OPSWAT

Metascan®

Microsoft® Exchange Server

APT 공격, 신종 및 변종 악성코드 탐지솔루션

[구성 사례]

익스체인지 메일 서버 이메일 보안 연동 방안

Microsoft Exchange Server

OPSWAT Metascan®

■ Metascan 멀티 안티바이러스 스캔 엔진 [한국수력원자력]

[118회] 3초에 하나씩 만들어지는 악성코드, 한국은 공격대상 2위!

입력 2014.12.11 (23:39) | 수정 2014.12.18 (17:51)

<이메일 '첨부파일' 클릭…컴퓨터, 이렇게 털린다!>:

최근 소니 영화사가 해킹을 당하면서 영화가 유출돼 곤욕을 치르고 있습니다. 이번 해킹의 주체가 어디인지는 명확하게 밝혀지지 않았지만 해킹 방법은 관계자의 이메일에 접근하는 방법을 사용했을 것으로 추정하고 있습니다.

보안이 요구되는 내용인 만큼 접근 권한이 있는 사람의 계정을 타깃으로 했을 것이라는 건데요. 이른바 '사회공학' 기법을 적용해 친분이 있는 사람 또는 업무상 중요한 메일인 것처럼 접근하는 방법입니다. 공격을 하는 입장에서는 보안이 강화된 시스템을 뚫는 것보다 사람에게 접근하는게 오히려 쉬울 수 있다는 것이 최근 동향이라고 합니다.

사람에게 접근할 때는 첨부파일 등으로 악성코드를 심어넣게 되는데요. 한 보안업체가 감지하는 공격 데이터를 보면 이 악성코드는 거의 3초에 하나씩 새롭게 만들어지고 있다고 합니다. 전 세계적으로 하루에 쏟아지는 변종 악성코드는 20만개 정도 된다고 할 정도인데요. 이는 악[illegible]으로 만들 수 있기 때문입니[illegible]

이런 변종 악성코드의 주 공[illegible] 95%의 기업, 기관들이 공격[illegible] 는 것이 미국 다음으로 공격[illegible]

한수원 직원 3명 중 1명, 악성코드 메일 받아

조석 사장 "지속적인 공격 시도 탐지돼"

퇴직한 한국수력원자력 직원 명의로 악성코드 300여 종이 들어있는 대량 메일이 지난 9일 한수원 임직원뿐만 아니라 전체 직원의 3분의 1에 해당하는 3500여 명이 받은 것으로 조사됐다.

이메일에 포함된 악성코드를 사전 탐지
외부의 위협으로 보호

■ Metascan 멀티 안티바이러스 스캔 엔진 [소니픽쳐스]

[경제투데이 이주현 기자] 해외 영화제작사 '소니 픽처스' 해킹사건과 '한국수력원자력'의 발전소 도면 유출 사건 등이 '스피어 피싱(Spear-phishing)'에 의해 발생된 것으로 밝혀졌다.

특정 대상을 목표로 정밀하게 해킹하는 수법인 스피어 피싱은 최근 사이버 표적 공격의 90%를 상회할 정도로 이용되고 있다.

전문가들은 이러한 스피어 피싱을 막으려면 모의 훈련 및 다중 보안 시스템 구축 등이 필요하고 있다.

11일 보안업계에 따르면 최근 특정인이나 특정 기업을 대상으로 정보를 빼내는 스피어 피싱 수법으로 자주 이용되고 있다.

스피어 피싱은 특정인이나 특정 기업에 악성코드를 심은 이메일을 보내 정보를 빼내는 해킹 수법이다. 특정 대상을 정해 작살(Spear)로 찍듯 정밀 타격하는 방식으로, 기존 불특정 다수를 겨냥한 공격보다 성공률이 높다.

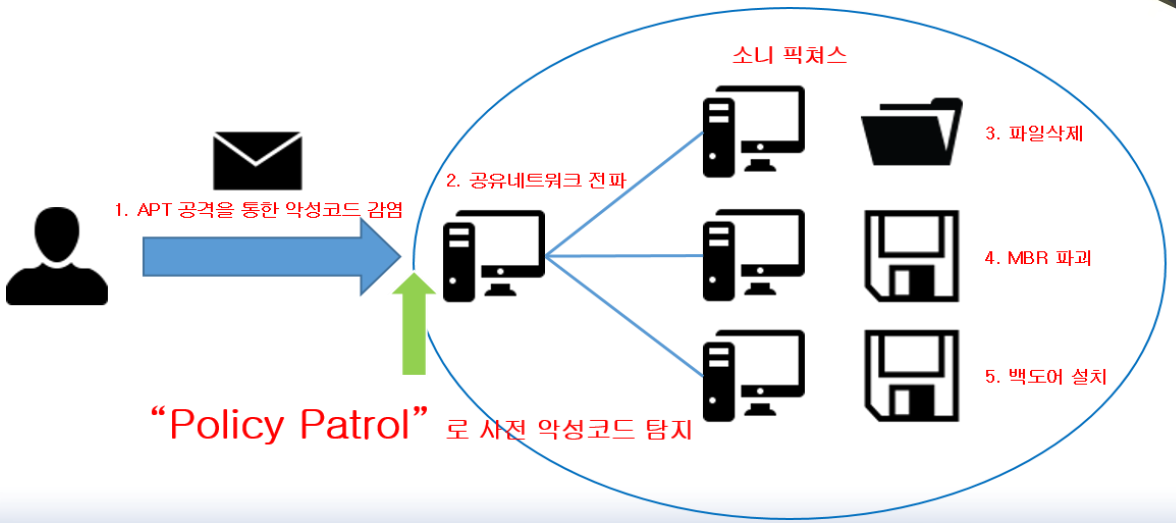
소니픽쳐스, 해킹 수습에만 1천500만弗 써

손경호 기자 sontech@zdnet.co.kr 2015.02.05 / PM 00:38 소니픽쳐스 , 소니픽쳐스 해킹

소니픽쳐스엔터테인먼트가 지난해 말 내부 시스템 해킹에 따른 임직 정보유출, 영화 자료 유출 등을 수습하기 위해 쓴 비용이 약 1천 (약 163억2천450만원)에 달하는 것으로 나타났다.

