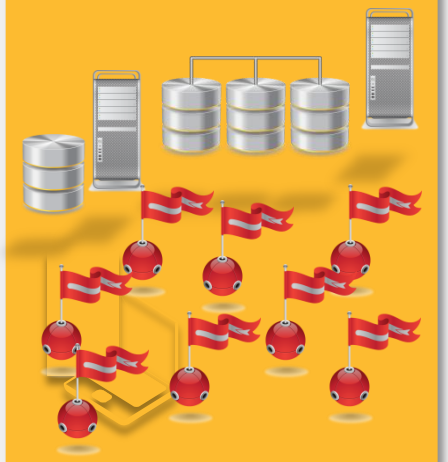
탐색

로긴 접속정보를 통해 공격자는 네트워크 구성을파악하고, 기밀정보를 보유하고 있는 서버로 공격을 넓혀나감





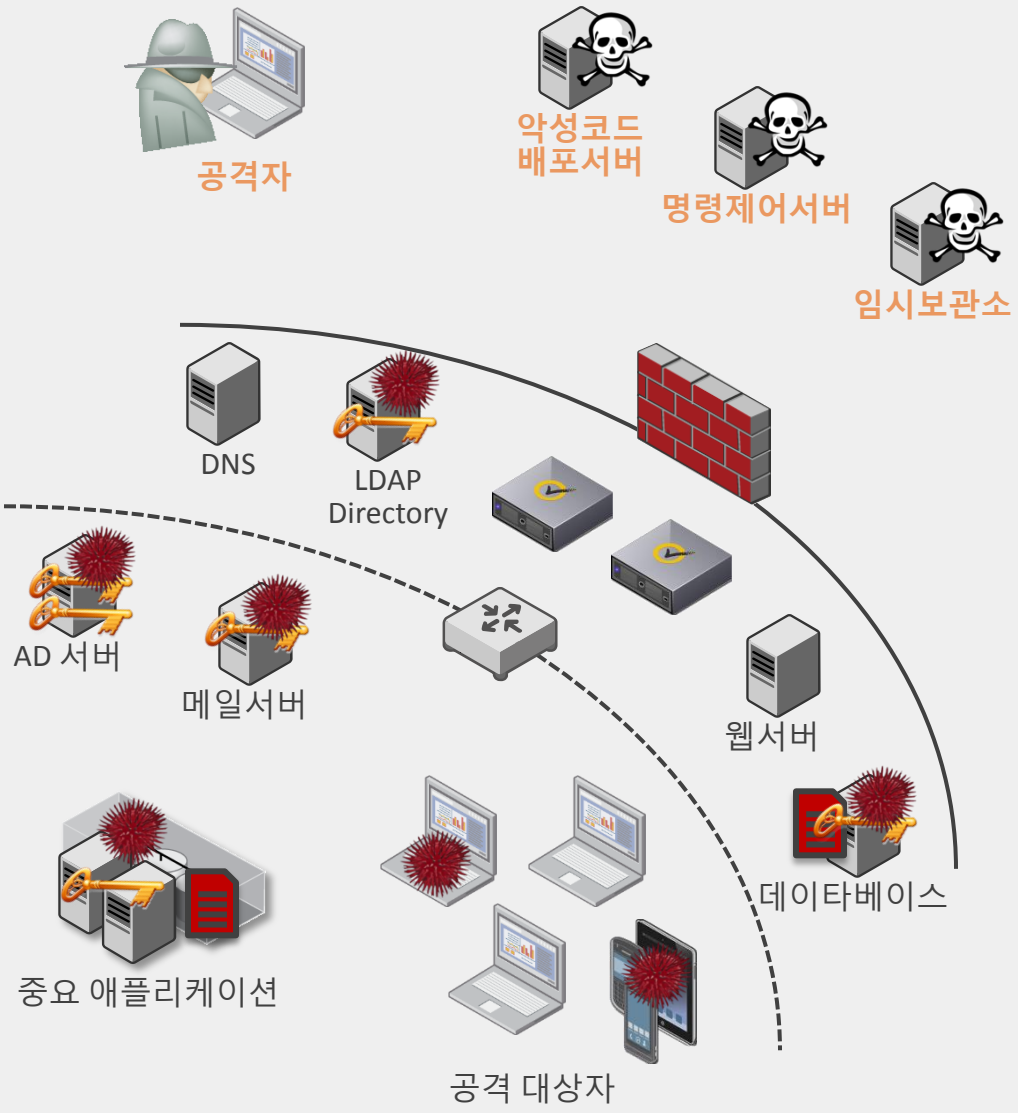
4단계: 수집



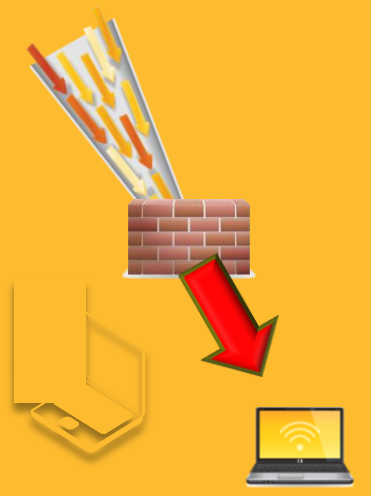
수집

공격자는 외부에 임시 보관소를 준비함

공격자는 임시로 내부 시스템에 기밀 데이타를 임시로 저장함



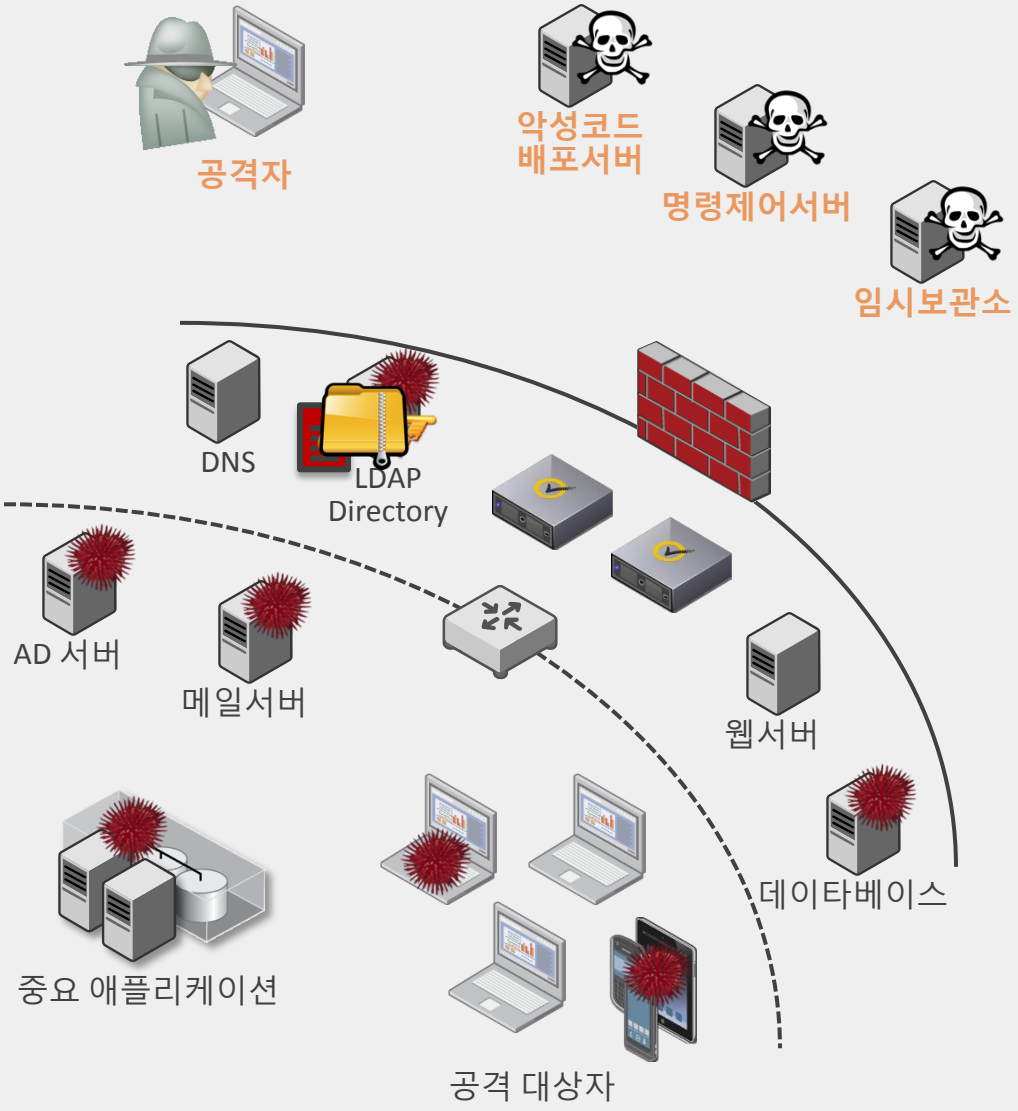
