IDG
STRATEGIC
MARKETING SERVICES

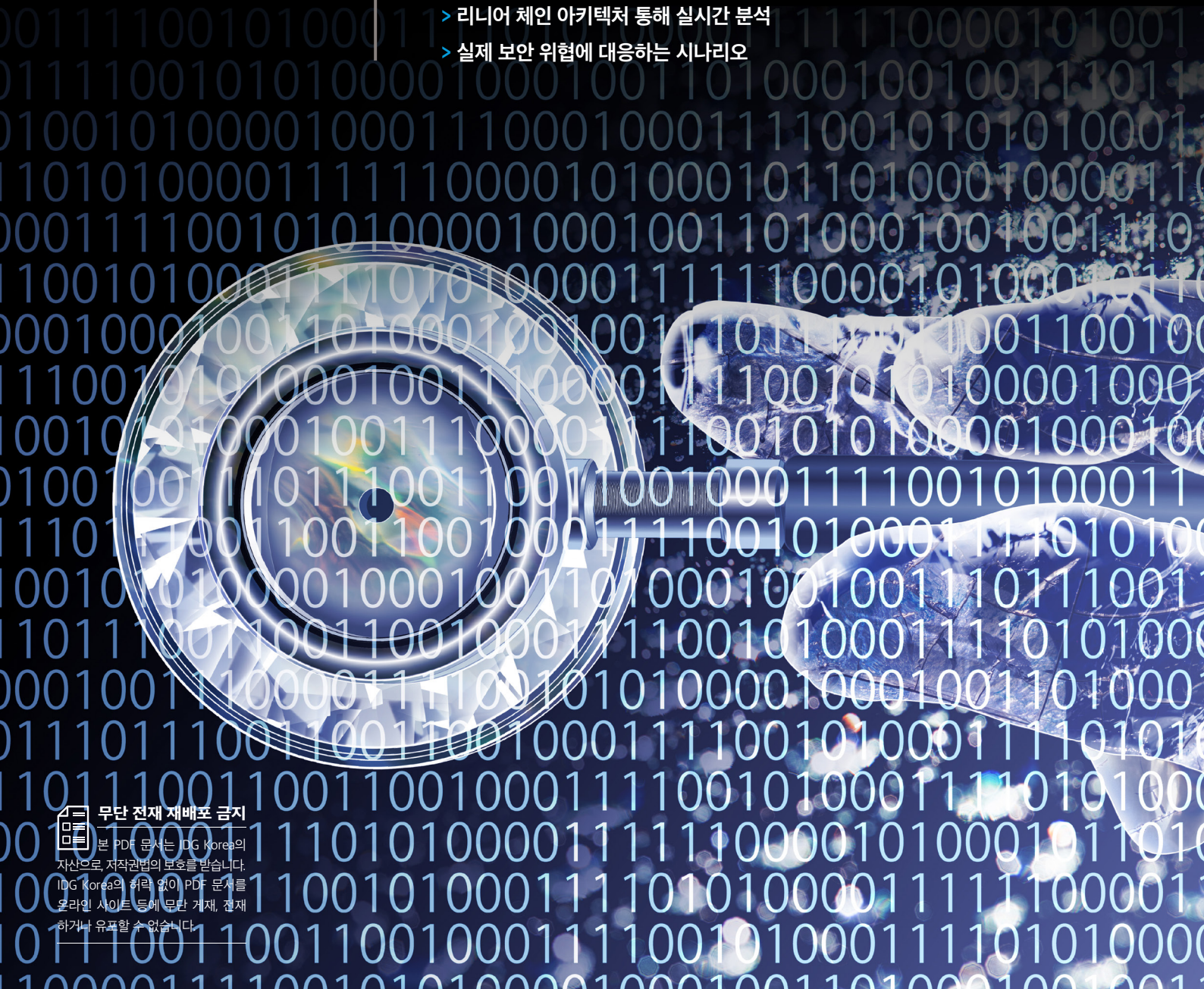
TANIUM

IDG Tech Dossier

"공격으로 보안 사고가 발생했다면 공격자는 9개월 전에 침투"

고도화된 랜섬웨어 공격에 대응하는 실시간 탐지 및 대응 전략

> 랜섬웨어와 APT의 결합, 기업 보안의 총체적 위기
> APT 대처 수단으로 등장한 EDR
> 태니엄 EDR, 엔드포인트 정보를 빠르고 가시성 있게 제공
> 사후 조치 측면에서의 실시간이 중요한 이유
> 리니어 체인 아키텍처 통해 실시간 분석
> 실제 보안 위협에 대응하는 시나리오



“공격으로 보안 사고가 발생했다면 공격자는 9개월 전에 침투”

고도화된 랜섬웨어 공격에 대응하는 실시간 탐지 및 대응 전략

보안 사고가 발생했을 때 피해 기업은 즉시 상황을 파악하고, 조치를 취해야 한다. 당연한 일일지 모르지만, 이를 실현할 수 있는 기업은 소수에 불과하다. 우리 기업에서 발생한 사건의 원인을 파악하고 대응하는데 몇일, 또는 몇주가 걸린다는 사실을 이해할 만한 의사결정권자는 과연 얼마나 될까? 최근 APT 공격에 대처하고자 등장한 EDR 솔루션마저도 랜섬웨어 방어에 한계를 보이는 가운데, 기업이 취할 수 있는 보안 전략에 대해 알아보자.

