

# 엔드포인트 행위의 연계 분석을 통한 악성코드 대응

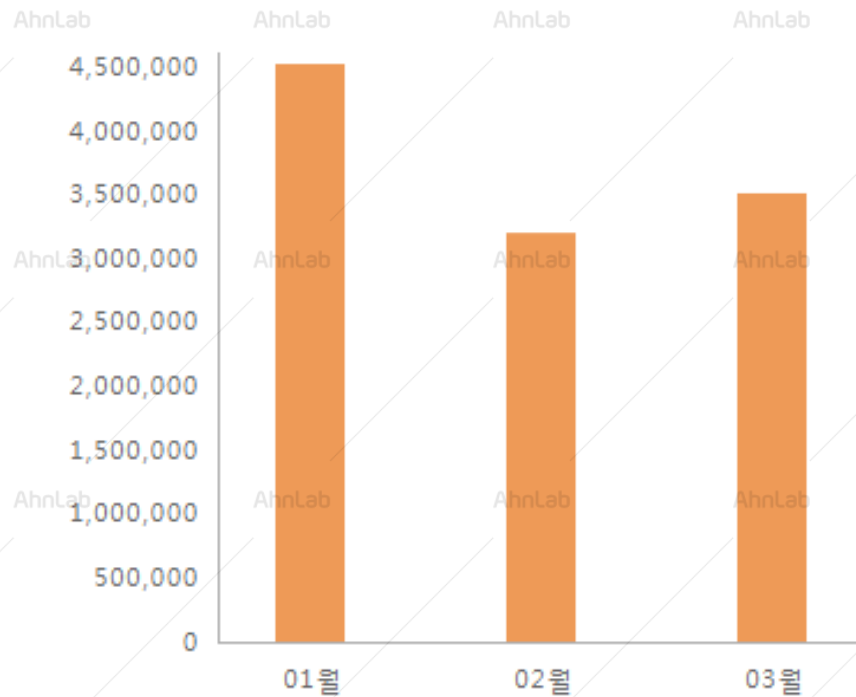
안랩 EP컨설팅팀 명재열 부장

AhnLab

A network diagram consisting of a series of interconnected nodes and lines. The nodes are represented by various icons: a person, a cloud, a document, a shield, a magnifying glass, a Wi-Fi symbol, a gear, a keyboard, a file, a globe, a padlock, and a brain. The diagram is set against a dark blue background with a white grid pattern.