5단계: 유출



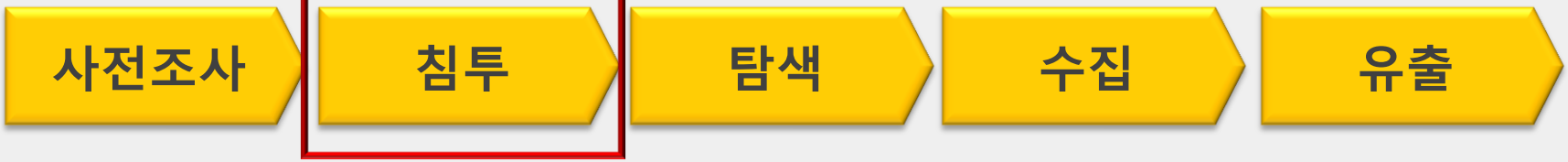
유출

공격자는 로긴정보와 기밀정보를 암호화함

외부에 사전에 준비한 저장소에 유출함



5단계의 성공적인 지능형지속공격



단계	지능형 지속공격
1단계	표적하는 대상의 다양한 정보 수집
2단계	수집된 내용을 기반으로 침투 시도
3단계	명령제어 서버와 통신및 추가 악성코드 다운로드하여 내부 시스템 탐색
4단계	기업의 기밀 데이터를 임시보관소에 수집
5단계	수집된 파일을 외부로 유출

