IDG
STRATEGIC
MARKETING SERVICES

TANIUM

IDG Summary | TANIUM

실시간 위협 헌팅의 중요성

“보안 위협, 탐지와 차단이 전부가 아니다”

실시간 위협 헌팅의 중요성
"보안 위협, 탐지와 차단이 전부가 아니다"

남인우 | 태니엄 전무

사이버 위협이 나날이 고도화되고 있다. 각종 공격 방법이 진화하고 APT(Advanced Persistent Threat)는 이미 일상적인 공격 유형이 됐다. 지난 해만 하더라도 로그4j(Log4j) 취약점을 비롯해 프린트나이트메어 위협, 윈도우 서버 취약점, 어도비 취약점과 같은 제로데이(Zeroday) 취약점이 기업을 위협했다. 이제 외부와 내부 네트워크의 경계에서 모든 사이버 위협을 탐지하고 차단하는 것으로는 충분한 대응이 어려워졌다.

이런 문제적 상황은 보안업계만이 아닌 전 산업, 전 세계적인 골치거리로 대두되고 있다. 이에 대응하기 위해 수많은 보안 대책과 기술이 제시되고 있는 가운데, 위협 헌팅(Threat Hunting), 특히 실시간 위협 헌팅은 현재 사이버보안이 안고 있는 많은 문제를 해결해준다. 로그4j에 적용한 위협 헌팅 사례를 통해 태니엄의 강점에 대해 알아본다.

지능형 위협에 대응하는 위협 헌팅

위협 대응 측면에서 사이버보안은 공격자의 유입 경로를 파악하는 일과 함께 잠복기에 있는 위협의 진행과 흔적을 사전에 파악, 색출하고, 보안 사고 발생 또는 발현 징후를 파악한 후에도 남겨진 숙주 또는 잔여 흔적과 잠복기에 이뤄진 여러 징후들을 색출해 제거하는 것이 중요하다.

기존 보안 기술을 우회하는 지능형 위협에 대응하기 위해 등장한 위협 헌팅은 위협이 발생하기 이전에 사이버 자산의 취약점을 찾아내고, 이를 제거해 위협이 발생하지 않도록 조치하는 모든 활동을 말한다. 위협 헌팅은 현대의 보안 위협에 능동적으로 대처하고 남겨진 흔적 및 침입 경로의 조사를 포함하며, 탐지뿐만 아니라 숙주 제거와 유입 및 전파 경로를 파악해 '위협 대응'을 하고 재발 방지를 위한 대책을 좀 더 적극적으로 하는 '침해 대응' 활동이다.

침해 대응에 있어 기업은 EPP(Endpoint Protection Platform)나 안티바이러스, 안티랜섬

웨어와 같은 탐지 역량도 필요하다. 하지만, 탐지가 어려운 변종이나 여러 경로로 감염돼 잠복기를 거치는 공격이 일상화된 상황을 고려한다면 정보 수집, 헌팅, 추적을 포함한 위협 헌팅은 무엇보다 중요하다. 전 세계적으로 위협 헌팅에 대한 중요성과 가치는 이미 잘 알려져 있다. SANS의 2020 위협 헌팅 설문조사에 따르면, 전 세계 대기업의 65%에서 위협 헌팅을 도입했으며, 29%는 1년 내로 도입한다고 밝혔다.

로그4j 관련 취약점이 위험한 이유

지난해 12월, 로그4j(Log4j)에서 악용하기 쉬운 취약점이 발견됐다. 로그4j는 자바(JAVA) 프로그램의 유지와 관리를 위해 기록으로 남기는 필수 라이브러리다. 공격자는 JNDI라는 취약한 클래스 파일을 이용해 공격을 수행하는데, 이 공격은 취약한 서버 내에 존재하는 로그4j 라이브러리를 통해 이뤄진다. 공격자가 준비해 놓은 악의적인 LDAP 서버를 통해 쿼리를 수행한 후 취약한 서버가 악성 클래스 파일을 다운로드하는 형태를 취한다. 이후 공격자는 원하는 코드를 추가, 실행할 수 있어 여러 가지 공격이 가능하다.

