Next Generation Network Security with PacketCYBER

A Real-time Cyber Threat Detection & Hunting Platform

2017-08-15

CQVista Inc.

Ver. 1.3

목차

지능형 위협: 보안 운영 센터(SOC)의 도전 및 해결책

기업 IT 조직은 새롭게 출현되는 IT기술들을 수용해야 하는 동시에, 널리 만연하고 있는 복잡한 사이버 위협을 사이버 보안에 통합하여야 하는 새로운 시대에 진입하였습니다.

기존의 침해사고 대응 인력 및 시스템(SIEM)은 엄청난 양의 공격 이벤트, 경보, 모니터링 및 분석 이슈에 의하여 압도되고 있습니다. SIEM에서 발생하는 하나의 경보를 처리하기 위해서 보안관제 요원은 약 45분 정도(오탐여부 검증: 15분, 위협 종류 및 정보자산에 미친 영향 파악: 30분)의 분석 시간을 사용하지만, 대부분의 경우, 이벤트 로그의 불충분한 정보 때문에 효과적인 분석에 실패하고 있습니다.

신종 악성코드에 대응하기 위하여 널리 사용되고 있는 악성코드 Sandbox 기술은 여전히 악성 코드 위협에 도움이 되지만 오탐 및 우회기법 등에 의한 문제점이 있습니다.
MIERCOM의 테스트에 따르면, 선도적인 Sandbox 벤더 및 차세대 방화벽과 Sandbox를 동시에 사용하는 경우 모두 약 80%의 악성코드 만을 탐지할 수 있는 것으로 밝히고 있습니다.

SIEM 이벤트 로그 정보의 문제점을 보완하기 위하여 출현한 FPC (Full Packet Capture) 및 DPI (Deep Packet Inspection) 네트워크 포렌직(Forensics) 솔루션은 SIEM 운영에서 부족한 정보를 채우기 위하여 운영되는 경우가 있지만 분석에 많은 시간, 분석가의 노력 및 지식이 요구되는 기술로서 신속한 위협 대응 측면에서는 많은 한계를 가지고 있습니다.

따라서 보다 효과적인 침해사고 탐지 및 대응 절차에 대한 전략을 마련하는 데 실패하는 조직은, 최근에 공격 목표가 되었었던 조직과 마찬가지로, 가까운 미래에 대규모의 해킹 피해 및 손실을 입을 위험에 직면하고 있습니다.

새로운 침해사고 탐지 및 대응 시스템은 네트워크 다운타임, 지적 재산 및 기밀 정보 유출, 명예 실추 및 규정 준수 실패 등에 따른 재정적 손실에 대비할 수 있어야 합니다.

지능형 위협들은 현재의 침해 사고 대응 인력 및 시스템 (SIEM, Sandbox, 네트워크 포렌직 등)에 감당할 수 없을 정도로 부담을 가중 시키고 있으며 따라서 다양한 위협을 자동으로 탐지하여 이에 대한 효과적인 분석을 통한 효율적인 대응 및 조치 가능한 정보를 생성할 수 있는 침해사고 대응 전략을 요구하고 있습니다. 즉, 현재의 수준의 보안 모니터링에 새로운 수준의 인텔리전스를 부여하는 새로운 기술과 절차의 출현을 요구하고 있습니다.

본 백서에서는 기존 보안 관리 도구들의 문제점 및 한계를 살펴보고, 이에 대한 해결책을 제시하고자 합니다.

악성코드 Sandbox 기술의 문제점

① 악성코드 Sandbox 기반 시스템은 Packing된 악성코드 탐지에 취약하다. (예, 3.20 대란 당시, A 사는 Themida 로 Packing 된 악성코드를 탐지 못함)
② 또 업체별 마케팅 자료와는 달리, 분석 지연시간이 존재한다. (F사의 경우, 평균 18분 소요)
③ 악성코드 Sandbox 기반 시스템은 VM을 최대 160개까만 사용 가능하여 따라서 고속 네트워크에서 운영이 불가능하다 (예: 10Gbps).
④ 악성코드 Sandbox 기반 시스템은 수집된 파일의 악성여부를 Antivirus와 파일 메타 데이터 또는 파일 구조 패턴으로서 선 처리 후에 실행하여 분석하는 과정을 거치는데, 선처리 과정은 시그니처 기반 솔루션과 마찬가지로 취약하여 악성코드의 일부만 조사될 가능성이 존재한다.
⑤ 악성코드 Sandbox 기반 시스템은 악성코드의 다양한 우회 기술에 취약하여 우회 가능성이 존재한다.
- Upclicker 악성코드는 사용자의 마우스 클릭을 탐지하여 사용자가 클릭하지 않을 경우 동작하지 않음
- Trojan Nap은 실행 지연 (네트워크워크 샌드박스의 실시간 분석 기능 공격)
⑥ 대부분의 악성코드는 특정 OS•특정 어플리케이션 버전에서만 동작하므로 모든 환경을 가상 환경에 적용하기 어렵다는 단점이 존재한다.
⑦ 선도업체의 경우, 문서기반 악성코드 및 zero-day 악성코드 탐지율이 약 50% 이하에 그치고 있어, 문서기반 악성코드와 Zero-day 공격에 취약하다 (Miercom, 2016).

위에 나열한 다양한 문제점들로 인하여, 선도 Sandbox업체 및 차세대 방화벽과 Sandbox 연계 솔루션들의 평균악성코드 탐지율은 약 83.5% (Miercom, 2016)로서 많은 한계를 지니고 있습니다.

SIEM의 문제점 (2015, Gartner)

보안 운영센터의 주요 솔루션의 하나인 SIEM은 악성코드 Sandbox, 차세대 방화벽 등 모든 보안 솔루션들로부터 발생한 이벤트 로그간의 상관관계를 분석하는 솔루션으로서 모든 보안 관제의 근간으로 널리 사용되고 있습니다.
그러나 SIEM 의 문제점을 Garner 그룹은 다음과 같이 지적하고 있습니다.