대표적인 표적 공격(APT) 침투 형태

스피어 피싱

표적으로 삼은 대상에게
이메일 발송

워터링 홀 공격

웹사이트를 감염시킨 후
잠복

이메일 보안의 위협

1 in 392
이메일 중 피싱
이메일 수

1 in 196
이메일 중 악성
이메일 수

25%
이메일 악성코드 중
URL Link를 통한
악성코드 비율

66%
전세계 이메일의
스팸 포함율

91%
전년도 대비 표적공격 증가율,
이메일은 표적공격의 최고 공격 매개체

Source: Symantec Internet Security Threat Report volume 19

스팸 차단 솔루션의 한계

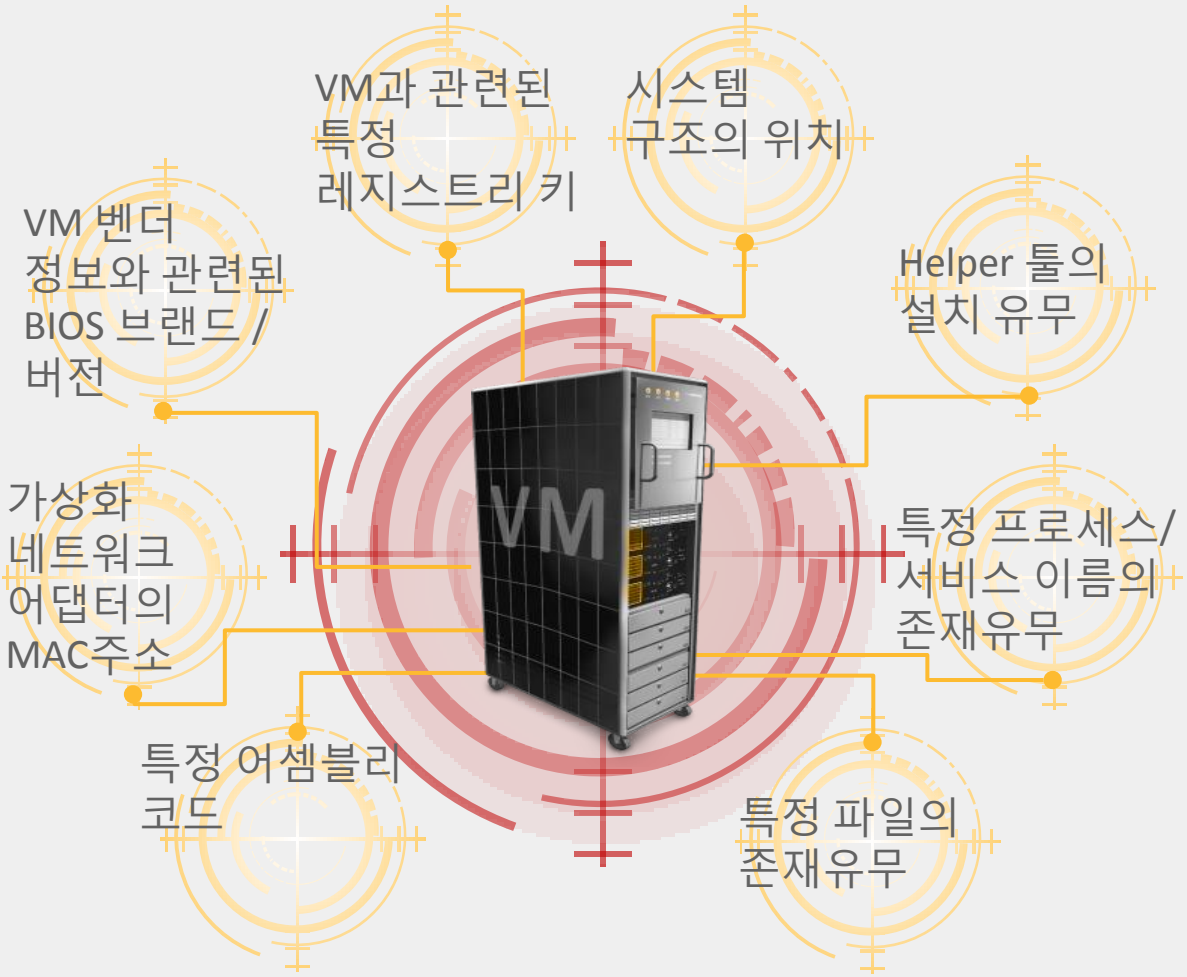
- 스피어 피싱 메일 탐지 불가능
  - 시그니처 탐지 방식 우회
  - 알려지지 않은 악성 코드 사용
  - 문서 파일을 위장한 악성 코드 사용
  - 악성코드가 심어져 있는 URL을 본문에 첨부
  - 신뢰하는 사람/기관을 발신자를 변경후 전송

문서 파일을 통한 표적 공격

Executable type	February	January
.doc	27.6%	46.1%
.txt	21.0%	8.3%
.xls	16.2%	7.8%
.scr	12.6%	–
.rar	7.6%	–
.rtf	4.9%	1.3%
.zip	2.3%	–
.exe	2.3%	2.0%
.bin	0.9%	8.0%
.ppsx	0.4%	–