대부분 웹 애플리케이션이 자바 기반으로 이뤄져 있으며, 상용 소프트웨어도 로그4j 라이브러리를 사용하는 사례가 많아 가히 상상할 수 없을 정도의 많은 기업이 이 취약점에 영향을 받고 있다. 심지어 자바 프로그램을 직접 사용하지 않더라도 기기에 내장되거나 미들웨어에 자바를 사용한 경우에도 마찬가지다. 로그4j를 관리하는 아파치재단은 이 취약점의 보안 위협 수준을 최고 등급인 10단계로 평가했다. 보안업체뿐만 아니라 관련한 모든 업체가 로그4j 취약점 패치를 발표했지만, 전문가들은 이 취약점과 관련한 공격은 상당히 오랜 기간 계속될 것으로 예상하고 있다.

로그4j 취약점을 패치한다고 위험한 상황이 끝나는 것이 아니다. 기업이 이 취약점을 신속하게 해결했더라도 공격자가 이미 침입해 숨어 있을 가능성을 배제할 수 없다. 따라서 공격을 감행한 흔적들이 탐지되고 있기 때문에 기업은 하루빨리 사내 로그4j 공격 흔적을 찾아내는 것이 어느 때보다 중요하다. 실제로 2021년만 하더라도 프린트나이트메어, MS 익스체인지 서버, 어도비 취약점을 악용한 제로데이 공격으로 많은 피해가 발생했다.

또한 로그4j 관련 위협이 사라졌어도 앞으로 어떤 취약점이 언제 어떻게 나타날지 모르는 위기 상황은 계속된다. 예를 들어, A 공급업체의 블루투스 펌웨어에서 새로운 취약점이 발견된다면, 로그4j와 같은 특정 파일만 찾는 툴은 아무런 소용이 없다.

게다가 로그4j 관련 문제는 단순히 jar 파일만 찾는다고 해결할 수 있는 것이 아니라 애플리케이션 계층에 숨어있는 파일까지 파악하는 것이 중요하다. 로그4j 라이브러리는 다른 소프트웨어에서도 사용할 수 있다. 이 과정에 jar 파일을 이름변경(rename)하거나 WAR

파일로 변환할 수도 있어 파일명만으로 헌팅하는 것은 한계가 있다.

일상화된 APT, 대다수 사이버 공격으로 확산

이렇게 치명적인 위협이 지속적으로 발생하는 상황에서 기업이 해야 할 일은 무엇일까? 지금까지 일반 악성파일 공격은 안티바이러스 프로그램 등으로 탐지, 삭제하거나 감염 PC를 포맷하는 등의 조치로 마무리할 수 있었다. 하지만 최근 위협은 악성파일을 지우는 것으로 해결하지 못할 수 있다. 10년 전, APT(Advanced Persistent Threat)라 부르던 지능형 지속 위협은 소수의 공격자가 특정 표적을 위한 고도화된 공격 형태였지만, 최근에는 공격자의 일상적인 공격 유형이 됐다. 때문에 위협이 발생한 기기를 찾아 악성코드를 지우거나 포맷을 하는 등의 대응 조치를 하더라도 이미 피해자 모르게 확산이 진행되어, 공격자는 침입 경로나 확산된 모든 곳에 그대로 남아있을 가능성이 높다.

그래서 탐지한 악성파일을 삭제하는 단순 대응이 아닌 공격자의 내부 이동(Lateral Movement), 내부 감염(Lateral Infection)의 흔적과 남아있는 다른 모든 잠재적인 위협을 찾아내는 것이 중요하다. 현대적인 공격 활동은 정보 수집, 침입, C&C 통신, 확산 등 일련의 프로세스를 거치게 된다. 랜섬웨어든, 정보 유출이든 어떤 공격이라도 내부 이동과 내부 감염의 실행 단계를 거쳐야 하기 때문에 어떤 형태로든 흔적을 남기게 된다.

