SPECIAL REPORT

SMB Vulnerability

반복되는 SMB 취약점의 망령, 무엇이 문제인가

2017년 워너크라이 랜섬웨어부터 페트야 랜섬웨어, 배드래빗 랜섬웨어, 2018년 갠드크랩 랜섬웨어 변종, 그리고 2019년 워너마인 채굴 악성코드와 클롭 랜섬웨어까지, 하나의 공통 인자가 있다. 바로 'SMB 취약점'이다. 올해 국내에서는 클롭 랜섬웨어로 인해 AD 서버와 함께 SMB 취약점이 다시 화두가 되었다. 잊을만하면 어김없이 다시 나타나는 SMB 취약점을 이용한 악성코드. 도대체 SMB 취약점이 무엇이길래, 더구나 관련 보안 패치까지 이미 배포된 알려진 취약점임에도 불구하고 우리는 왜 여전히 이것으로 고통받고 있는가. SMB 취약점 기반 공격의 연대기를 통해 피해가 반복되는 이유와 질긴 악연을 끊어낼 해법은 없는지 알아본다.

SMB 취약점이 그 존재감을 본격적으로 드러낸 것은 지난 2017년 5월, 워너크라이(WannaCry, 또는 Wanna-Cryptor) 랜섬웨어를 통해서다. 당시 전 세계 150여 개국 30만대 이상의 시스템을 마비시킬 만큼 워너크라이 랜섬웨어가 파괴력을 발휘할 수 있었던 것이 바로 SMB 취약점 덕분(?)이다. 대체 SMB가 무엇이길래 그토록 엄청난 파급력을 보였을까.

SMB는 '서버 메시지 블록(Server Message Block)'의 약자로, 네트워크 상 존재하는 노드들 간에 자원을 공유할 수 있도록 설계된 윈도우(Windows) 운영체제의 프로토콜이다. 네트워크에 연결된 컴퓨터끼리 파일, 프린터, 포트 또는 기타 메시지를 전달하는 데 사용된다. 이를 통해 서로 다른 운영체제 간에도 자원을 쉽게 공유할 수 있으며 NAS, 네트워크 스캐너 등 리눅스 기기와의 파일 공유 시 클라이언트 없이 탐색기로 직접 수정할 수 있다는 장점이 있어 널리 쓰이고 있다.

이러한 호환성 때문에 SMB 프로토콜은 오랜 시간 자리를 지켜왔으나 동시에 여러 보안 취약점으로 인해 공격자들에게 악용되어 왔다. 대표적인 사례가 바로 몇 년 전에 등장한 워너크라이, 혹은 워너크립터(WannaCryptor)로 불리는 랜섬웨어다. 그러나 SMB 취약점을 이용한 악성코드 연대기는 이보다 무려 10년 전으로 거슬러 올라간다.

SMB 취약점(MS08-067) 전설의 서곡, 컨피커

2008년 후반에 본격적으로 유포되기 시작해 2010년 전 세계 650만 대 컴퓨터를 감염시켰던 컨피커(Conficker)는 윈도우 서버 서비스 원격코드 실행 취약점을 이용하여 전파되는 웜(worm) 바이러스 형태의 악성코드다. 컨피커는 주로 윈도우 보안 취약점(MS08-067)과 관리 공유 폴더(IPC$, ADMIN$), 이동식 디스크를 통해 전파된다. 즉, MS08-067 취약점이 존재하는 시스템이 컨피커에 감염되면 주변의 다른 시스템으로 감염이 확산되어 랜덤한, 또는 B 클래스 IP 대역을 대상으로 리모트 TCP 445 포트를 통해 대량의 트래픽을 발생시켜 조직의 네트워크 자원을 소모한다.

컨피커 웜이 한창 창궐하던 당시, 안랩의 엔지니어들은 고객사 내부에서 확산되던 컨피커를 막기 위해 전용 백신과 보안 패치를 담은 USB를 들고 나섰다. 한 달 남짓 USB 하나를 손에 들고 고객사의 수많은 시스템을 치료하고 패치하여 재부팅하기를 반복하던 안랩의 한 엔지니어가 USB를 통한 컨피커 감염을 직접 경험하고, 결국 자사 제품에 컨피커를 차단할 수 있는 기능을 추가해줄 것을 요구했다. 안랩은 신속히 관련 기능을 제품에 추가했고, 그 결과 보다 빠르고 효과적으로 컨피커 웜 대응이 가능했다. 맨 몸으로 컨피커 웜을 막아보고자 했던 안랩 엔지니어의 열정이 제품에 녹아들 때까지, 그의 마음은 새카맣게 타 들어갔을 것이다.

