First Victim 포기할 것인가?

지능형 보안 위협에 대한 최선의 대응 방안

More security,
More freedom

NES 2016

안랩 / 정광우 차장

AhnLab

Contents

More security,
More freedom

AhnLab

01. 최신 보안 위협 동향

More security,
More freedom

AhnLab

Incidents

AhnLab

2009 7·7 DDoS

2011 3·4 DDoS

2011 N금융기관 해킹 사고

2011 N포털 개인정보 유출

2012 J언론 해킹사고

알려지지 않은 신종 악성코드가 침해사고에 핵심적인 역할 수행

- 특정 대상에 대한 표적 공격
- 최신 보안 솔루션을 구축·운영 중인 기업/기관도 해킹 발생
- 개인정보 / 내부정보 유출, 전산망 마비 등의 치명적인 유·무형 피해 발생

2015 랜섬웨어

2014 H기관 내부정보 유출

2013 3·20 전산망 마비

AhnLab

True or False

First Victim

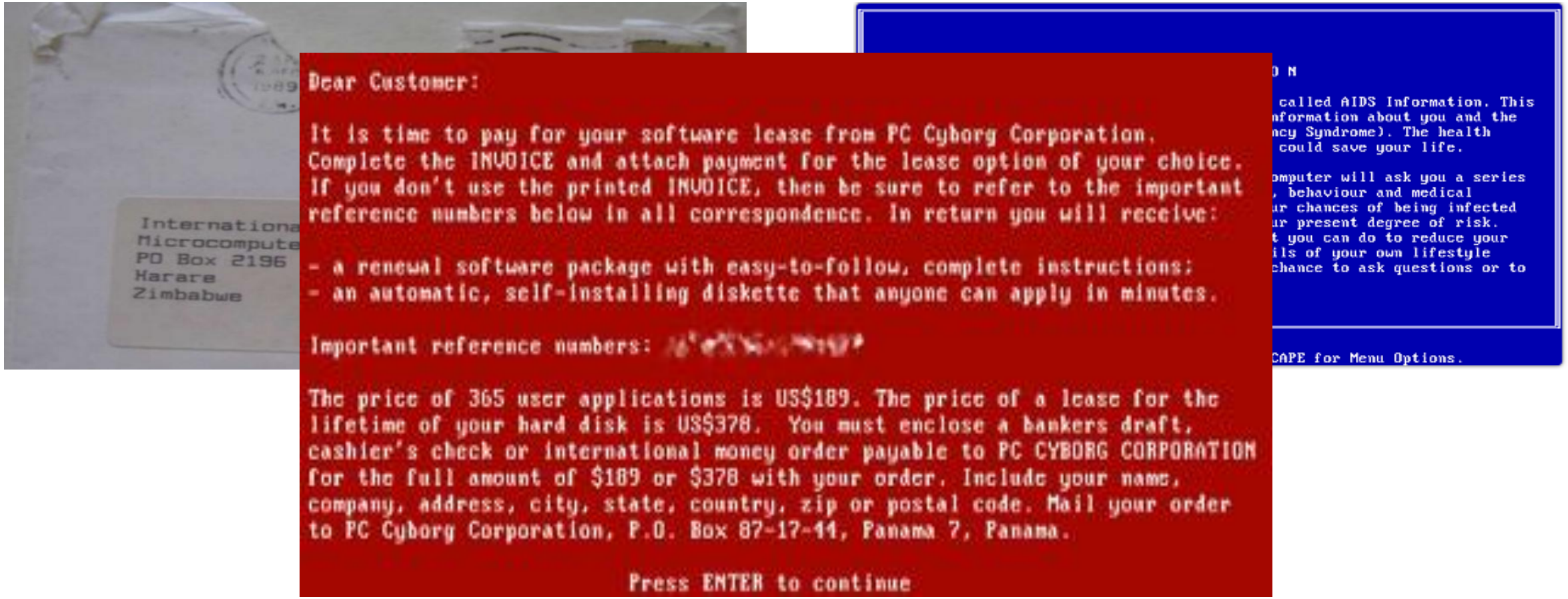
지능형 랜섬웨어로 인한 First Victim은

방어하기 힘들다?

주요 랜섬웨어 변화 - AIDS

AhnLab

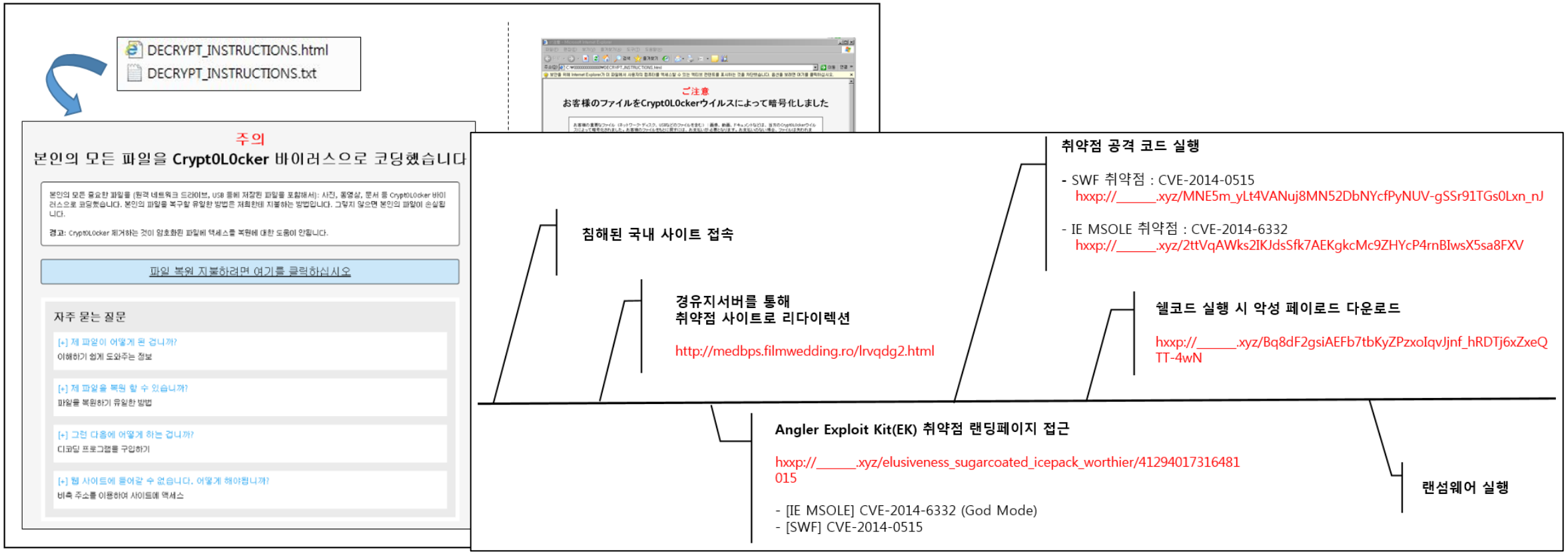
Ransomware	발생년도	주 유포경로	확산 범위	암호키	결제방법
AIDS	1989	우편	Local PC	N/A	우편 전달



주요 랜섬웨어 변화 - Crypt0L0cker

AhnLab

Ransomware	발생년도	주 유포경로	확산 범위	암호키	결제방법
Crypt0L0cker	2015.04	Web	Local PC	C&C	Bitcoin



