THREAT ANALYSIS

EPS FILE THREAT

악성 한글(HWP) 파일 공격 기법

공공기관 · 기업 위협하는 EPS 파일 공격, 핵심은?

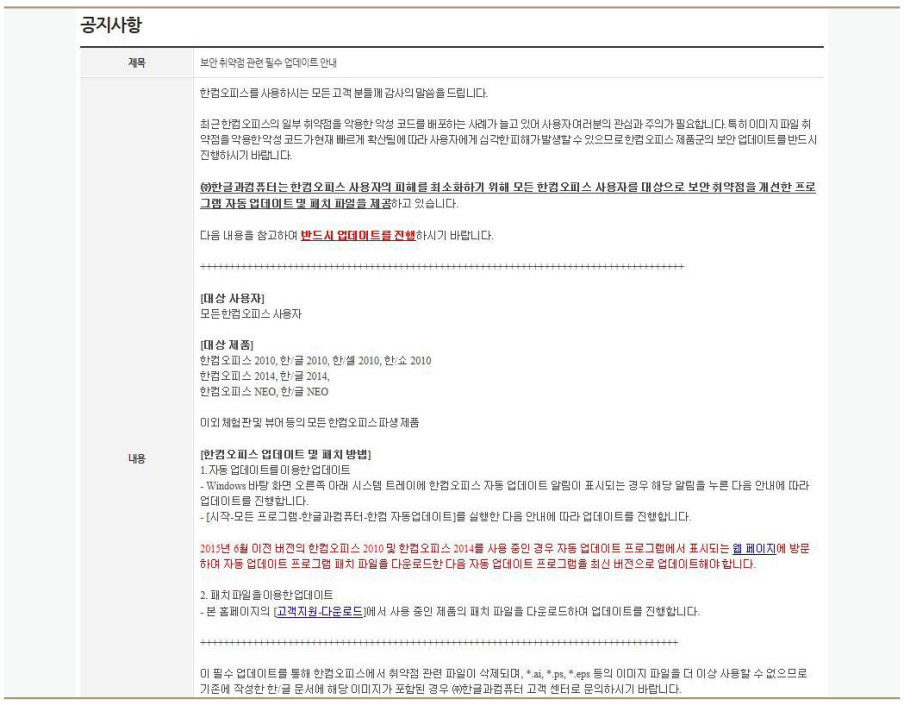
최근 '기록부'라는 이름의 악성 한글(HWP) 파일이 첨부된 이메일이 발견됐다. 해당 파일은 악성 EPS 파일과 관련된 것으로, 주요 공공기관 및 기업을 노린 한글 파일 공격에 악성 EPS 파일을 이용하는 사례가 지속적으로 증가하고 있다. 악성 EPS 파일이 한컴오피스 프로그램 자체의 문제는 아니지만, 한글과컴퓨터는 지난 2017년 이와 관련된 보안 패치를 배포한 바 있다. 그럼에도 불구하고 EPS 파일을 이용한 악성 한글 파일 공격이 지속적으로 발생하고 있다. 이 글에서는 EPS 파일의 악성 행위 발생 과정과 이에 대한 피해 예방법을 살펴본다.

안랩의 악성코드 분석 및 대응 조직인 시큐리티대응센터(AhnLab Security Emergency response Center, ASEC)에 따르면, 국내 주요 공공기관 및 기업을 대상으로 악성 한글 문서 파일(*.HWP)이 지속적으로 유포되고 있다. 또한 지난 2016년부터 2018년 11월 현재까지 보고된 악성 한글 파일 중 상당수가 EPS 취약점(EPS 파일)을 이용한 것으로 확인됐다.

EPS(Encapsulated PostScript) 파일은 일종의 그래픽 파일 형식으로, 어도비(Adobe)에서 제작한 포스트스크립트(PostScript) 프로그래밍 언어를 이용하여 그래픽 이미지를 생성하는 파일이다. EPS를 이용해 각종 고화질 벡터 이미지를 표현할 수 있기 때문에 한컴오피스에서는 문서에 EPS 이미지를 포함하거나 볼 수 있는 기능을 제공하고 있다.