가상실행기술의 문제점 - Px(Physical execution)이 필요한 이유

출현하는 악성코드 중 약 20%이상이 가상시스템을 우회함



자동 분석 시스템의 우회

Vx 형태의 자동분석 시스템 우회에 사용되는 기술

도전과제

시스템은 특정 시간 내에 결정을 내려야 함

자동화 분석 도구를 우회하는 여러가지 기술사용

시스템 지연

- 다수의 리부팅을 기다림
- C&C로 부터 느리게 다운로드

사용자 개입

- 마우스 클릭 & 움직임
- CAPTCHAS

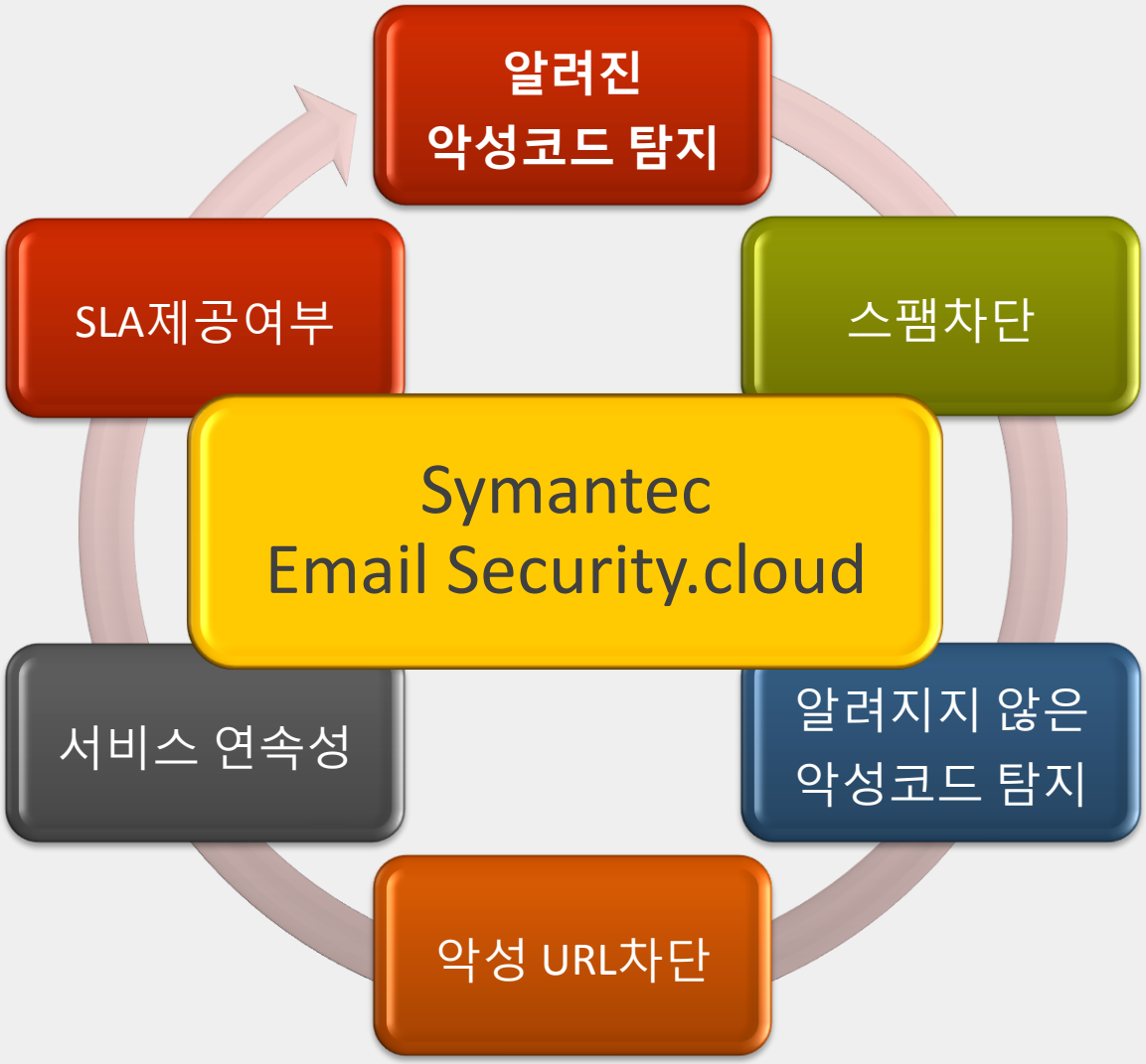
후킹 숨김

- API notification에서 unregister
- 메모리상에서 직접 실행

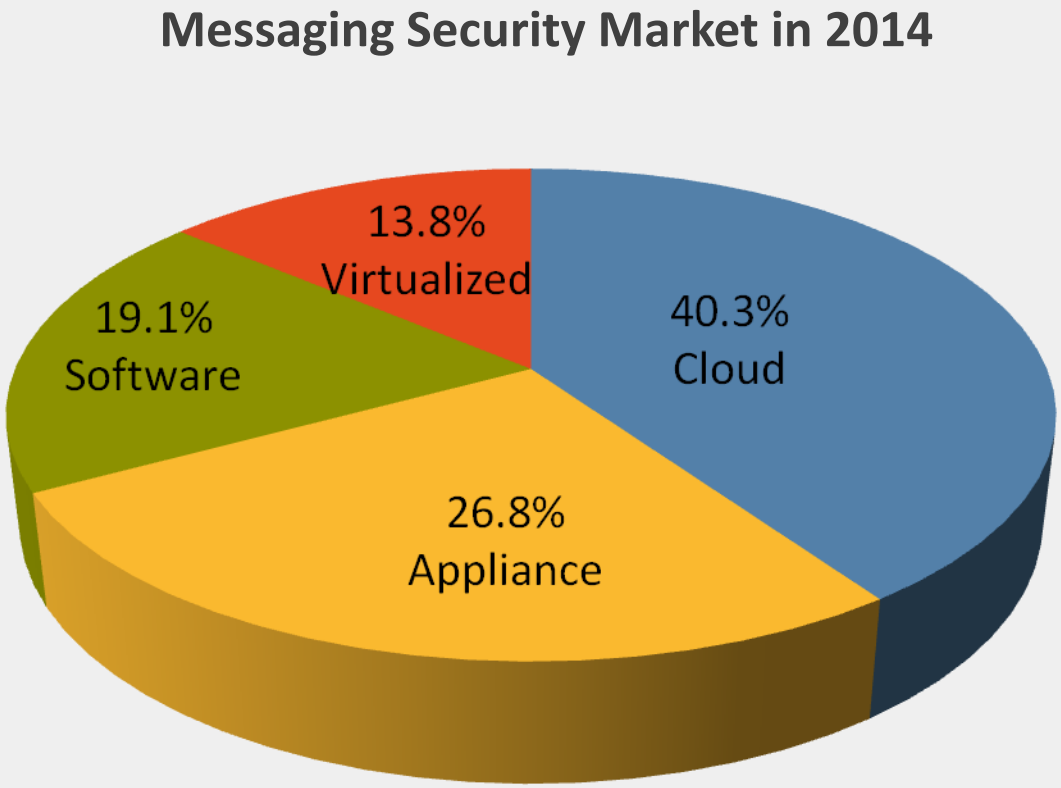
환경 조사

- 실행 파일 점검
- 네트워크 연결 상태 확인

강력한 이메일 보안시 필요한 사항



2014년도 Email 보안 시장 현황

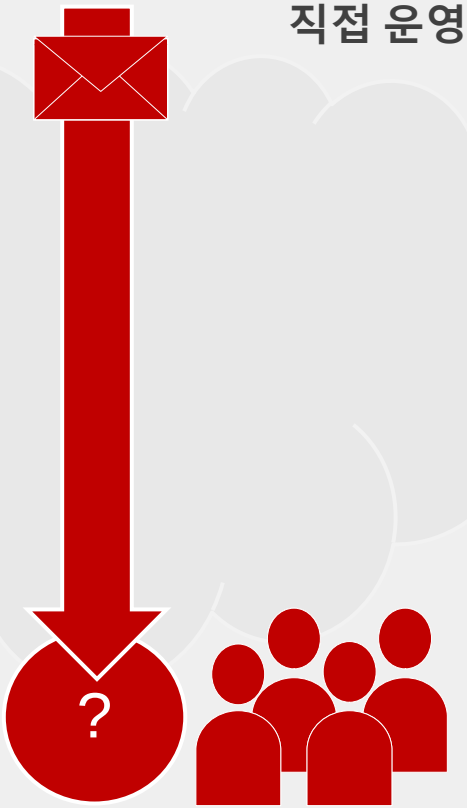