주요 랜섬웨어 변화 - Locky

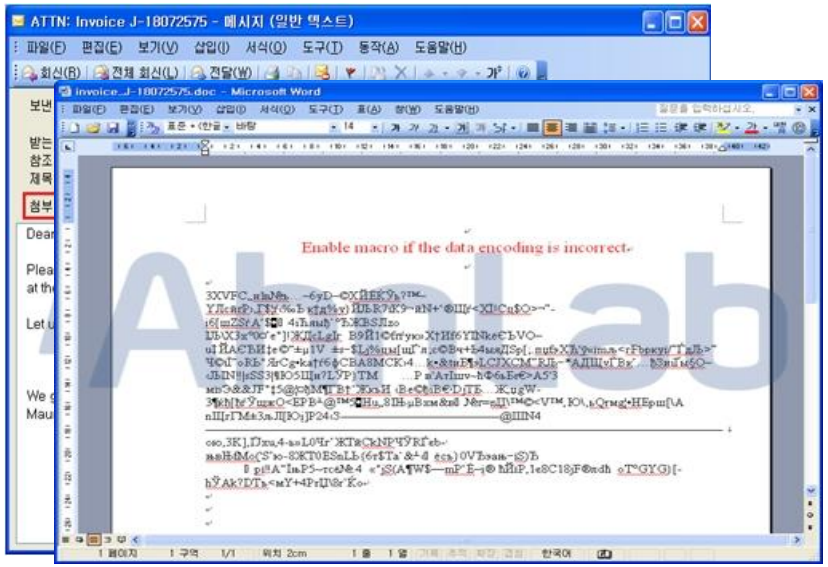
AhnLab

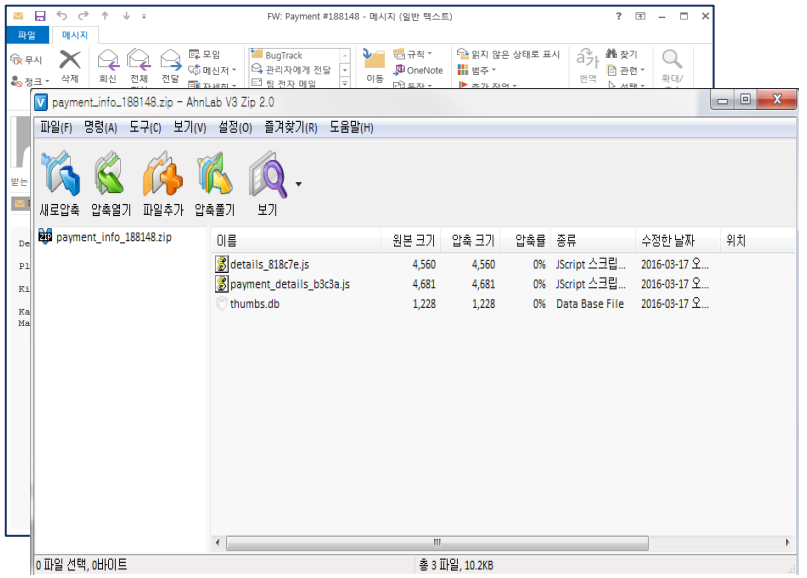
Ransomware	발생년도	주 유포경로	확산 범위	암호키	결제방법
Locky	2016.02	Mail, Web	Local PC, 공유 폴더	C&C	Bitcoin

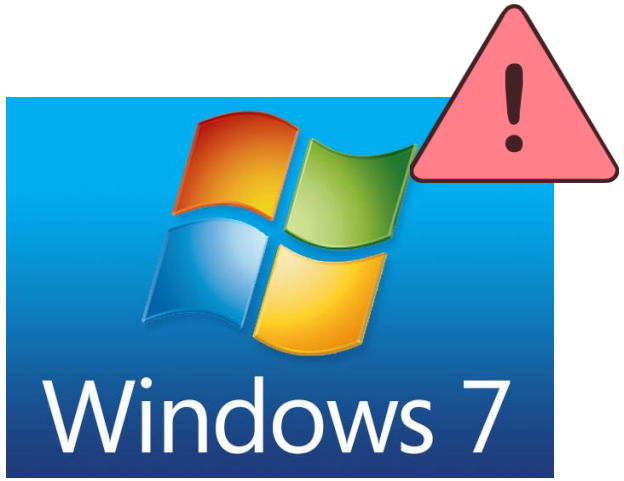
2016.02
메일 첨부파일
*.doc 문서 (Macro)

