

# 지능형 보안 위협에 대한 트렌드 및 종합적인 대응 방안

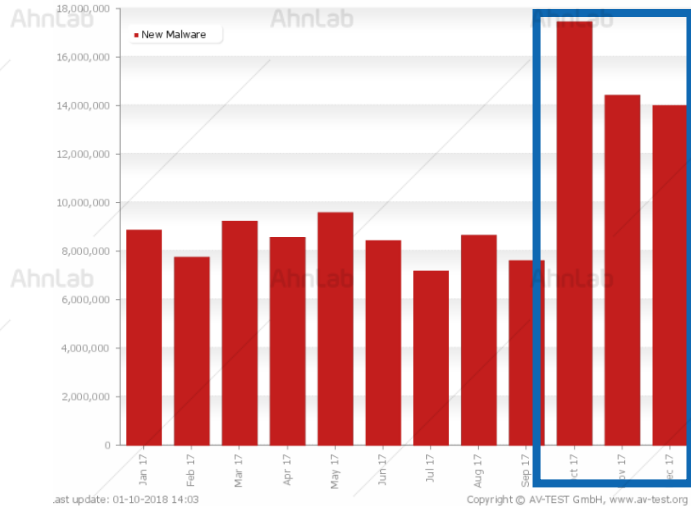
## NES 2018' 차세대 기업보안 세미나&전시회

제품기획팀 백민경 부장 / Product Evangelist

AhnLab



# 숫자로 보는 악성코드 동향



33만

2017년 하루 평균 New Malware

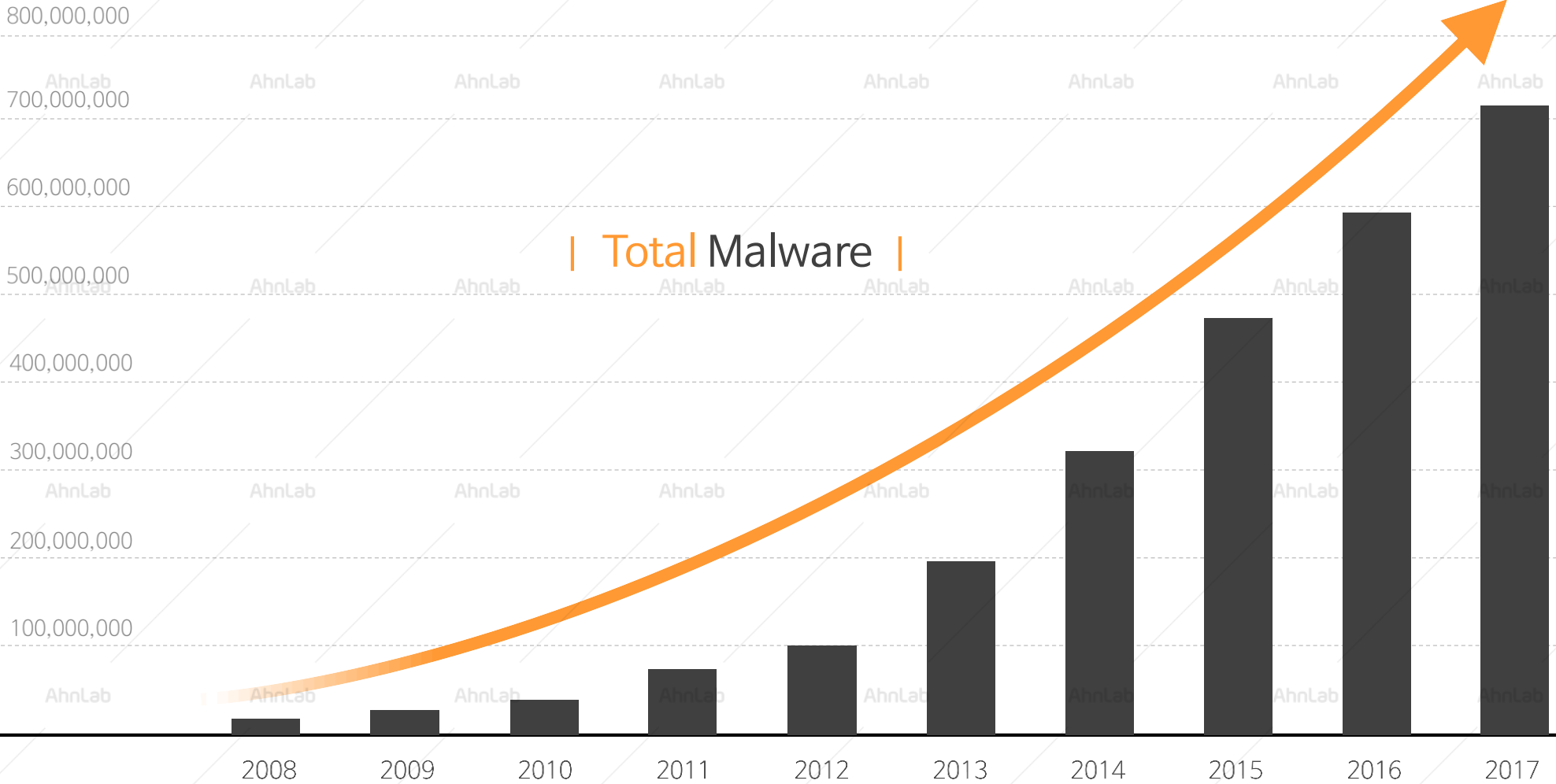
2017년 4분기에 발견된 Malware

4,500만

2009년 발견된 Total Malware

※ 출처: AV-TEST GmbH, www.av-test.org

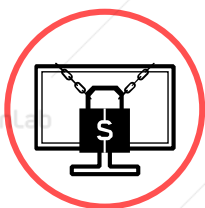
# 최근 10년 동안 전체 악성코드 추이



Endpoint 시스템을 노리는  
다양한 악성코드



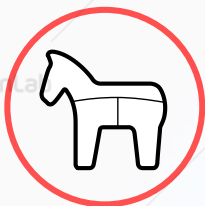
Zero-Day 공격



사회공학기법



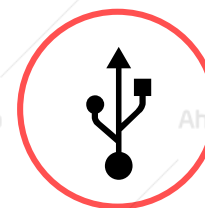
표적공격



O/S, S/W 취약점



다양한 경로를 통한  
악성코드 감염 및 정보유출



USB



인터넷



Bluetooth



Wifi



Print / FAX

2016-12-30 (금) 오후 5:15  
@gmail.com <@gmail.com>  
내부지침사항

받는 사람

메시지 내부지침사항.egg (342 KB)