Source: IDC Worldwide Messaging Security 2010-2014

차별점

유입되는 메일의 90%이상은 바이러스, 피싱 및 기타 유해한 것이 포함되어 있음

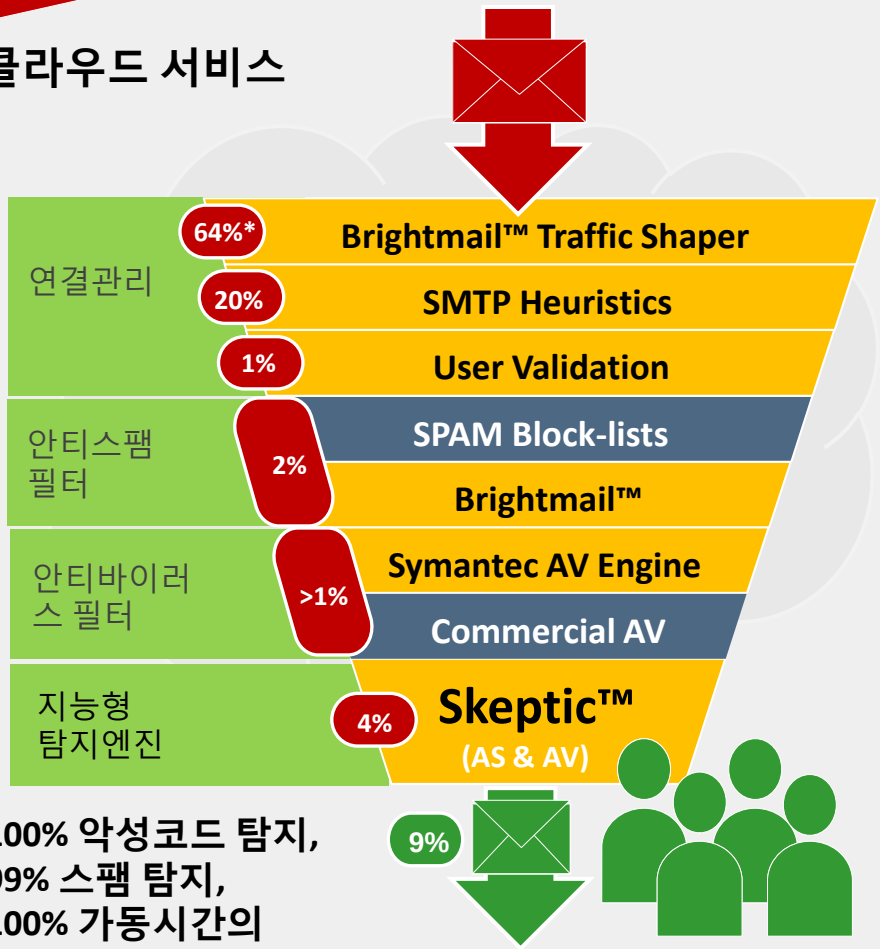
직접 운영 vs 클라우드 서비스



외부로 부터 100% 필터되지 않은 상태로 유입됨

Management Overhead

- Procurement
- Deployment
- Testing
- Performance Tuning
- Policy Administration
- Capacity Planning
- High Availability
- Patching
- Upgrades



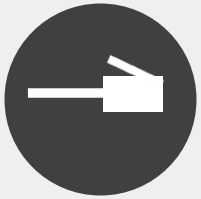
100% 악성코드 탐지,
99% 스팸 탐지,
100% 가동시간의 SLA

Matthew W. Cain, Tom Austin
Gartner Group

"향후 10년 이내의 기업의 이메일 시장은 클라우드 기반이 65%이상을 차지할 것이다."