2016.03
메일 첨부파일
*.js 파일

2016.04
Web
CVE-2015-1701 취약점



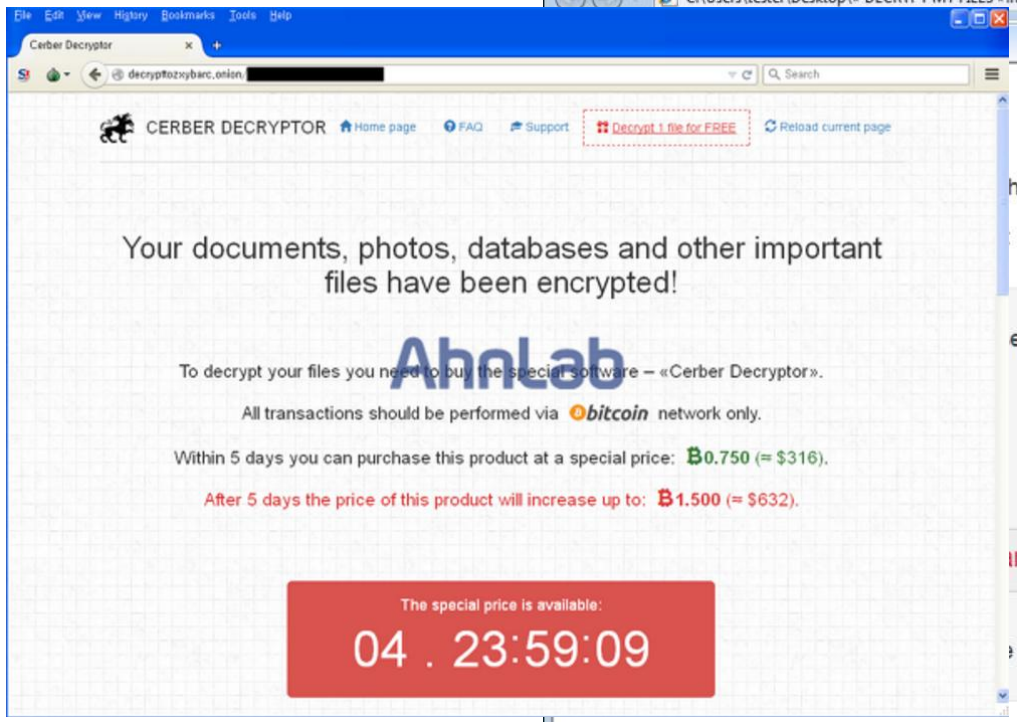




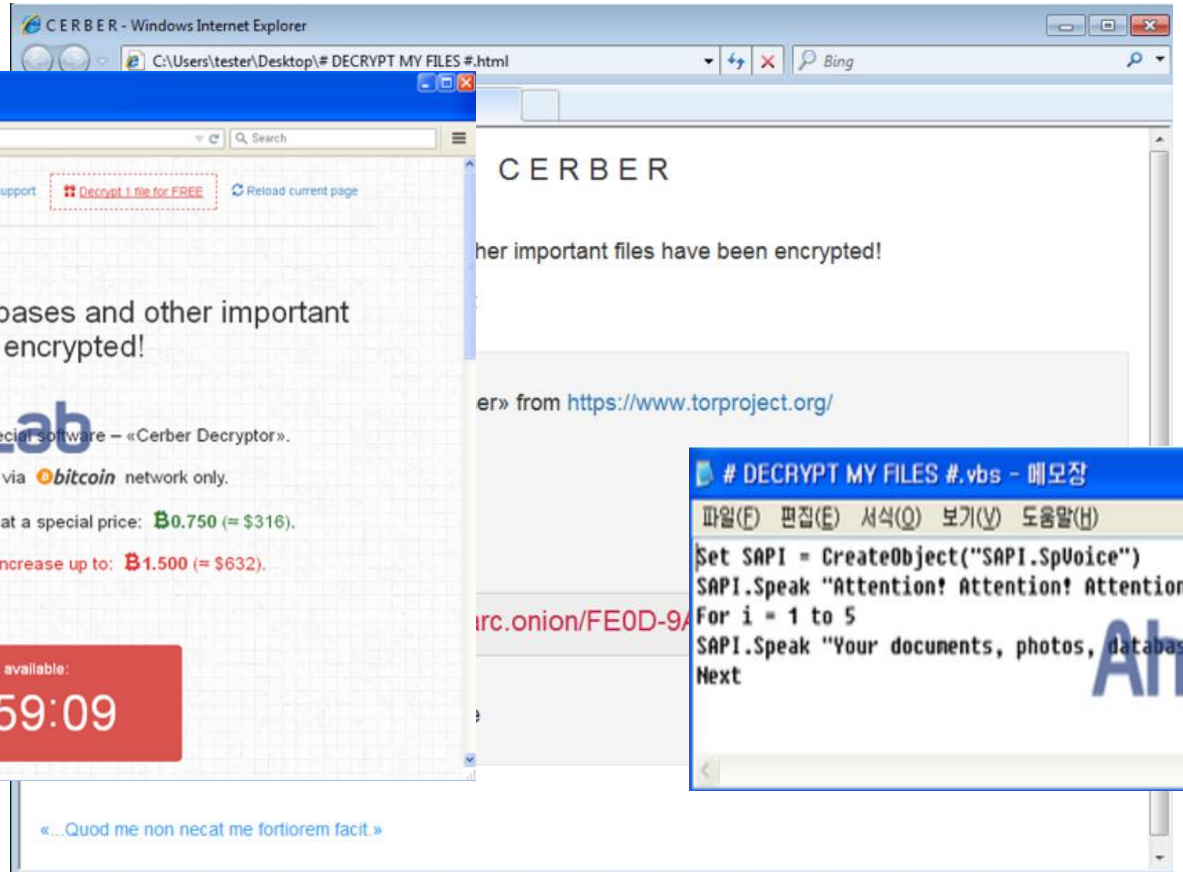
주요 랜섬웨어 변화 - Cerber

AhnLab

Ransomware	발생년도	주 유포경로	확산 범위	암호키	결제방법
Cerber	2016.03	Web, 멀버타이징	Local PC	Local (악성코드 내부)	Bitcoin



토르 웹 브라우저
(bitcoin 결재 안내)



VBS를 활용한 음성 안내

* **멀버타이징(Malvertising)** : 멀웨어(Malware) + 애드버타이징(Advertising)

주요 랜섬웨어 변화

AhnLab

구분	AIDS	Crypt0L0cker	Locky	Cerber
발생 년도	1989	2015.04	2016.02	2016.03
유포 경로	우편	Web	Mail, Web	Web, 멀버타이징
유포 파일	exe	exe, scr	doc, js, exe	exe
확산 범위	Local PC	Local PC	Local PC, 네트워크 공유 폴더	Local PC
암호 키	N/A	C&C	C&C	Local (악성 코드 내부)
결제 방법	우편	bitcoin	bitcoin	bitcoin
기타	Floppy Disk, 우편	한국형, SWF, IE 취약점	빠른 확산, Macro, Win7	음성안내, RaaS 디자인

다양화
랜섬웨어 유포 방법의 다양화

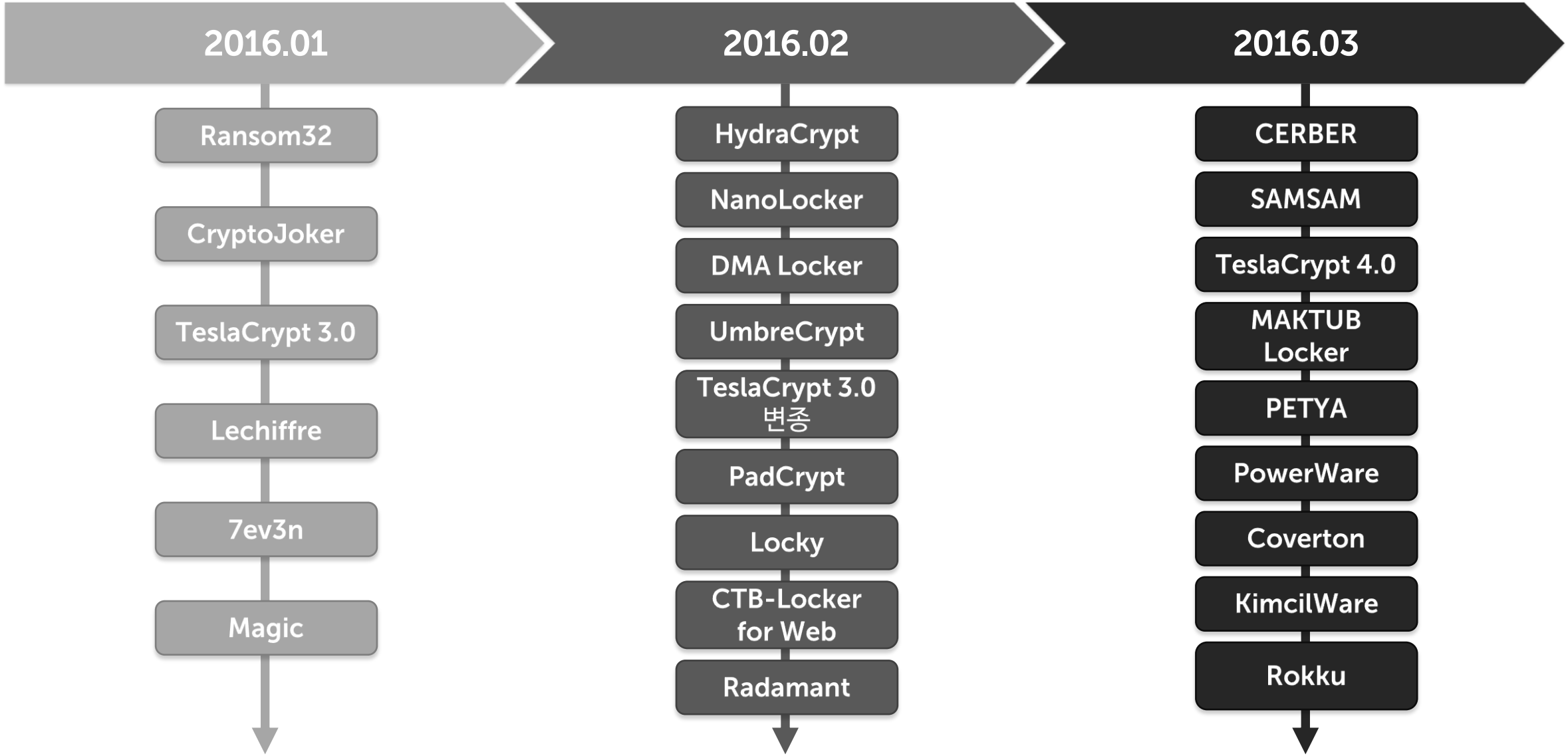
확대
유포 파일 형태의 확대

서비스화
랜섬웨어의 '서비스화'