예를 들어, 2021년 8월 대만의 컴퓨터 부품업체와 유수의 IT 컨설팅 업체의 랜섬웨어 감염 사건에서 볼 수 있듯이 이중 갈취 수법은 일상적인 공격 활동으로 자리잡았다. 이때 공

격자는 침입 성공이후, 특정 파일만 탈취, 암호화해 협박한 것이 아니라, 오랫동안 잠복하면서 내부 이동, 내부 감염 등의 공격 활동을 해왔다. 이것이 위험한 이유는 안티바이러스나 안티랜섬웨어와 같은 탐지 도구나 로그에 의존해서는 해당 위협을 근본적으로 제거할 수 없으며, 몸값을 지불하더라도 재발하지 않는다고 보장할 수 없기 때문이다. 따라서 사고 이후 재발 방지와 공격자와의 교섭력을 강화하기 위해서라도 빠르게 공격자의 침입 경로와 방법, 내부 이동, 감염 흔적 등을 파악하는 것이 중요하다.

공격자의 흔적을 제대로 탐지하지 못하는 이유

하지만 공격자의 공격 경로나 방법 등을 제대로 파악하는 것은 좀처럼 쉽지 않고, 많은 시간이 든다. 기업이 공격자의 내부 이동, 내부 감염 등을 제대로 탐지하지 못하는 이유는 대략 3가지로 설명할 수 있다.

첫 번째, 위협 헌팅을 하지 않는다. 공격자가 침입한 이후 기업이 침해를 인지하는 데 걸리는 시간은 평균 수 개월 이상으로 알려져있다. 이는 공격자가 침입해 사고가 발생하거나 기업이 인지하기까지 공격자가 내부에서 이동하고 확산하는 등 공격 활동을 하는 평균 기간이다. 지난 몇 년동안 전 세계적으로 기업은 점점 더 빠르게 위협을 찾아내 방어하고 있지만, 아태 지역의 경우 그 기간이 길어지는 추세다. 위협 헌팅은 사고 이후 조치뿐만 아니라 사고 이전 공격 활동에서 남긴 흔적을 찾는 과정도 모두 포함한다.

두 번째, 악성코드 탐지 시 대부분 원인을 파악하지 않고 안티바이러스를 통한 치료나 시스템 포맷 등 단순 조치로 대응을 종료한다. 앞서 설명했듯이 일반적인 악성코드라면 탐지 후 제거하거나 감염된 기기를 포맷하는 것으로 완료할 수 있으나 최근 일상적인 공격이 방식이었다면 파일 하나 지우는 것만으로는 해결할 수 없다.

세 번째, 공격자는 공격 파일을 잘 알려진 방어 툴로 미리 테스트하기 때문에 기존 방어 툴로는 탐지할 수 없다. 기업의 방어 툴 선택 기준이 파일 탐지율과 적중률인 상황에서는 현대적인 위협을 방어하기 어렵다.

위협 헌팅, '다양한 형태' '실시간' 정보 중요

위협 헌팅은 툴이나 시스템을 도입하지 않고 자체 보안 인력으로도 가능하다. 예를 들어 이모탯(Emotet) 랜섬웨어의 경우, 상당히 복잡다단한 흔적을 남긴다. 이모탯이 남긴 다운로드 경로나 파워셸을 통해 발생시킨 새로운 차일드 프로세스, 이로 인해 생성된 파일에 대한 내용, 바이러스토탈(VirusTotal)이나 기타 사이트에서 알려진 악성 파일에 대한 해시값, IOC 값들은 무료로 얻을 수 있다. 이런 정보를 기반으로 주기적으로 헌팅하고 검사, 조회하는 것만으로도 상당부분 위협을 줄일 수 있다.