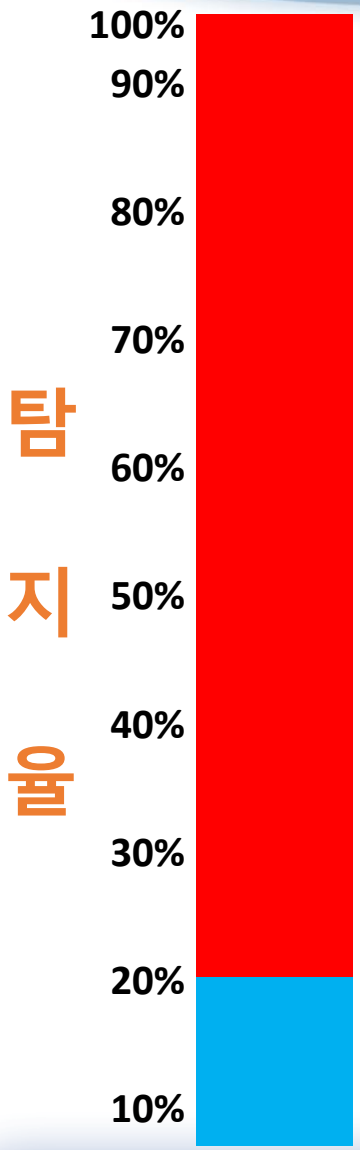
발표한 회계연도상 2014년 3분기(10월~12월) 소니픽쳐스는 "사이버 공격으로 인한 를 입었다"며 "관련 조사 및 예방을 매출하락 등으로 영업이익이 지 난해 다"고 밝혔다.

소 잃고 외양간 고치기?
Policy Patrol를 이용한 사전 탐지



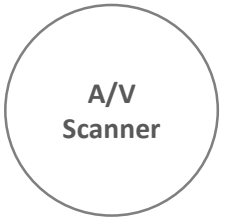
싱글 안티바이러스의 한계점

탐지 범위 제한적
탐지율 저조!



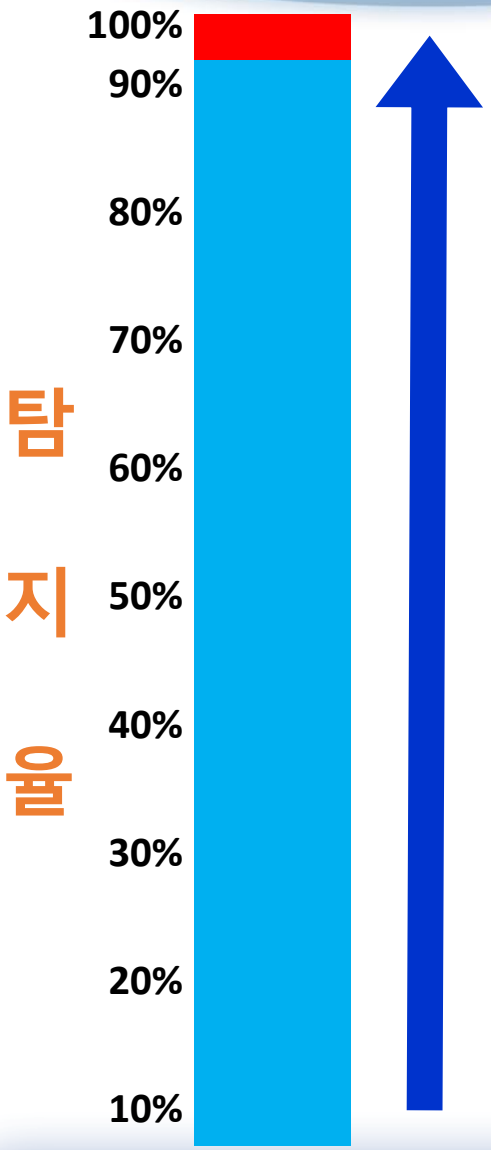
1개 안티바이러스
엔진의 탐지 한계

3억 4천만개
[340,000,000]
2015년 3월 현재

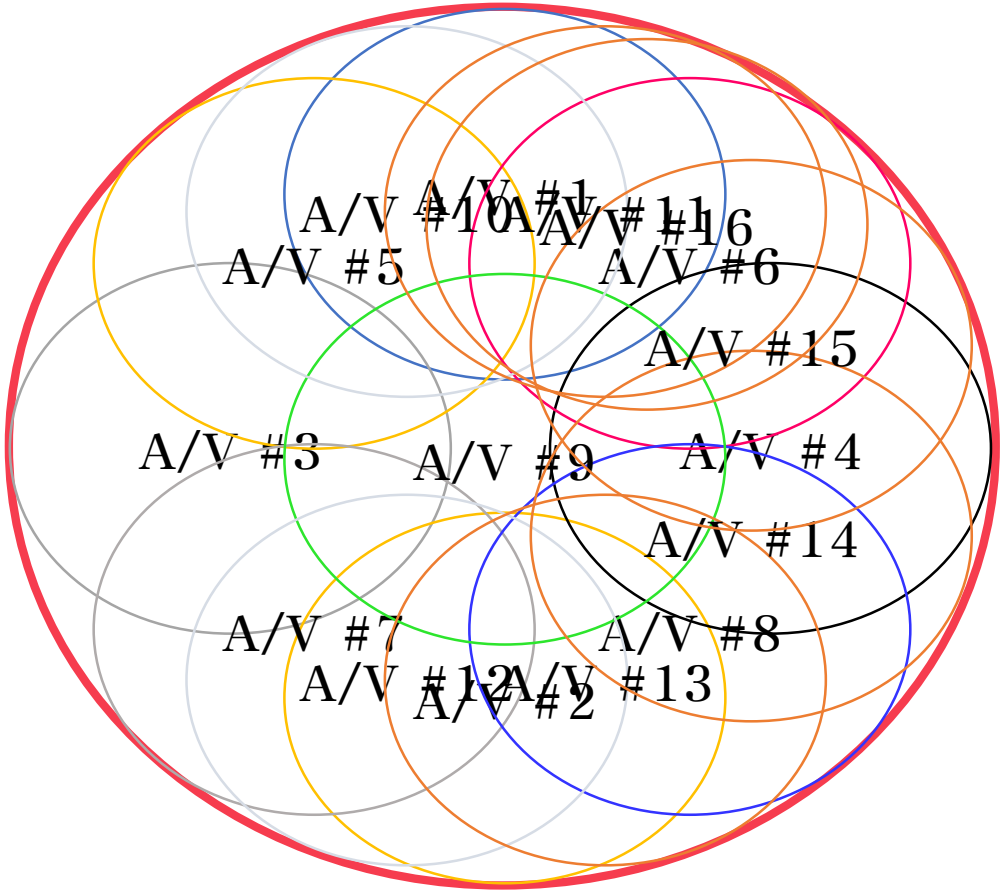


안티바이러스 엔진
1개

멀티안티바이러스의 장점



탐지 범위
탐지율 급속 증가!