* **RaaS** : Ransomware as a Service

2016 1분기 랜섬웨어 결산

AhnLab



02. 최신 보안 위협 대응의 어려움

More security,
More freedom

- Ransomware

AhnLab

랜섬웨어 대응의 어려움

AhnLab

기존 보안 제품을 통한 신/변종 악성코드 대응 관점에서 직면하게 되는 기술적 한계에 대비해야 한다.

최초 감염(First Victim, Patient Zero) **발생 불가피**

기존 보안 제품으로 탐지가 안되는 신/변종 랜섬웨어

랜섬웨어를 통한 피해 범위 예측 불가

기존 보안솔루션의 대응 한계

AhnLab

기존 보안 제품으로 탐지가 안되는 신/변종 랜섬웨어

기존 보안솔루션		한계점
Firewall & NGFW 네트워크 접근 통제 및 어플리케이션 통제를 통한 랜섬웨어 유입 차단		허용된 주소, 프로토콜, 어플리케이션을 통한 **랜섬웨어 유입 차단 불가**
IDS & IPS 네트워크 기반 룰을 통한 랜섬웨어 유입 탐지 및 차단		탐지 패턴화 되지 않은 **신·변종 랜섬웨어 탐지 불가**
AV 시그니처 매칭을 통한 랜섬웨어 유입·실행 차단		신·변종 랜섬웨어 **탐지 불가**
APT 솔루션 (NW sandbox 기반) 네트워크 레벨 가상환경(**sandbox**)에서 랜섬웨어 의심 파일 분석 및 탐지		지능형 랜섬웨어 탐지하더라도 엔드포인트 레벨에서 **랜섬 행위 피해** (파일 암호화 등) **사전 차단 불가**

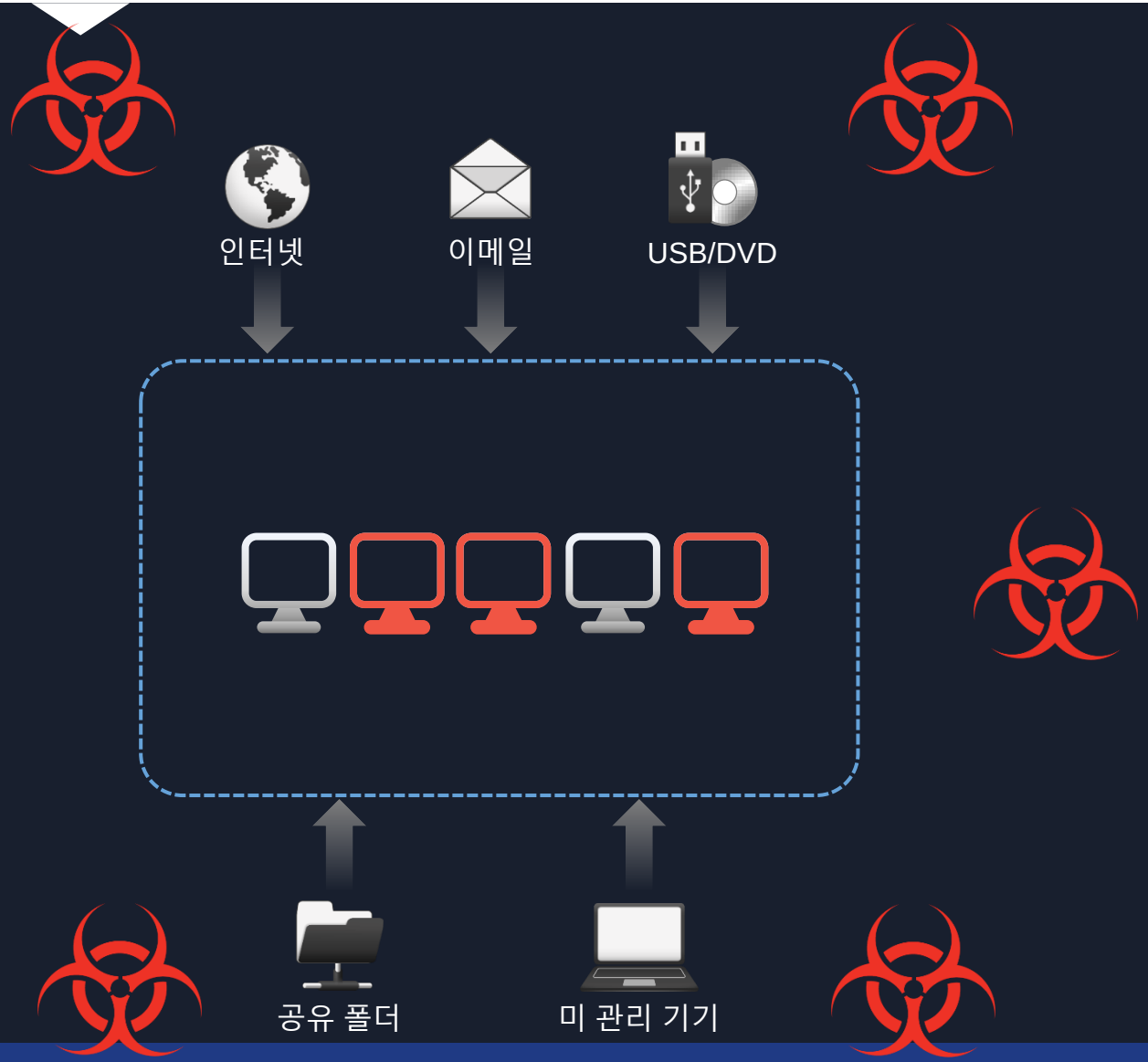
암호화만 막으면 될까?

랜섬웨어를 통한 피해 범위 예측 불가

암호화만 막으면 될까?

랜섬웨어를 통한 피해 범위 예측 불가

AhnLab



암호화만 막으면 될까?

랜섬웨어를 통한 피해 범위 예측 불가

AhnLab

파일 암호화 랜섬웨어

암호화된 파일

금전 요구 불응 시

중요 파일 복구 불가

암호화만 막으면 될까?

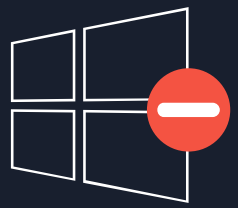
랜섬웨어를 통한 피해 범위 예측 불가

AhnLab

HDD 암호화 랜섬웨어

암호화된 MBR

금전 요구 불응 시



PC 정상 동작 불가

암호화만 막으면 될까?