① TOO COMPLEX
적절한 이벤트 데이터들을 수집, 취합 및 정규화하여 서로 다른 기술들의 상관관계를 하나의 통합된 View에서 제공하는 것은 매우 어려운 작업이다.

② TAKES TOO LONG
SIEM에 투자하는 대부분의 조직은 긴급을 요하지만 대부분의 SIEM 구축은 초기 구축에만 수개월이 소요되며, 실제적인 운영을 위해서는 더 많은 시간이 요구된다.

③ TOO EXPEPACKETCYBERVE
SIEM은 설계, 통합, 다양한 외부 데이터 소스 데이터 피드의 정규화 및 수집 스케줄 등을 구현하는 고비용 컨설턴트를 고용해야 하므로 S/W 라이선스 비용의 최소 2배를 고려해야 한다.

④ TOO NOISY
SIEM 경보 및 경고는 "과도하게 발생하지만, 일반적으로 SIEM S/W 자체에서 발생하는 경고는 보안 분석가가 침해 사고 대응 및 분석을 위해서 필요한 컨텍스트를 제공하지 못하는 경우가 대부분이다.

SIEM 운영을 위해서는 하나의 경보 발생시, 아래의 4 가지 단계의 작업을 수행하여야 합니다.

- ✓ **검증 (Validate):** 탐지가 정확하다는 사실을 뒷받침해 주는 데이터 관점 제공
- ✓ **범위 (Scope):** 관련된 속성이 악성인지를 결정. 더 이상 새로운 악성 속성이 없을 때까지 새로운 Scope을 Pivot
- ✓ **복구(Recover):** 위협으로부터 접속을 차단하는 동시에 자산을 동결 및 복구할지를 결정
- ✓ **추적(Track):** 해당 위협과 관련된 이벤트가 더 이상 발생하지 않는 것을 보장하기 위하여 지속적으로 위협 및 위협 속성을 관찰

즉, 현재 발생한 경보에 대한 오탐 여부를 확인하는 **"검증"**을 거친 후, 정탐일 경우, 악성여부 및 위협의 종류를 확인하여, 어떠한 정보 자산에 어떠한 영향을 미쳤는지를 판단하는 **"범위"**를 특정하는 작업을 수행하여야 합니다. 또 해당 작업 후에 복구 및 추적 작업이 이루어져야 합니다.
일반적으로 "검증"작업에 약 15분이 소요되며, "범위" 작업에 약 30분이 소요되어, 경보 한 개당 약 45분의 시간이 소요됩니다. (Cisco)

예를 들어, 16,937개의 SIEM 경보가 일주일 동안 발생하였을 경우, 일간 약 2, 450개의 SIEM 경보가 발생하므로 이를 처리하기 위해서는 약 1,102 시간이 소요되며, 이는 약 46일의 시간이 소요됨을 의미합니다. 이를 보다 효과적으로 처리하기 위하여 10명의 보안관제 요원이 투입된다고 가정하면, 인당 약 4.6일이 소요되는데, 결국 이 수치는 결국 SIEM으로 효과적인 보안 관리가 불가능하다는 사실을 방증한다고 볼 수 있습니다.

네트워크 포렌직의 문제점

SIEM 운영 시, 특정 경보에 대한 이벤트 상관관계 분석을 통하여 분석한 후, 보다 상세한 정보 및 분석을 원하는 경우, 모든 패킷을 분석해 볼 수 있는 네트워크 포렌직을 이용해 볼 수 있습니다.

그러나 네트워크 포렌직 솔루션이 제공하는 분석은 DPI (Deep Packet Inspection) 기반의 다양한

프로토콜 디코딩을 통한 수작업들이 주를 이루며, 여러 단계에 걸친 분석 작업이 필요하므로 작업의 난이도가 매우 높으며 또한 많은 작업 시간이 소요됩니다.

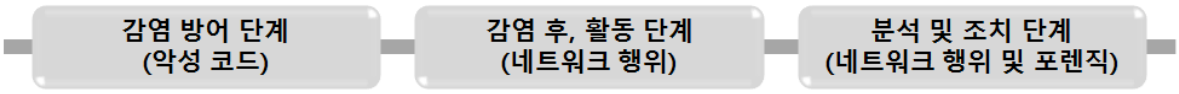
또 한가지의 문제점은 지능형 위협이 탐지되지 않고 네트워크에 상존하는 기간이 약 5 ~ 7개월인데 반하여 네트워크 포렌직의 데이터 보존기간은 평균 약 1 개월 이하라는 점입니다.

PacketCYBER: 실시간 사이버 위협 탐지 및 헌팅 플랫폼

PacketCYBER는 메타 데이터 기반 실시간 사이버 위협 탐지 및 헌팅(Hunting) 기능을 제공하는 플랫폼으로서 악성코드 탐지, 침해징후 (IOC: Indicator of Compromise) 탐지, 네트워크 이상 행위 탐지 그리고 그러한 결과들을 침입 킬-체인 관점에서 유기적인 상관관계 분석을 제공하는 플랫폼으로서 기존의 보안 관리 도구 및 인력 비용의 일부만으로도 지능형 위협 요소에 대한 심도 깊은 분석 및 이해를 제공함으로써 증가하고 있는 지능형 위협에 효과적으로 대응할 수 있습니다.

결과적으로 PACKETCYBER는 지능형 위협에 대응하기 위하여 보다 신속•정확하게 공격 소스를 진단하여 대응하도록 함으로써 기존 보안 인력의 업무 효율성을 극대화할 수 있으며, 새로운 인적•기술적 자원에 대한 요구사항을 최소화할 수 있습니다.