문제는 공격자가 악의적으로 EPS를 만들어 한컴오피스의 한글 문서에 포함하면 사용자가 해당 문서 파일을 실행할 때 악의적인 기능이 수행된다는 점이다. 한컴오피스 프로그램 자체의 문제는 아니지만 EPS 파일을 읽고 처리하는 과정에서 실행되는 하위 프로세스에서 악성 행위가 발생한다.

이와 관련해 한글과컴퓨터는 지난 2017년 초, 한컴오피스의 EPS 파일 처리 과정에서 악성코드가 실행되는 문제를 막기 위한 보안 업데이트를 배포하고 [그림 1]과 같이 홈페이지를 통해 관련 내용을 상세히 안내한 바 있다. 해당 업데이트를 적용한 한컴오피스 프로그램에서는 한글 문서 파일에 포함된 악성 EPS 파일이 동작하지 않는다. 그러나 여전히 해당 보안 패치를 적용하지 않은 기관 및 기업이 많아 피해가 우려된다.



공지사항

제목	보안 취약점 관련 필수 업데이트 안내
내용	한컴오피스를 사용하시는 모든 고객 분들께 감사의 말씀을 드립니다. 최근 한컴오피스의 일부 취약점을 악용한 악성 코드를 배포하는 사례가 늘고 있어 사용자 여러분의 관심과 주의가 필요합니다. 특히 이미지 파일 취약점을 악용한 악성 코드가 현재 빠르게 확산됨에 따라 사용자에게 심각한 피해가 발생할 수 있으므로 한컴오피스 제품군의 보안 업데이트를 반드시 진행하시기 바랍니다. ㈜한글과컴퓨터는 한컴오피스 사용자의 피해를 최소화하기 위해 모든 한컴오피스 사용자를 대상으로 보안 취약점을 개선한 프로그램 자동 업데이트 및 패치 파일을 제공하고 있습니다. 다음 내용을 참고하여 반드시 업데이트를 진행하시기 바랍니다. ++ [대상 사용자] 모든한컴오피스 사용자 [대상 제품] 한컴오피스 2010, 한/글 2010, 한/셀 2010, 한/쇼 2010 한컴오피스 2014, 한/글 2014, 한컴오피스 NEO, 한/글 NEO 이외 체험판및 뷰어 등의 모든 한컴오피스 파생 제품 [한컴오피스 업데이트 및 패치 방법] 1. 자동 업데이트를 이용한 업데이트 - Windows 바탕 화면 오른쪽 아래 시스템 트레이에 한컴오피스 자동 업데이트 알림이 표시되는 경우 해당 알림을 누른 다음 안내에 따라 업데이트를 진행합니다. - [시작-모든 프로그램-한글과컴퓨터-한컴 자동업데이트]를 실행한 다음 안내에 따라 업데이트를 진행합니다. 2015년 6월 이전 버전의 한컴오피스 2010 및 한컴오피스 2014를 사용 중인 경우 자동 업데이트 프로그램에서 표시되는 웹 페이지에 방문하여 자동 업데이트 프로그램 패치 파일을 다운로드한 다음 자동 업데이트 프로그램을 최신 버전으로 업데이트해야 합니다. 2. 패치 파일을 이용한 업데이트 - 본 홈페이지의 [고객지원-다운로드]에서 사용 중인 제품의 패치 파일을 다운로드하여 업데이트를 진행합니다. ++ 이 필수 업데이트를 통해 한컴오피스에서 취약점 관련 파일이 삭제되며, *.ai, *.ps, *.eps 등의 이미지 파일을 더 이상 사용할 수 없으므로 기존에 작성한 한/글 문서에 해당 이미지가 포함된 경우 ㈜한글과컴퓨터 고객 센터로 문의하시기 바랍니다.