현재까지
악성코드
전체

3억 4천만개
[340,000,000]
2015년 3월 현재

A/V
Scanner

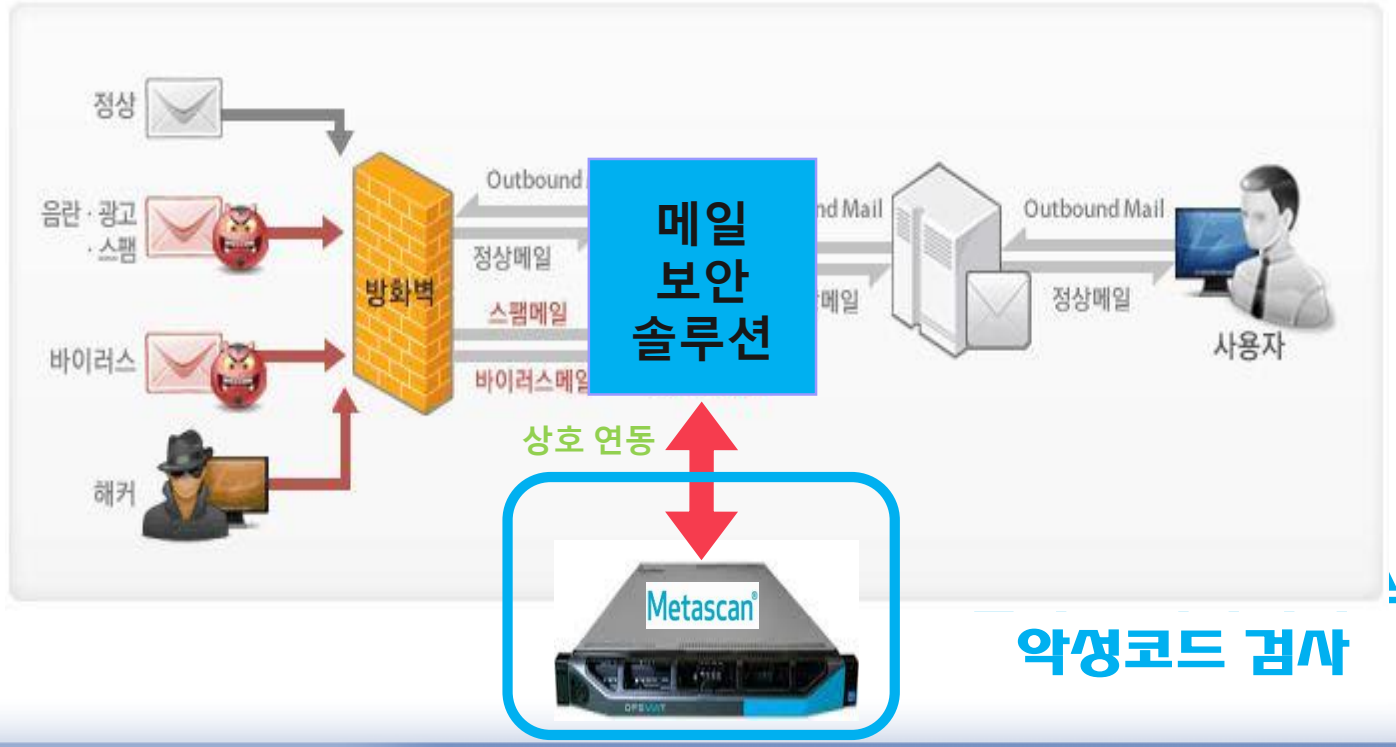
■ Metascan 구성안 [메일 보안 게이트웨이]

이메일에 대한 악성코드 검사

- 송수신 이메일에 대한 악성코드 검사 수행
- 글로벌 30개 안티바이러스 엔진 동시 검사 수행

메일 보안솔루션 연동

Metascan =



■ Metascan 구성안 [익스체인지 메일서버(Exchange Mail Sever)]