효과적인 위협 탐지 및 대응

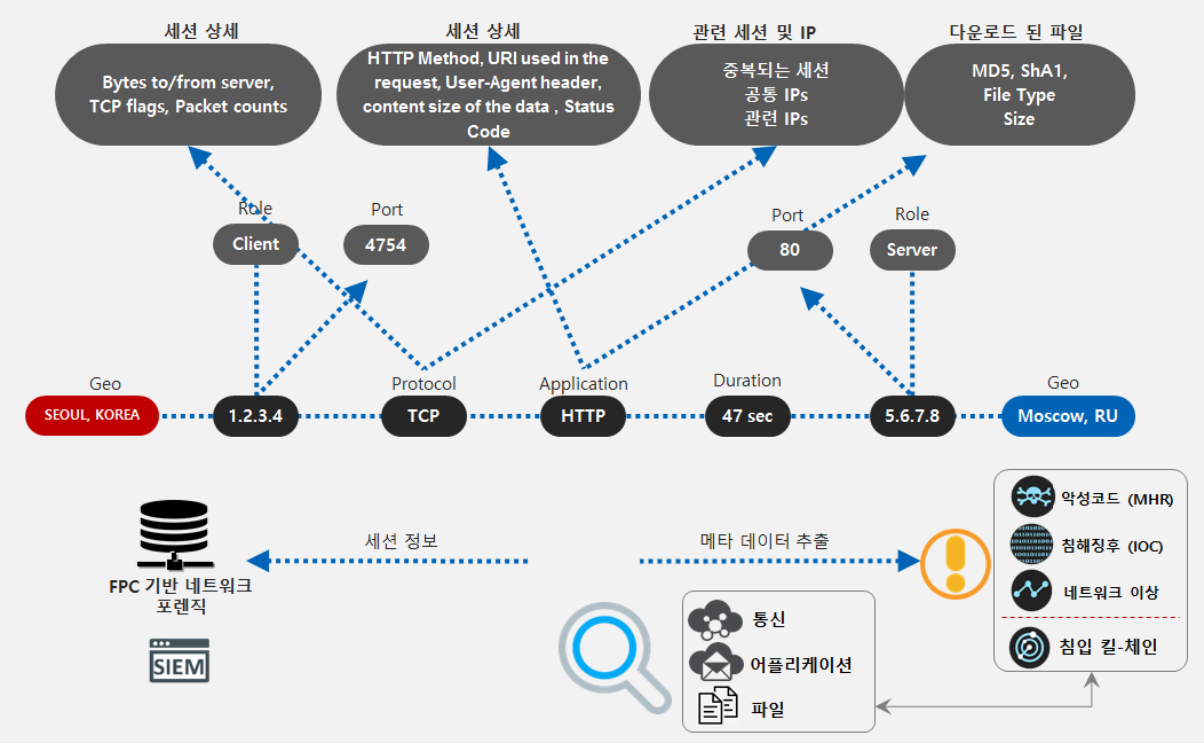


효과적인 위협 탐지 및 대응을 위해서는, 감염방어단계, 감염 후, 활동 단계 및 분석 및 조치단계의 3 단계 작업이 유기적으로 이루어져야 합니다.

이를 위하여 PacketCYBER는 먼저 모든 트래픽에서 메타 데이터를 추출합니다.

PacketCYBER 메타 데이터 추출

PacketCYBER는 모든 트래픽에서 메타 데이터를 아래 그림과 같이 추출합니다.



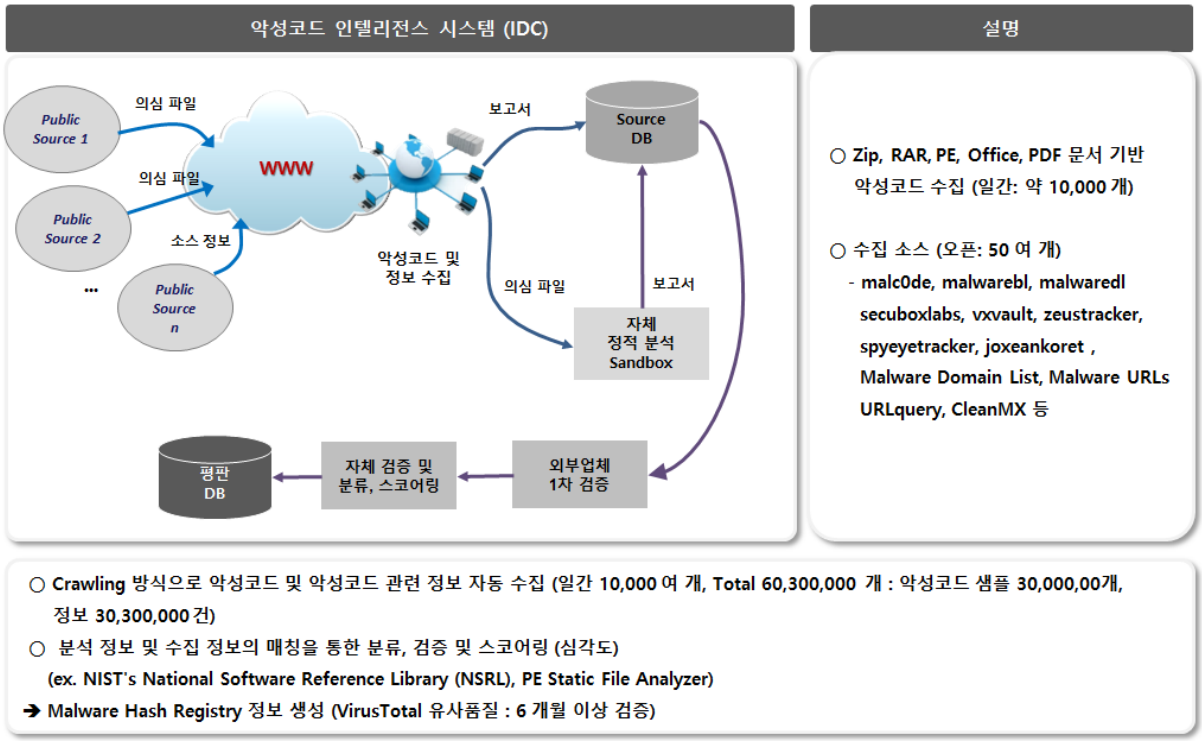
위 그림에서, TCP 통신에 대한 메타 데이터를 추출하여, Geo 정보를 추가하고, 어플리케이션 (ex. HTTP)를 식별하여 추가정보를 추출합니다. 만일 해당 HTTP 세션을 통하여 파일을 주거나 받은 경우, 파일 관련 메타 데이터를 추출합니다.