Email Security.Cloud 주요 특장점

알려진, 신종의
바이러스에 대해 100%
보호



오직 깨끗한 이메일만
내부 네트웍에 유입됨

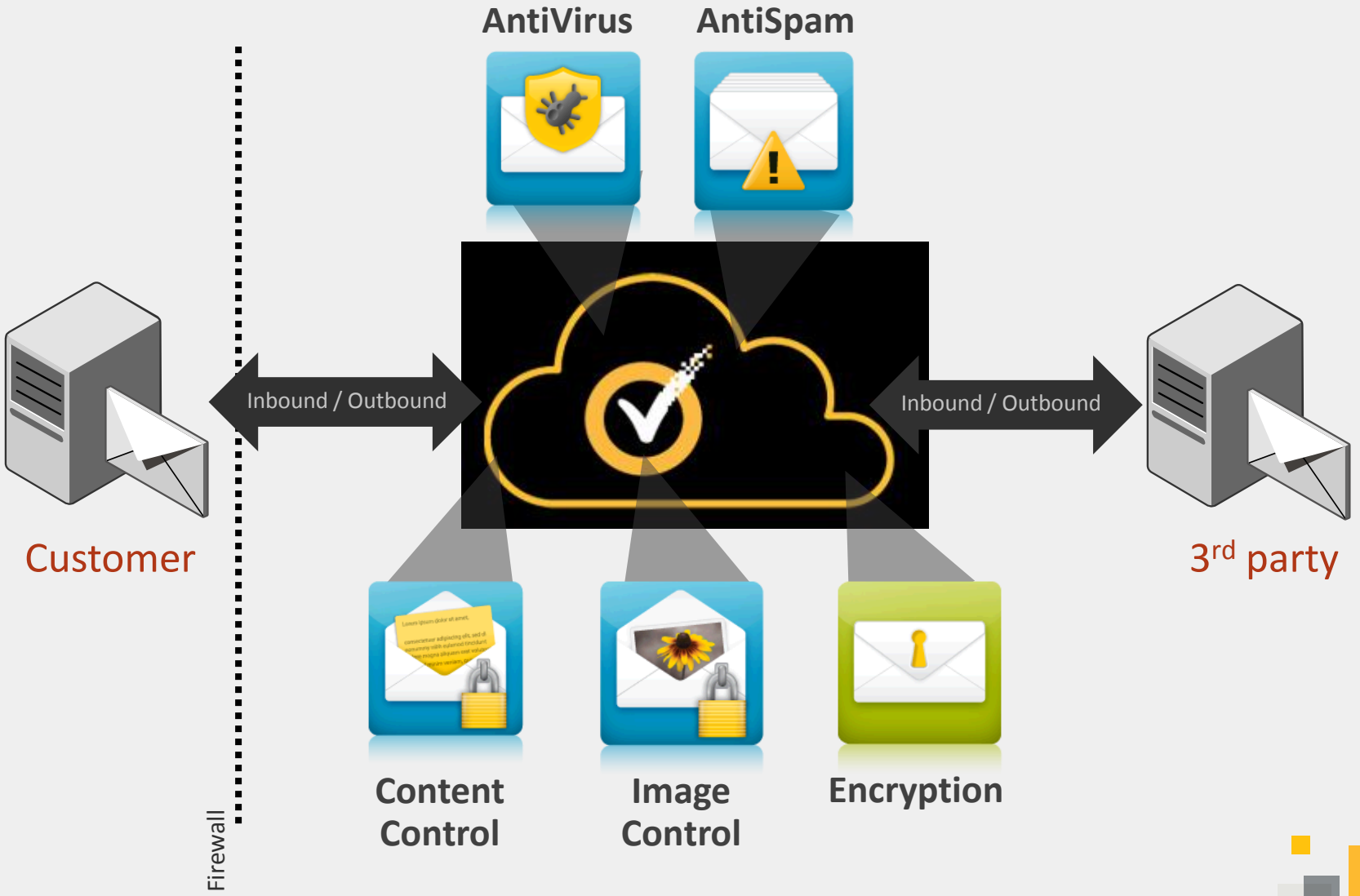
99% 스팸탐지율
0.0003% 미만의 오탐율

글로벌 위협정보 공유

Email 에 첨부된 링크의
위협에 대한 보호

적극적인 성능 레벨에
부합되는 SLA 제공

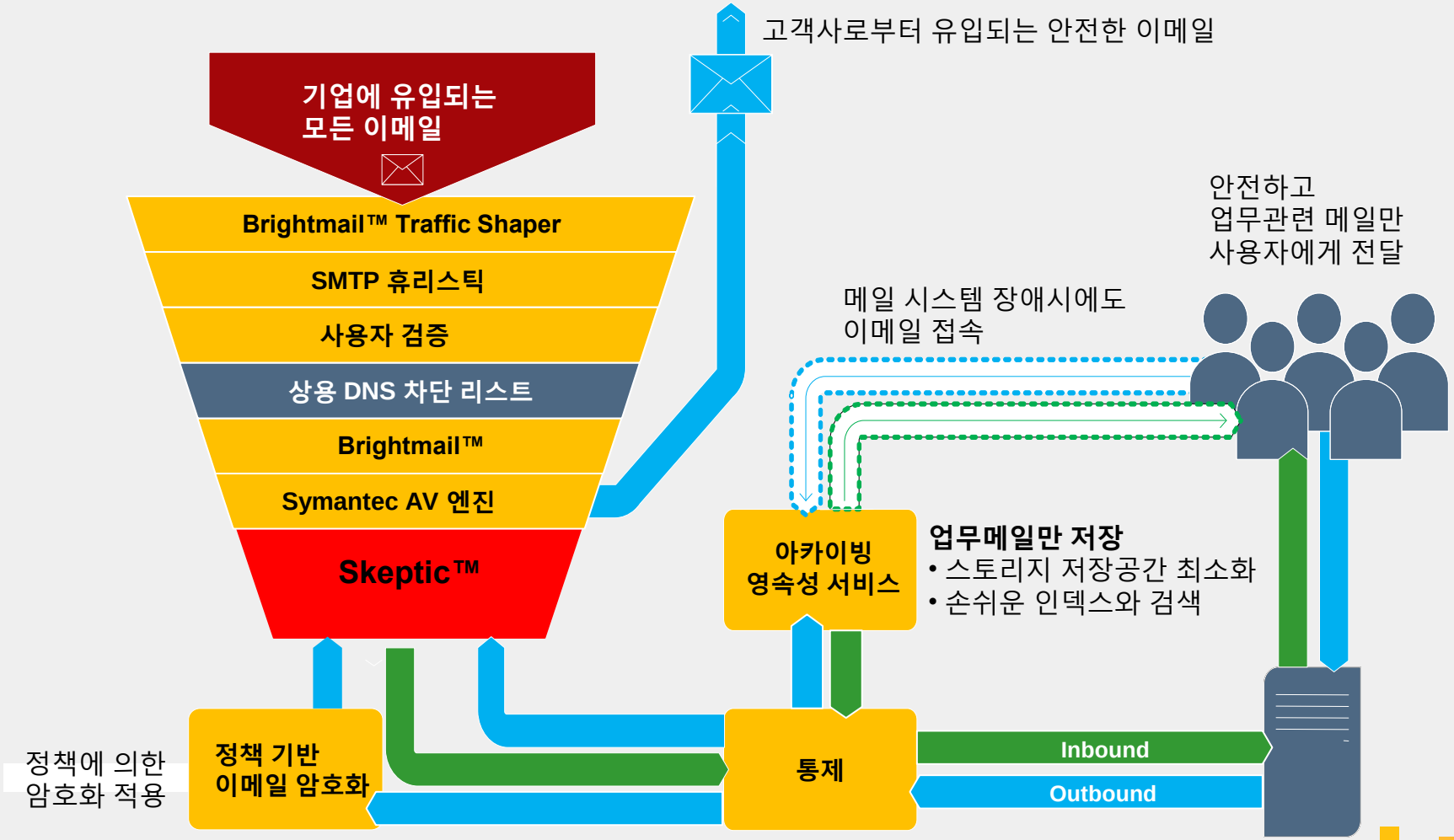
Email Security.cloud 주요기능



Email Security.Cloud 탐지 엔진

Skeptic Technology

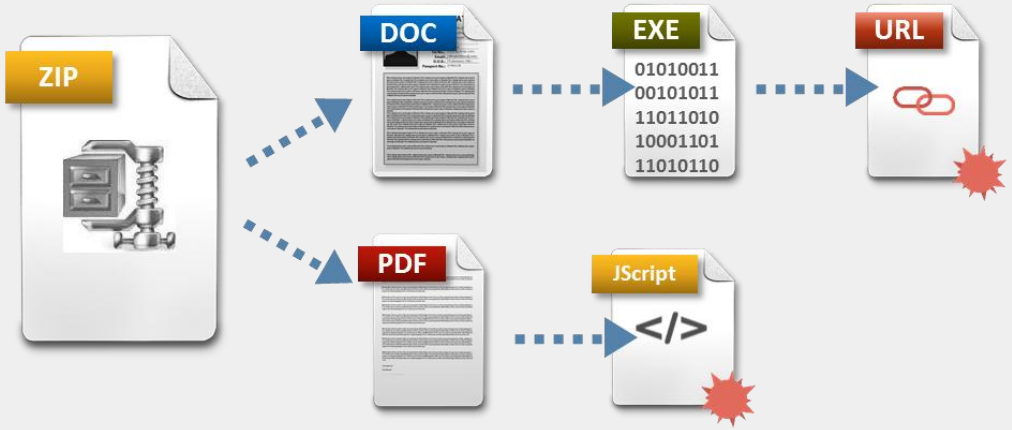
문서 및 URL 탐지를 위한 새로운 엔진 “Skeptic”



Skeptic 엔진이란?

- 문서 형태의 코드 분석 및 탐지 엔진