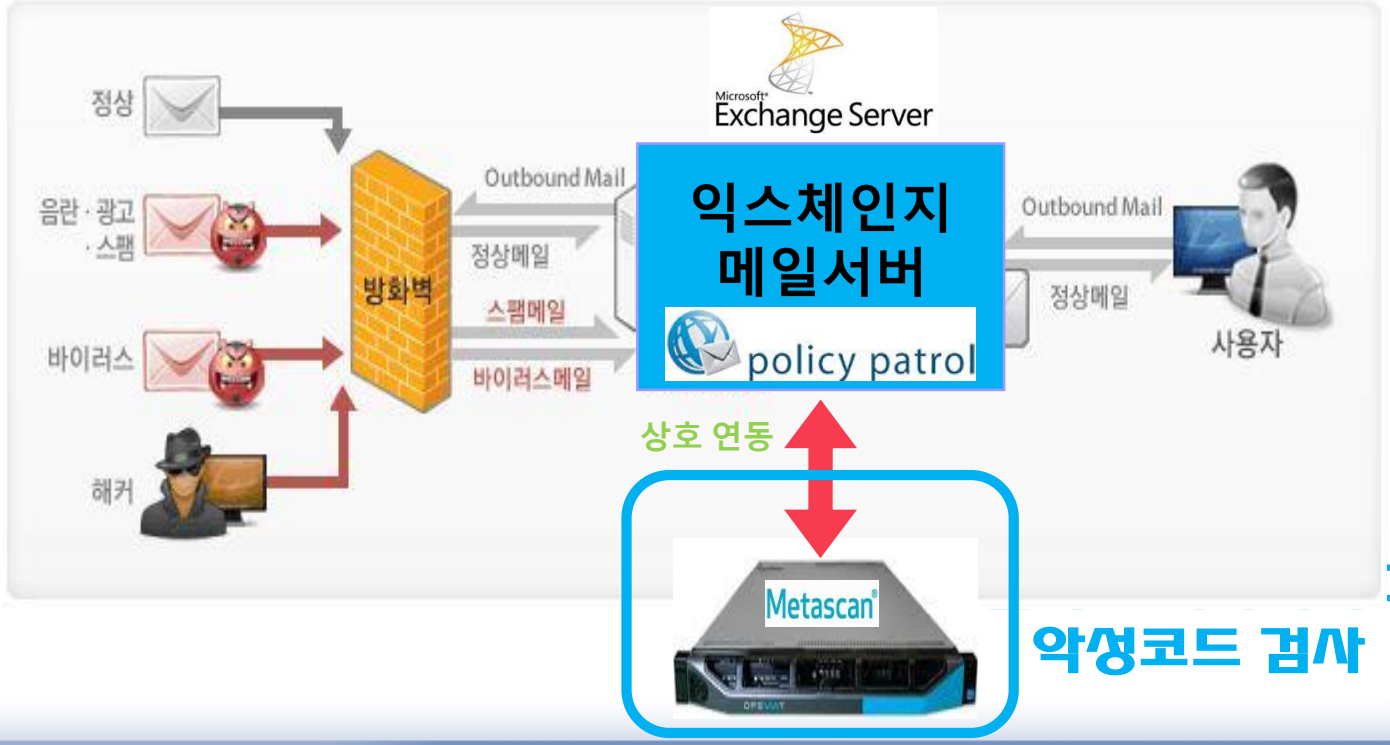
익스체인지 메일서버 연동

첨부파일 악성코드 검사

Metascan =

이메일에 대한 악성코드 검사

- 송수신 이메일에 대한 악성코드 검사 수행
- 글로벌 30개 안티바이러스 엔진 동시 검사 수행



■ Metascan 구성안 [익스체인지 메일서버(Exchange Mail Sever)]

APT 공격, 신종 및 변종 악성코드 탐지 솔루션

수신

송신

Microsoft Exchange Server

policy patrol

익스체인지
메일서버

상호 연동

첨부 파일

OPSWAT Metascan®

이메일로
송수신되는
각종 첨부파일에 대한
악성코드 검사 수행

글로벌 30개
안티바이러스 스캔

Ahnlab, ESET, Avira, Bitdefender
Kaspersky, nProtect, AVG
Symantec, MacAfee, F-Secure
MicroSoft, Trend Micro

메일서버 연동
[익스체인지]

■ Metascan 구성안 [익스체인지 메일서버(Exchange Mail Sever)]

수신메일
첨부파일

멀티 안티바이러스 스캔
엔진 서버

송신메일
첨부파일

전송

패턴검사

글로벌 30개 이상
안티 바이러스 엔진

패턴검사

동시에!
멀티 안티바이러스 스캔 검사

additional
anti-malware
engines

■ Metascan 구성안 [익스체인지 메일서버(Exchange Mail Sever)]

APT 공격, 신종 및 변종 악성코드 탐지 솔루션

APT 공격

수신

신종, 변종 악성코드

송신

탐지

상호 연동

첨부 파일

익스체인지 메일서버

OPSWAT

Metascan®

이메일로
송수신되는
각종 첨부파일에 대한
악성코드 검사 수행

글로벌 30개
안티바이러스 스캔

Ahnlab, ESET, Avira, Bitdefender
Kaspersky, nProtect, AVG
Symantec, MacAfee, F-Secure
MicroSoft, Trend Micro

메일서버 연동
[익스체인지]

■ Metascan 구성안 [익스체인지 메일서버(Exchange Mail Sever)]

패턴분석

동적분석

Microsoft Exchange Server

Exchange
메일 서버

이메일로
송수신되는
각종 첨부파일에 대한
악성코드 검사 수행

상호 연동

첨부 파일

OPSWAT Metascan®

글로벌 30개
안티바이러스 스캔

Ahnlab, ESET, Avira, Bitdefender
Kaspersky, nProtect, AVG
Symantec, MacAfee, F-Secure
MicroSoft, Trend Micro

메일보안 솔루션, 메일서버 연동

상호 연동

파일전송

FireEye
Next Generation Threat Protection

FORTINET

악성코드 동적분석
샌드박스

GFI

ThreatAnalyzer

NORMAN

BlueCoat

데모

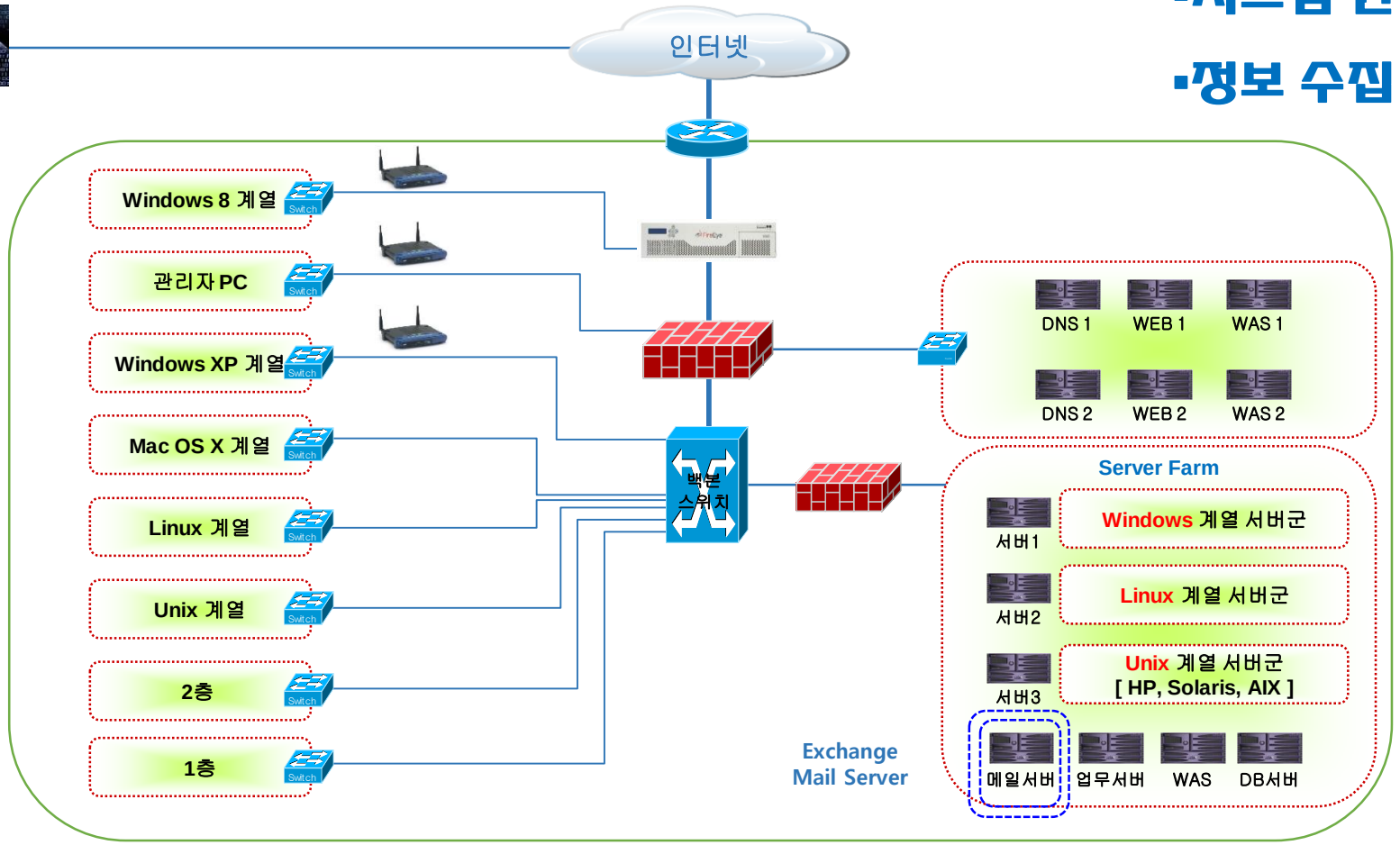
[시연 1]