메타 데이터 기반 PacketCYBER의 감염 방어 단계 (악성코드 탐지)

"감염 및 방어 단계"는 임직원과 파트너 PC에 대한 다양한 경로(주로 피싱 이메일, 웹 사이트 방문을 통한 Drive-by-download 등)를 통한 악성코드 감염을 방어하는 단계로서 주로 악성코드 sandbox에 의존하고 있으나, 위에서 지적한 대로 문제점 및 한계가 존재합니다.

PacketCYBER의 파일관련 메타 데이터 중 해시 값을 이용하여 자체 악성코드 레지스트리 (MHR: Malware Hash Registry) 정보와 비교됩니다. 이 과정에서 이미 알려진 악성코드의 경우, 대부분이 검출됩니다.

Cf.) MHR: Malware Hash Registry 정보 생성 및 품질



자체 MHR은 2017년 현재, 약 6천만개 이상의 악성코드 분석 정보를 포함하고 있으며, 일간 약 10,000 여건씩 추가되고 있습니다.

6개월 이상의 자체적인 검증 결과, 2013년 이후 발생한 악성코드는 VirusTotal과 거의 동일한 품질로 유지되고 있습니다.

머신 러닝 기반 PacketCYBER의 감염 방어 단계 (악성코드 탐지)

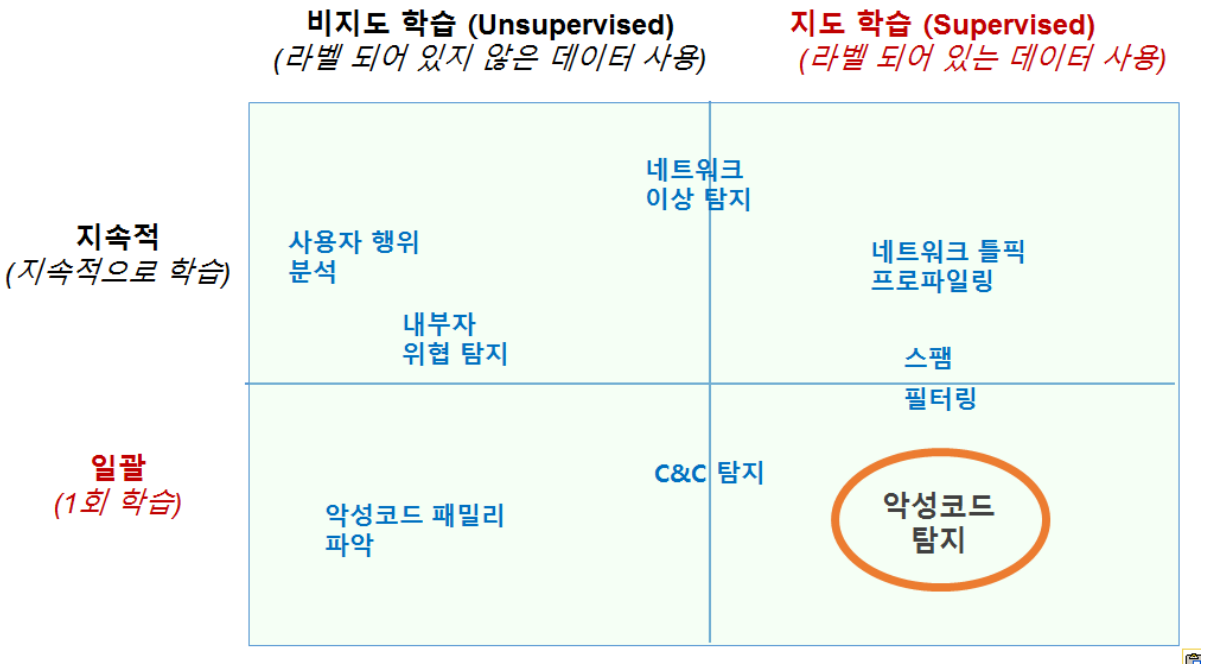
글로벌 기업들은 안티바이러스나 샌드박스(Sandbox) 기술만으로는 해결하기 어려운 악성코드 탐지 문제에 머신 러닝(Machine Learning) 기술을 접목한 고성능 악성코드 탐지 제품을 선보이고 있으며 대규모 투자유치 및 글로벌 마케팅을 통하여 빠르게 성장하고 있습니다. 또 미국의 벤더 중립적인 보안 제품 테스트 기관인 Miercom사의 2016년 보고서에 따르면, 선도업체들의 평균 악성코드 탐지율이 83.5%에 그치고 있는 반면, 머신 러닝(Machine Learning) 기술을 활용한 악성코드 탐지 솔루션들의 탐지율은 98% 이상이라고 밝힘으로써 머신 러닝 기반 악성코드 탐지 기술의 유용성을 확인한 바 있습니다.

이러한 이유는 진정한 신종 악성코드는 거의 없으며, 소프트웨어 개발의 어려움으로 인하여 악성코드 개발자도 코드 및 코드 패턴 재사용하는 경향이 있습니다. 따라서 악성코드 분석가도 악성코드(변종 등)의 고유 패턴 및 유사성을 활용하여 악성코드를 탐지 및 관리 할 수 있습니다.

악성코드 작성자가 코드 및 코드 패턴을 재사용하기 때문에 악성코드는 고유 패턴 및 유사성을 가지게 되는데, 머신 러닝(machine learning)은 이러한 고유 패턴과 유사성을 찾는 학문이기 때문입니다.