이렇게 SMB 취약점의 쓴 맛을 봤음에도 불구하고 이것은 곧 사람들의 뇌리에서 조금씩 잊혀졌다. 수많은 기업에서 관련 보안 패치를 적용하지 않은 다수의 시스템이 그대로 운용되는 동안 우리는 또 다른 위기가 다가오는 것을 짐작조차 하지 못 했다.

강렬한 존재감으로 돌아온 SMB 취약점(MS17-010), 워너크립터(일명 워너크라이)

컨피커 웜 사태가 일단락되고도 5~6년이 지난 어느 날, SMB 취약점(MS17-010)을 악용한 워너크립터 랜섬웨어가 전 세계를 강타했다. 당시 대부분의 랜섬웨어가 이메일 첨부 파일이나 손상된 웹사이트를 통해 감염되던 것과 달리 워너크립터 랜섬웨어는 SMB 원격코드 실행 취약점(MS17-010)을 통해 감염됐다.

[그림 1] 워너크립터 랜섬웨어의 랜섬 노트

2017년 전 세계를 휩쓴 워너크립터의 파괴력은 실로 어마어마했다. 당시 사태의 심각성을 인지한 마이크로소프트(MS)에서는 해당 취약점과 관련해 이미 단종된 윈도우XP와 윈도우 서버 2003에 대한 긴급 보안 패치를 예외적으로 배포했을 정도다. 국내에서도 종합 병원, 공장을 비롯해 대형 멀티플렉스 영화관의 시스템이 워너크립터 랜섬웨어에 감염되는 등 적지 않은 피해가 발생했다.

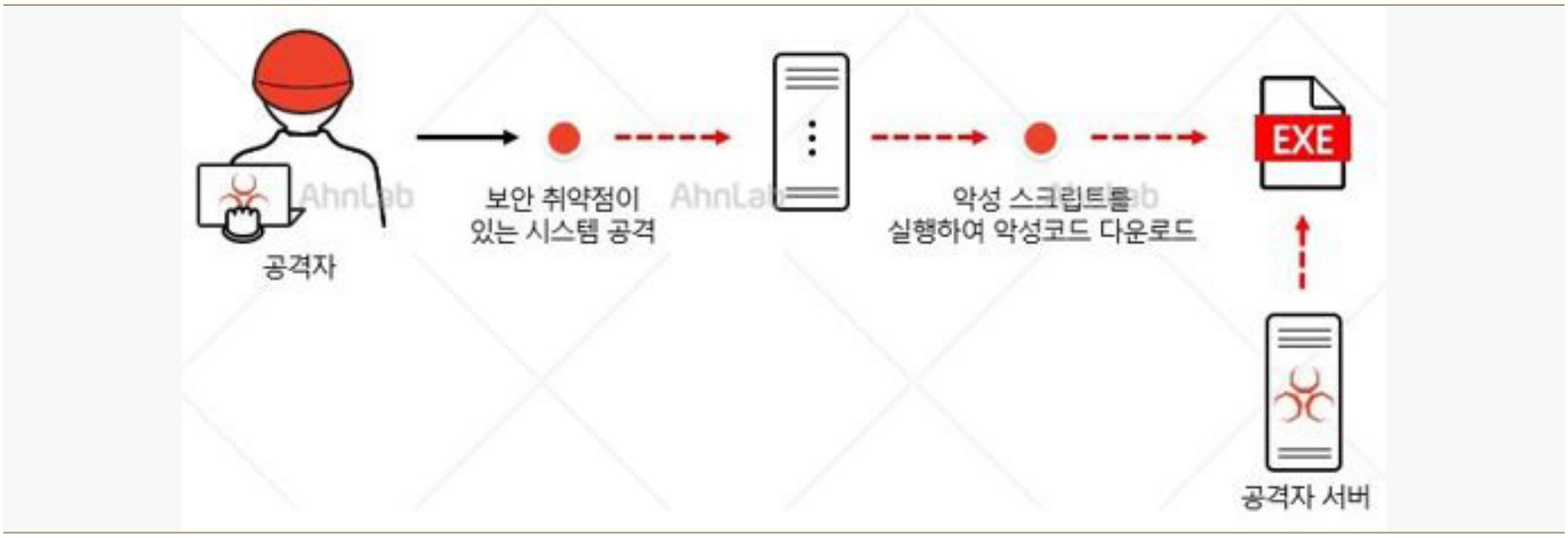
워너크립터 사태를 계기로 국내에서도 보안 패치의 중요성에 대해 다시금 인지하게 되었다. 실제로 당시 많은 기업에서 패치 관리 솔루션에 대해 관심을 갖고 신규 도입을 추진하거나 기 도입된 솔루션의 운영 상태를 재정비했다. 이로써 SMB 취약점은 더 이상 우리에게 위협이 되지 않을 것으로 여겨졌다.