  - 정교하게 조작된 악성코드에 대한 탁월한 탐지율 제공
  - 문서 내용 중 악의적인 컨텐츠 식별
  - 90개 형식의 파일 타입 지원
- 파일로부터 정보를 추출 후 AV엔진으로 검색 및 Skeptic휴리스틱엔진으로 분석

Example: Zip contains a doc, which contains an EXE, with a malicious URL



Example: PDF contains malicious JavaScript

리다이렉션 추적
http://www.widgetscorp.com.br
/images/fotos/fotos/A/

리다이렉션 추적
http://www.acmecorp.com/ima
ges/logos/Z1/img.php

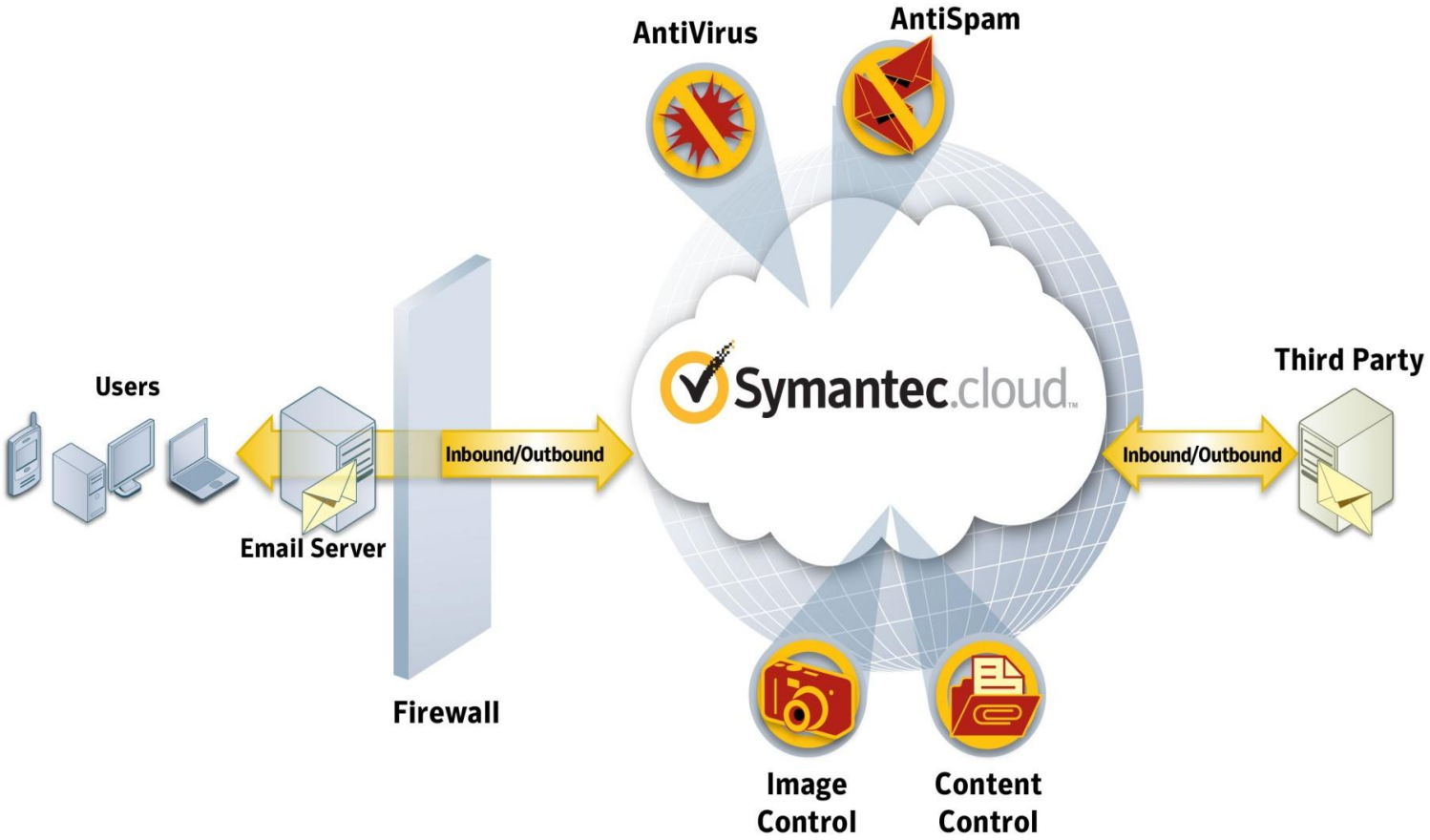
리다이렉션 추적
http://www.acmewidgets.com/c
ontent/home/index.html