# 악성코드 위협

AhnLab



2019년 3월

**3,512,805개 탐지**

AhnLab 보안통계



# 엔드포인트의 행위 정보 수집

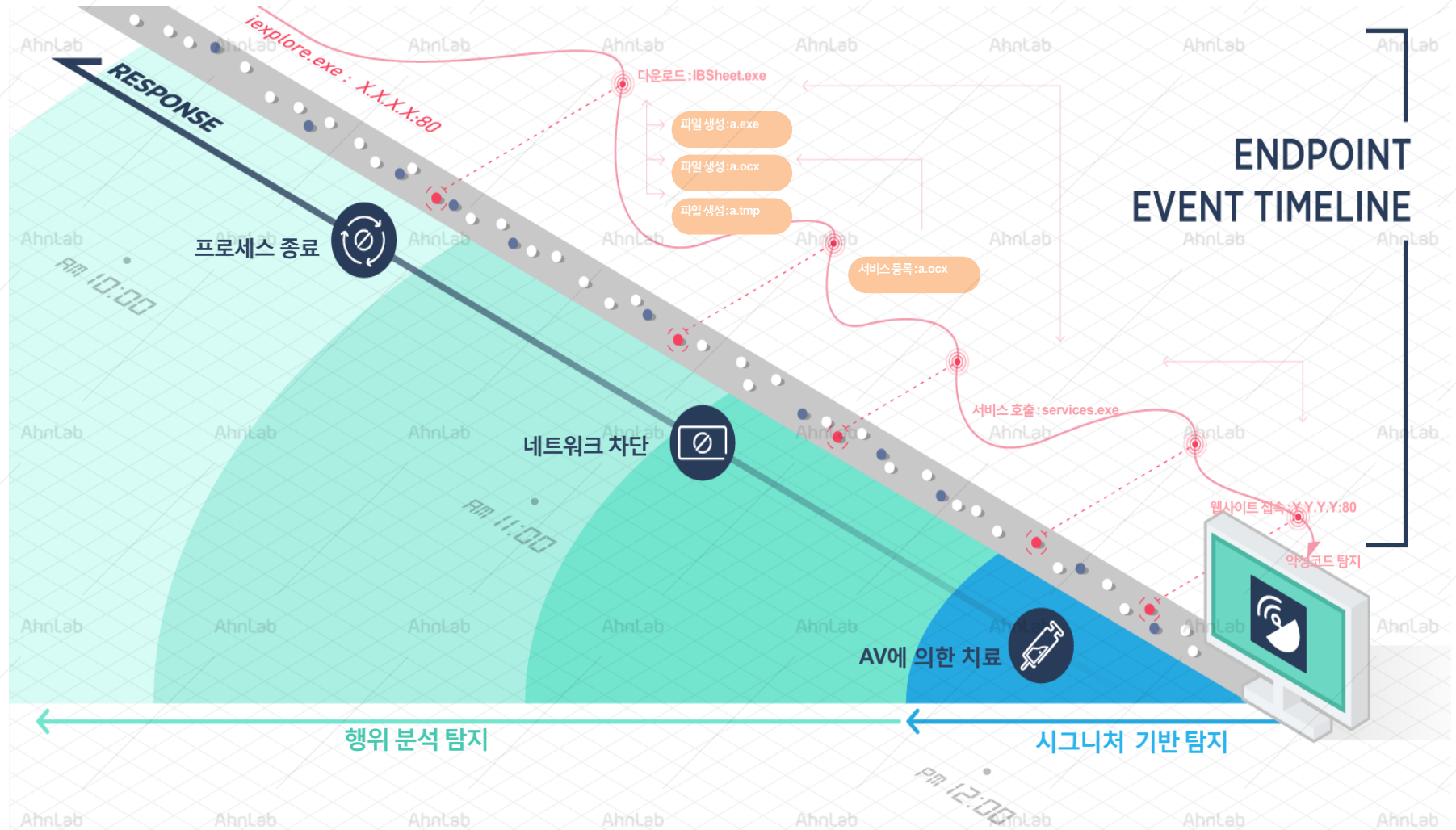


## Threat Hunting

## Centralization

특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장  
필요 시 언제든지 위협 및 관련 정보 확인 가능  
중앙화된 로그 저장 및 관리