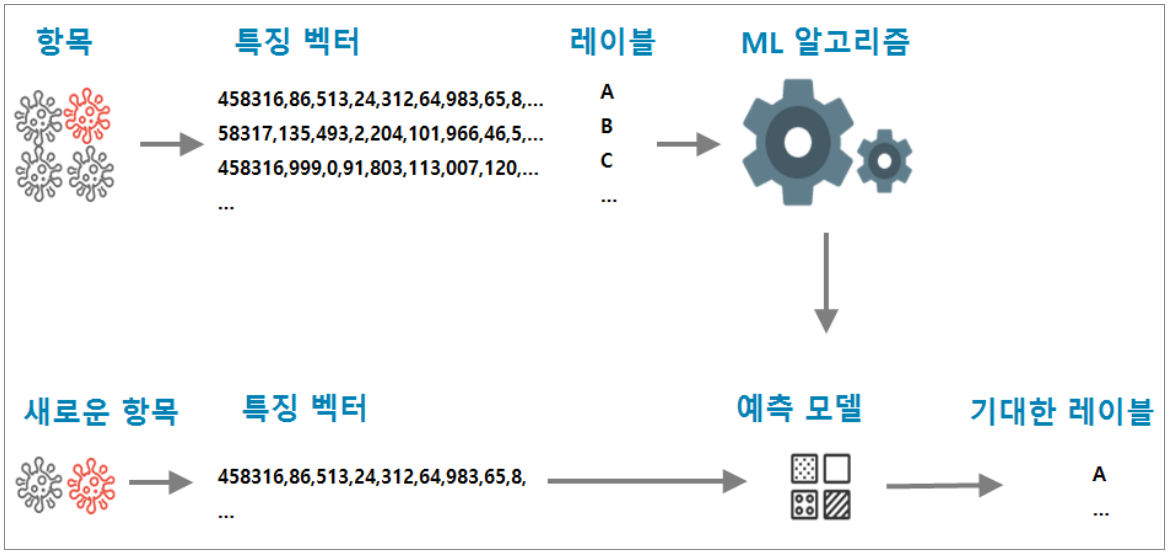
한편 Verizon사의 2016년 DBIR 데이터 유출조사보고서에 따르면, 보안사고의 90%에서 악성코드가 사용되고 있으며, 지속적인 변종 생성으로 98%의 동일 악성코드에 대한 변종이 58초마다 발생, 표적형(Targeted) 공격을 위한 악성코드는 표적용으로 특별 제작, 정상적인 파일로 위장한 악성코드 등장 등 다양한 원인으로 악성코드의 정확한 탐지를 어렵게 하고 있다고 밝히고 있습니다.

사이버 보안 분야와 인공지능(머신 러닝) 분야의 접목 시, 가장 적합한 방법과 기술은 아래 표에서 확인할 수 있습니다.



PacketCYBER도 현재 지도학습법을 이용하여 PE 계열의 악성코드를 탐지하고 있습니다.

지도학습법의 개요는 아래 그림에 나타나 있습니다.



즉, 악성코드 및 정상 파일의 데이터 세트를 충분히 수집하여, 이들로부터 적절한 특징을 추출 및 처리하여 머신 러닝 알고리즘을 이용하여 탐지 모델을 생성합니다.

이후 유입되는 파일을 수집하여 특징을 추출하여 탐지 모델에 제공하면, 탐지 모델의 인텔리전스에 의하여 악성 및 정상 여부를 판별합니다.

이론적으로는 탐지 모델을 표준 10 중 교차 검증으로 평가 시, 99%이상의 탐지율을 확보할 수 있다고 주장하는 연구가 다수 있으나, 실제로는 학습에 사용되지 않은 새로운 악성 파일 테스트 시, 탐지 모델 정확도가 0.5-5 % 감소현상이 발생합니다. 따라서 PacketCYBER는 학습 데이터가 아닌 다양한 출처의 악성코드에 대해서도 테스트하여 악성코드 탐지 모델을 개선하였고 제로데이 악성코드 탐지율을 개선하였습니다.

메타 데이터 기반 PacketCYBER의 감염 후 활동 단계 탐지 (네트워크 행위 및 IOC)

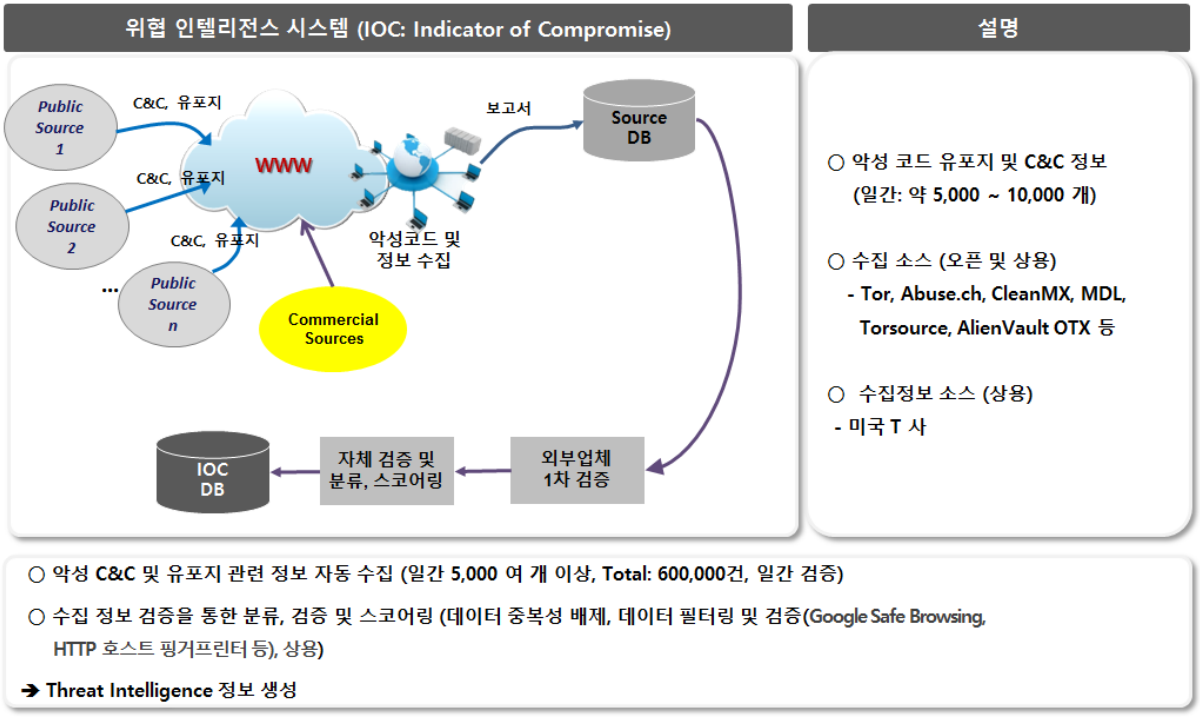
악성코드 감염 이후에는 포트 및 취약점 스캔, 악성코드 추가 배포, 권한 상승시도(Supervisor), 활동 발판 구축 (숙주 호스트), 외부 C&C서버 접속, 악성코드 업데이트 등 다양한 활동이 발생합니다.