데모 시연 - 1 [이메일 공격]

※ 스피어 피싱
[Spear Phishing]

- 시스템 권한 획득
- 정보 수집 및 점령

공격자



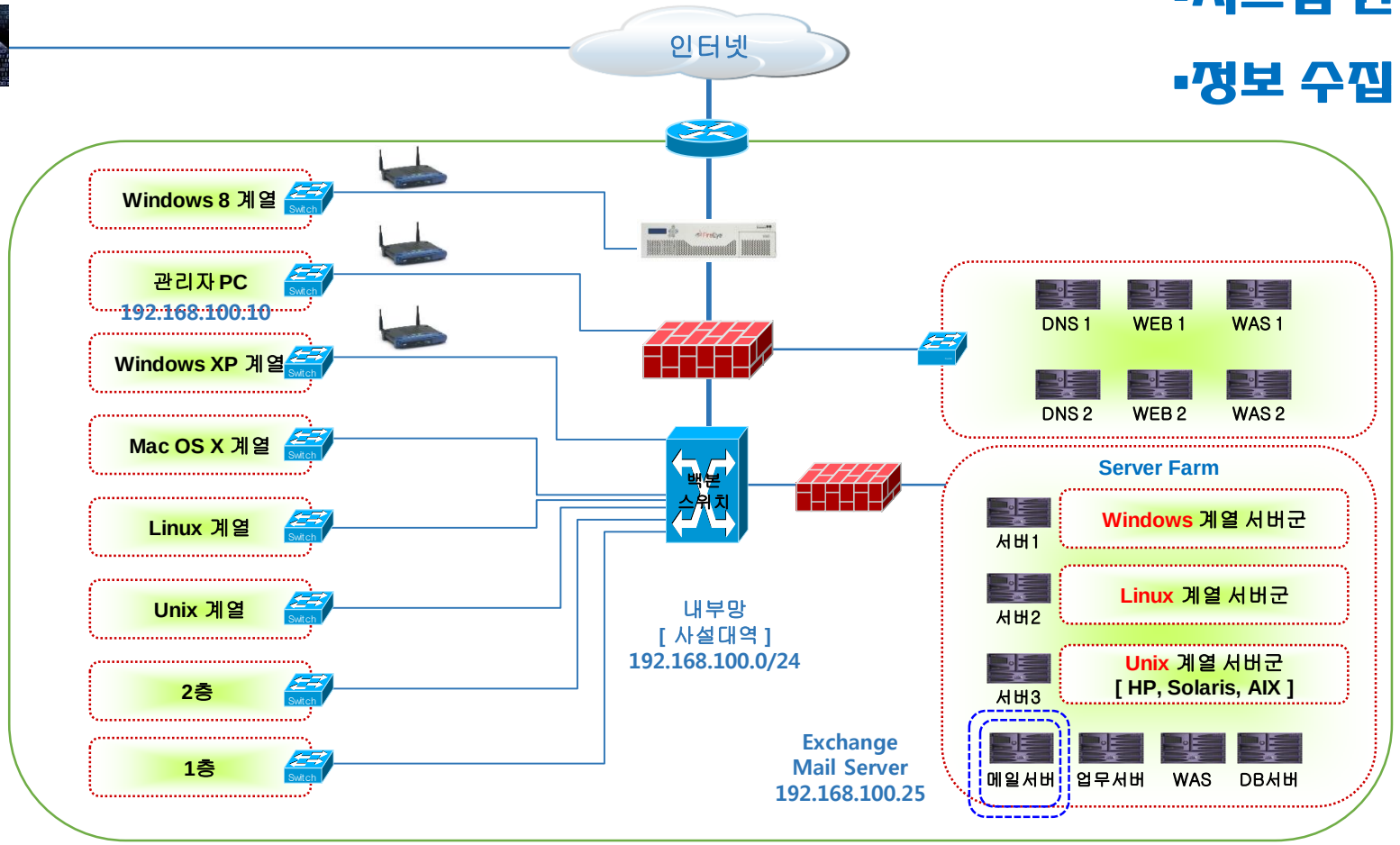
데모 시연 - 1 [이메일 공격]

※ 스피어 피싱
[Spear Phishing]