랜섬웨어를 통한 피해 범위 예측 불가

AhnLab

정보 유출 협박형 랜섬웨어

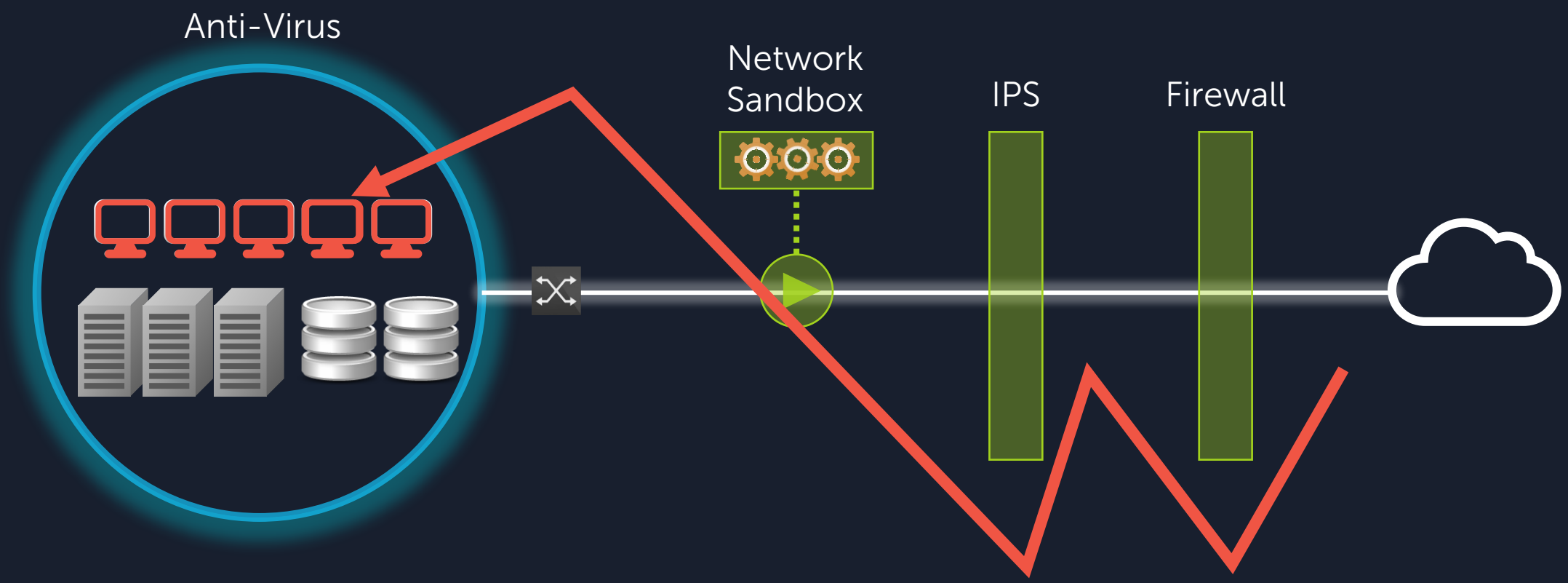
암호화된 파일

금전 요구 불응 시

블랙마켓 유출 가능

최초 감염(First Victim, Patient Zero) 발생 불가피

AhnLab



03. 최선의 대응 방안은?

More security,
More freedom

AhnLab

AhnLab MDS, 주요기능 & 기술

AhnLab

Analysis

동적 행위 분석 엔진

Dynamic Behavior Analysis

- 가상 머신 기반으로 실행(PE)형 악성코드 행위 분석
- 운영체제 상의 의심스러운 행위 정보 모니터링
- 연관 파일 행위 및 평판 정보 종합 분석 및 악성 판정

동적 콘텐트 분석 엔진

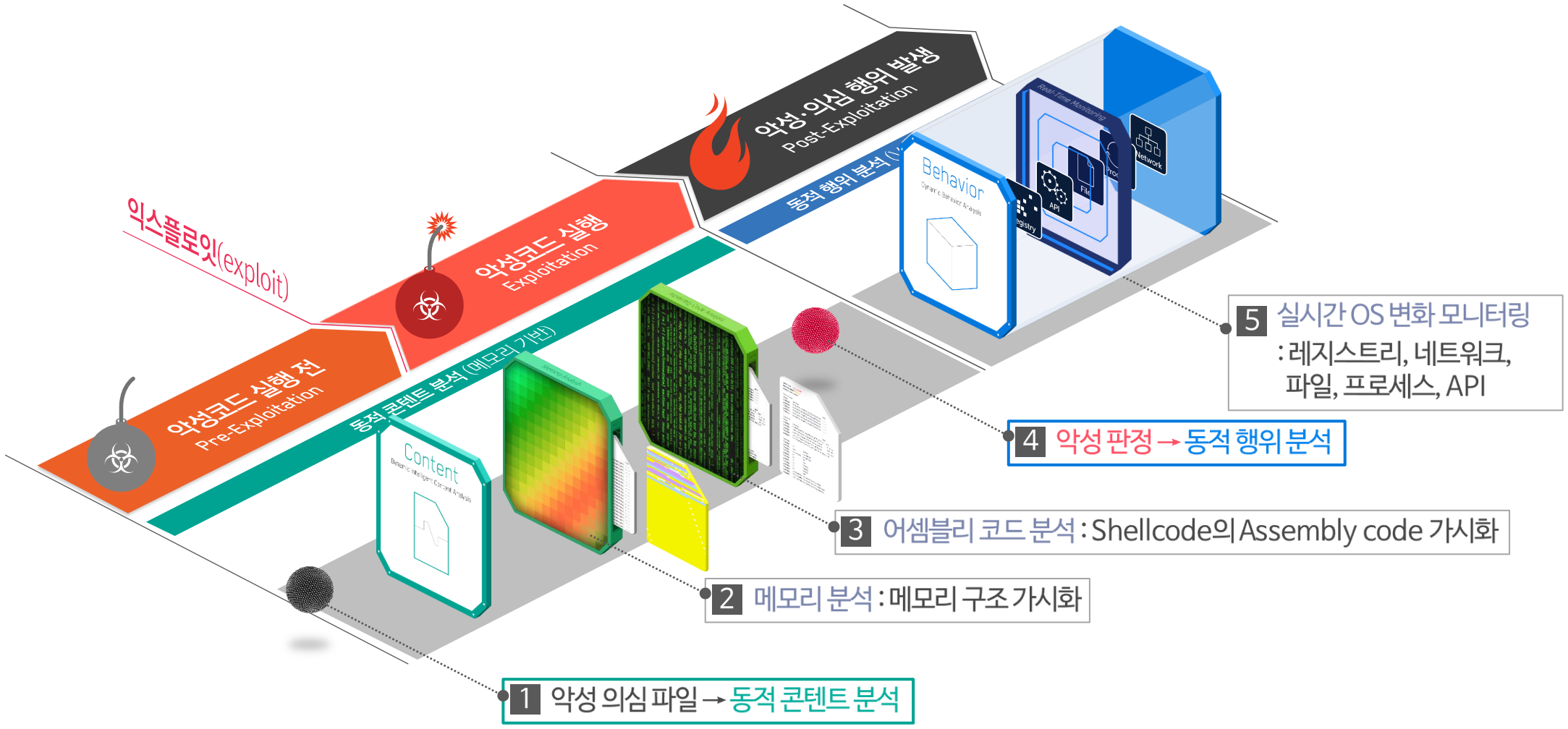
Dynamic Intelligent Content Analysis

- 문서 등 비실행(non-PE)형 악성코드 정밀 분석
- 리버스 엔지니어링 기법의 메모리 분석
- 보안 취약점 공격 (exploit) 단계에서 악성 판정
- 악성 쉘코드의 실행 전 단계에서 악성 판정
  (행위 발생 여부와 관계없이 탐지 가능)