# 시간 순서 기반 행위 분석 및 대응



# EPP & EDR

AhnLab

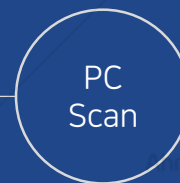


## 개별적인 정책

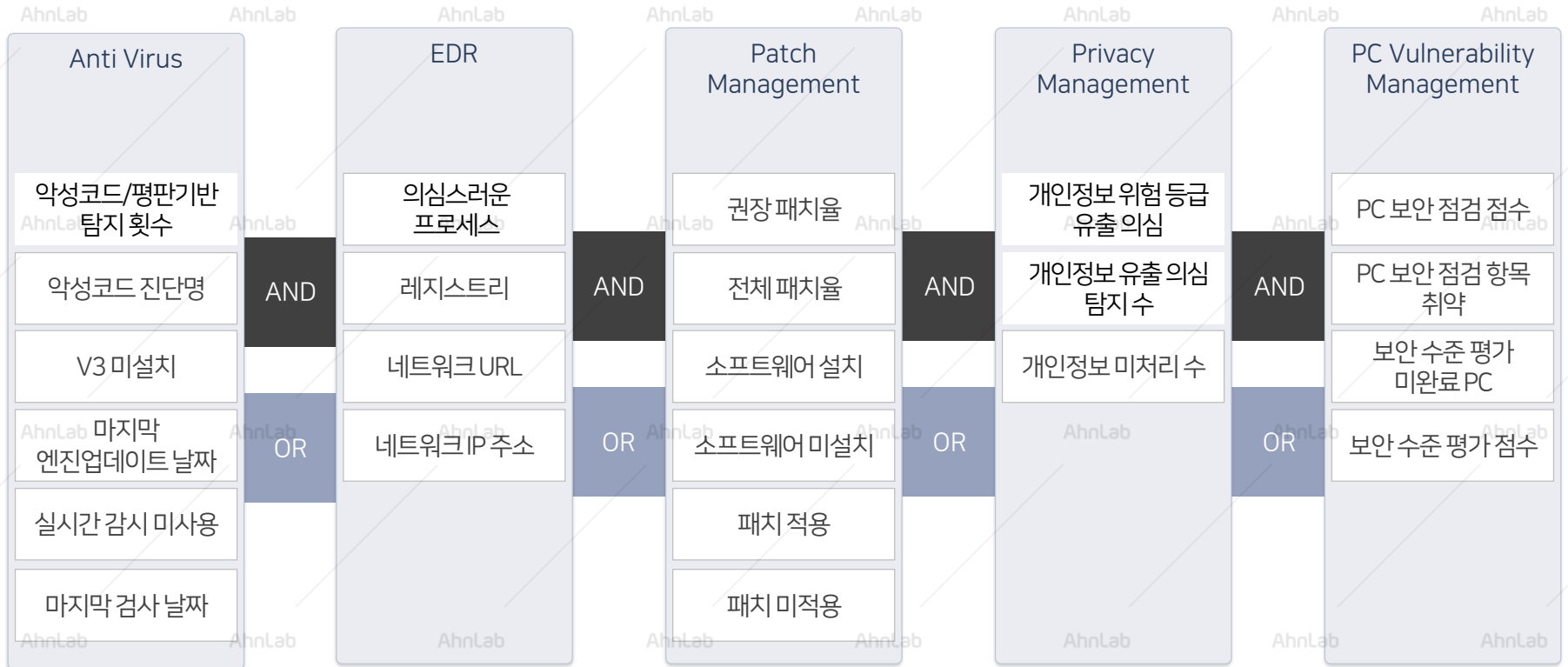


VS

## 복합적인 조건 및 대응







# EPP & EDR 대응 사례

악성코드 감염 PC 정보 조사

Anti-Virus 엔진 업데이트 확인

전체 PC 정밀 검사 실시

백신관리시스템에서 탐지 로그 검색

감염 PC에 대한 네트워크 차단 조치

감염 PC에 정밀 검사 실시

전체 정밀 검사 재실시 후  
추가 감염 PC 확인

백신관리시스템에서 보고서 산출

EDR에서 감염 PC의  
악성행위 분석 및 상세 정보 확인

EPP의 연계 규칙으로 추가 감염 PC 탐지

EPP의 연계 규칙으로 탐지된 추가 감염 PC  
네트워크 차단 및 악성코드 검사

보고서 산출

## 악성코드 감염



# 엔드포인트 악성 행위 탐지



## EDR 연계 규칙 - 탐지 조건

**탐지 조건**

규칙 설정

EDR ▼ 프로세스 이름 ▼ 프로세스 이름: cactls.exe = +

프로세스 경로: C:\Windows\syswow64\

파일 해시값: b2b69786120ca206040dc1f196f77b42 = Like 3 분

V3 ▼ 악성코드 진단명 ▼ Malware/MDP.Pharm.M1402

OR +

EDR ▼ 네트워크 URL ▼ users.qzone.qq.com/ = +

OR x

EDR ▼ 네트워크 IP 주소 ▼ 203.205.151.50 = +

**네트워크 연결**

행위 발생 시각: 2019-03-05 09:07:05

규칙 - 네트워크

**EDR 상세 행위 정보**

[프로세스 정보]