감염 이후 활동에 대한 인지 및 실시간 모니터링을 위해 사용할 수 있는 기술은 많지 않으며, 최근 출현한 다양한 네트워크 행위 분석 솔루션들이 도움이 될 수 있습니다.

PacketCYBER는 Port Scan, IP Sweep, 다양한 패스워드 Brute-Forcing 행위, Drive-by-download, DGA/Fast-Flux C&C, Ransomware 감염 행위, 데이터 유출 의심 행위 등을 탐지합니다.

이와 더불어 알려진 C&C 및 악성코드 배포 사이트 접속 탐지를 위한 IP 및 도메인 평판 (IOC: Indicator of Compromise)을 사용합니다.

Cf.) IOC: Indicator of Compromise 정보 수집 및 품질



자체 IOC 정보는 약 600,000건이 유지되고 있으며, 일간 검증 및 갱신 작업이 진행되고 있습니다.

PacketCYBER의 감염 및 감염 후 활동 단계의 침입 킬-체인 분석

PACKETCYBER에 의해 로컬 자산이 지능형 위협에 감염되었다는 최종 판단에 이용된 모든 양방향 통신 상세 정보는 감염 생명 주기(사이버 킬 체인)의 단계별로 구분됩니다.

PACKETCYBER가 사용하는 양방향 통신 상관관계 분석 모델에서는 5 단계의 잠재적 양방향 통신 단계가 존재합니다:

공격 단계	분 류
C1	C&C 통신 (C2 Communication)
C2	에그(바이너리) 다운로드 (Egg Download)
C3	정찰 (Reconnaissance)
C4	내부망 확산 (Lateral Movement)
C5	정보 유출 (Exfiltration)

PACKETCYBER의 침입 킬-체인 상관관계 분석 상세

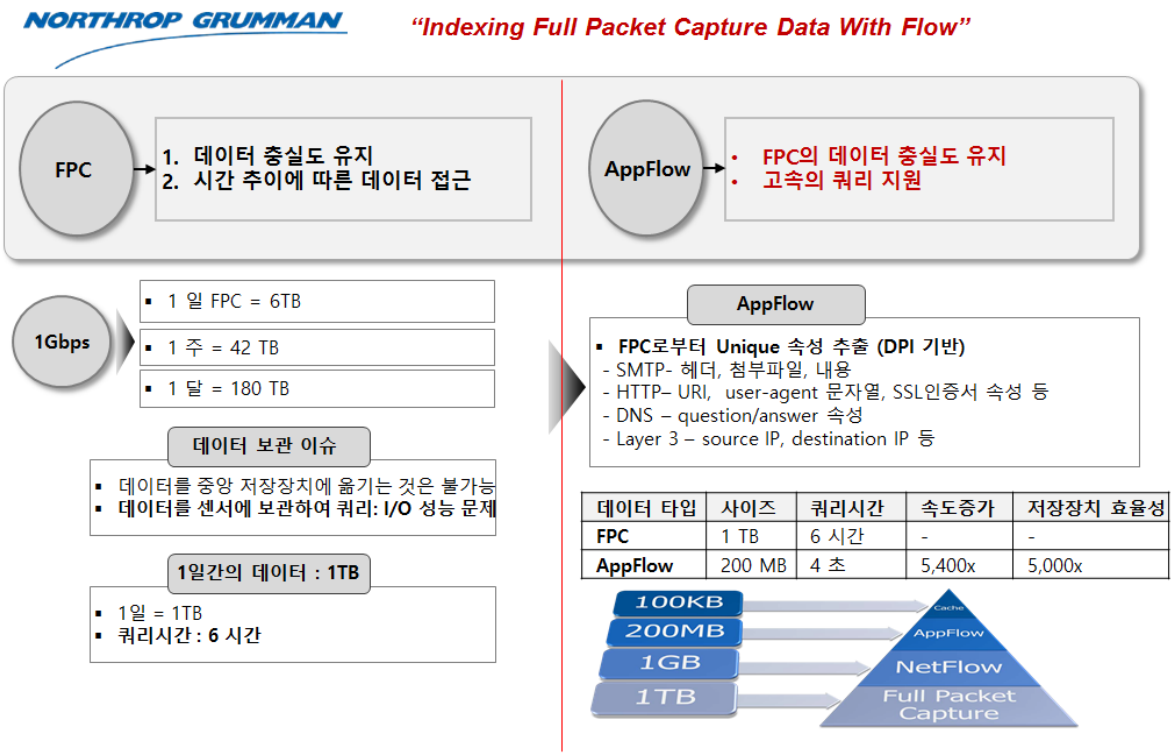
C3	**정찰 (Reconaissance)**	"스캔 후 감염" 악성코드에 적용된다. 이 통신 단계는 잠재적인 공격 소스에 의한 전조 행위를 나타낸다. 이 단계는 네트워크 주소 스캐닝을 통해 새로운 대상을 수집하지 않는 스팸 기반의 전파에는 적용할 수 없다. • 악성코드 관련 스캔
C4	**내부망 확산 (Lateral Movement)**	"스캔 후 감염" 악성코드에 적용된다. 여기서 내부 빅팀 호스트는 R2L 또는 L2L로의 네트워크 통신 채널을 통하여 공격을 받는다. • HTTP Brute-Forcing • FTP Brute-Forcing • SSH Brute-Forcing • SQL Injection Attempt • Exploit kit 탐지 등
C2	**에그(바이너리) 다운로드 (Egg Download)**	대대수의 악성 코드 패밀리의 검출에 적용된다. 일단 감염이 되면, 감염된 호스트는 원격 에그 다운로드 사이트 (대개 공격 소스)에서 전체 악성코드 코드 베이스를 다운로드 하여 실행하는 주체로 탈바꿈된다. 이메일 스팸 기반의 전파나 HTTP 관련 악성코드 다운로드를 탐지한다. • Drive-by-download • 모든 MHR 매칭 통신 • 머신 러닝 기반의 악성코드 탐지
C1	**C&C 통신 (C2 Communication)**	C&C 를 이용하는 지능형 악성코드에 검출에 적용된다. 이 통신 단계는 중앙 집중 방식의 C&C 통신 서버를 감시한다. 또 Domain Fast-flux 및 도메인 생성 알고리즘(DGA)를 이용한 C&C 회피 기법을 감시한다. 또 로컬 자산이 악성 코드 전파 활동에 초점을 맞추고 있는 경우를 검출한다. • 도메인 Fast-Flux 행위 • 도메인 생성 알고리즘 (DGA) 행위 • 모든 IOC (Indicator of Compromise) 관련 IP 및 도메인 접속 관련 통신
C5	**정보 유출 (Exfiltration)**	이 통신 단계는 로컬 호스트가 다른 호스트로의 정보 유출 시도를 탐지한다. • 내부에서 외부로의 대량의 데이터 전송 행위 탐지