AhnLab MDS, 주요기능 & 기술

AhnLab

Analysis

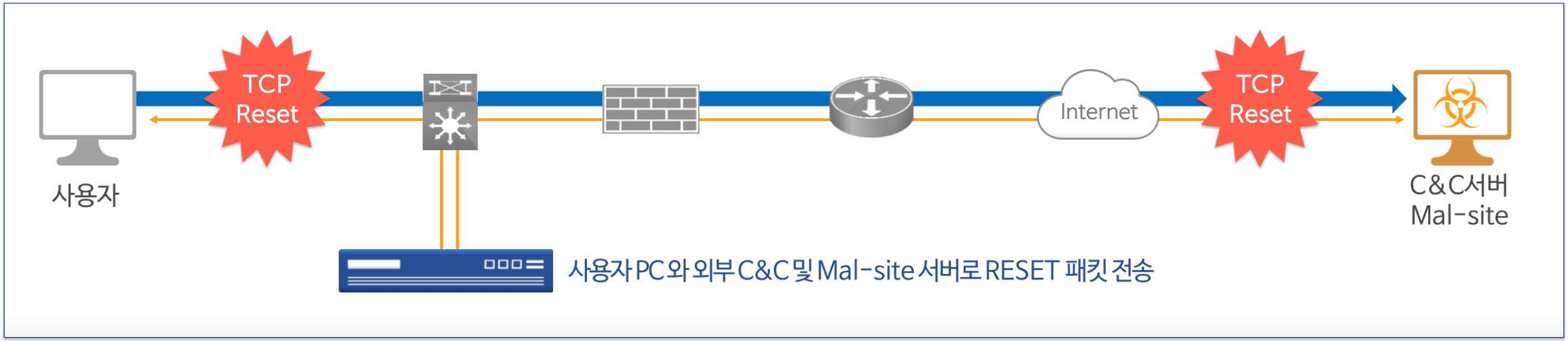


AhnLab MDS, 주요기능 & 기술

AhnLab

Response

네트워크 레벨 차단 기능



네트워크 level 차단 대상 이벤트

- C&C 트래픽 탐지 이벤트
- Malsite 접속 탐지 이벤트

네트워크 level 차단 방식

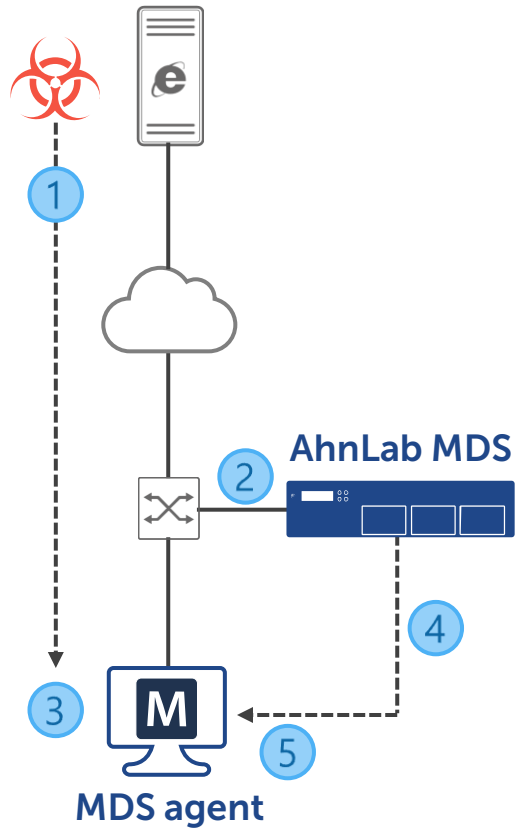
대상 프로토콜	차단 방식
TCP	TCP RESET 패킷을 client-server 양측에 전송
UDP	ICMP Unreachable 패킷을 client-server 양측에 전송

AhnLab MDS, 주요기능 & 기술

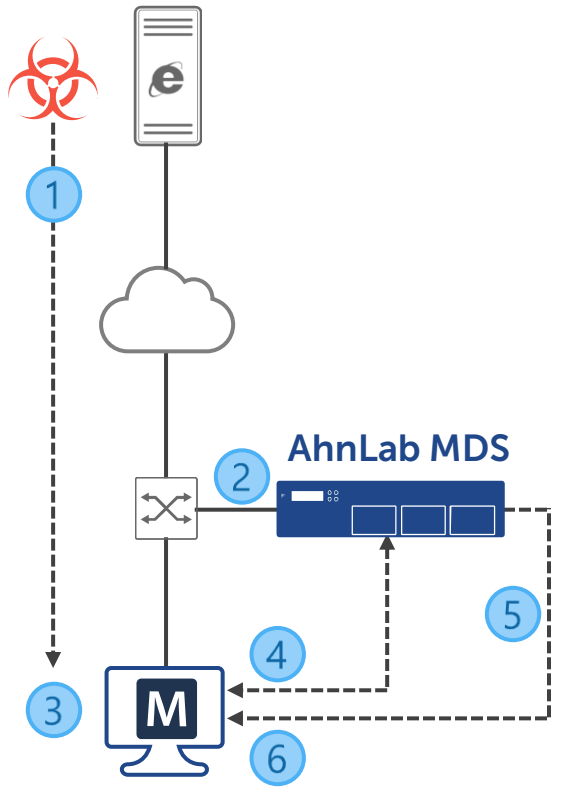
AhnLab

Response

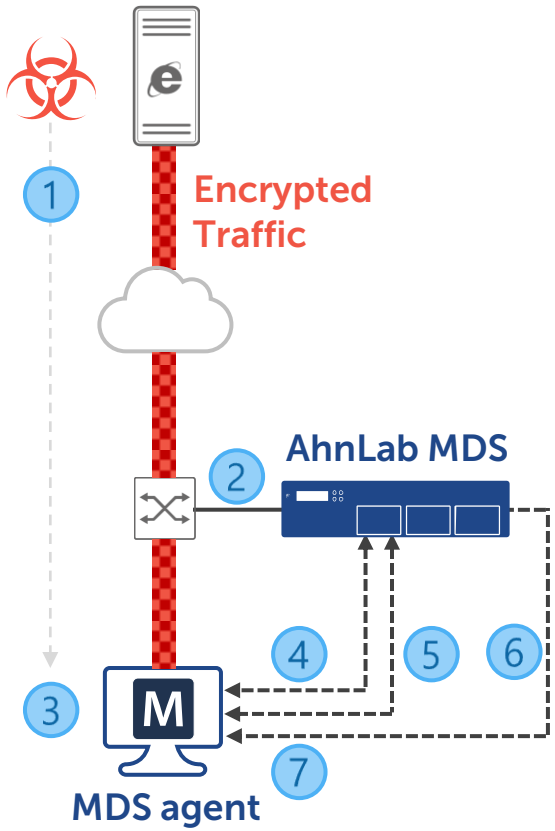
Remediation
(삭제)



Execution Holding
(실행 보류)