다시 나타난 SMB 취약점(MS17-010)의 그림자, 워너마인

워너크립터, 그리고 동일한 취약점을 이용한 랜섬웨어들이 잠잠해진 후 1년 여가 지난 2019년 우리는 또 다시 MS17-010 취약점 패치를 찾아야만 했다. 이번엔 랜섬웨어가 아닌 암호화폐 채굴(mining) 악성코드 때문이었다.

암호화폐 채굴 악성코드가 증가하며 전파 방식 또한 더욱 다양화되고 있던 중에 SMB 취약점을 이용해 감염·확산되는 암호화폐 채굴 악성코드, 일명 워너마인(WannaMine)이 등장했다. 워너마인은 파일리스(file-less) 방식의 악성코드로, 시스템에서 암호화폐를 채굴하는 동시에 공격자의 서버로부터 또 다른 악성 파일을 다운로드한다. 이때 다운로드하는 것이 바로 워너크립터 랜섬웨어가 사용했던 SMB 취약점 공격 도구인 '이터널블루(EternalBlue)'다. 워너크립터와 동일한 취약점과 공격 도구를 사용했다는 점에서 이 채굴 악성코드는 워너마인으로 명명됐다.

워너마인 악성코드가 보안 담당자를 유달리 긴장시켰던 더 큰 이유는 올해 6월 기승을 부렸던 클롭 랜섬웨어와 함께 유포된 사례가 등장했기 때문이다. 워너마인 악성코드는 SMB 취약점뿐만 아니라 WMI, ADMIN$ 공유 폴더 등을 이용해 내부로 감염이 확산된다.



[그림 2] 워너마인 공격 과정

모래밭의 바늘 같은 SMB 취약점을 잡는 법!

관련 보안 패치가 배포되었음에도 불구하고 몇 년 동안 동일한 취약점이 공격 포인트로 악용되고있다는 것은 많은 것을 시사한다. 어떻게 보안 패치가 적용되지 않은 단말이 존재하는 것일까? 과연 패치 관리가 제대로 되고 있는 것인가? SMB 프로토콜을 계속 사용해도 되는가?

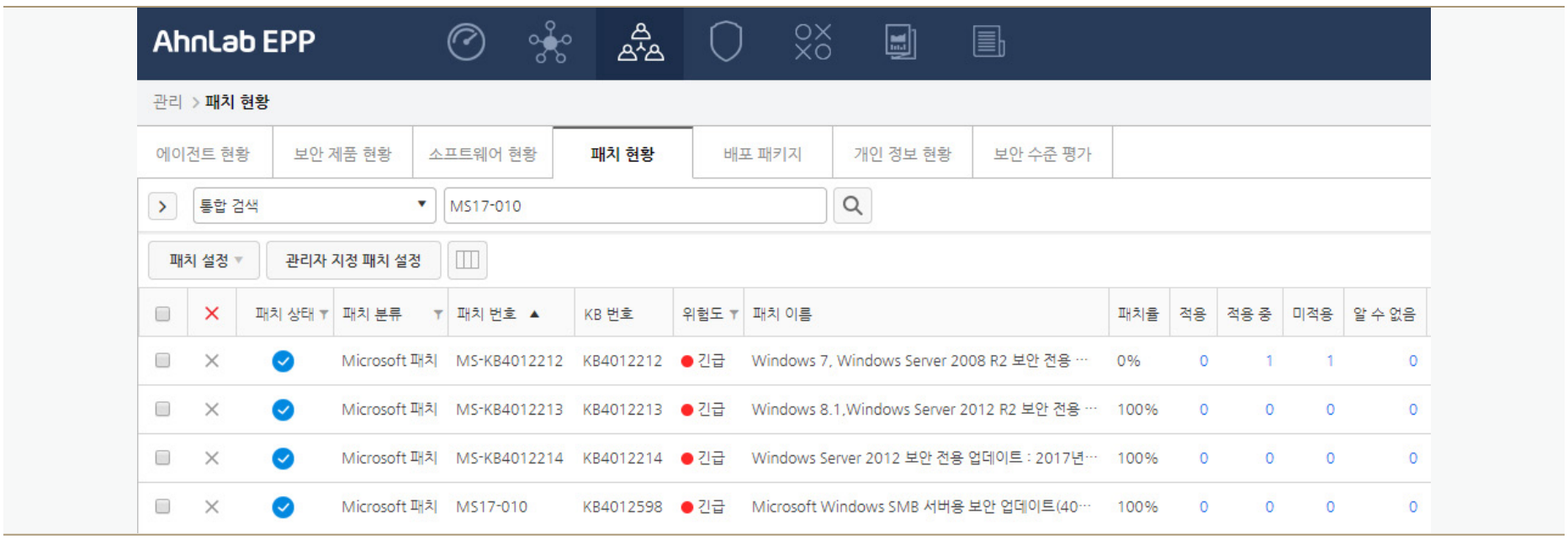
이기종 운영체제 간의 자원 공유를 편리하게 해주는 SMB 프로토콜을 보다 안전하게 사용할 수 있는 방법은 결국 보안 패치를 하는 것이다. 그것도 제대로 해야 한다. 조직 내 모든 단말에 보안 패치가 설치되었는지 확인하고 설치되지 않은 시스템에 적절히 조치할 수 있는 패치 관리 체계가 마련되어 있어야 한다. 현재 패치 관리 솔루션이 없거나 도입하기 여의치 않은 상황이라면 다른 보안 제품으로 대응할 수 있는 부분은 없는지 대책을 마