안녕하세요  
사내 내부지침사항이 있습니다  
반드시 확인하시고 정확히 인지하셔서 불이익을 당하시는 일이 없도록 바랍니다  
아직은 확정사항은 아니지만  
미리 숙지하셔서 꼭 참고하시기 바랍니다

2017-02-14 (화) 오전 10:29  
@gmail.com  
2017년도 병역지정업체대상 교육일정안내 공지

받는 사람

메시지 2017병역지정업체 교육안내.7z (516 KB)

안녕하세요  
벌써 2017년도 2월이 되었네요  
이번에 2017년도 병역지정업체대상으로 교육을 진행하게 되었습니다  
각 분야별로 일정과 함께 진행되는 내용들에 대해서는 첨부파일 확인을 바랍니다  
차후 실무에 도움이 되는 실질적인 교육과정들을 준비하였으니

2017-01-16 (월) 오전 12:24  
@naver.com  
저기 블로그님 블로그님이 작성하신 글에 제 얼굴이 나왔어요 ㅠㅠ 글좀 내려주세요

받는 사람

중요도가 높은인 메시지를 보냈습니다.  
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다

메시지 문제가된 사진.zip (410 KB)

처음엔 장난인줄 알았는데 들어가서 확인해보니 정말 제가 나왔어요 ㅠㅠ  
제 딸래미랑 제가 같이 나왔는데 카페에서 같이 손잡고 있는게 찍혔더라고요  
그냥 넘어갈려 하다가 그래도 아미가 찍혀서 아미만이라도 모자이크를 좀 해주셨음 해서 이렇게 메일 드려요  
첨부파일에 제가 빨간펜으로 표시해 놨어요  
거기 나온 빨간 점퍼 입은 애가 제 딸래미 입니다. 확인해 보시고 답장 부탁드립니다  
**비밀번호는 1234 이고요 모바일로는안열릴게 예요**

2017-04-12 (수) 오후 1:16  
@gmail.com  
[인터파크] 개인정보 유출관련 사과공지 및 보상정책 안내

받는 사람

메시지 header\_title.png (11 KB) 개인정보확인.7z (476 KB)

항상 인터파크를 이용해주시는 고객 여러분께 사과 드립니다.  
인터파크는 해커 조직에 의해 APT(지능형 지속가능 위협) 형태의 해킹에 고객 정보 일부가 침해당한 사실을 인지하였으며, 경찰청 사이버 안전국에 신고하여 공조를 시작하였습니다.  
인터파크는 2015년 개인정보관리체계(PIMS) 인증을 획득한 바 있고, 개인 정보보호 및 보안에 많은 노력을 기울여왔음에도 이번 해커 조직의 범죄에 고객 정보를 지키지 못한 점에 대해서 진심으로 사과 드립니다.  
이번에 침해 당한 회원 정보는 이름, 아이디, 이메일, 주소, 전화번호로 추정하고 있으며, 개인별로 유출 항목에 차이가 있습니다.  
또한 고객님의 주민번호와 금융정보 등은 유출되지 않았으며, 비밀번호는 암호화되어 있어서 안전합니다.  
인터파크를 믿고 이용해주신 고객 여러분께 심려 끼쳐드린 점에 대해 다시 한번 사과 드리며, 이번 일을 계기로 개인정보 보중에 더욱 최선을 기할 것을 약속드립니다

# 운영체제 및 응용프로그램 취약점

Microsoft | TechNet

Security TechCenter

홈 보안 업데이트 라이브러리 학습 다운로드 지원 커뮤니티

보안 권고 및 공지 > 보안 공지 > 2017

- MS17-020
- MS17-019
- MS17-018
- MS17-017**
- MS17-016
- MS17-015
- MS17-014
- MS17-013
- MS17-012
- MS17-011
- MS17-010
- MS17-009
- MS17-008
- MS17-007
- MS17-006

## Microsoft 보안 공 긴급

### Windows 커널용 보안

게시된 날짜: 2017년 3월 15일

버전: 1.0

### Adobe Flash Player용 보안

게시된 날짜: 2017년 3월 15일

버전: 1.0

이 보안 업데이트는 Microsoft Windows 10 및 Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 10 및 Windows 8.1용 Adobe Flash Player의 취약성을 해결합니다.

심각도는 긴급입니다. 이 업데이트는 특히 Internet Explorer 11에서 사용되는 Adobe Flash Player의 취약성을 해결하는 데 중요합니다. 이 업데이트를 설치하면 보다 효과적인 서비스를 받을 수 있습니다.

Adobe에 보안 문제를 알릴 때에는 이 페이지를 방문하시면 됩니다.

이 페이지에는 특정 버전의 Adobe 제품에 영향을 줄 수 있는 보안 취약점에 대한 중요한 정보가 들어 있습니다. 이 정보를 사용하여 앞서 설명한 수정 조치를 수행하십시오. 향후의 권고 조치에 대한 전자 메일 알림 메시지를 받도록 등록하시면 보다 효과적인 서비스를 받을 수 있습니다.