- 악성 컨텐츠 발견
- 시만텍 글로벌 인텔리전스 에 내용 업데이트

링크분석
http://ac.me/1234

메일 도착 전에
실시간 차단

Email Security.cloud 구성



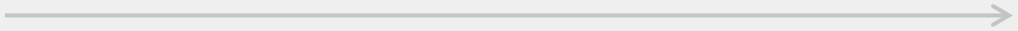
MX 레코드 변경으로 손쉬운 적용

MX lookup 조회(서비스 변경 전)

securityEmail.com MX preference = 20, mail exchanger = mail2.securityEmail.com

securityEmail.com MX preference = 100, mail exchanger = mailedge.securityEmail.com

securityEmail.com MX preference = 10, mail exchanger = mail1.securityEmail.com



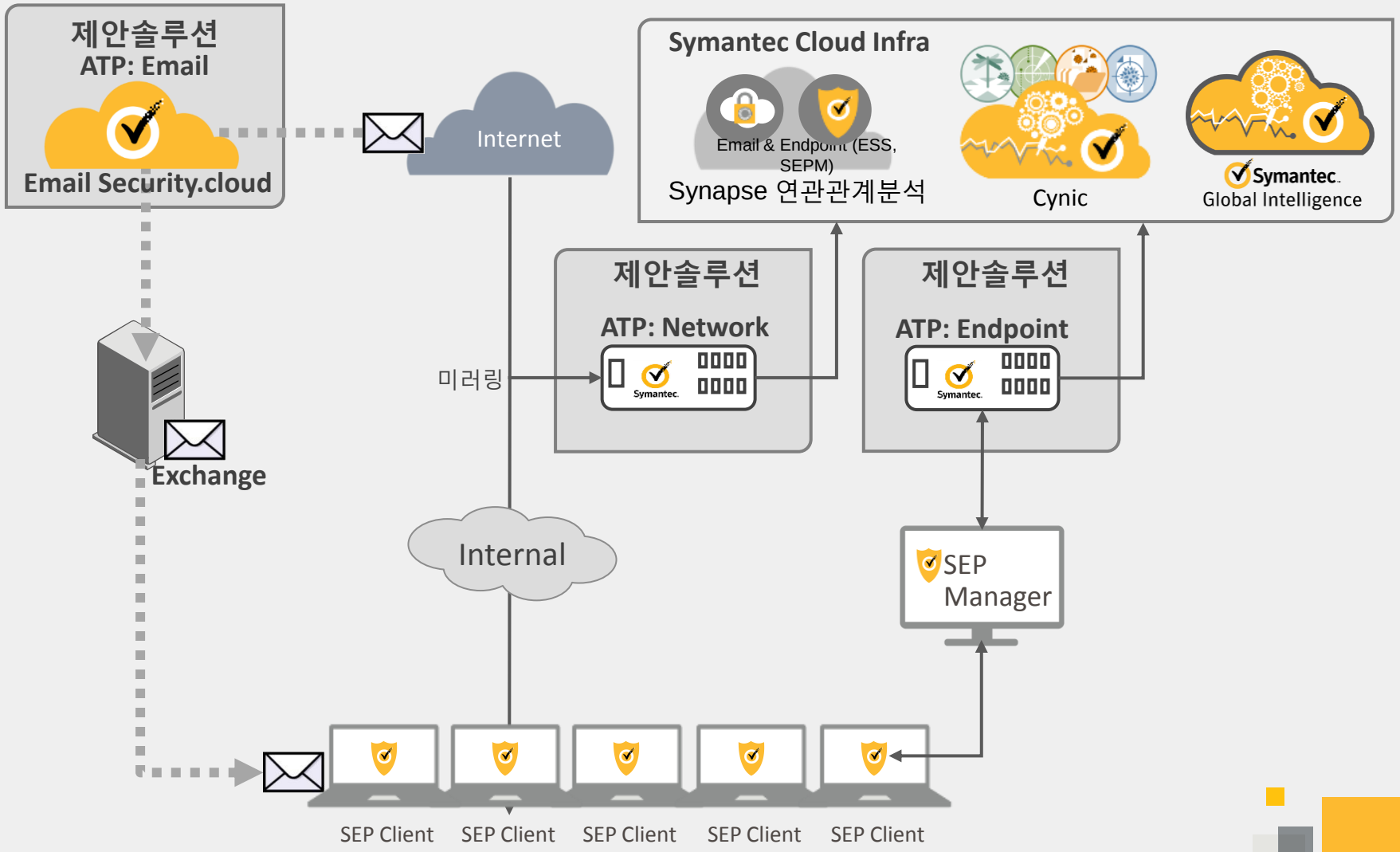
메일발송

admin@securityEmail.com

MX lookup 조회(서비스 변경 후)

kraulife.com MX preference = 10, mail exchanger = cluster6.us.messagelabs.com
kraulife.com MX preference = 20, mail exchanger = cluster6a.us.messagelabs.com

ATP 솔루션 구성


제안솔루션
ATP: Email
Email Security.cloud
Internet
Symantec Cloud Infra
Email & Endpoint (ESS, SEPM)
Synapse 연관관계분석
Cynic
Symantec.
Global Intelligence
제안솔루션
ATP: Network
제안솔루션
ATP: Endpoint
미러링
Exchange
Internal
SEP Manager
SEP Client
SEP Client
SEP Client
SEP Client
SEP Client