련하는 것도 중요하다.

보안 패치가 배포된 지 2년여가 지난 SMB 취약점 MS17-010을 중심으로 안랩의 여러 제품을 활용한 SMB 취약점 대응 방안을 살펴본다. 각 기업의 상황에 따라 다음에 소개하는 최신 롤업 패치 적용 및 적용 여부 확인 방법 중 가장 적절한 것을 찾아 즉시 실행할 것을 강력히 권장한다.

1. AhnLab EPP Patch Management를 통한 SMB 취약점 패치 적용

엔드포인트 보안 플랫폼 '안랩 EPP(AhnLab EPP)' 기반의 패치 관리 솔루션 '안랩 EPP 패치 매니지먼트(AhnLab EPP Patch Management, 이하 APM)'를 통해 손쉽게 사내 MS17-010 패치 적용 현황을 파악하고 조치할 수 있다. [그림 3]과 같이 '관리 > 패치 현황' 메뉴에서 패치 미적용 부분의 숫자를 클릭하여 에이전트 리스트 화면으로 이동해 패치 실행 명령을 전송하면 된다.



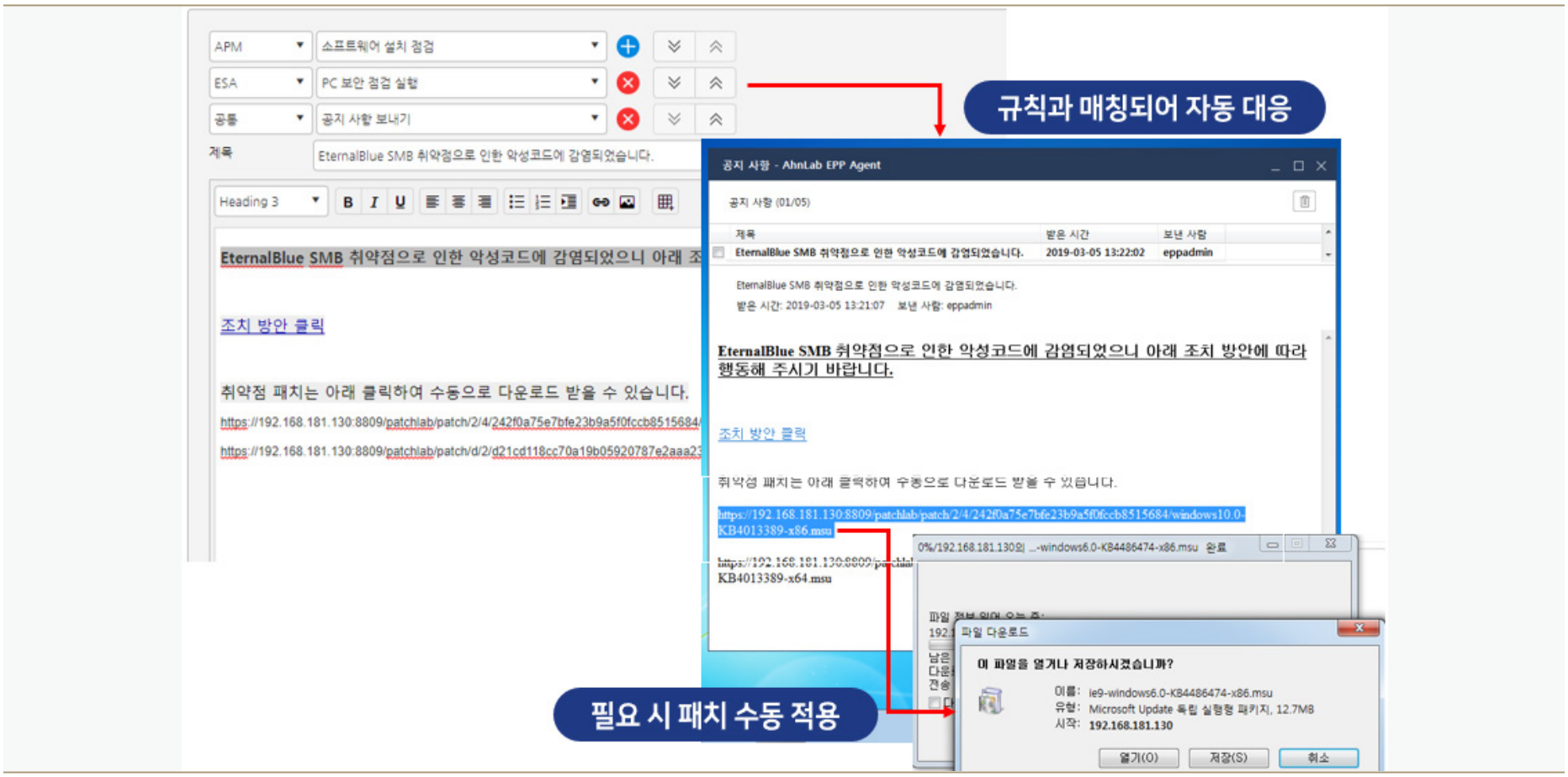