[그림 1] 한컴오피스 보안 패치 관련 공지 사항
(*출처: 한글과 컴퓨터 홈페이지, www.hancom.com)

EPS 파일의 동작 방식

한컴오피스 프로그램에서 EPS 파일을 읽고 처리하는 프로세스를 상세히 살펴보자. 한글 문서 파일, 즉 HWP 파일의 구조를 보면, EPS 이미지 파일은 복합 파일(Compound File) 구조 상 BinData 스토리지에 zlib으로 압축되어 존재하며, *.EPS 또는 *.PS의 확장자를 갖는다. EPS 파일은 포스트스크립트 코드로 만들어졌기 때문에 이를 실행하기 위해서는 별도의 인터프리터(Interpreter)가 필요하다. 이와 관련해 한컴오피스 프로그램의 설치 경로에는 아래와 같이 고스트스크립트(GhostScript) 인터프리터가 포함되어 있다.

> dir "<한글프로그램설치경로>\Bin\ImgFilters\GS"
- gbb.exe: 한글과컴퓨터가 제공하는 포스트스크립트 인터프리터 – gsdll32.dll 로드를 통해 동작
- gsdll32.dll: 고스트스크립트 인터프리터 핵심 라이브러리
- gswin32.exe: 고스트스크립트 인터프리터 GUI 버전 – gsdll32.dll 로드를 통해 동작
- gswin32c.exe: 고스트스크립트 인터프리터 커맨드 버전 – gsdll32.dll 로드를 통해 동작

EPS 파일이 포함된 HWP 파일이 이미지를 로드할 때 한컴오피스 프로그램의 OLE 구조상 BinData 스토리지(폴더)에 있는 EPS 파일(스트림)은 임시 파일로 생성된다. 한컴오피스 프로세스는 생성된 임시 파일을 인터프리터가 전달받아 처리하도록 gbb.exe 프로세스와 gswin32c.exe 프로세스에 임시 파일 경로를 인자로 전달하여 실행한다. 따라서 프로세스 트리(Process Tree)는 hwp.exe 프로세스 실행 후 차일드 프로세스(Child Process)로 gbb.exe 프로세스와 gswin32c.exe 프로세스가 실행되는 구조다.

EPS를 이용한 악성 한글 파일이 처음 등장했던 것은 2016년으로, 이후 지속적으로 증가하는 추세다. 악성 EPS 파일은 실행 방식 및 역할에 따라 ▲취약점 익스플로잇(Exploit)을 통한 쉘코드(Shellcode) 실행 ▲악성 파일 생성 등 두 가지로 나눌 수 있다. 한동안은 시그니처 기반의 탐지가 어려운 취약점 익스플로잇 유형이 대부분이었으나 현재는 악성 파일을 생성하는 드롭퍼(Dropper) 유형이 증가하며 고도화되는 추세다.

EPS 파일을 이용한 두 가지 공격 방식을 좀 더 상세히 살펴보자.