하지만 위협은 언제, 어떤 방식으로 나타날지 모른다. 로그4j 취약점은 파일 네임이 큰 것이 특징이며, 어떤 위협은 레지스트리 정보를 수정하는 것으로 흔적을 남긴다. 또 다른 위협은 소프트웨어 버전이 변경되거나, 오피스 파일에 보안 설정이나 매크로가 수정되는 등 다양한 징후로 파악할 수 있다. 물론 이런 징후들은 기존 보안 장비와 툴로도 모두 파악할 수 있다.

여기서 '실시간'이라는 키워드가 등장한다. 사건이 발생하거나 취약점이 등장하면 기업은 보안 인력을 동원해 빠르게 각종 흔적을 찾거나 취약점을 해결할 수 있을 것이다. 하지만 전 세계에 수백 개의 지점, 지사가 있는 기업, 여러 개의 네트워크를 운용하는 기업이라면 어떨까? 보안 인력을 총동원하더라도 이에 대응하는 데 수일 혹은 수주일이 소요될 수 있으며, 그동안 해당 위협을 통한 공격에는 무방비 상태가 될 수도 있다.

그래서 로그4j와 같은 특정 파일을 찾는 툴을 보유하는 것이 중요한 것이 아니라 애플리케이션 정보, 사용자 행위 정보, 하드웨어 상세 정보, 네트워크 정보 등 가능한 한 많은 양의 정보를 실시간으로 볼 수 있는 체계를 갖춰야 한다.

태니엄, 수만 대 기기의 실시간 정보 가시성과 조치 방안 제공

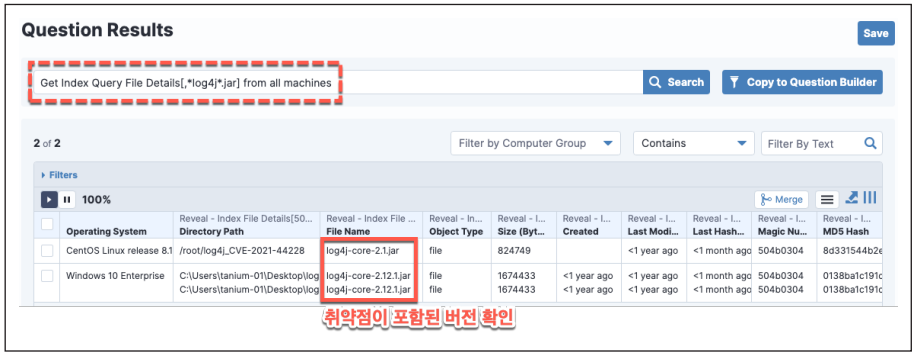
기업은 취약한 기기가 탐지되면 해당 목록을 확인하고, 필요하다면 개별 기기나 그룹에 대해 즉각적인 조치를 취할 수 있어야 한다. 대부분의 위협에 대한 1차적인 가이드는 소프트웨어를 패치하거나 업데이트하는 것이 가장 우선인데, 바로 업데이트하기가 어려운 경우가 많기 때문에 다른 위협 완화 대책을 수행할 필요가 있다.

태니엄은 전 세계 수만 대의 기기와 소프트웨어, 프로세스, 레지스트리 정보, 보안 설정 값, 사용자 행위, 네트워크 행위 등과 각종 운영, 자산, 보안, 추적, 포렌직과 관련한 모든 정보를 실시간으로 조회할 수 있다. 또한 전체 기기에서 로그4j 관련 파일 존재 여부, 파일명, 위치 등의 정보를 실시간 검색한 것처럼 1,700여 가지 모든 위협에 대해서도 똑같은 형태의 실시간 정보 가시성을 제공한다.

사실 이렇게 많은 정보를 메뉴 형태로 구성할 수는 없다. 태니엄 사용자는 화면과 같이 인터넷 검색엔진에서 자료를 찾듯이 “Get 원하는 파라미터 from 대상 기기 + 상세 옵션”의 즉석 쿼리를 통해 정보를 찾을 수 있다.