[그림 3] 안랩 EPP 패치 매니지먼트의 패치 적용 현황 정보

엔드포인트 중앙 관리 시스템인 '안랩 EMS(AhnLab EMS)' 기반의 안랩 패치 매니지먼트를 사용 중인 고객사에서도 마찬가지로 패치 적용 현황을 확인하고 미적용 에이전트에 대해 실시간으로 패치 실행 명령을 전송할 수 있다.

2. AhnLab EPP 기반의 연계 규칙을 활용한 자동 대응

보안 롤업 패치는 이전 달의 롤업 패치와 이번 달의 보안 패치들이 포함된 누적 형태로 제공된다. 따라서 MS17-010의 경우, 지난 2017년 3월 이후에 릴리즈된 보안 롤업을 설치하면 해당 패치도 적용된다.

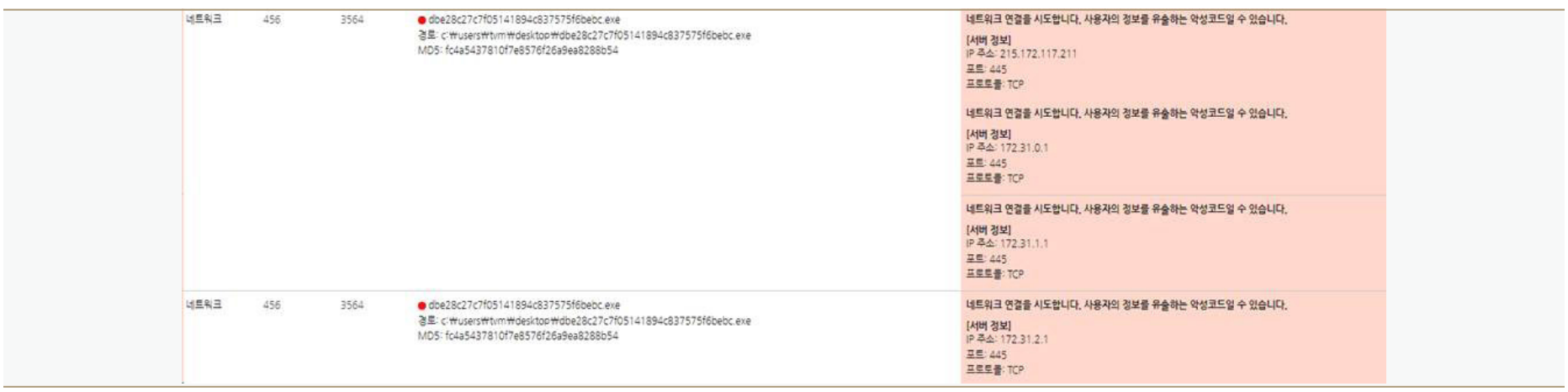
APM을 이용해 최신 보안 롤업 패치를 자동으로 적용할 수 있지만, 엔드포인트 보안 플랫폼인 안랩 EPP의 연계 규칙을 활용하면 각 기업의 환경에 따라 보안 담당자가 입력한 조건에 맞춰 보다 능동적이며 자동화된 대응이 가능하다.