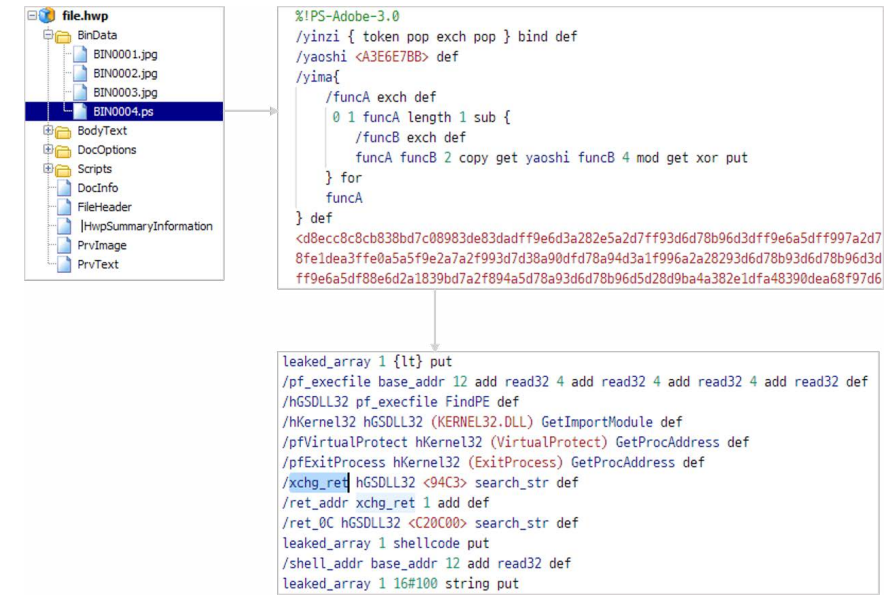
EPS 파일 공격 방식 1: 익스플로잇 및 쉘코드 실행

EPS 파일 뷰어 또는 인터프리터 취약점을 익스플로잇하여 쉘코드를 실행하는 유형으로, 취약점별로 세분화할 수 있다. 올해 확인된 EPS 파일 공격 방식은 대부분 CVE-2017-8291 취약점을 이용했다. CVE-2017-8291는 고스트스크립트 취약점으로, 9.21 버전 이하에 동작한다. 한컴오피스 프로그램에 포함된 고스트스크립트의 버전은 해당 취약점에 영향을 받는 8.6 또는 8.71 이다. 따라서 한컴오피스 사용자는 한컴오피스에서 지난 2017년 배포한 보안 패치를 반드시 적용해야 한다.

한편, 포스트스크립트 코드는 대개 스트링 패턴 기반의 탐지를 우회하도록 인코딩되어 있다. 이를 디코딩하여 분석하면 메모리에서 쉘코드를 실행하기 위해 의도적으로 코드를 비정상적으로 구성한 것을 확인할 수 있다. 포스트스크립트는 스택 기반의 프로그래밍 언어로, 메모리 주소에 값을 저장하고 스택을 참조해서 값을 가져온다. 따라서 쉘코드 HEX 스트링을 저장한 변수를 필수로 포함한다.

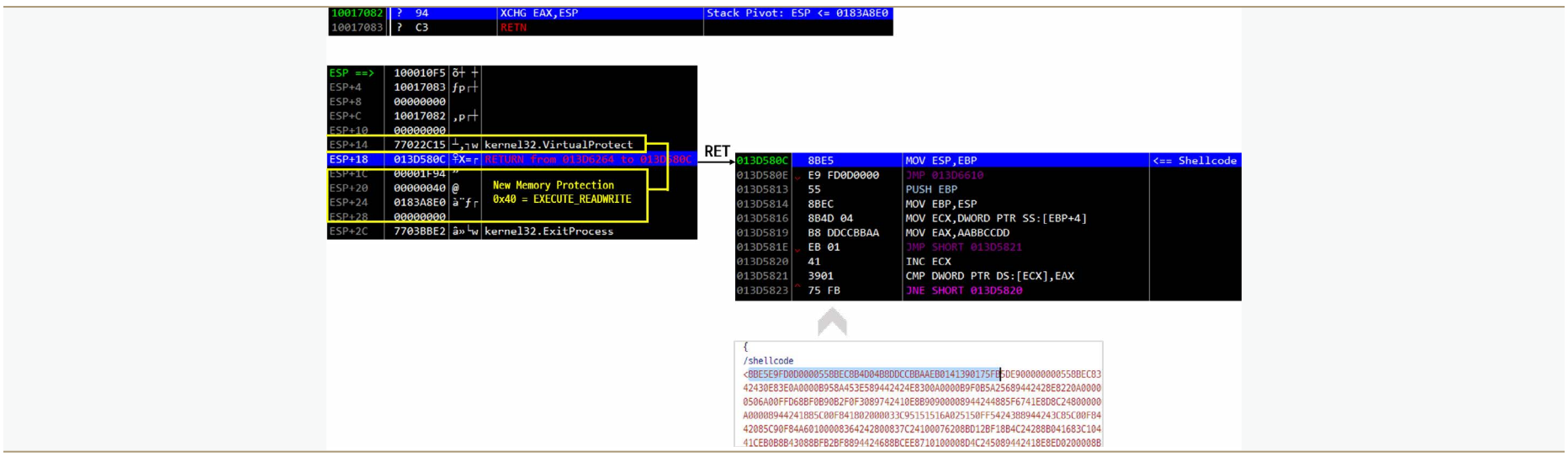
EPS 인터프리터인 gbb.exe 또는 gswin32c.exe 프로세스를 디버깅하면 EPS 파일의 로드 시 익스플로잇이 발생하는 과정을 상세히 확인할 수 있다. [그림 3]은 ROP(Return Oriented Programming) 구성 후 레지스터 값을 변경한 스택 피벗(Stack Pivoting)의 일부로, 포스트스크립트에서 쉘코드 부분(8BE5E9FD…)의 코드가 실행되는 것을 알 수 있다.