PacketCYBER: 메타 데이터 기반 분석 및 조치 단계

분석 및 조치 단계에서는 SIEM과 네트워크 포렌직 등이 널리 사용되고 있으나, 앞서 지적하였듯이 SIEM은 너무 많은 경보, 연관 이벤트 부재, 이벤트 충실도 부재, 제안된 컨텍스트로 인하여 제한된 분석만이 가능하다는 문제점이 있으며, 네트워크 포렌직을 사용하는 경우에는 운영이 복잡하며, 분석 난이도가 높고 분석 시간이 오래 걸린다는 문제점과 데이터 보존기간이 짧다는 문제점이 있습니다.

PacketCYBER에서는 **FPC로부터** 통신정보(IP, TCP, UDP 및 ICMP connection), 어플리케이션 통신정보(DNS, HTTP, SMTP, SSL, SSH, FTP 등) 및 파일에 대한 메타 데이터를 추출함으로써, 고속 분석을 통한 대응을 지원합니다.

Cf.) FPC (Full Packet Capture) vs. Meta-Data



데이터 타입	사이즈	쿼리시간	속도증가	저장장치 효율성
FPC	1 TB	6 시간	-	-
AppFlow	200 MB	4 초	5,400x	5,000x

PacketCYBER 결론

신속하고 효과적인 위협 탐지 및 헌팅(Hunting) 플랫폼

- **실시간 사이버 공격 가시성:** 실시간 악성코드 탐지, 공격 행위 및 위협인텔리전스의 자동화된 침입 Kill-Chain 상관 관계 분석 결과를 통한 트래픽 및 파일에 대한 자동 위협 헌팅 (Hunting) 플랫폼 제공
- **블라인드 스팟없는 위협 탐지:** 모든 장치의 작동에 관한 충실도 높은 가시성 확보를 위하여 모든 네트워크 트래픽 및 파일을 분석하며 이에 대한 증거 (Evidence)를 통한 수동 위협 헌팅 (Hunting) 플랫폼 제공
- **정확한 위협 컨텍스트를 실시간에 제공:** 효과적인 위협 탐지 및 헌팅(Hunting)을 위하여 가장 연관성이 높은 정보와 컨텍스트를 실시간으로 제공함으로써 신속한 위협 탐지 및 대응
- **기존 보안 인프라 강화:** 기존 방화벽, 엔드포인트 보안, 네트워크 접근 통제 등을 통한 공격 차단 방법의 자동화 방안 제시 및 SIEM 및 네트워크 포렌직 도구 등 기존 위협 관리 솔루션들의 효율성 향상

Let the Hunt Begin!

Appendix I

Dissecting the NSA's Six-Phase Playbook for Hacking Networks vs. PacketCYBER

"Think Like the NSA to Keep Your Network Secure" – by Rob Joyce:
25-year veteran of the National Security Agency (NSA

Phase 1: Initial Reconnaissance (초기 정찰)
해커 공격 행위
● 해커는 호스트 및 운영 체제를 식별하고 취약점에 대한 조사를 수행하기 할 수 있는 수많은 네트워크 스캔 도구를 가지고 있음 ● 해커가 취약한 OS, 클라이언트 데이터베이스, 민감한 데이터를 처리하기 위한 다른 기술을 식별 할 수 있다면? 이미 문제가 심각
대응 방안
● 최소한 실행되고 있는 스캐닝 방법을 탐지 또는 방지 할 수 있어야 함 ● 중요 자산과 자산에 접촉하는 사람을 지속적으로 모니터링 하기 위한 시스템, 기술 및 절차를 확보하여야 함. 내부 네트워크내의 시스템간 통신("east-west)을 지속적으로 모니터링 할 수 있는 능력을 확보함으로써 해커보다 네트워크를 잘 파악하는 데 중요한 부분임
PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 지능형 네트워크 이상 행위 탐지 (Egg Down., C&C, Recon, Lateral Mov., Exfiltration, DGA/ Fast-flux DNS 등) ● 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