[그림 4] AhnLab EPP의 연계 규칙을 통한 패치 적용 및 대응

3. AhnLab MDS의 C&C 트래픽 현황을 통한 탐지 및 대응

지능형 위협 대응 솔루션 안랩 MDS(AhnLab MDS)는 행위 분석 정보를 통해 알려지지 않은 SMB 취약점 공격을 확인하고 대응할 수 있다. 이상 트래픽(Traffic anomaly)을 모니터링해 445 포트로 특정 IP와 통신을 시도하는 것을 탐지할 수 있으며, 트래픽 미러링을 통해 네트워크를 통한 내부 확산도 탐지할 수 있다.

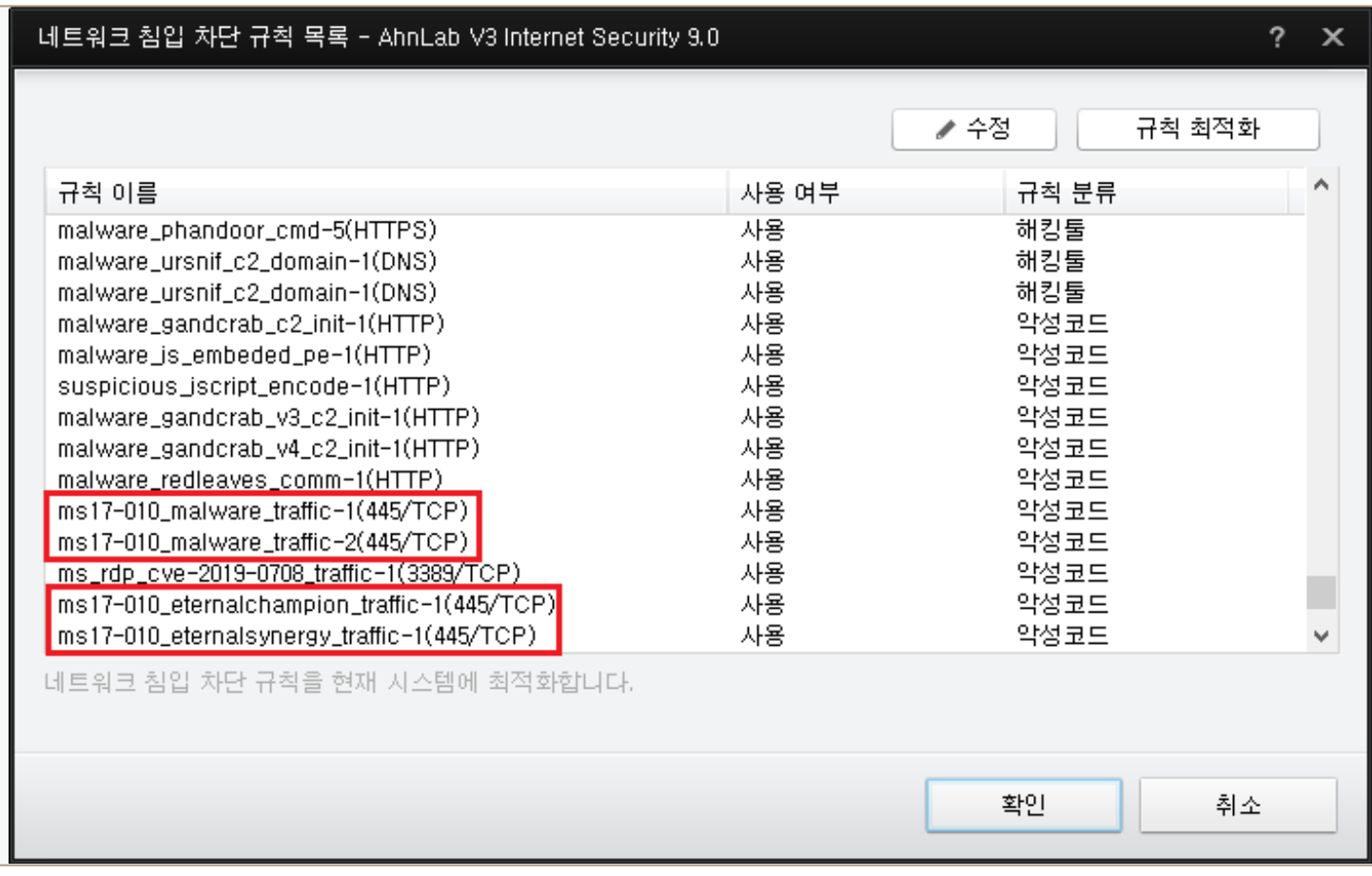


[그림 5] AhnLab MDS가 탐지한 SMB 취약점 공격 행위 로그

또한 이상 트래픽이 발생하는 PC의 안리포트(AhnReport)를 수집해 엔진 기반의 대응이 가능하다. 실제로 안랩 MDS를 구축한 고객사에서는 이상 트래픽을 발생시키는 PC를 추적하여 악성코드를 발견, 이를 V3 엔진에 반영하여 진단한 사례가 있다.