개인 사용자에게 많은 피해를 입혔던 랜섬웨어가 수년 전부터 표적을 기업으로 확대하면서 지능적이고 고도화된 공격으로 진화했다. 랜섬웨어 공격자는 표적형 전달 메커니즘, 관리도구 및 유틸리티를 사용한 매뉴얼 해킹(manual hacking), 은밀한 네트워크 정찰과 같은 정교한 APT 기술을 활용해 수많은 기관과 기업에 피해를 입혔으며, 피해 규모는 나날이 커져가고 있다.

랜섬웨어 전문 보안업체 코브웨어(Coveware)에 따르면, 2020년 3분기에 평균 몸값 지불액이 2분기에 비해 31% 이상 증가한 23만 3,000달러에 달했다. 암호화폐 포렌식 업체 체인어낼리시스(Chainanalysis)는 2020년에 암호화폐를 사용한 몸값 지불이 전체적으로 311%나 증가했다고 밝혔다.

시장조사기관인 ESG의 최근 보고서에 따르면, 사이버공격 탐지의 개선은 기업 보안 운영의 최우선 과제이며, 기업의 83%가 향후 12~18개월 동안 위협 탐지 및 대응 관련 지출을 늘릴 계획이다. 사실 위협 탐지 및 대응은 항상 기업 보안의 최우선 순위였다. 하지만 지난 몇 년 동안 사이버보안 기술에 수백만 달러를 투자했음에도 불구하고, 대부분의 기업은 여전히 적절한 시간 내에 사이버 공격을 탐지하거나 대응할 수 없다. 오히려 상황이 악화되고 있다고 해도 무방하다.

랜섬웨어와 APT의 결합, 기업 보안의 총체적 위기

APT 공격은 산업별, 또는 해당 기업의 특수한 상황이나 기업이 도입한 소프트웨어나 기기들의 취약점을 악용해 공격한다. 이는 표적 기업에 맞춤화된 공격을 한다는 것이다.

금융 업종을 공격하는 공격자는 기밀 정보를 탈취하거나 서비스 취약점을 악용한 사기, 시스템 파괴 후 금전을 요구하는 것을 목적으로 한다. 공격 대상은 인트라넷 서버나 직원 PC, 오피스 기기, ATM과 같은 고객 서비스 기기까지 사실상 모든 기기가 해당된다. 한 공격 그룹은 외환거래전문업체인 트레블렉스(Travelex)의 VPN 취약점을 악용, 침투해 6개월 동안 5GB 데이터를 탈취한 후, 600만 달러를 요구했다. 트레블렉스는 초기에 해킹 사실을 부인하다가 랜섬웨어 공격을 받은 후, 공격자에게 230만 달러를 지불했다.

제조 및 기반 시설을 노리는 공격자는 산업 시설에 침투, 파괴하는 데 목적을 두고 있으며, 시스템을 감염시킨 후 금전을 요구하기도 한다. 2019년 3월, 세계적인 알루미늄 제조업체인 노르스크 하이드로(Norsk Hydro)는 랜섬웨어 공격을 받았다. 공격자는 소셜 엔지니어링 공격을 통해 인증 정보를 탈취한 후 원격으로 내부 프로그램을 실행시켰다. 결국 노르스크 하이드로는 PC만 감염된 것이 아니라 실제 생산 시설의 OT(Operation Technology) 장비까지도 문제가 발생했다. 이 회사는 몸값은 지불하지 않았고, 약 6,000만 달러의 손실을 입었다.