보안 게시판  
통지 서비스  
Adobe에 알림  
심각도 등급  
감사의 말  
PSIRT PGP 키

### 보안 게시판 및 권고 조치

제목	최초 게시일	마지막 업데이트
<a href="#">APSB17-09 Adobe Campaign에 대한 보안 업데이트</a>	2017/4/11	2017/4/11
<a href="#">APSB17-10 Adobe Flash Player에 대한 보안 업데이트</a>	2017/4/11	2017/4/11
<a href="#">APSB17-11 Adobe Acrobat 및 Reader에 대한 보안 업데이트</a>	2017/4/6	2017/4/11
<a href="#">APSB17-12 Adobe Photoshop CC에 대한 보안 업데이트</a>	2017/4/11	2017/4/11
<a href="#">APSB17-13 Creative Cloud 데스크톱 응용 프로그램에 대한 보안 업데이트</a>	2017/4/11	2017/4/11

제품별 게시판 및 권고 조치

제품명	게시판	권고 조치
Adobe Acrobat	Adobe DNG SDK	Adobe LiveCycle ES
Adobe AIR	Adobe Document Server	Adobe LiveCycle Form Manager
Adobe After Effects	Adobe Download Manager	Adobe LiveCycle Workflow
Adobe Analytics	Adobe Dreamweaver	Adobe MX 2004 products
Adobe Animate	Adobe Experience Manager	Adobe PageMaker
Adobe Audition	Adobe Experience Manager Forms	Adobe Photoshop
Adobe BlazeDS	Adobe Flash Communication Server	Adobe Photoshop Album
Adobe Brackets	Adobe Flash Media Server	Adobe Photoshop Elements
Adobe Breeze	Adobe Flash Player	Adobe Premiere Pro
Adobe Bridge	Adobe Flex	Adobe Presenter
Adobe Campaign	Adobe Flex Client	Adobe Reader
Adobe ColdFusion	Adobe Form Designer	Adobe Reader Mobile
Adobe Connect	Adobe Forums	Adobe RobotHelp
Adobe Contribute Publishing Services	Adobe GoLive	Adobe RobotHelp Server
		Adobe Shockwave Player

Bing으로 TechNet 검색

## Microsoft 보안 공지 MS17-014 - 중요

### Microsoft Office용 보안 업데이트(4013241)

게시된 날짜: 2017년 3월 14일 | 업데이트된 날짜: 2017년 4월 11일

버전: 2.0

### 요약

이 보안 업데이트는 Microsoft Office의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 Microsoft Office 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 악용에 성공해 공격자는 현재 사용자의 컨텍스트에서 원격 명령을 실행할 수 있습니다.

### 이 페이지의 내용

- 요약
- 영향을 받는 소프트웨어 및 취약성 심각도
- 업데이트 FAQ
- 취약성 정보
- 보안 업데이트 배포
- 감사의 말
- 고지 사항
- 수정 내역