파일 이름: cactls.exe

해시값: b2b69786120ca206040dc1f196f77b42

파일 경로: C:\Windows\syswow64\cactls.exe

파일 크기(bytes): 25600

[대상]


Host 주소: users.qzone.qq.com

IP 주소: 203.205.151.50

포트 번호: 80

URL: users.qzone.qq.com/cgi-bin/cgi\_get\_portrait.fcgi?uins=2464258288

## EDR 연계 규칙 - 대응 조건



정책 | **연계 규칙**

← EDR탐지분석 정보활용

대응 설정

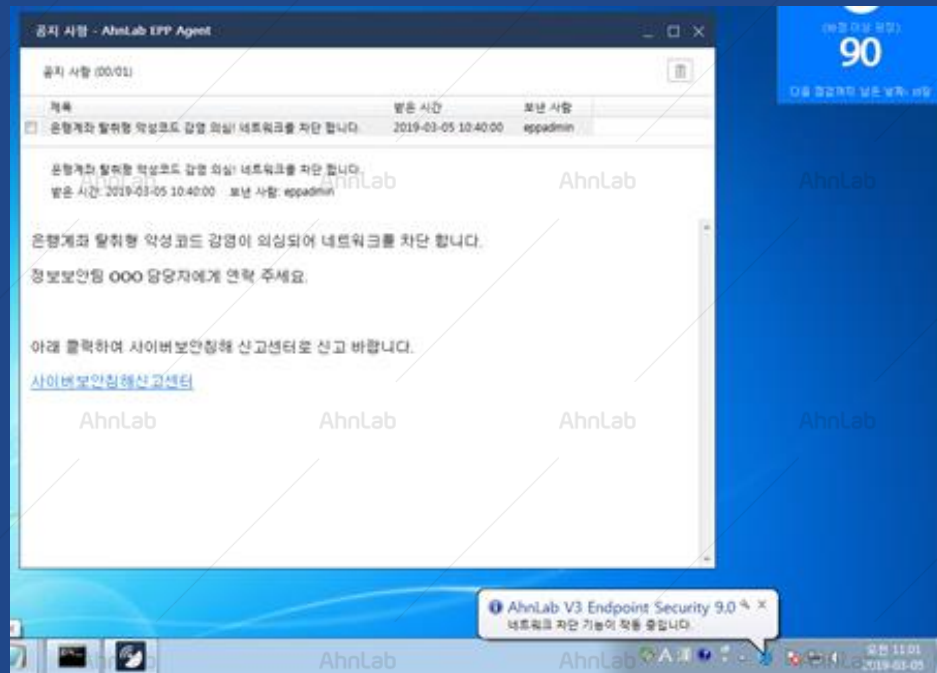
V3	네트워크 완전 차단	+	⌵	⌶
공통	공지 사항 보내기	×	⌵	⌶

제목: 은행계좌 탈취형 악성코드 감염 의심! 네트워크를 차단 합니다.

Format: B I U [List Icons]

은행계좌 탈취형 악성코드 감염이 의심되어 네트워크를 차단 합니다.  
정보보안팀 OOO 담당자에게 연락 주세요.  
아래 클릭하여 사이버보안침해 신고센터로 신고 바랍니다.  
[사이버보안침해신고센터](#)

## EDR 연계 규칙 대응 결과



## 알림 및 보고서

정책/연계 규칙 > 연계 규칙 > 알림/보고서 생성

정책 연계 규칙

← server OS **알림 설정**

기본 설정 규칙 설정 예외 대응 설정 알림/보고서 설정

**알림 설정**

☒ 알림을 제한 시간: 1 분

☒ 알림 기간: 2019-04-16 ~ 2019-04-16

☒ 알림 채널 발송: 연계규칙 알림 채널

이메일 발송할: 연계규칙 알림 채널

이메일 받는 사람: ☒ 해당 관리자/담당자 이메일 주소

☐ 직접 입력

☒ 보고서 생성

보고서 내용: 내부 정보

버전: 1.0.0

**요약**

그룹: 전체 그룹  
기간: 2019-04-01 ~ 2019-04-30  
시작: 2019-04-01 00:00:00  
종료: 2019-04-30 23:59:59

