WannaCry 랜섬웨어 사전방어 Case Study

2017년 5월 12일 전세계를 대상으로 역대 최고 수준의 랜섬웨어 공격이 이루어졌습니다. 해당 랜섬웨어는 미국 NSA에서 운영한 취약점으로 ShadowBrokers 해킹그룹에 의해 공개되었으며, Microsof는 3월에 이를 패치한 MS17-010 보안 업데이트를 발표하였습니다. 본 문서에서는 WannaCry 랜섬웨어에 대한 특징과 함께 사전 예방법 및 감염 시 대응방안을 설명합니다.

주요 특징

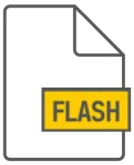
Worm 방식으로 SMB 취약점을 이용한 원격 코드실행으로 감염됩니다. 네트워크에 연결만 되어있어도 MS17-010 패치가 이루어지지 않은 PC로 자체 확산되어 감염됩니다.
감염 대상 파일은 주요 오피스 파일 및 (.ppt, .pptx, .doc, .docx, .xls, .xlsx) 다수의 이미지 파일(.tiff, .jpg, .bmp, .png) 등을 포함한 약 176개 파일 확장자 입니다.

주요 백신 탐지명

Ransom.Wannacry
Ransom.CryptXXX
Trojan/Win32.WannaCryptor

기존 랜섬웨어보다 심각한 이유

기존의 랜섬웨어는 이메일을 통한 유포 및 웹사이트 방문만으로 감염이 되는 것이 일반적인 감염경로 였습니다. 이메일 첨부 파일로 사용자의 클릭을 유도하거나, 웹사이트의 광고 서버를 해킹, 광고 등으로 위장하여 사용자가 웹페이지를 방문하는 시점에 랜섬웨어를 실행시키는 방식으로 유포되었습니다.

기존 유포 방식		새로운 유포방식
		
스팸 메일	광고 위장	네트워크 연결

그러나 WannaCry 랜섬웨어는 자체적으로 전파되는 Worm 타입의 랜섬웨어로 네트워크 연결만 있어도 윈도의 취약점을 이용하여 감염됩니다. MS17-010 패치가 되지 않은 윈도는 감염의 위험에 노출되어 있습니다.

KillSwitch 활성화?

5월 12일 최초로 배포된 WannaCry 랜섬웨어는 인터넷에 특정 도메인이 존재할 경우 더 이상 동작하지 않았습니다. 한 보안 전문가가 테스트를 위해 해당 도메인을 등록하였고, 의도하지 않았지만 WannaCry 랜섬웨어가 일시적으로 동작이 중지되었습니다. 그러나 5월 14일 이러한 **KillSwitch가 제거된 WannaCry 랜섬웨어가 추가로 유포**되었으며, 다시 빠르게 확산되고 있습니다.

대형병원 방어 사례

국내 고객사는 수천여대의 내부 PC에 유명 AV 제품을 사용 중으로, 앱체크를 도입하였습니다. 일부 PC에 랜섬웨어 감염 시도가 이루어졌으나, 대다수의 PC에서는 확산이 일어나지 않았으며, 실제 감염 시도된 PC에서는 앱체크에서 이를 탐지, 차단한 것으로 확인되어 WannaCry 랜섬웨어로 인한 피해가 전혀 없었습니다.

2017-05-12 19:48:32	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b (3).JPG	복원
2017-05-12 19:48:32	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b (4).JPG.WNCRYT	제거
2017-05-12 19:48:31	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b (4).JPG	복원
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b (5).JPG.WNCRYT	제거
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b (5).JPG	복원
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b.JPG.WNCRYT	제거
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124b.JPG	복원
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (1).JPG.WNCRYT	제거
2017-05-12 19:48:30	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (1).JPG	복원
2017-05-12 19:48:29	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (2).JPG.WNCRYT	제거
2017-05-12 19:48:29	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (2).JPG	복원
2017-05-12 19:48:28	랜섬가드	랜섬웨어 파일 생성	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (3).JPG.WNCRYT	제거
2017-05-12 19:48:28	랜섬가드	랜섬웨어 파일 훼손	파일	C:₩Users₩[redacted]₩Desktop₩[redacted]₩A5df124c (3).JPG	복원
2017-05-12 19:48:28	랜섬가드	랜섬웨어 행위 탐지	파일	C:₩ProgramData₩qilsprredrpdy586₩tasksche.exe	제거

앱체크의 사전 방어가 가능한 이유

위의 로그에서 확인할 수 있듯이 WannaCry 랜섬웨어 유포 관련 언론 보도시점은 한국시간 기준 13일이며, 체크멀 센터로 보고된 최초 탐지 로그는 12일 오후 7시 48분으로, VirusTotal에서 해당 랜섬웨어 샘플을 수집한 시간보다 빨랐습니다. 앱체크는 새로운 유포방식 및 새로운 랜섬웨어에도 업데이트 없이 사전 방어에 성공하였으며, 이러한 방어가 가능했던 이유는 앱체크만의 독특한 **"상황 인식 기반 랜섬웨어 행위 탐지 엔진"**이 사용되었기 때문입니다.