### 아래한글 임의코드 실행 취약점 보안 업데이트 권고

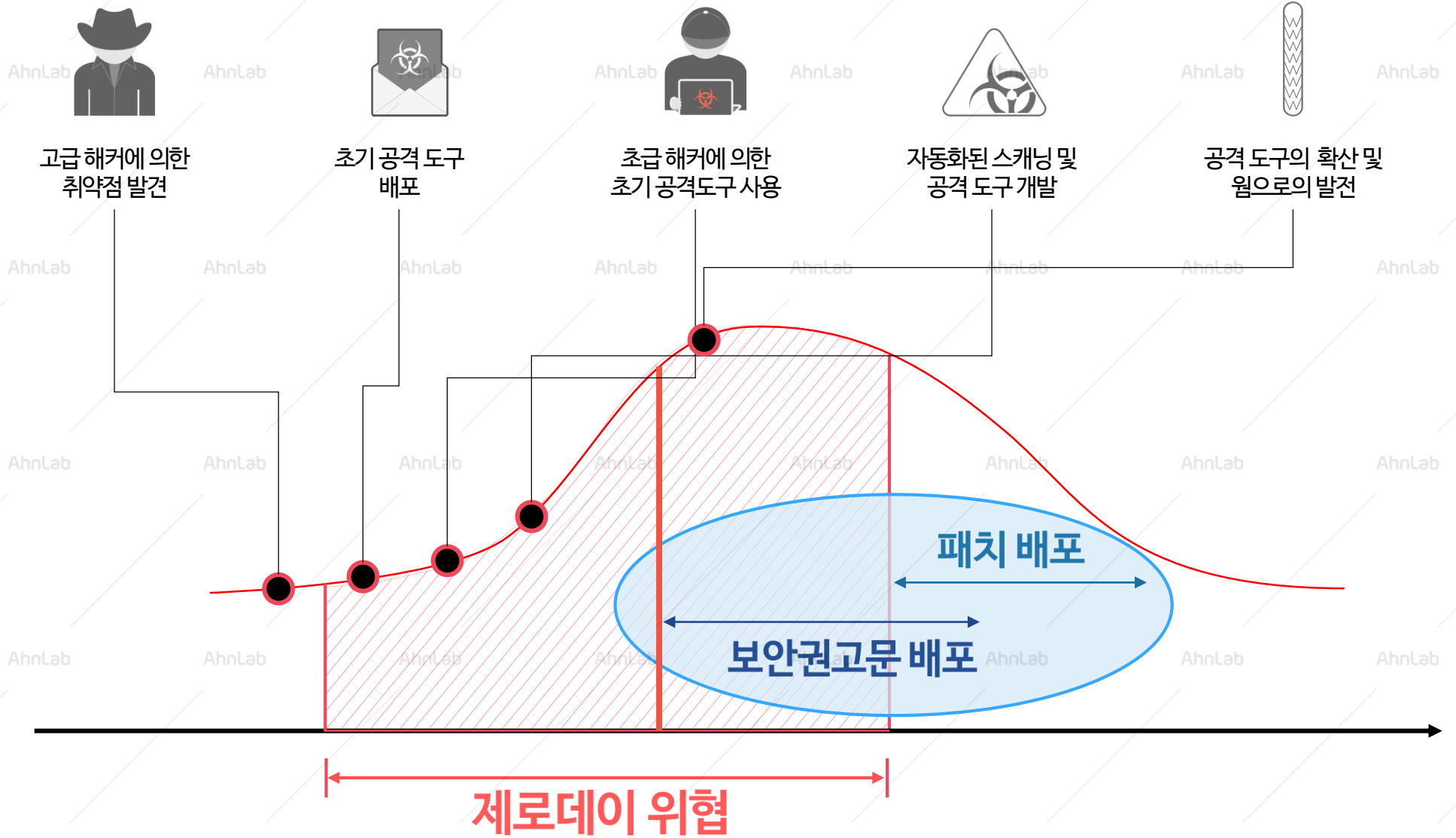
2015.06.25

### 개요

- 한글컴퓨터의 한글 등 오피스 프로그램에서 임의 코드실행이 가능한 취약점이 발견됨 [1]
- 공격자는 특수하게 조작한 웹페이지 방문 유도 또는 웹 게시물, 메일, 메시지를 링크 등을 통해 특수하게 조작된 문서를 열어서 유도로 임의코드를 실행시킬 수 있음
- 영향을 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 긴급하고 해당 시스템

제품군	세부제품	영향을 받는 버전
한컴오피스 2014	공통 요소	9.1.0.2562 이전버전
	한글	9.1.0.2421 이전버전
한컴오피스 2010	한글	9.1.0.2427 이전버전
	한쇼	9.1.0.2512 이전버전
한컴오피스 2007	공통 요소	8.5.8.1521 이전버전
	한글	8.5.8.1459 이전버전
한컴오피스 2005	한글	8.5.8.1371 이전버전
	한쇼	8.5.8.1515 이전버전
한글 2005	공통 요소	7.5.12.707 이전버전
	한글	7.5.12.715 이전버전
한글 2005	한쇼	7.5.12.772 이전버전
	한쇼	7.5.12.915 이전버전
한글 2005	한글 2005	6.7.10.1131 이전버전

# Zero-Day 공격 라이프사이클



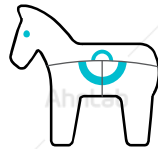
# 보안회사 R&D 관점에서 대응



## Spyware

시스템설정

2004



## Trojan

변종 대량 확산

2007



## Rootkit

탐지회피

2009



## APT

은밀성 (Stuxnet)