### 보고서

시간 기준 집계 현황

세그먼트	알림	이메일	이메일	이메일	이메일	이메일
서버 OS	52	92%	48	4	90%	44
APM	67%	33	16	10	84%	41

정책 기준 집계 현황

정책	이메일	이메일	이메일	이메일	이메일	이메일
서버 OS	50	2	0	32	0	1
APM	42	5	1	37	1	1
EDR	42	1	1	37	1	1
APM	32	0	1	39	2	0
EDR	32	0	1	39	2	0
APM	32	0	1	39	2	0

V3

백신 엔진 설치 여부/상태

IP	백신 엔진	백신 엔진	백신 엔진
172.20.0.100	24	24	24
172.20.0.102	3	3	3
172.20.0.101	1	1	1
172.20.14.45	1	1	1
192.168.111.102	1	1	1

백신 엔진 설치 여부/상태

IP	백신 엔진	백신 엔진	백신 엔진
172.20.0.100	24	24	24
172.20.0.102	3	3	3
172.20.0.101	1	1	1
172.20.14.45	1	1	1
192.168.111.102	1	1	1



# EPP & EDR 대응 사례

- 악성코드 정보 : 'EternalBlue'SMB 취약점(MS17-010)을 통한 악성코드 감염확산(2019.02.13)
- ※ 출처 (<https://asec.ahnlab.com/1196?category=342979>)

## [중상 및 요약]

EternalBlue SMB 취약점으로 국내 POS 장비에 코인 마이너 전파 공격

## [시스템 행위]

- 파워셸 명령어를 통해 윈도우 계정 패스워드 확인 툴 MINIKATZ 실행
- MIMIKATZ 툴을 통해서 얻은 계정정보와 사용자 도메인 정보를 c:\windows\temp\wmkatz.ini에 저장

## [네트워크 행위]

- 로컬 시스템의 60124번 포트 바인딩
- 445번 포트 방화벽 설정
- 파워셸 명령어를 통해 특정 도메인(v.beahh.com)에서 스크립트 다운로드

## [SMB 취약점 패치]

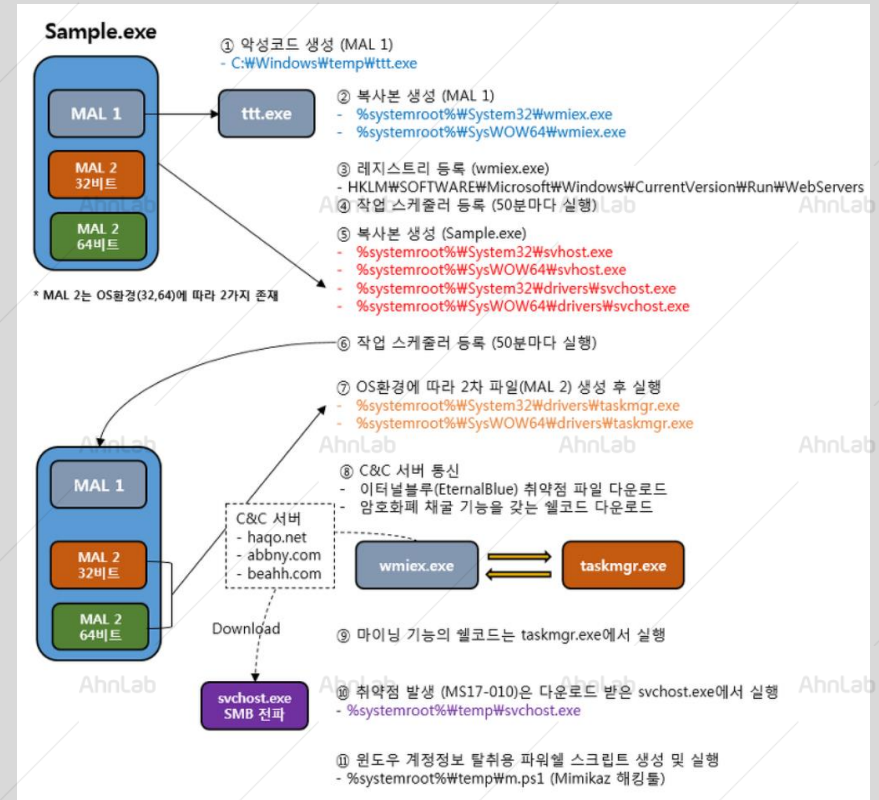
<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