ESP 레지스터를 변경한 다음 RETN을 통해 실행 흐름이 변경되고, ROP로 버추얼프로텍트(VirtualProtect) 함수를 구성하여 쉘코드를 실행할 메모리



[그림 2] EPS 취약점을 이용한 한글 파일 구조와 포스트스크립트 코드

를 재정의한다. 이때 버추얼프로텍트가 호출되는 스택 구조를 보면 특정 메모리 영역(쉘코드 부분)에 실행 권한(EXECUTE_READWRITE)을 주고 함수 RETN 이후 공격자가 의도한 쉘코드(0x13D580C)로 분기하는 것을 확인할 수 있다. 이 쉘코드는 위에서 언급한 바와 같이 HEX 스트링 형태로 포스트스크립트에 변수로 선언되어 있다.

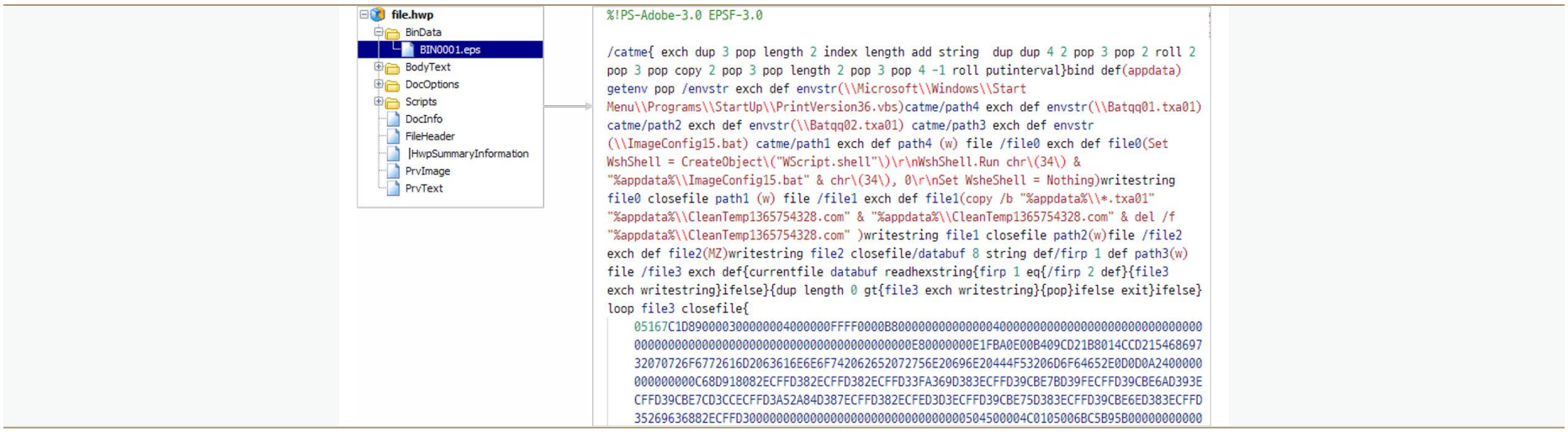


[그림 3] 악성 쉘코드 실행 과정

EPS 파일 공격 방식 2: 정상 문법 패턴을 이용한 악성 파일 생성

앞서 살펴본 EPS 파일 공격 유형이 포스트스크립트의 문법 또는 인터프리터의 실행 과정상의 결함을 이용한 것이라면, 이번에 살펴볼 악성 파일을 생성하는 유형은 정상적인 포스트스크립트의 실행 결과라 할 수 있다.

파일 객체를 생성하고 접근할 수 있는 특성을 이용하여 readhexstring, writefile 등의 명령어를 통해 로컬 시스템에 파일을 생성한다. 메모리에서 쉘코드를 실행하는 방식이 아닌 파일을 생성하는(Drop) 방식이기 때문에 상대적으로 시그니처 기반의 보안 솔루션에 탐지될 가능성이 높다. 이 점 때문에 최근 공격 방식에서는 단일 파일이 아닌 다수의 파일을 생성하고, 이를 조합해 최종 악성 실행 파일을 생성하는 양상을 보인다.