- 시스템 권한 획득
- 정보 수집 및 점령

공격자

200.200.10.200



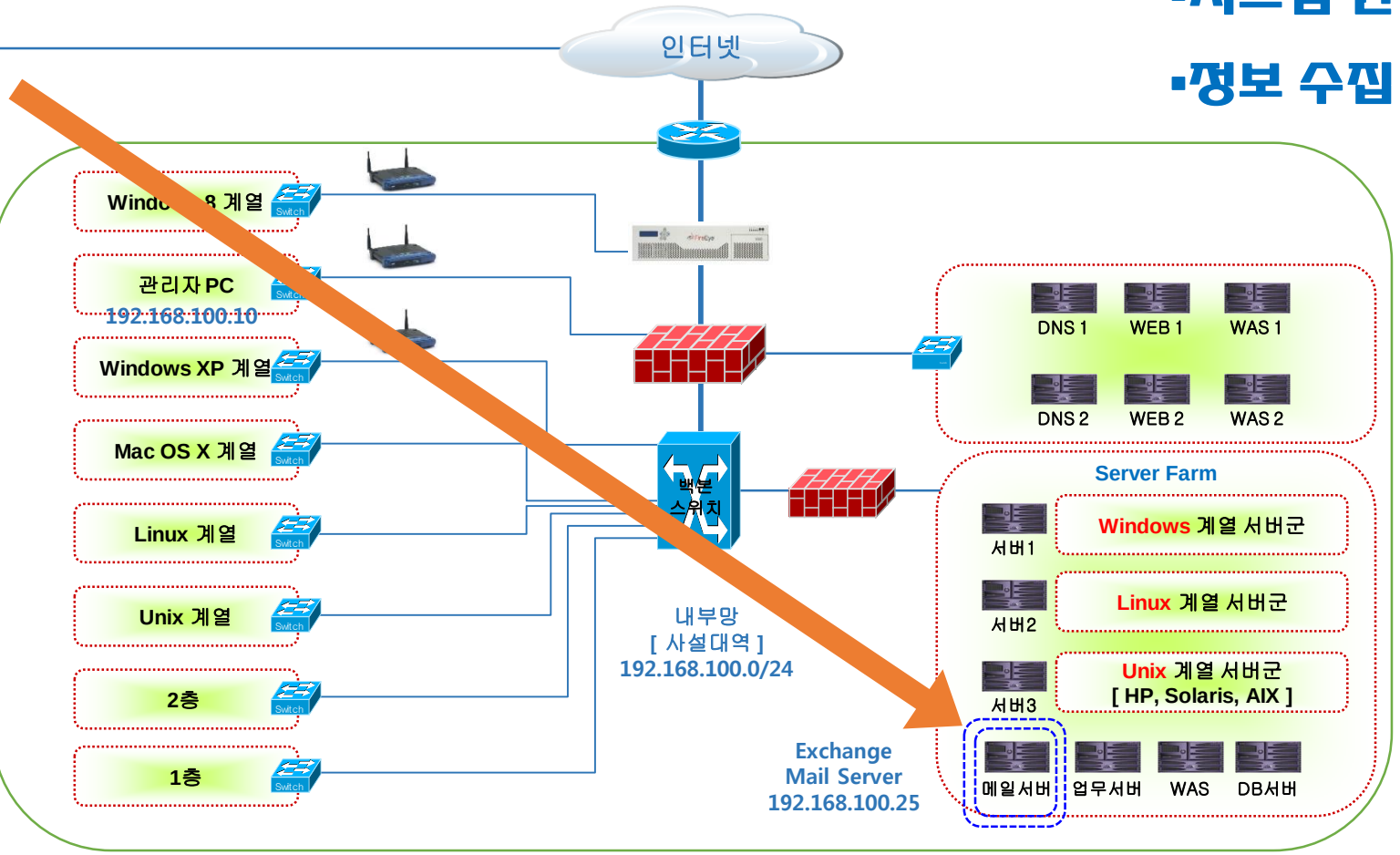
데모 시연 - 1 [이메일 공격]

※ 스피어 피싱
[Spear Phishing]

- 시스템 권한 획득
- 정보 수집 및 점령

공격자

200.200.10.200



데모

[시연 2]

데모 시연 - 2 [이메일 공격]

비트코인 요구하는 랜섬웨어 급증

2013년 12월 10일 (화) 03:31:42

컴퓨터나 파일을 인질로 잡고 비트코인을 요구하는

파이낸셜타임스는 해커들이 컴퓨터나 파일을 통짜
후 사이버 몸값을 요구한다고 보도했다.

지난 3분기 300만 건에 달하는 랜섬웨어 사고가
일이 암호화돼 접근할 수 없게 된 피해자는 수백
몸값으로 추적이 어려운 비트코인을 원한다. 가치
다.

정보보호를 담당하는 영국 국립 범죄부는 지난달
생됐는데 이 메일에 첨부된 파일을 열면 컴퓨터가
된다고 경고했다.

미국 매사추세츠 크립토로커에 감염된 후 사진과
한 일을 보고했다.

비트코인의 익명성이 지하경제의 새로운 결제수단
1500만~4500만 달러 규모의 마약 등 밀수거래 시
다. 비트코인은 온라인 암시장인 실크로드에서 마
였다.

기존 '크립토락커' 랜섬웨어 기능에 디도스 기능 추가_
코드삽입 방식으로 디도스 기능 활성화해 백신 진단 우회 시도_
PC사용자는 보안수칙 생활화, IT관리자는 보안관리 강화 등 필요

[보안뉴스 김경애] 최근
랜섬웨어의 일종인
Locker)의 변종이 랜섬
스(DDoS, Distributed
분산서비스거부) 공격
로 밝혀져 이용자들의
된다.

안랩(대표
http://www.ahnlab.cor
에 발견된 디도스 기능
파일 형태로 만들어지는
사용자의 인터넷 브라우
방식(injection 방식)으
않아 악성파일을 잡아내

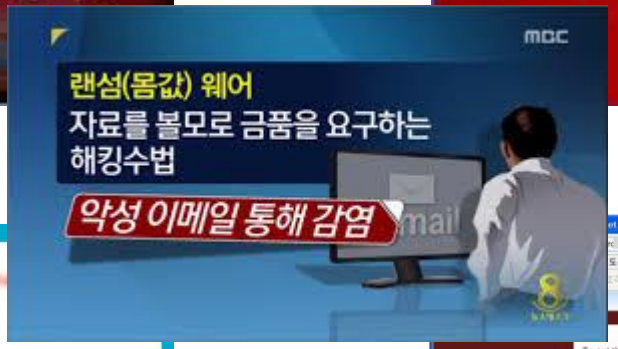
해당 악성코드는 국내 유
버전'의 기능을 동일하
한다. 여기에 'Nitol'이라
구동시킨다. 해당 기능(
사용되는 서버)에 접속하
도스 공격을 수행한다.

'변종 랜섬웨어' 확산…백신 깔아놔도 무용지물

강은성 기자 esther@dt.co.kr | 입력: 2015-05-03 19:09

컴퓨터 내 중요 자료를 암호화 해놓고 이를 인질 삼아 돈을 요구하는 악성코드 '크립토락커 랜섬웨어'가 분산서비스거부(DDoS; 이하 디도스) 공격 기능까지 갖춘 변종 형태로 퍼지고 있다. 변종이기 때문에 보안 백신으로 잡아낼 수 조차 없다. 랜섬웨어 유포에는 한국