백신을 사용중임에도 왜 피해가 지속되는가?

KillSwitch가 제거된 WannaCry의 변종이 다시 배포되는 데에는 단 2일이 소요되었으며 해당 변종의 개수는 약 452종으로 파악되고 있습니다. 이렇게 랜섬웨어의 변종은 매우 빠른 시간내에 새로 제작 및 배포가 가능합니다. 기존의 탐지기법은 랜섬웨어 샘플을 확보하고 난 후 분석하여 업데이트가 배포되어야 탐지가 가능합니다. 또한 랜섬웨어 유포자는 사전에 탐지 테스트를 진행 후 유포하기 때문에 기존 백신에서는 탐지가 어렵습니다.

따라서 새로운 랜섬웨어 변종이 출현했을 때 즉시 차단이 불가능하므로 분초를 다루는 상황에서는 즉각적인 대응이 어렵습니다.

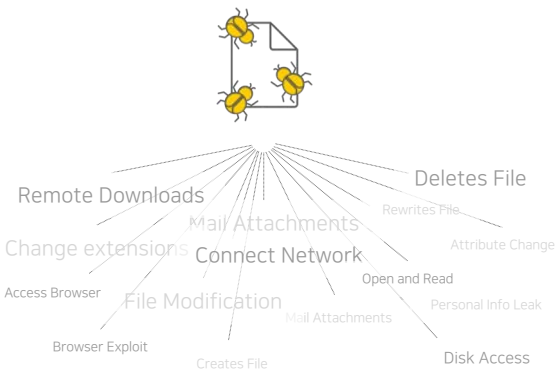
물론 시그니처 방식의 탐지 방법 외에도 기존 범용적인 백신에서는 랜섬웨어 탐지 기능이 추가되어 있으나, 단순한 미끼파일을 자체적으로 생성하여 이에 대한 변조를 탐지하는 방식, 특정 의심행위만을 탐지하는 방식으로는 다양한 랜섬웨어의 감염방식과 파일 변조행위를 모두 탐지하기 어렵습니다.

앱체크는 기존의 솔루션과 다르게 단 하나의 시그니처도 보유하고 있지 않으며, 순수하게 **"상황 인식 기반 랜섬웨어 행위 탐지 엔진"**만으로 현재까지 완전히 새로운 수백 여종의 랜섬웨어를 모두 탐지 및 차단하고 있으며, 새롭게 출현한 WannaCry 랜섬웨어와 관련 변종 모두 사전에 탐지, 차단하였습니다.

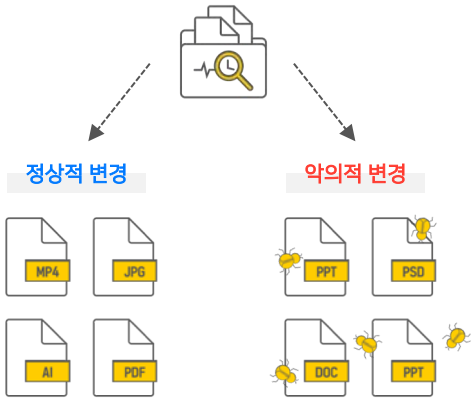
상황 인식 엔진이란?

상황 인식 기반 랜섬웨어 탐지 기술은 기존 방식처럼 랜섬웨어 콘텐츠를 보는 것이 아닌 파일의 변조 시점에 정상적 변경과 악의적 변경을 판단합니다.