4. V3를 활용한 SMB 취약점 탐지 및 대응

V3의 '네트워크 침입 차단(IPS)' 기능은 네트워크를 통해 침입하는 웜이나 트로이목마와 같은 악성코드를 탐지하여 차단한다. 안랩은 지속적으로 최신 위협을 분석해 V3의 IPS 탐지 룰에 추가한다. 보안 관리자는 업데이트된 최신 IPS 탐지 룰을 활용해 만에 하나 내부에 감염 PC가 발생하더라도 동일한 네트워크 상에 존재하는 다른 PC로 확산되지 않도록 위협을 차단할 수 있다.



[그림 6] V3의 네트워크 침입 차단(IPS) 규칙 예시

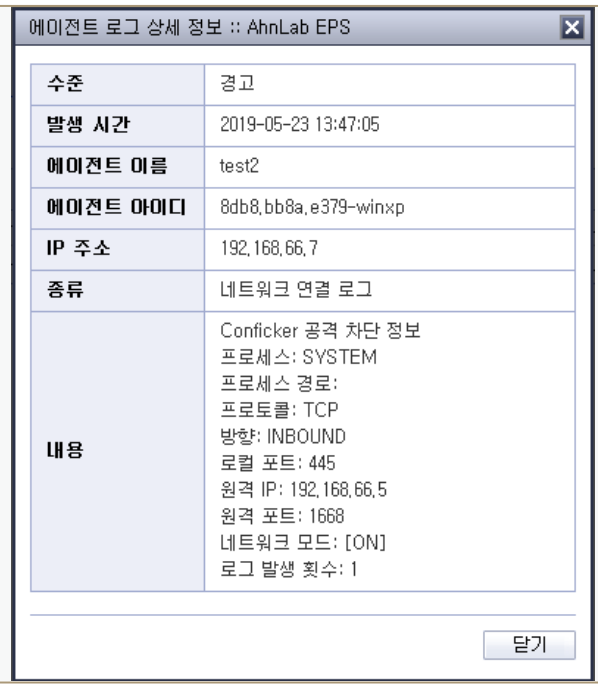
5. AhnLab EPS를 활용한 생산설비의 SMB 취약점 대응

컨피커 웜은 일반 PC가 아닌 POS 단말기나 생산설비 등 특수 목적 시스템을 타깃으로 한다. 안랩의 특수 목적 시스템 전용 보안 솔루션인 안랩 EPS(AhnLab EPS)는 MS08-067 취약점을 통해 공격하는 컨피커를 차단하는 기능을 제공해 컨피커의 내부 전파를 차단하는 것은 물론, 숙주까지 찾아낸다. 인바운드(inbound) 및 아웃바운드(outbound) 로그를 통해 공격하고 있는 숙주 IP와 감염된 노드를 식별할 수 있다. 즉, 인바운드 로그를 통해 현재 감염이 되어 외부로 공격하는 시스템을 확인할 수 있으며, 같은 네트워크 상에 존재하는 감염 시스템으로부

터 들어오는 공격을 받는(아웃바운드) 시스템을 파악할 수 있다.