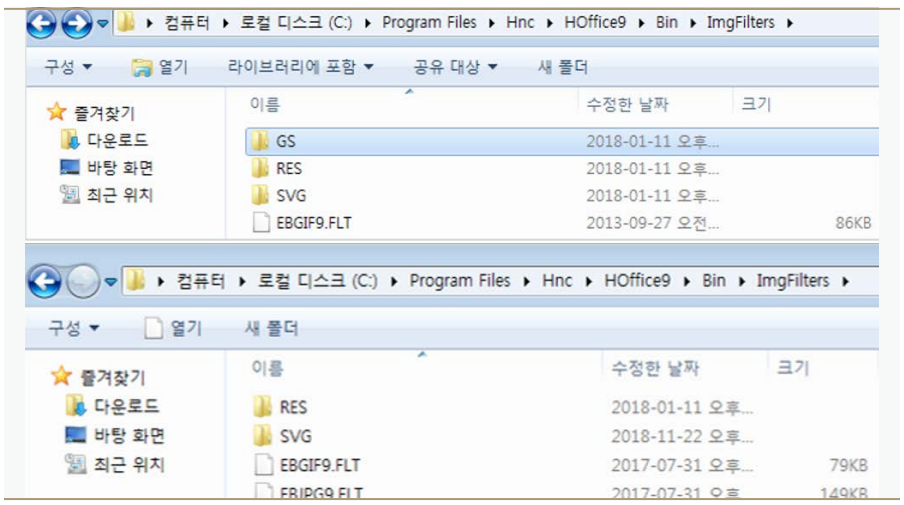


[그림 4] readhexstring 등의 명령어를 이용한 파일 생성

보안 업데이트 적용 시급…패치 관리 자동화 방안 강구해야

한컴오피스는 주로 정부나 학교 등 공공기관, 금융 관련 기업, 민간 단체 등에서 사용하는 만큼 악성 한글 파일은 이들을 노린 타깃형 공격에 주로 이용된다. 따라서 각별한 주의와 함께 적절한 사전 대응 조치가 필요하다.

우선, 앞서 언급한 한컴오피스 보안 업데이트를 적용해야 한다. 해당 보안 업데이트를 적용하면 한글 프로그램 설치 경로에 *.EPS 또는 *.PS 확장자의 파일 처리를 위한 인터프리터 프로그램이 삭제된다. [그림 5]와 같이 한컴오피스 프로그램 설치 경로에서 \Bin\ImgFilters\GS 디렉토리 자체가 삭제되는 것으로, 현재 해당 디렉토리가 남아있는 시스템이라면 반드시 관련 보안 업데이트를 적용해야한다.



[그림 5] 보안 업데이트 적용 전(위)과 후(아래)

취약점에 대한 보안 패치가 배포되더라도 해당 패치가 기업 및 기관의 모든 시스템에 실제로 적용되기까지는 상당한 시일이 소요된다. EPS를 이용한 악성 한글 파일 공격이 지속적으로 국내 공공기관 및 기업을 노리는 이유도 이 때문이다. 따라서 기업 및 기관의 보안 관리자들은 평소 각 엔드포인트 시스템의 패치 적용 여부를 중앙에서 확인하고 관리하는 방안이 필요하며, 특히 패치를 적용하지 않은 시스템에 대해 중앙에서 수동 및 자동 조치할 수 있어야 한다. 이와 함께 실제 엔드포인트 시스템을 사용하는 실사용자의 적극적인 패치 적용을 유도하는 것도 필요하다.

한편, 현재 V3, MDS 등 안랩 제품은 EPS 파일을 이용한 악성 행위를 탐지하고 있다. 또한 차세대 엔드포인트 보안 플랫폼인 안랩 EPP는 연계 정책을 통해 기업 및 기관의 패치 현황을 실시간으로 파악하며 설정에 따라 자동 조치를 제공한다.