Phase 2: Initial Exploitation (초기 익스플로잇)
해커 공격 행위
● Joyce에 따르면 zero-day 익스플로잇과 새로운 네트워크 침해 기법의 중요성은 지나치게 과장되어 있으며, 실제로는 대부분의 침입은 3 가지 초기 공격 벡터 중 하나를 통해서 유입 : – 이메일 첨부파일 클릭; – 악의적인 웹사이트 접속을 통한 불법 컨텐트 실행; – 감염된 이동식 매체
대응 방안
● 네트워크를 위험에 빠뜨리는 내부 네트워크 트래픽 및 계정 사용 모니터링 및 이미 감염된 사용자 계정에 의한 의심스러운 행위 모니터링

PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 웹•이메일(HTTP, SMTP) 기반 악성코드 탐지 (MHR) ● 지능형 네트워크 이상 행위 탐지 (Drive-by-download., C&C, Recon, Lateral Mov., Exfiltration, Fast-flux DNS 등) ● IOC(침해징후) 탐지 : C&C 사이트 및 악성코드 배포사이트 접속 ● 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

Phase 3: Establish Persistence (지속성 확립)
해커 공격 행위
● 해커가 네트워크 침입에 성공하면, 추가적인 백도어를 생성하여 보다 강력한 발판을 다지며 일반적으로 탐지나 축출이 어렵게 만듦. ● 지속성은 더 높은 권한 인증정보(계정)을 탈취하고 삭제해도 재설치 되는 악성코드를 이용하여 확립
대응 방안
● Mandiant 2015 보고서에 따르면, 탐지되기 146일 전부터 네트워크에서 활동 ● "정상 네트워크 행위"를 구성하는 사용자, 세그먼트, 기능 구역을 파악함으로써, 해커가 들키지 않고 장시간 비 인가된 접속을 유지하는 것을 어렵게 만듦. ● 애플리케이션 및 사용자 행위의 지속적 모니터링을 통하여 베이스라인을 수립할 것
PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 지능형 네트워크 이상 행위 탐지 (Egg Down., C&C, Recon, Lateral Mov., Exfiltration, DGA/Fast-flux DNS 등) ● 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

Phase 4: Install Tools (추가 공격 도구 설치)
해커 공격 행위
● NSA나 다른 공격자는 시스템에 추가 소프트웨어를 설치함으로써 데이터를 유출 하거나 위협 행위자를 확고히 하는데 도움이 될 수 있는 추가적인 소프트웨어를 다운로드 하는 것이 표준 절차임
대응 방안
● 평판 서비스 (파일, 도메인) 이용 평판 서비스는 알려진 실행파일에 대한 클라우드 기반 데이터베이스를 이용하여 해당 프로그램이 스팸, 악성코드, 피싱 또는 일반적인 음성 행위를 하는 지를 검사. 일부 평판 서비스는 특정 소프트웨어가 호출하는 도메인 이름도 확인하기 때문에 클라이언트가 특정 도메인을 호출하는 경우 멀웨어 "C&C"일 수 있다는 경고를 제공.
PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 웹•이메일(HTTP, SMTP) 기반 악성코드 탐지: MHR (악성파일 평판) 기반 탐지

- 네트워크 이상 행위 탐지 (Drive-by-download)
- IOC (침해징후) 탐지: 도메인, IP 평판
- 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

Phase 5: Move Laterally (내부망 이동)
해커 공격 행위
● 네트워크는 언제든지 침해 될 수 있다고 가정해야 하며, 따라서 네트워크에서 의심스러운 측면 이동(Lateral Mov.)을 탐지 할 수 있어야 함. ● 즉, 공격자는 침입하기 쉬운 지점에 침입한 후, 민감한 네트워크 공유 또는 데이터베이스로 선회함
대응 방안
● 지속적인 네트워크 시각화, 허용된 행위에 대한 사전 정의된 정책 및 통제는 측면 이동(Lateral Mov.)을 억제하는 데 중요 ● 내부 네트워크에 대한 모니터링 및 탐지 ● 공격을 당했다고 가정, 침입자가 네트워크 내에서 무엇을 하는지 알 수 있어야 공격자를 방해할 수 있음. 따라서 내부 East-West 트래픽을 감시하는 것이 중요
PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 지능형 네트워크 이상 행위 탐지 (Egg Down., C&C, Recon, Lateral Mov., Exfiltration, DGA/Fast-flux DNS 등) ● 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

Phase 6: Collect, Exfil., and Exploit (수집, 유출 및 해킹)
해커 공격 행위
● 공격자가 적극적으로 데이터를 유출
대응 방안
● 현재 보다 상황이 더 악화될 수 있으므로 침해사고 대응 계획 수립이 필요함. ● 데이터 손상, 데이터 조작, 데이터 파괴를 어떻게 처리할 것인가를 파악해야 함. ● 실시간으로 네트워크의 활동을 볼 수 있는 경우, 해커가 접촉하고 있는 대상을 알 수 있으며, " 중요 자산"에 접근하기 전에 잠재적으로 차단할 수 있음.
PacketCYBER기반 위협 탐지 및 헌팅(Hunting)
● 지능형 네트워크 이상 행위 탐지 (Drive-by-download., C&C, Recon, Lateral Mov., Exfiltration, DGA/Fast-flux DNS 등) ● 지속적인 자동 위협 헌팅 (악성코드, 네트워크 이상 행위, 침해징후의 탐지 및 상관관계 분석) ● 모든 통신, 애플리케이션 통신, 파일 다운로드 모니터링 및 분석 (중장기 데이터)

NSA 결론

- NSA에는 세계 최고 수준의 해커들이 있으며, 따라서 NSA가 자신들의 Best Practice를 제시하였으므로, 주의를 기울일 가치가 있음.

- Joyce 얘기의 핵심은 **"네트워크에 대한 지식과 가시성의 불균형이 취약점을 생성하는 핵심 요소"**라는 것임.
- 모든 단계에서, 해커는 조직의 보안 관리자가 네트워크에서 (파악)하고 있지 못하는 것을 파악하기 위하여 자신들의 능력을 활용할 것이며, 보안을 침해하기 위해서 보안 관리자의 (네트워크)에 대한 지식 부족을 이용할 것임.