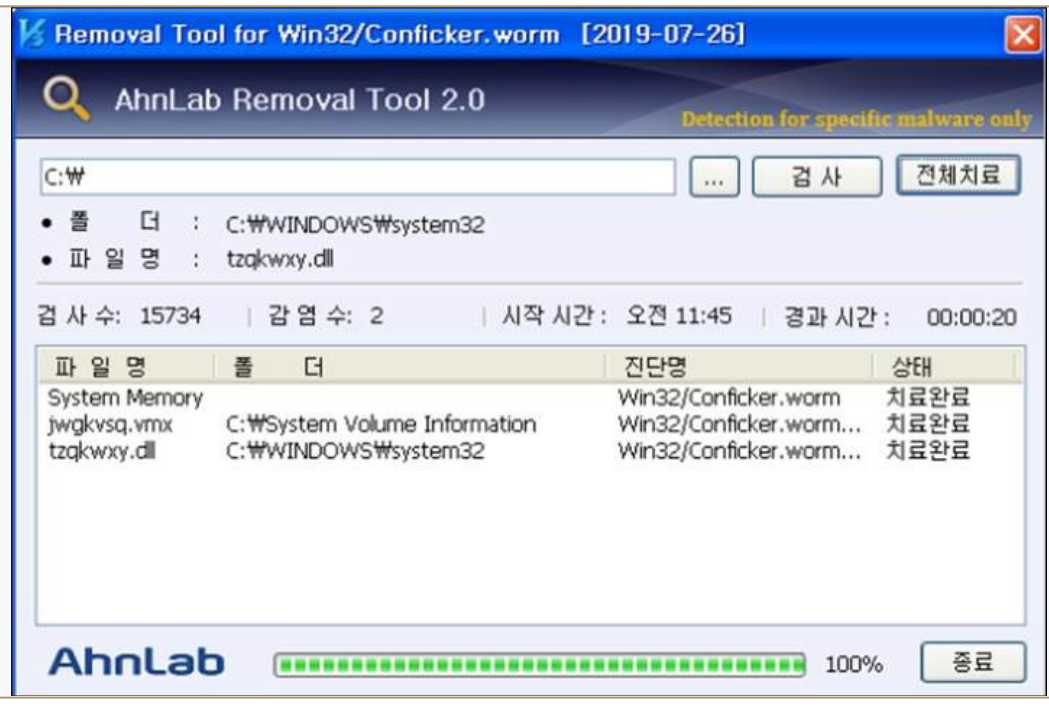
수준	발생 시간	에이전트 이름	종류	내용
경고	2019-05-23 13:49:44	test2	네트워크 연결 로그	Conficker 공격 차단: [ON] OUTBOUND 원격 IP: 192.168.66.5 원격 포트: 445 (TCP)
경고	2019-05-23 13:47:05	test2	네트워크 연결 로그	Conficker 공격 차단: [ON] INBOUND 원격 IP: 192.168.66.5 원격 포트: 1668 (TCP)

[그림 7] AhnLab EPS의 컨피커 공격 탐지 로그



[그림 8] AhnLab EPS의 인바운드/아웃바운드 및 에이전트 상세 로그 정보

안랩 EPS를 통해 컨피커 감염이 의심되는 시스템이 확인되면 전용 백신을 관리자 권한으로 실행하여 스캔 및 치료를 진행한다. 전용 백신을 통해 치료하면 쓰레드(thread)가 종료되지 않기 때문에 반드시 재부팅 해야한다.



[그림 9] 컨피커 전용백신을 이용한 진단 및 치료

6. 패치 관리 솔루션(PMS)이 없는 경우

별도의 패치 관리 솔루션이 없거나 위와 같은 제품의 기능을 활용할 수 없는 경우라도 SMB 취약점 패치를 적용할 수 있으니 좌절하지 말자. 기본적으로 PC의 '윈도우 자동 업데이트' 기능을 통해 업데이트를 하거나, 다음과 같이 한국인터넷진흥원(KISA)이 인터넷보호나라 사이트를 통해 제공하는 관련 가이드를 참고할 수도 있다.

▶ KISA 'SMB 취약점을 이용한 랜섬웨어 공격 주의 권고' 바로가기
▶ KISA 'SMB 취약점 관련 Windows XP, Server 2003 등 긴급 보안 업데이트 권고' 바로가기

폐쇄망 환경이라면 마이크로소프트(MS) 홈페이지를 통해 운영체제별 패치 파일을 다운로드한 후 이를 폐쇄망 내 시스템에 적용하는 방법이 있다. 이런 여러 방법으로도 관련 보안 패치를 적용할 수 없다면 방화벽을 통해 SMB 포트를 차단하고 운영체제의 설정을 이용하여 SMB 프로토콜을 비활성화 시킨다. RDP(Remote Desktop Protocol, 원격 데스크톱 프로토콜)를 사용할 경우, IP 접근 통제와 기본 포트 번호 변경을 권고한다.

손자병법에 따르면 '최고의 승리는 싸우지 않고 이기는 것'이라 한다. 또 '적을 알고 나를 알면 백 번을 싸워도 백 번 다 이길 수 있다'고도 한다. SMB 취약점을 이용해 공격해오는 적(해커)과 싸우는 대신, 보안 패치를 잘 적용하고 있는지 파악하여 조치만 해두면 백 번의 공격에도 싸우지 않고 손쉽게 승리할 수 있을 것이다. 문제점도 알고, 해결법도 알면서 당하는 상황을 더 이상 반복하지 않도록 하자.