## [파일 진단]

V3에서 아래 진단명으로 진단

파일명	진단명
svchost.exe (SMB 전파)	Trojan/Win32.Trickster.R254998
svchost.exe (sample.exe)	Malware/Win32.Generic.C2950422
wmiex.exe (MAL 1)	Trojan/Win32.Agent.R254993
taskmgr.exe (MAL 2 32bit Binary)	Malware/Win32.Nsanti.C2957178
taskmgr.exe (MAL 2 64bit Binary)	Trojan/Win64.Agent.C3009705
m.ps1 (윈도우 계정탈취)	SCRIPT/Powershell

## [공격 흐름도]



## 연계 규칙 탐지 조건

V3	악성코드 진단명	Trojan/win32.Trickster.	=	Like	3	+
V3	악성코드 진단명	Malware/Win32.Generic.C295042	=	Like	3	×
V3	악성코드 진단명	Trojan/Win32.Agent.R254993	=	Like	3	×
V3	악성코드 진단명	Malware/Win32.Nsanti.C2957178	=	Like	3	×
V3	악성코드 진단명	Trojan/Win32.Agent.C3009705	=	Like	3	×
V3	악성코드/평판 기반 탐지 횟수	5	>	≥	=	≤
APM	패치 미적용	Security Update for Microsoft Windows	=	Like		×
APM	소프트웨어 설치	MINIKATZ 다운로드	=	Like		×
APM	소프트웨어 설치	악성코드설치여부(svhost.tt.wmiex.exe)	=	Like		×
EDR	레지스트리	키: HKEY_LOCAL_MACHINE\SOFTWARE\M	=			×
		값: WebServers				
		데이터: %systemroot%\system32\wmiex.exe				

악성코드 진단명

관련 패치 설치 확인

악성코드 설치 이력

OR +

EDR	네트워크 URL	haqo.net/	=	+
EDR	네트워크 URL	abbny.com/	=	×
EDR	네트워크 URL	beahh.com/	=	×
EDR	네트워크 URL	v.beahh.com/	=	×

C&C 통신

## 연계 규칙 대응 조건

← 2.EternalBlue SMB 취약점 대응

대응 설정

APM	소프트웨어 설치 점검	+	⌵	⌶
ESA	PC 보안 점검 실행	×	⌵	⌶
공통	공지 사항 보내기	×	⌵	⌶

제목

EternalBlue SMB 취약점으로 인한 악성코드에 감염되었습니다.

Heading 3

**B I U** [List Icons] [Link Icon] [Table Icon]

EternalBlue SMB 취약점으로 인한 악성코드에 감염되었으니 아래 조치 방안에 따라 행동해 주시기 바랍니다.