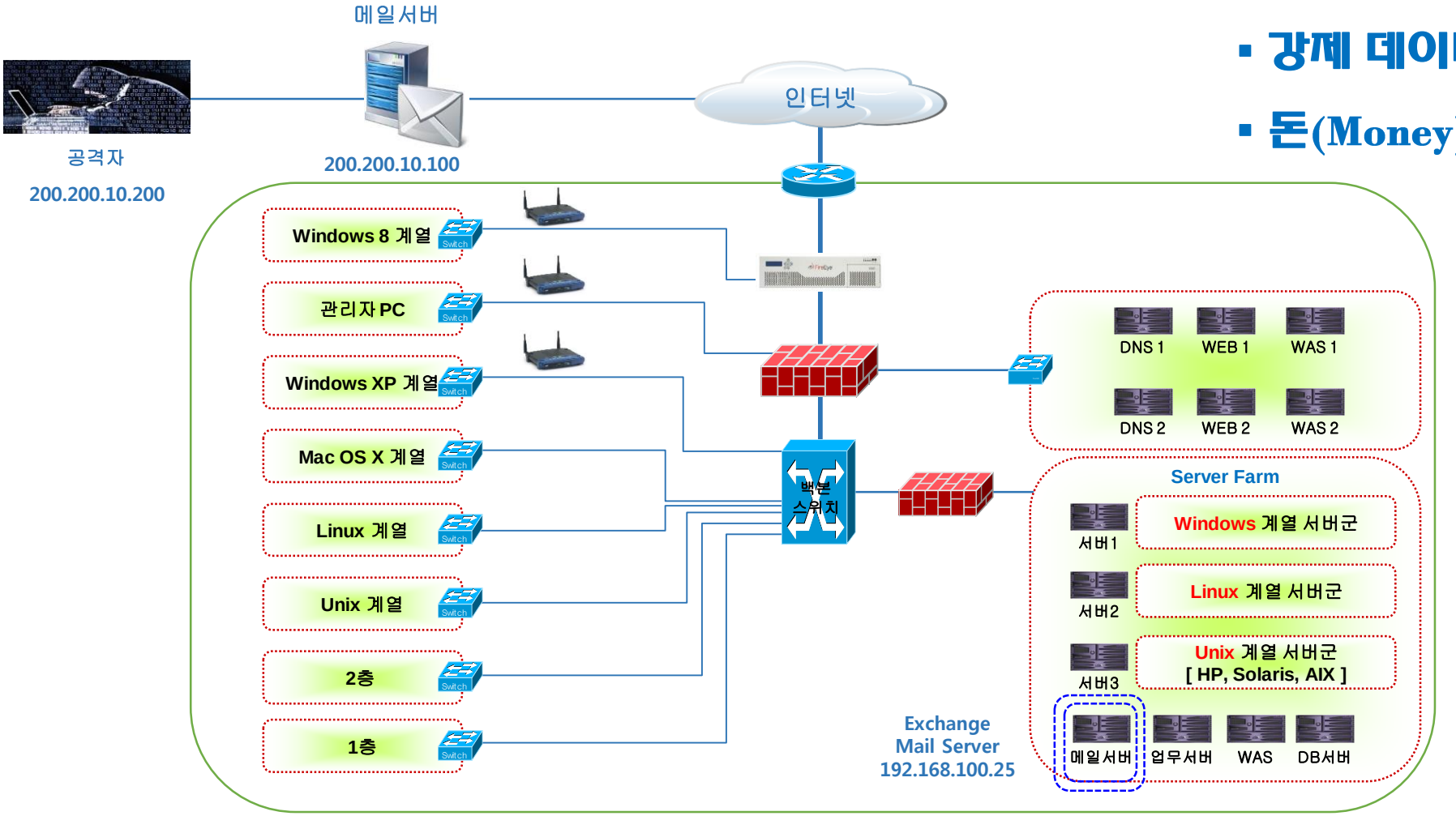
데모 시연 - 2 [이메일 공격]



데모 시연 - 2 [이메일 공격]

※ 랜섬웨어
[Ransomware]

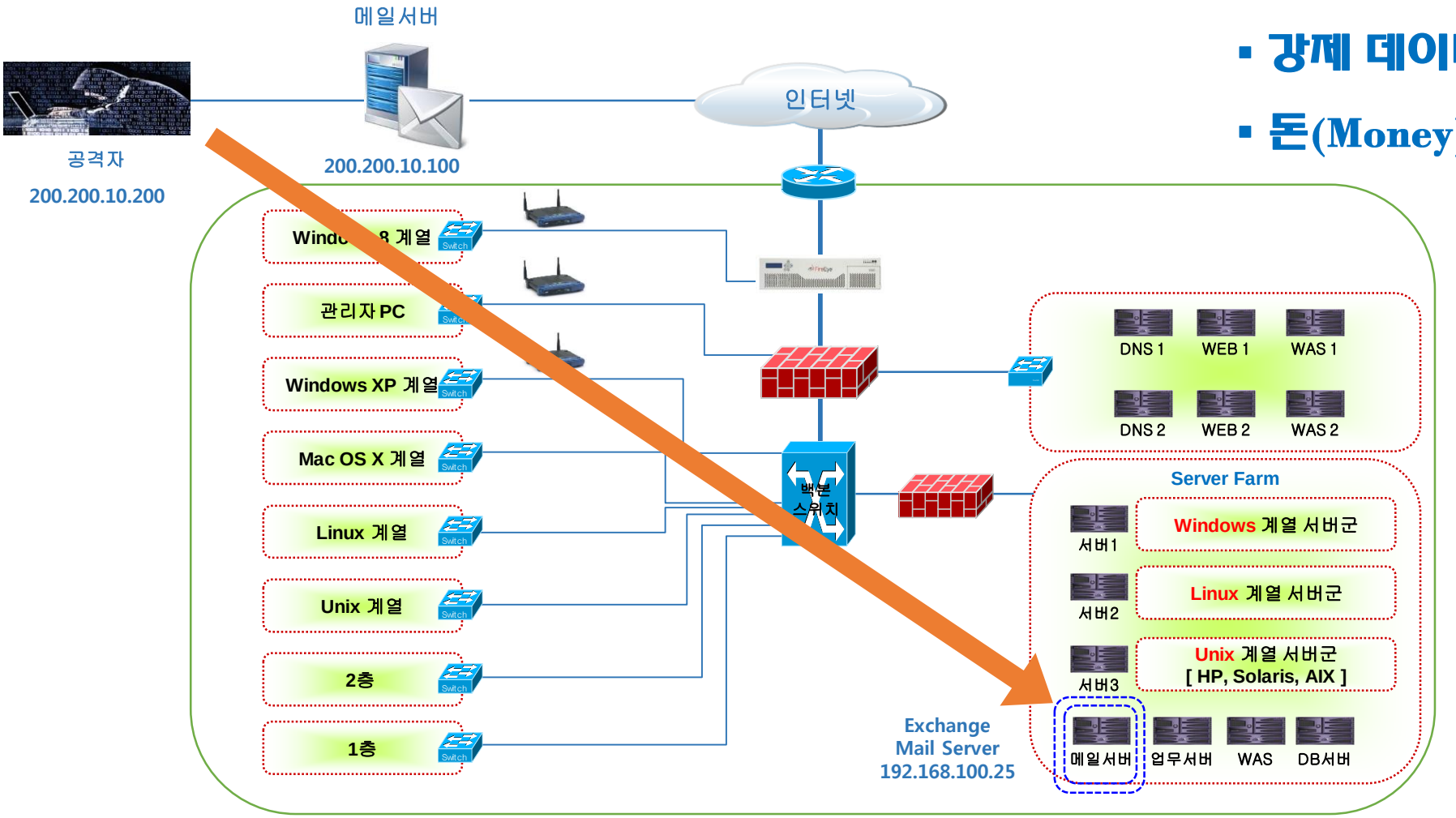
- 강제 데이터 암호화
- 돈(Money) 요구



데모 시연 - 2 [이메일 공격]