2011



## PUP

동의 후 탐지 필요

2010



## 7.7 DDoS / Phishing / Pharming

IT 확대 기반 활동

2009



## Online game Hack

AV Killer / AV 대응

2012



## Mobile Malware

플랫폼 확장

2014



## Ransomware

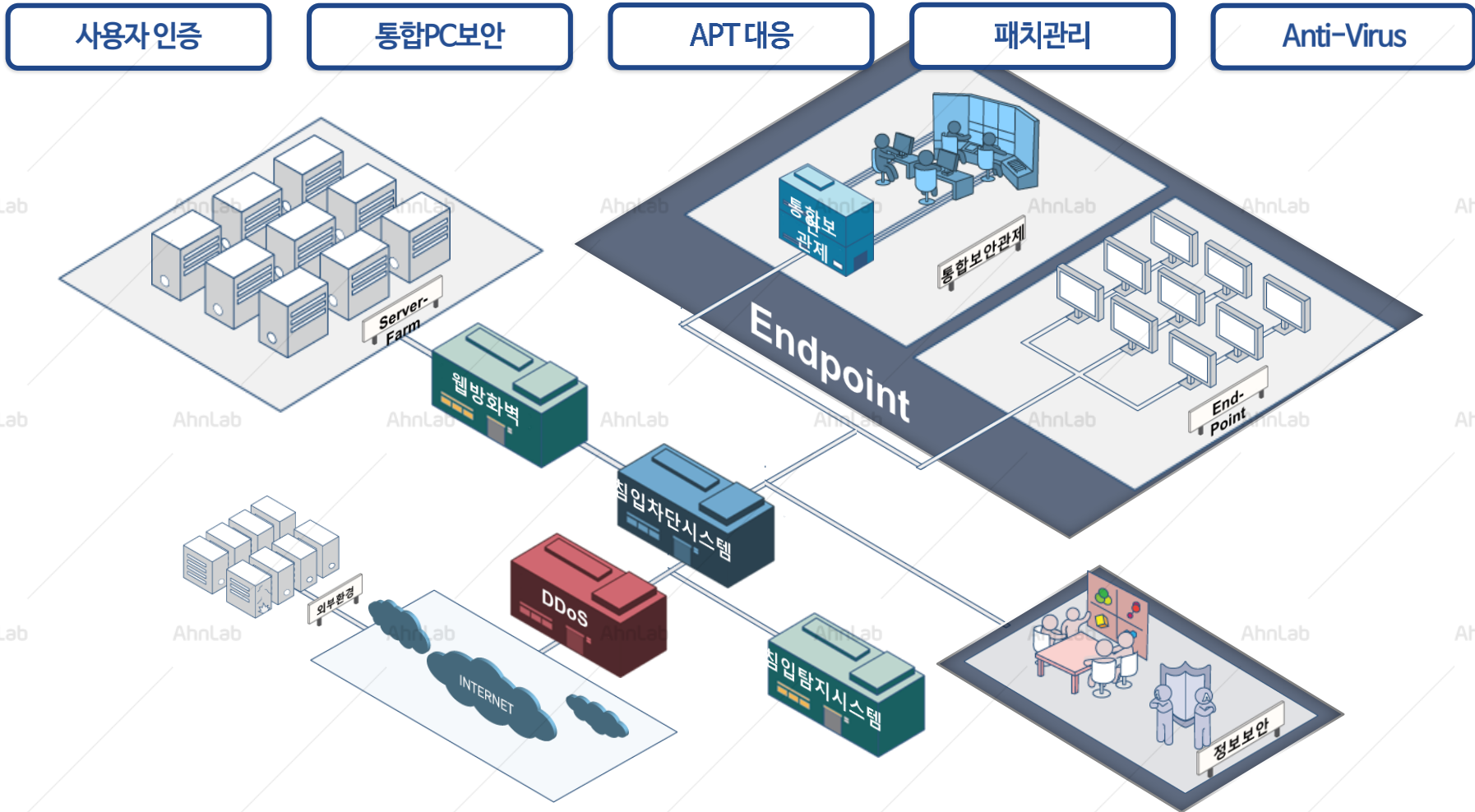
복구한계

2015~2017



# 기업 관점의 보안사고 대응

네트워크 보안 제품 중심의 이벤트(로그)를 통합보안관제 시스템을 이용하여 관제



# 그럼에도 왜 계속 피해는 발생하는가?

2009  
7·7 DDoS

2011  
3·4 DDoS

2011  
금융기관 해킹 사고

2011  
포털 개인정보 유출

2012  
언론 해킹사고



**보이지 않는 신종 악성코드**가 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

MALWARE

2016  
인터넷쇼핑몰  
개인정보 유출

2015  
랜섬웨어

2014  
기관 내부정보 유출

2013  
3·20 전산망 마비

# 무엇이 부족할까?

1

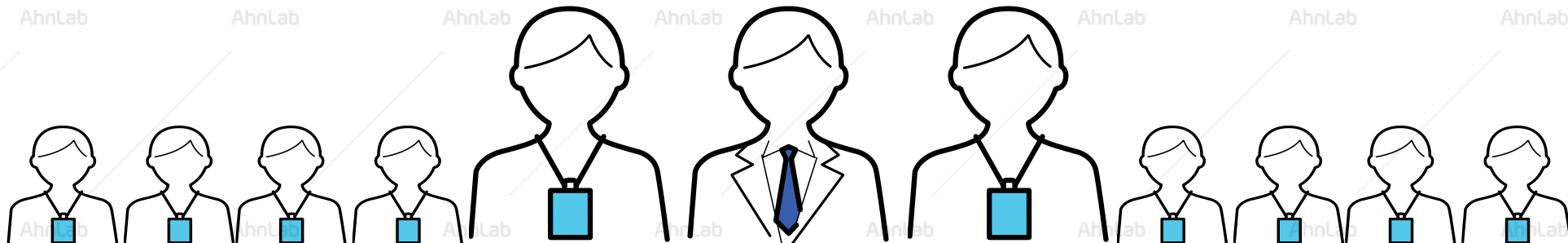
엔드포인트 보안 영역별 대응 솔루션 부족

2

보안정책 내재화 부족

3

능동적 위협 대응방안 부족



# 어떻게 해야 할까?

1

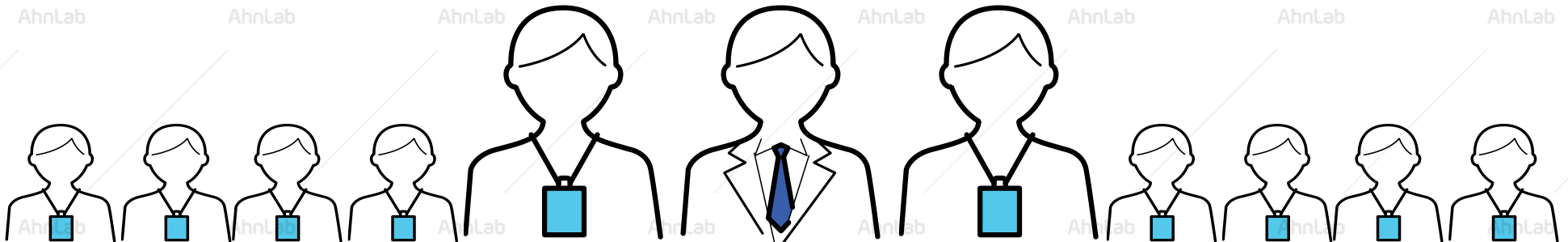
Endpoint Hardening을 통한 공격표면 최소화

2

임직원 모두 자기주도 보안 실행

3

보안 담당자의 능동적·적극적 위협 방어



# AhnLab EDR: 위협 가시성 확보/대응

고도화되는 신·변종 위협에 의한 침해사고 대응력을 강화하고 잠재적인 위협을 최소화하기 위한 보완책으로 엔드포인트단에서의 위협 정보 수집·분석·대응 관점의 EDR이 주목받고 있습니다.



## ※EDR(Endpoint Detection & Response)이란?

엔드포인트단에서 지속적인 모니터링 및 대응을 제공하는 보안 솔루션으로, 엔드포인트단에서의 위협의 탐지, 통제, 분석, 치료 등의 기능을 제공한다.

엔드포인트 보안을 위한 보조적인 툴(tool)로서, 안티바이러스 등 기존 보안 솔루션과의 연계를 통해 더욱 효과를 발휘한다.

AhnLab EDR(Endpoint Detection & Response)은 엔드포인트 영역에 대한 지속적인 모니터링을 통해 위협 탐지 및 분석, 대응을 제공하는 엔드포인트 위협 탐지 및 대응 솔루션입니다.