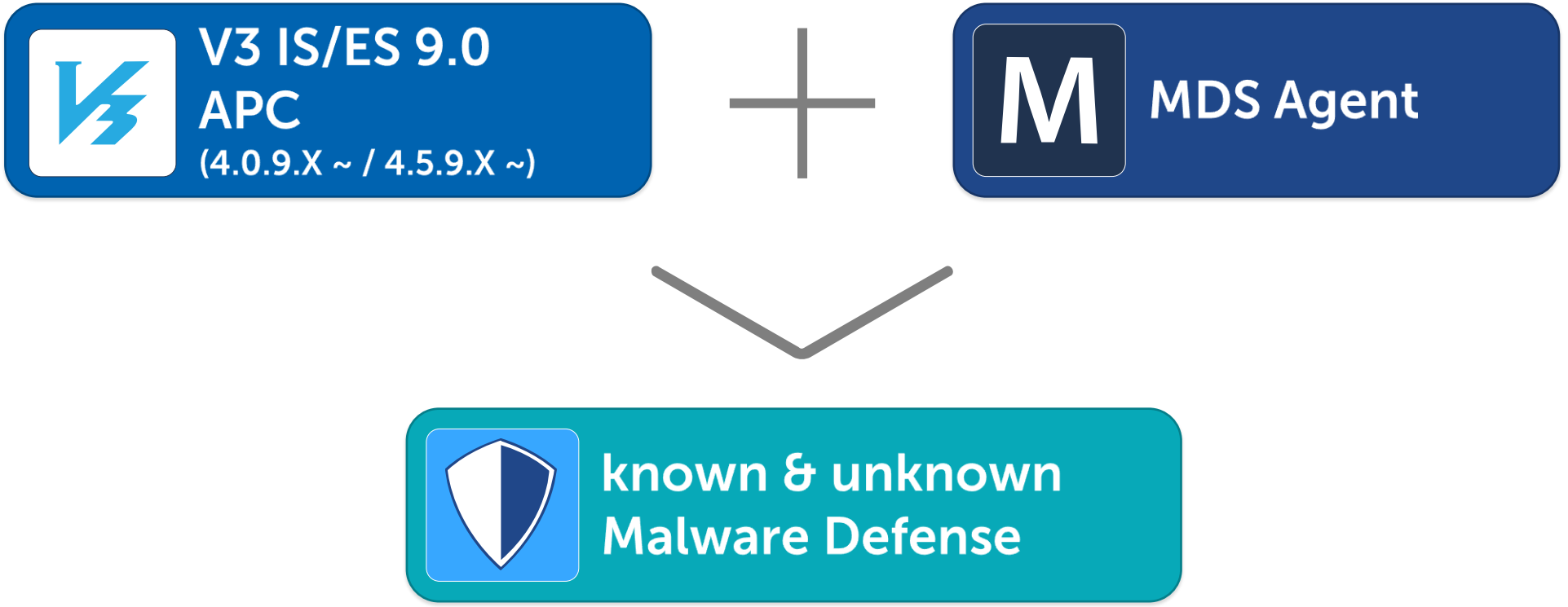
File Upload for Analysis
(파일 업로드 분석)