사용자는 자주 사용하는 쿼리를 저장해 클릭만으로도 다시 볼 수 있으며, 정형 데이터뿐만 아니라 비정형 데이터도 실시간으로 검색할 수 있다. 이와 함께 침해된 컴퓨터에서 내부 확산 가능 경로에 대한 가시성을 제공하며, 기기, 그룹, 사용자로 내부 확산 영향이 큰 대상

화면 | 로그4j 실시간 헌팅



을 리스트로 표시하고 비인가 네트워크 연결을 모니터링한다.

기업은 태니엄을 통해 위험한 해시값이나 IOC 등의 징후만으로도 공격을 탐지할 수 있으며, 기본 보안 설정으로 비인가 네트워크 트래픽 발생을 탐지해 보안 사고를 상당히 막을 수 있다.

이런 실시간 가시성 기술 덕분에 전 세계에 지점을 보유한 소매점이나 은행에서 태니엄을 많이 활용하고 있다. 태니엄 서버를 통해 기업은 서비스나 프로세스 종료뿐만 아니라 파일 삭제, 레지스트리 삭제/수정/생성, 네트워크 격리 등을 단일 플랫폼에서 보고, 조치가 가능하다. 또한 태니엄은 실시간 조회된 정보를 다양한 SIEM과 여러 가지 다른 솔루션과 연동하며, HTTP, 이메일, SQL 서버 등의 프로토콜도 자유롭게 지원한다.

탐지부터 차단, 통합 연계까지 위협 단계별 완벽 대응

태니엄은 데이터 수집, 탐지, 헌팅, 대응, 포렌식, 차단, 통합 연계 등 위협 대응 단계별로 탁월한 기능을 제공한다. 보안 위생을 위한 정보 수집 단계에서 태니엄은 기기와 수집 데이터 종류에 제약 없이 현황 정보와 보안 이벤트를 제공한다. 즉각적인 데이터 수집과 SIEM과의 연계를 통한 고도화가 가능하다. 커스터마이징이 가능한 뷰를 제공하며, 정기적인 취약점/컴플라이언스 보고서로 활용할 수 있다.

태니엄은 실시간/주기적 이상행위 탐지를 위해 실시간 탐지와 주기적 스캔 방식을 모두 지원한다. 커스터마이징된 탐지 조건을 입력할 수 있으며, 외부 인텔리전스와 연동할 수 있다. 탐지된 이상행위의 전사적인 분포 확인 단계에서 태니엄은 한 번에 전체 기기를 대상으로 헌팅이 가능하다. 현재 상태뿐만 아니라 과거 행적을 기반으로 헌팅할 수 있다.

이상행위에 대한 긴급 대처에서 태니엄은 제한적 범위 내에 알려진 위협에 대해 자동 대응이 가능한데, 조건과 항목에 제약 사항없이 커스터마이징이 가능하다. 관리자 확인 하에

적극적인 대응이 필요한 수동 대응은 실시간 정보를 기반으로 판단한다. 긴급 대응 과정에서는 포렌식을 위한 증적 확보도 가능하다.

상세 정보를 기반으로 한 이상행위 분석 단계에서 태니엄은 이상행위 분석 뷰를 제공하며, 분석 시 필수적인 다양한 증적 덤프 기능(MTF, 다양한 캐시, 메모리 덤프, 이벤트 로그, 인증 등)을 제공한다. 이상행위에 대한 실행 차단 단계에서 탐지, 헌팅, 대응, 포렌식 등 각 단계에서의 차단 정책 입력을 지원하며, 많은 수의 차단 정책을 별도로 관리할 수 있다. 분석 고도화와 업무 자동화를 위한 연계에서 태니엄은 다양한 종류의 데이터를 다양한 형식으로 다양한 시스템과 연계할 수 있으며, 세밀한 REST API를 제공해 서비스 자동화가 가능하다.