- 국내 최초의 행위 기반 분석 엔진을 통한 위협 행위 분석 및 모니터링
- 엔드포인트 가시성 기반의 진일보한 위협 탐지 및 대응
- 최고의 엔드포인트 보안 및 악성코드 분석 전문 기업의 기술력이 응집된 EDR

행위 정보 탐지·분석을 통한  
엔드포인트 가시성 확보 및 대응

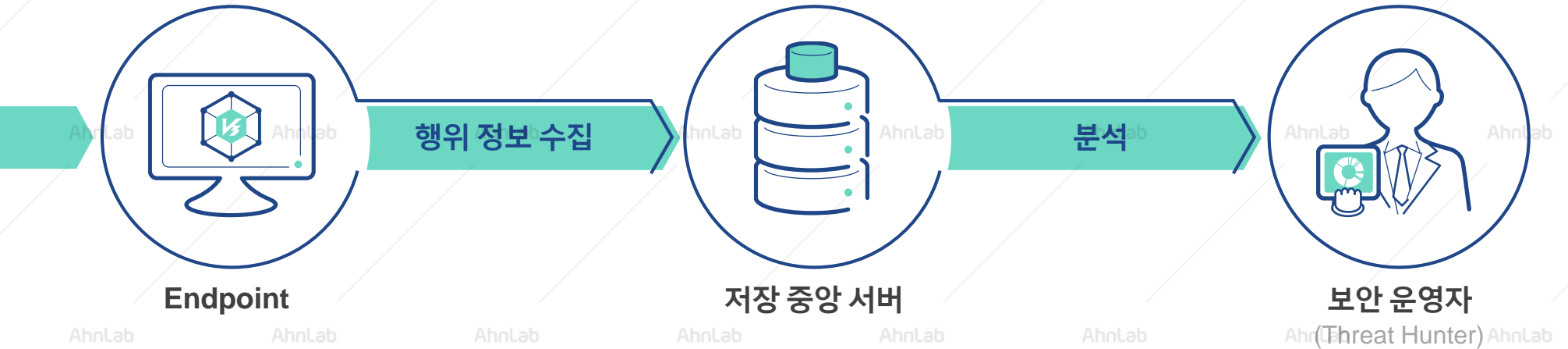
## AhnLab EDR

간편한 구축, 손쉬운 운영,  
더 강력한 위협 대응



# AhnLab EDR: 엔드포인트 행위 정보 수집을 통한 위협 가시성 강화

AhnLab EDR은 안랩의 독자적인 행위 기반 엔진인 MDP 엔진을 통해 엔드포인트의 모든 행위 정보를 수집, 저장하고 탐지된 위협에 대한 유입 경로를 추적, 분석함으로써 기업 및 기관의 위협 가시성을 강화합니다.



## Threat Hunting

- 특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장
- 필요 시 언제든지 위협 및 관련 정보 확인 가능 - 사후 위협 분석 가능

## Centralization

- 중앙화된 로그 저장 및 관리 - 모든 엔드포인트 로그를 중앙 서버에 저장
- 로그 관리 및 분석 편의성 향상

# AhnLab EDR 주요기능 : 위협 가시성

## 위협 이벤트/ 공격 흐름도 Visibility 제공

위협에 대해 상세한 '공격 흐름도' 제공  
 위협의 종류, 행위 및 공격 단계에 따라 적절한 대응 및 조치가 가능  
 AhnLab Family 제품 사용시 연계 정책을 통한 다양한 대응정책 수립 가능

탐지현황
아이전트
파일
행위
IOC
Search

← A.exe 약칭: Backdoor/Win32.Zacom.C2445988  
fe724b83f9845f974ac3cdc0570bc752

연관 관계 다이어그램

Tree Right

구분	Current	행위	Target	탐지 시각
프로세스	파일명: explorer.exe PID: 8084 경로: C:\Windows\explorer.exe	프로세스생성	파일명: A.exe PID: 13254 경로: C:\Users\이자영\Downloads	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:\Users\이자영\Downloads	프로세스생성	파일명: jzsg.exe PID: 4460 경로: C:\Users\이자영\Downloads\jzsg	2017-08-07 10:52:15
프로세스	파일명: jzsg.exe PID: 4460 경로: C:\Users\이자영\Downloads\jzsg	비정상적인 네트워크 패킷 탐지	파일명: explorer.exe PID: 8084 경로: C:\Windows\explorer.exe	2017-08-07 10:52:15
파일	파일명: explorer.exe PID: 8084 경로: C:\Windows\explorer.exe	파일 생성	파일명: mizp PID: null 경로: g:\sample_5\mizp	2017-08-07 10:52:15
프로세스	파일명: jzsg.exe PID: 4460 경로: C:\Users\이자영\Downloads\jzsg	파일 생성	파일명: A.cab PID: null 경로: g:\sample_5\mizp	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:\Users\이자영\Downloads	파일 생성	파일명: jzsg.exe PID: 4460 경로: C:\Users\이자영\Downloads\jzsg	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:\Users\이자영\Downloads	파일 생성	10.2.5.1:80	2017-08-07 10:52:15



## 공격 흐름도 기반 에이전트 즉시 대응

공격흐름도를 통한 즉시 대응  
프로세스, 에이전트, 파일 등에 대한 프로세스 종료/네트워크 차단 등

**규칙 설정**

공통 에이전트 버전 1.0.0.2 = Like

V3 V3 마지막 검사 날짜 10 > ≥ = ≤ <

APM 전체 패치 대상 퍼치율(%) 70 % > ≥ = ≤ <

OR

V3 악성코드/광판 기반 탐지 횟수 5 > ≥ = ≤ < 480 번

**대응 설정**

공통 공지사항 보내기

V3 악성코드 검사

APM 소프트웨어 설치 정책 실행

EDR 파일 검색

파일 이름: testf3ile.exe

해시값: MD5 e9aab7fc954599f16ca8ff1d7efef33

파일 크기: 25

파일 경로: c://

하위 경로 포함

파일 생성 시간  조건 추가

2017-12-05 00 : 00 ~

2018-04-04 00 : 00



## 에이전트, 파일, 행위, IOC 등 검색/상세조회

에이전트, 파일, 행위 등 정보 단위로 검색, 조회, 검색결과 기준 대응 /정책 수립  
IOC파일 import를 통한 검색 가능

The screenshot displays the AhnLab EDR search interface. It is divided into several sections:

- Search Filter:** Includes tabs for '에이전트' (Agents), '파일' (Files), '행위' (Behaviors), 'IOC', and '검색' (Search). A search bar and dropdown menus for '대응하기' (Respond) and '내보내기' (Export) are present.
- Agent List:** A table listing agents with columns for IP, hostname, and status.
 