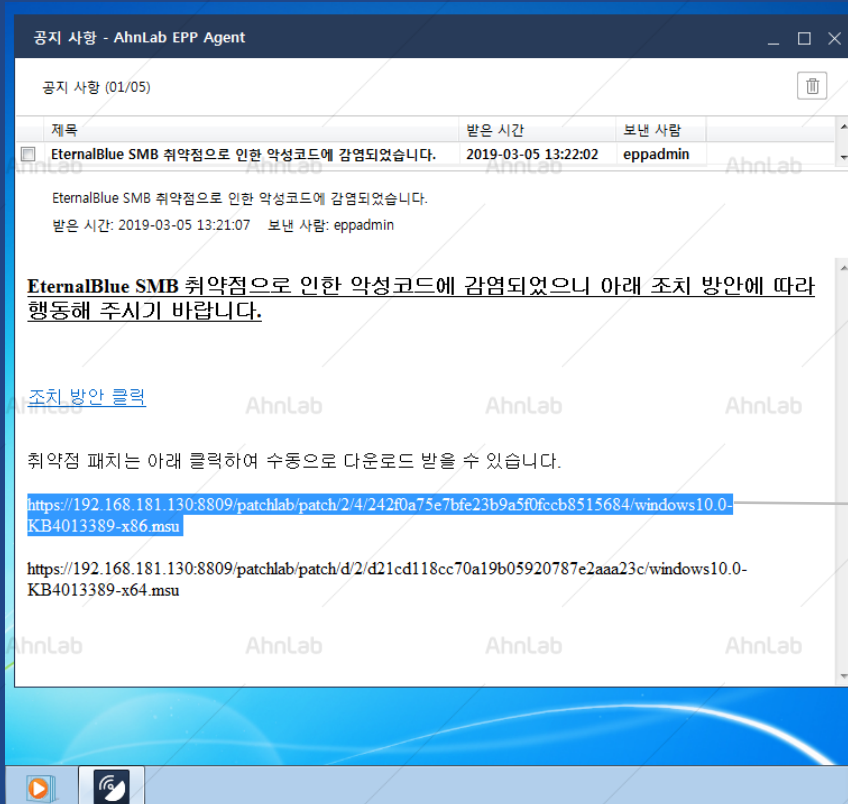
[조치 방안 클릭](#)

취약점 패치는 아래 클릭하여 수동으로 다운로드 받을 수 있습니다.

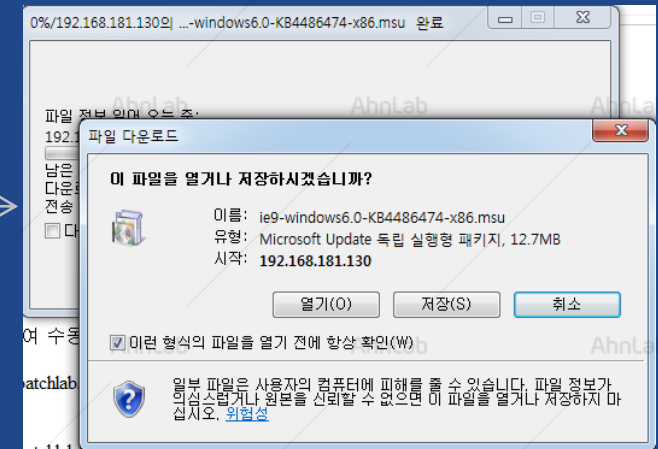
[https://192.168.181.130:8809/patchlab/patch/2/4/242f0a75e7bfe23b9a5f0fccb8515684/windows10\\_0-KB4013389-x86.msu](https://192.168.181.130:8809/patchlab/patch/2/4/242f0a75e7bfe23b9a5f0fccb8515684/windows10_0-KB4013389-x86.msu)

[https://192.168.181.130:8809/patchlab/patch/d/2/d21cd118cc70a19b05920787e2aaa23c/windows10\\_0-KB4013389-x64.msu](https://192.168.181.130:8809/patchlab/patch/d/2/d21cd118cc70a19b05920787e2aaa23c/windows10_0-KB4013389-x64.msu)

## 연계 규칙 매칭 결과



패치 수동 적용



# EPP & EDR 대응 사례

- 악성코드 정보 : PUP/Win32.vGrid.C2774628
- ※ 출처 (<https://www.ahnlab.com/kr/site/securityinfo/asec/asecCodeView.do>)

## [증상 및 요약]

PUP/Win32.vGrid.C2774628, Win-PUP/Grid.Exp 는 설치 파일의 반복적인 재실행을 통해 **디스크 및 CPU 사용률을 급격하게 증가**시킨다.