랜섬웨어 콘텐츠에 집중



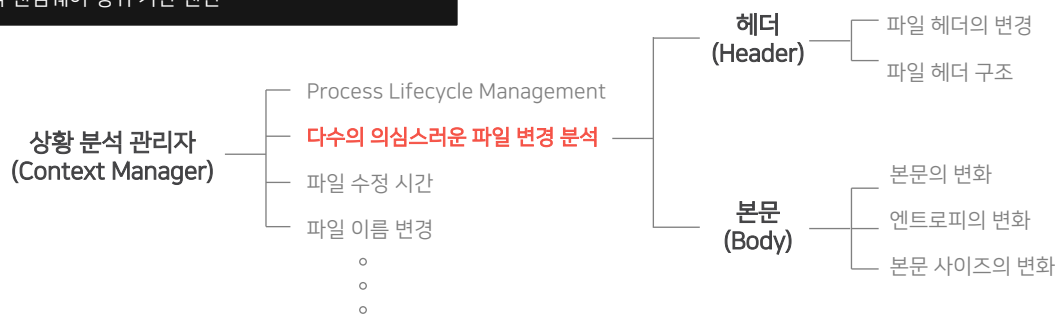
파일 변경 시점 상황 인식



파일이 변경되는 시점에 확인이 가능한 정보는 매우 다양하며, 이를 추적하고 관리하여 정상적인 파일의 변경과 악의적인 파일의 변경에 대한 구분이 가능합니다. 예를 들어 파일을 정상적으로 변경 했을 경우 파일의 헤더는 변경되지 않고 내용만 변경되며, 랜섬웨어로 인해 악의적으로 변경되는 경우 기존 파일의 헤더를 무시한 채 모두 암호화 합니다. 앱체크는 이러한 파일의 변경 특성을 포함하여 다양한 파일 의 변조 여부를 추적하고 파일의 정상 또는 악성 변경여부를 판단합니다.

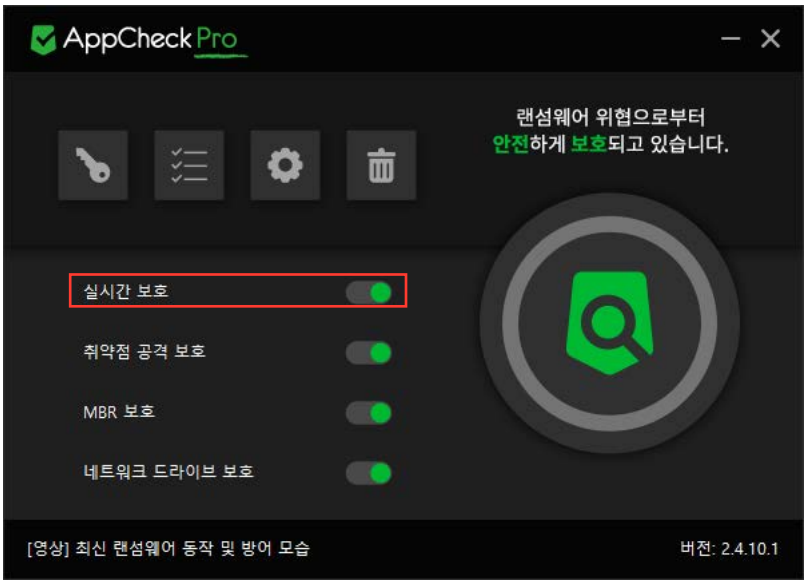
주요 관심 포인트

Context Awareness Ransomware Behavior detection engine
상황 인식 랜섬웨어 행위 기반 엔진



사전 예방 방법

1. 홈페이지에서 앱체크를 다운로드 받고 설치합니다. https://www.checkmal.com
2. 앱체크의 버전이 최신인지 확인합니다.
3. 실시간 보호가 켜져 있는지 확인합니다.



4. 윈도우 PC(XP, 7, 8, 10 등) 또는 서버(2003, 2008 등)에 대한 최신 보안 업데이트를 수행합니다.
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
5. 기업용 제품 구매를 원하시는 경우, 아래 링크를 통해 총판사에 문의하여 주시기 바랍니다.
https://www.checkmal.com/page/shop/distributor/

사전 예방 방법

랜섬웨어 차단 영상
https://www.checkmal.com/page/resource/video/?detail=read&idx=416&p=1&pc=20

WANNACRY 랜섬웨어 공지사항
https://www.checkmal.com/page/support/notice/?detail=read&idx=417

관련 보도자료
http://www.junggi.co.kr/article/articleView.html?no=18864
http://ciobiz.etnews.com/20170515120012
http://news.inews24.com/php/news_view.php?g_serial=1023187&g_menu=020200&rrf=nv
http://news.joins.com/article/21815933
www.boannews.com/media/view.asp?idx=57452&kind=1
http://www.boannews.com/media/view.asp?idx=68009&kind=1