※ 랜섬웨어
[Ransomware]

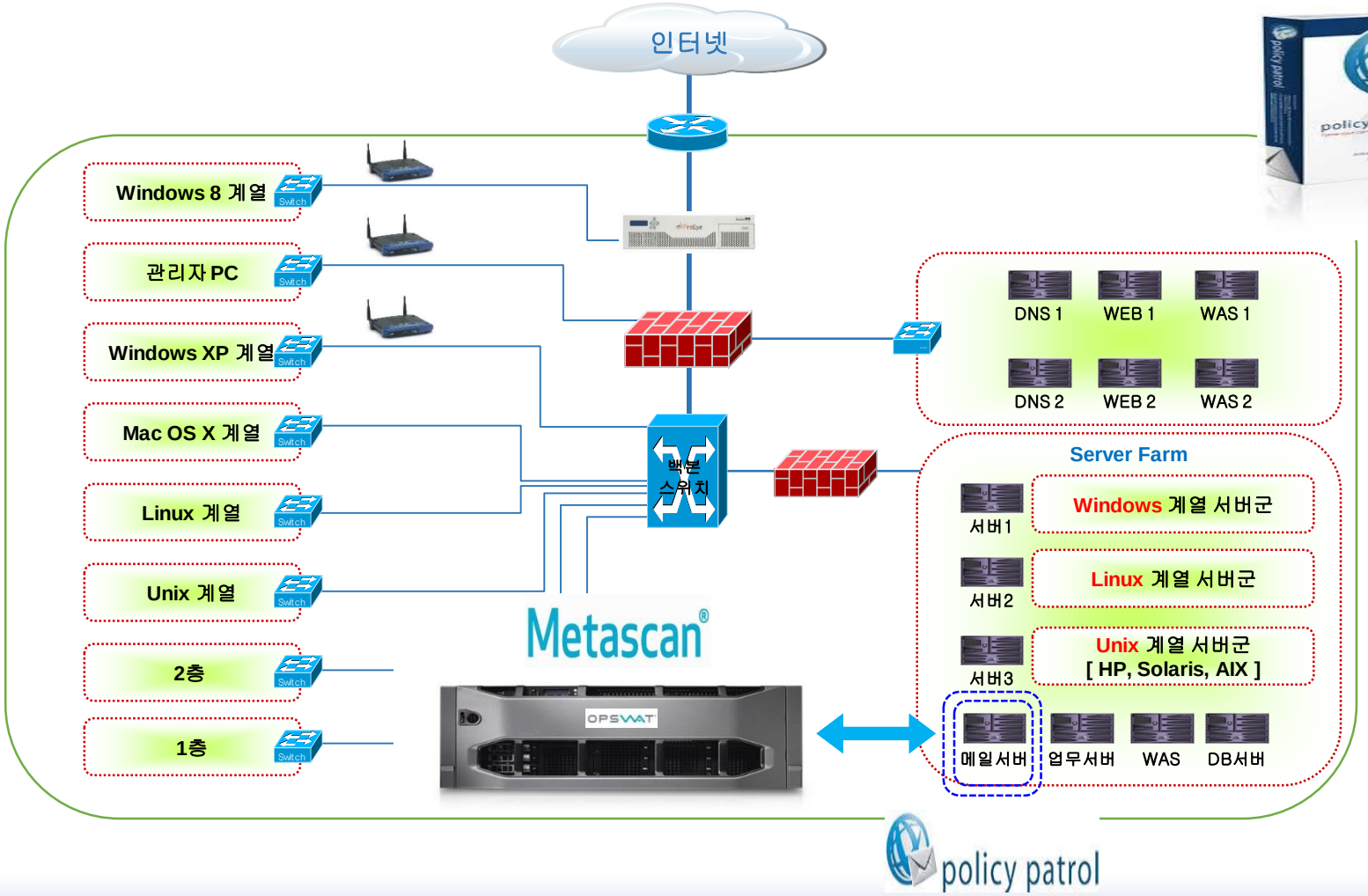
- 강제 데이터 암호화
- 돈(Money) 요구



데모

[시연 3]

데모 시연 - 3 [이메일 보안]



데모 시연 - 3 [이메일 보안]

※ 스피어 피싱
[Spear Phishing]

※ 랜섬웨어
[Ransomware]

공격시연

공격자
200.200.10.200

메일서버
200.200.10.100

인터넷

Windows 계열
관리자 PC
Windows XP 계열
Mac OS X 계열
Linux 계열
Unix 계열
2층
1층

백본 스위치

Metascan®

DNS 1 WEB 1 WAS 1
DNS 2 WEB 2 WAS 2

Server Farm
서버1 Windows 계열 서버군
서버2 Linux 계열 서버군
서버3 Unix 계열 서버군 [HP, Solaris, AIX]
메일서버 업무서버 WAS DB서버

Exchange Mail Server
192.168.100.25

policy patrol

데모 시연 - 3 [이메일 보안]

Microsoft Exchange Server

익스체인지
메일서버 보안

첨부 파일에 대한
30개 멀티 안티바이러스
스캔 검사

수신

송신

policy patrol

Microsoft Exchange Server

익스체인지
메일서버

상호 / 연동

첨부 파일
전송

OPSWAT Metascan®

송신 메일
수신 메일
모든 첨부 파일
스캔 검사

데모

[시연 4]

데모 시연 - 4 [이메일 보안]

동적분석

Microsoft Exchange Server

익스체인지
메일서버 보안

수신

송신

GFI NORMAN
ThreatAnalyzer BlueCoat
FireEye FORTINET
Next Generation Threat Protection

악성코드 동적분석
샌드박스

상호 | 연동

policy patrol

Microsoft Exchange Server

익스체인지
메일서버

상호 / 연동

첨부 파일
전송

OPSWAT
Metascan®

첨부 파일에 대한
30개 멀티 안티바이러스
스캔 검사