AhnLab MDS, 주요기능 & 기술

AhnLab

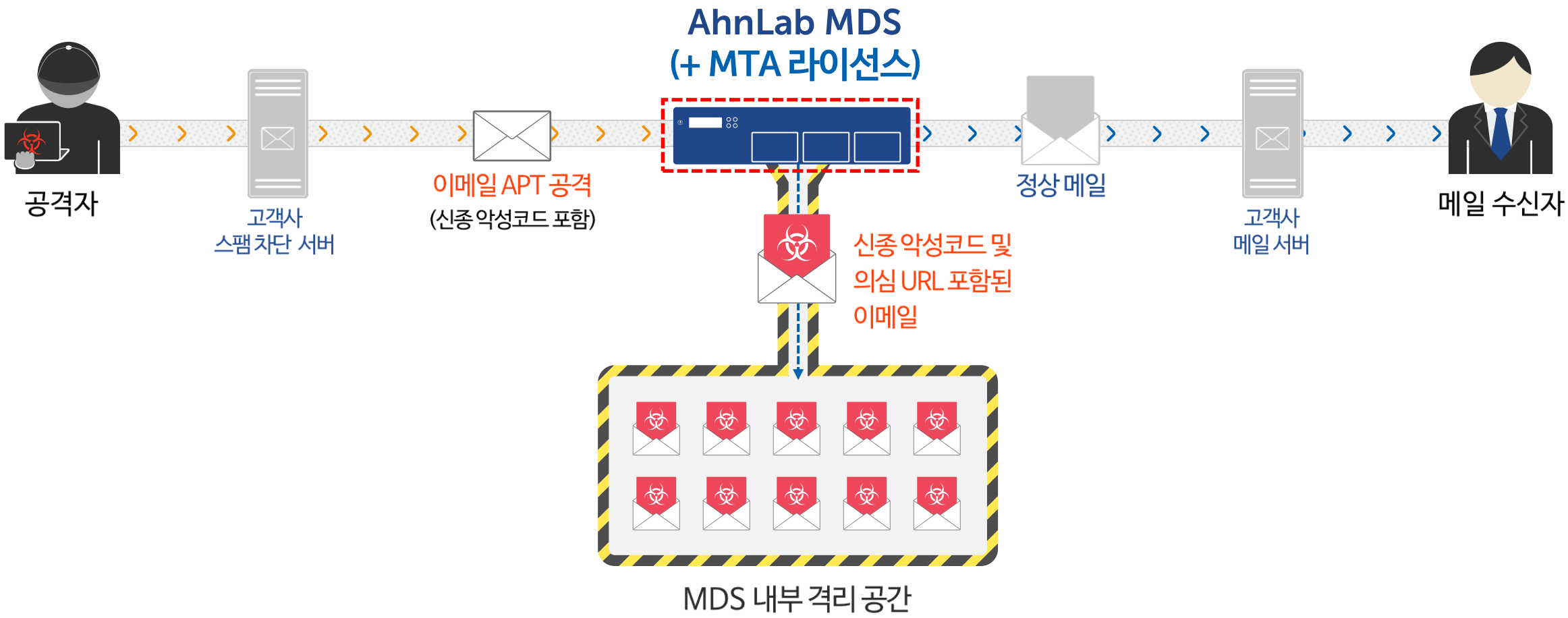
Response



AhnLab MDS, 주요기능 & 기술

AhnLab

Response



04. Case Study

More security,
More freedom

- Ransomware 대응

AhnLab

Web을 통한 랜섬웨어 유입 - Network Sandbox 도입 전

AhnLab

Web을 통한 랜섬웨어 유입 - Network Sandbox 도입 후

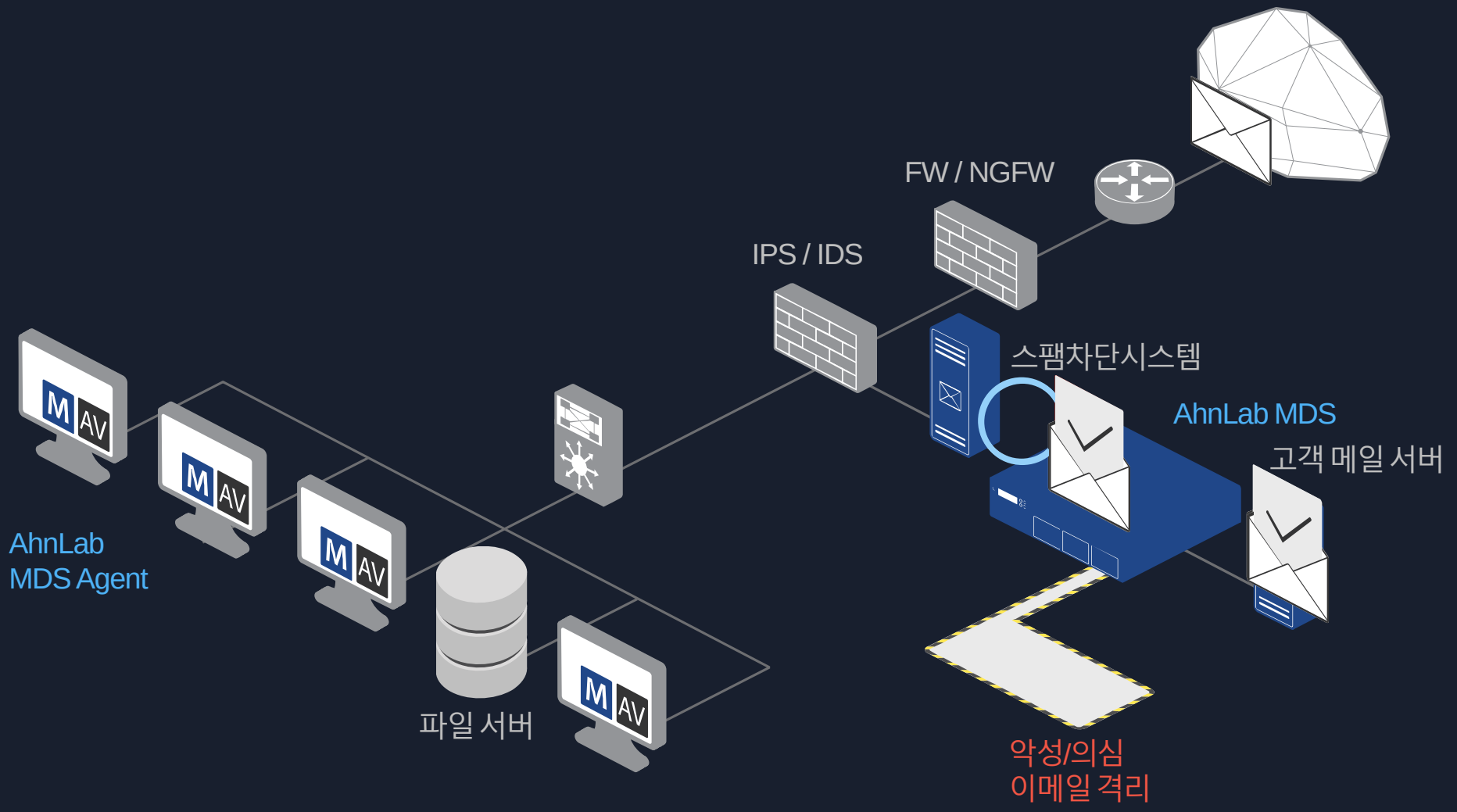
AhnLab

Web을 통한 랜섬웨어 유입 - MDS 도입 후

AhnLab

이메일을 통한 랜섬웨어 유입 - MDS 도입 후

AhnLab



지능형 보안 위협에 대한 최선의 대응 방안

AhnLab

현실적인 검증을 통해 알려지지 않은 위협을 확인하고 대응할 수 있는 지능형 위협 대응 솔루션 도입 필요

Network Sandbox

네트워크 레벨
동적 분석
사후 대응

한계

암호화 채널
가상환경 분석 시간
First Victim 발생

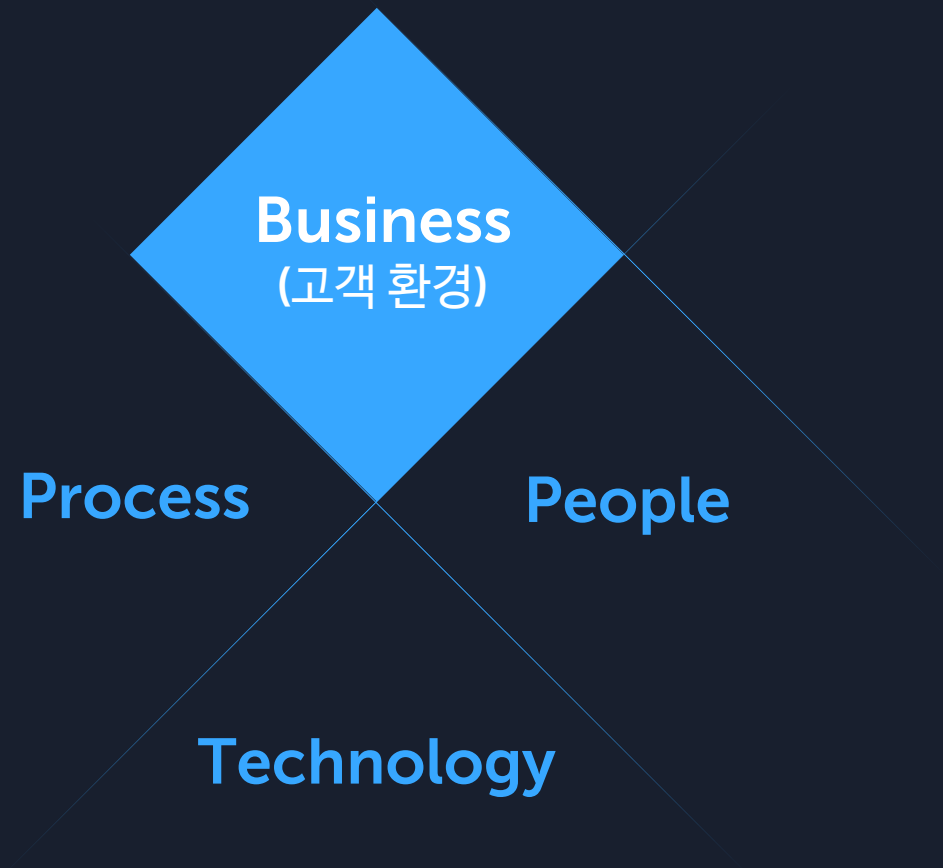
최선의 선택

네트워크 & 엔드포인트
동적분석 + 정적분석
가시화
사전 대응 (First Victim 제거)

중요한 것은 기본

AhnLab

'기술' 의존적인 대응이 아닌 'People - Process - Technology'의 조화로운 보안 체계 수립 및 생활화 필요



AhnLab MDS

AhnLab

AhnLab MDS는 진화하는 보안 위협에 대한 대응 솔루션이다.
신종 악성코드 및 익스플로잇(exploit)에 대한 '예방-탐지- 분석- 대응' 프로세스를 통해 타깃 공격, 고도화된 공격에 효과적으로 대응한다.

AhnLab MDS

Malware Defense System

의심 실행형 파일 실행 보류

멀티 엔진 지능형 위협 분석

네트워크 및 엔드포인트 다단계 차단

예방 엔드포인트 레벨 실행 보류 및 의심파일 추출

탐지 웹, 이메일, 파일공유, 암호화 트래픽

분석 하이브리드 기반의 위협 분석

대응 네트워크, 에이전트 기반 위협 대응

AhnLab

True or False

지능형 랜섬웨어로 인한 First Victim은
방어하기 힘들다?

More security, More freedom

AhnLab