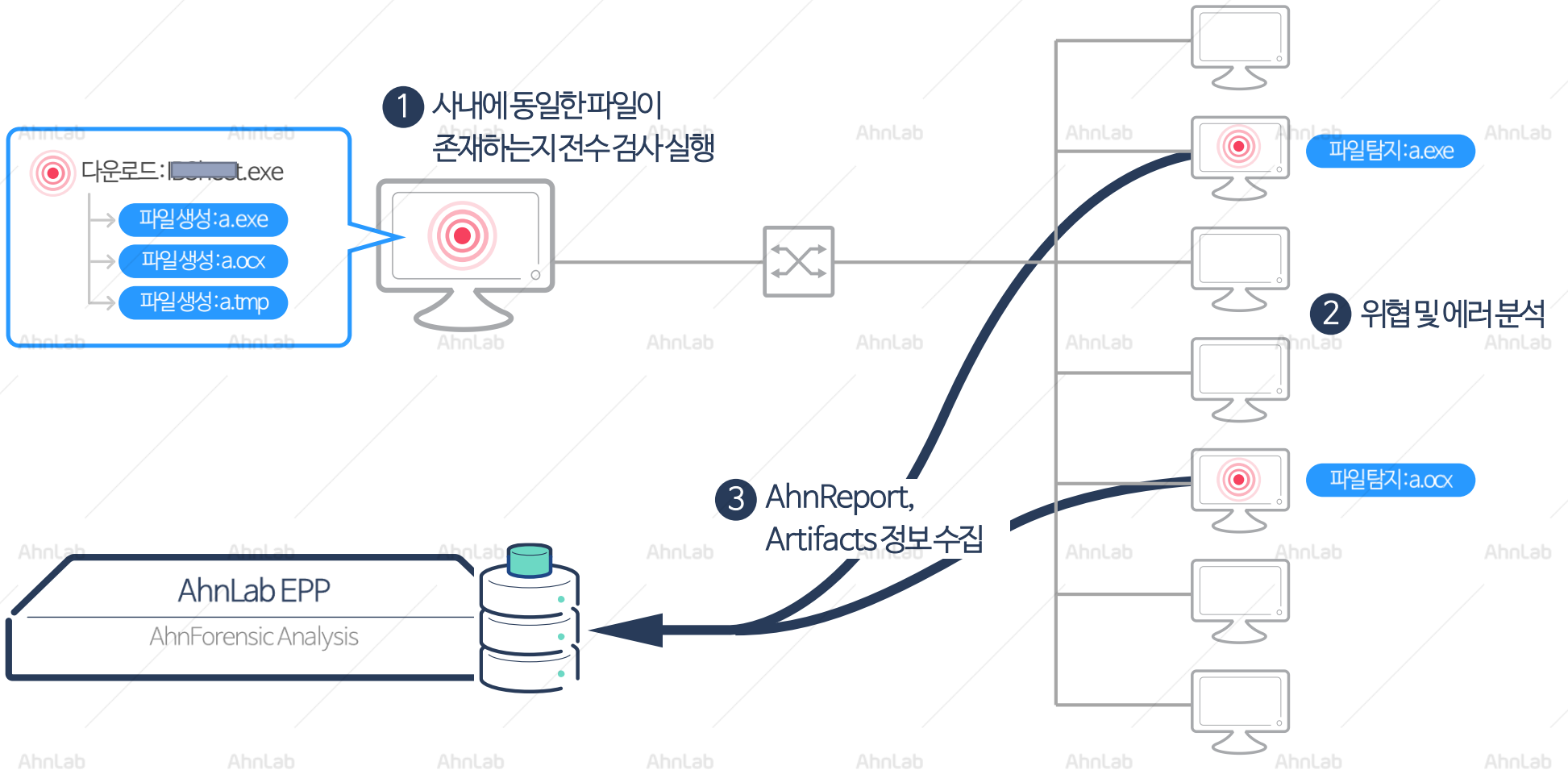
IP	Hostname	Status
1.1.1.1	HONG_PC (정기동)	정기동
172.20.9.12	995-PC (장기동)	장기동
127.0.0.1	994-PC (우기동)	우기동
172.20.9.11	993-PC (양기동)	양기동
2.2.2.11	992-PC (안기동)	안기동
172.27.2.70	compute_name (신기동)	신기동
172.27.2.2	2-PC (김기동)	김기동
172.27.2.1	1-PC (홍기동)	홍기동
- IOC List:** A table showing IOCs with columns for '탐지 현황' (Detection Status), '에이전트' (Agent), and '파일' (File).
 

탐지 현황	에이전트	파일
×	Observable-Pattern-cc5c00ce-98a6-4cbe-8...	
×	Observable-7b97c8a2-2d0b-4af7-bcf0-cad...	
×	Observable-1c798262-a4cd-434d-a958-88...	
×	Observable-Pattern-cc5c00ce-98a6-4cbe-8...	
×	Observable-1c798262-a4cd-434d-a958-88...	
×	Observable-556fa703-8cee-4f23-a135-22ff4d4c1255	
×	Observable-7b97c8a2-2d0b-4af7-bcf0-cad28f2fea5a	
×	Observable-Pattern-cc5c00ce-98a6-4cbe-8474-59eaecdb018f	
- Agent Detail View (172.1.1.1):**
  - 에이전트 정보:** 에이전트 아이디: 9028.343C.8133-win7XX, 컴퓨터 이름: mypc\_test\_01-PC, 서버 접속 IP: 10.2.1.160, Windows 작업 그룹: WORKGROUP, 마지막 로그인 시간: 2017-07-07 14:52:00, 로그인한 사용자: CANO-PC.
  - 사용자 정보:** 사용자 이름: 이자영, 소속 부서: 계통기획팀, 전화번호: 010-0000-0000, 메일 주소: jayoung.lee@ahnlab.com, 사원 번호: 20056005, 관리자 수경 여부: -.
  - 운영체제 정보:** 이름: Microsoft Windows7 Professional K, 상세 정보: Microsoft Windows7 Professional KK..., 플랫폼: Windows NT...
  - 가상화 시스템 정보:** (Expanded arrow)
- V3 현황 (V3 Status Summary):**
  - 연결상태: 연결됨
  - 정책 적용 상태: 모두 적용됨
  - 무결성: 손상되지 않음
  - 에이전트 버전: 1.2
  - V3 연결 버전: 2016.12.14.00
  - 무결성: 손상됨
  - 악성코드 탐지 수: 3건 / 미치트: 1건 (최근 30일)
  - 의심행위 탐지 수: 10건 (최근 30일)
  - 라이선스 만료: ~2018/07/04
- 에이전트 주요 이력 (Agent Activity Table):**