## [실행 후 증상]

C:\WProgram FilesWv\_service 폴더에 파일을 생성한다.

레지스트리에 서비스 등록을 하여 시스템 시작 시 v\_service.exe 파일을 자동 실행하고 v\_member.exe 파일을 추가 로딩 하여 메모리에 상주.

자동 실행 후 5분 동안 동작 없이 대기하며 5분이 경과하면 v\_member.exe 파일은 프로그램을 업데이트하고 V-Grid 서버와 통신을 시도한다.

이 과정에서 짧은 시간 동안 디스크 읽기를 과도하게 시도하여 디스크 및 CPU 사용률이 급격하게 증가한다.

## [파일 생성]

- C:\Windows\Temp\ctrls.exe
- C:\Users\vmuser\Desktop\309.exe
- C:\WProgram FilesWv\_serviceWv\_service.exe
- C:\WProgram FilesWv\_serviceWv\_member.exe
- C:\WProgram FilesWv\_serviceWuninstall.exe

## [레지스트리 값 등록]

- 키 : HKLM\SYSTEM\CurrentControlSet\services\Wv\_Service\Start
- 값 : 2
- 키 : HKLM\SYSTEM\CurrentControlSet\services\Wv\_Service\ImagePath
- 값 : C:\WProgram FilesWv\_serviceWv\_service.exe

## [차단 권고 URL]

- idx99.vgrid.co.kr
- up.vgrid.co.kr

## 연계 규칙 탐지 조건

V3	악성코드 진단명	PUP/Win32.vGrid.C2774628	=	Like	3	+
APM	소프트웨어 설치	vGrid설치여부	=	Like		×
EDR	레지스트리	키: HKLM\SYSTEM\CurrentControlSet\services	=			×
		값: Start				
		데이터: 2				
EDR	레지스트리	키: HKLM\SYSTEM\CurrentControlSet\services	=			×
		값: ImagePath				
		데이터: C:\Program Files\vv_service\vv_service.exe				
ESA	PC 보안 점검 취약 항목 수	3	>	≥		×
OR +						
EDR	네트워크 URL	idx99.vgrid.co.kr/	=			+
EDR	네트워크 URL	up.vgrid.co.kr/	=			×

악성코드 진단명  
파일 생성

레지스트리 값

취약점 점검

유입 경로

## 연계 규칙 대응 조건

← 3.수동처리가 어려운 PUP 악성코드 대응

대응 설정

ESA	PC 보안 점검 실행	+	⏏	⏏
APM	소프트웨어 설치 점검	×	⏏	⏏
공통	공지 사항 보내기	×	⏏	⏏

제목

PUP/Win32.vGrid 악성코드 감염이 되었으니 삭제 처리 바랍니다.

Format

**B** *I* U [List Icons]

불필요 프로그램인 PUP/Win32.vGrid에 감염되었습니다.

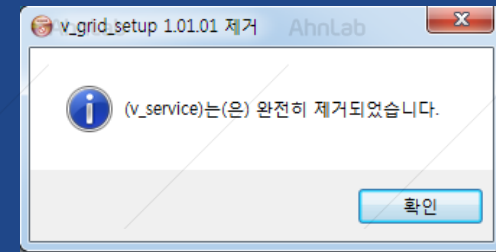
내PC지키미 12번 항목(불필요프로그램 삭제) 보안 조치를 하시거나  
아래 경로를 클릭하여 불필요 프로그램을 바로 삭제하세요.

[vGrid 통합삭제](#)

## 연계 규칙 매칭 결과



수동 삭제





# More security, More freedom

AhnLab