	6/27 화	6/28 수	6/29 목	6/30 금	7/1 토	7/2 일	7/3 월
연진 업데이트	✓	○	✗	✓	○	✓	○
수동 검사	✓	○	✗	✓	○	✓	○
악성코드 탐지	87	0	65	43	77	60	20
의심 행위 탐지	87	0	65	43	77	60	20

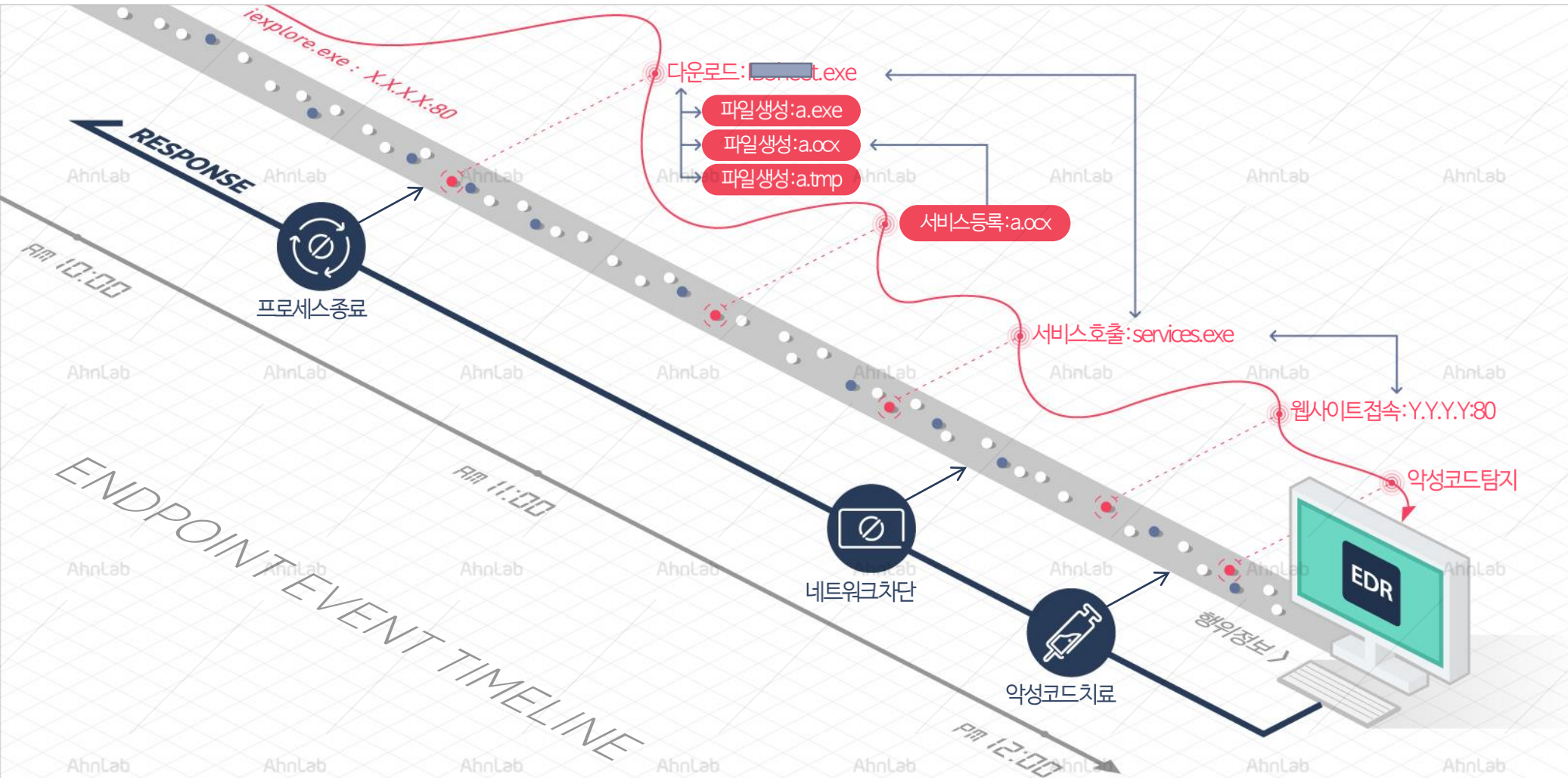
## 파일 수집/검색

에이전트를 통한 실시간 파일 검색/수집 가능  
수집된 파일에 대한 분석 후 대응정책 수립



# 특장점 - 가시성 기반의 강력한 위협 대응력

AhnLab EDR은 엔드포인트 레벨에서 실제 OS 기반의 행위 정보 탐지 및 분석, 위협 이벤트의 타임라인 분석을 통한 엔드포인트 위협 가시성을 제공해 기업 및 기관의 더 강력한 위협 대응력 확보에 기여합니다.



# More security, More freedom

AhnLab