표 | 산업별로 다른 목적과 행동을 보이는 APT

산업	목적	대상	사례/공격 방법
금융	• 내부(기밀) 정보 탈취, 서비스 취약점 악용한 사기, • 시스템 파괴 후 금액 요구	• 인트라넷 서버, 직원 PC 및 오피스 내 기기, 대고객 서비스 기기, ATM, 서버	• 트레블렉스 VPN 취약점을 이용해 침투, 5GB 데이터를 6개월 동안 탈취, 600만 달러 요구
제조 & 기반 시설	• 산업 기반 시설 중단, R&D 정보 탈취, 시스템 파괴 후 금액 요구	• 산업 시설 내 기기, 다양한 종류의 센서, 제조 핵심 기기, 연구소 내 기기	• 노르스크 하이드로(세계 최대의 알루미늄 제조) 소셜 네트워크 공격을 통해 인증 정보 탈취, 원격에서 PsExec 수행, OT 영역의 시스템으로 확산
의료	• 의료(개인/민감) 정보 탈취, R&D 정보 탈취, 의료 기기 파괴 후 금액 요구	• 의료정보 서비스 서버, 의료기기, 연구소 및 오피스 내 기기	• 피싱을 통한 전염, 샘샘(SamSam) 랜섬웨어 수행(RDP), reGeorg로 HTTP 터널링으로 침투
유통 & IT 서비스	• 신용카드 및 결제 정보 탈취 • 고객 개인정보 탈취	• POS 시스템, 온라인 지불결제 서버, 서비스 서버(웹, 모바일)	• POS, 서버 취약점 발굴 시도, Wifi 네트워크 취약점을 이용한 침투, 서버 침투 후 데이터 유출

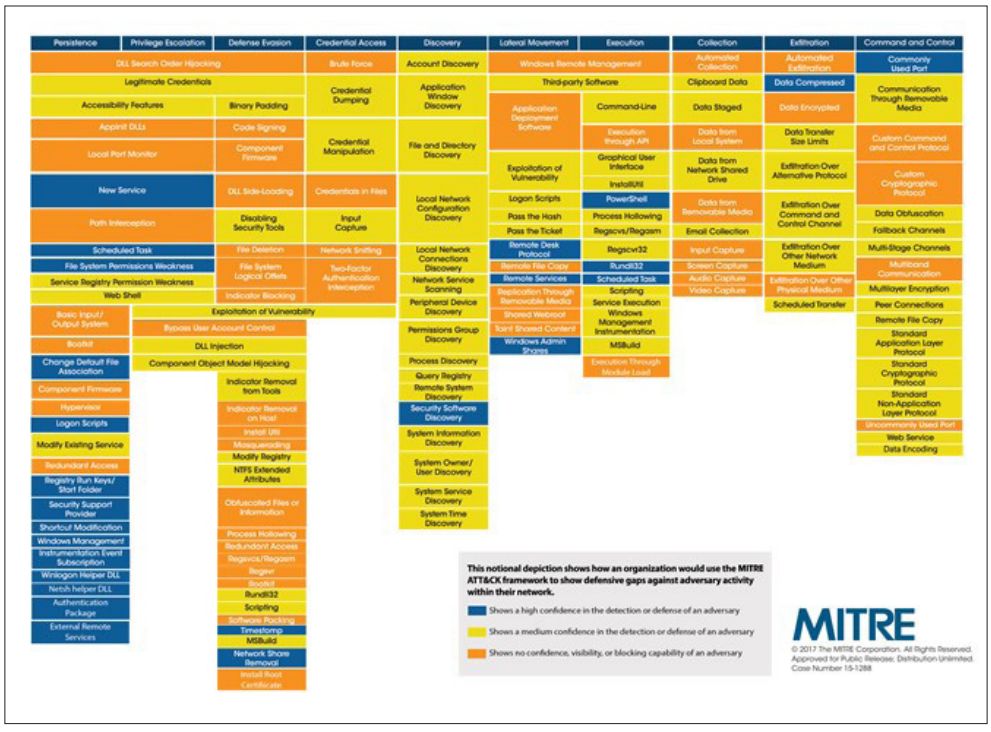
의료 분야는 데이터가 어느 산업보다 민감하다. 공격자는 의료 정보나 R&D 정보를 탈취하거나 의료 기기를 감염시킨 후 금전을 요구한다. 독일의 한 병원에서는 랜섬웨어 공격으로 병원 시스템이 마비되어 중환자를 다른 병원으로 이송하다 사망하기도 했다. 유통이나 IT 서비스 분야 또한 많은 공격이 발생하고 있다.

APT 공격은 여러 단계를 거친다. 처음 감염/침입 전에 탐색 단계를 거쳐, 감염/침입 직후에는 내부 전파 및 어떤 공격이 효율적일지 파악하기 위해 평균 9개월의 잠복기를 가진다. 파악이 끝난 공격자는 C&C 서버를 통해 DDoS, 정보탈취/유출, 랜섬웨어 등 다양한 공격을 할 수 있다. 일단 '공격이 실행'되면 기업의 피해는 불가피하다. 즉각 회복은 불가능하며, 우선 감염된 다수의 내부 엔드포인트를 색출하고, 침입 경로를 추적하며, 로그 분석 및 포렌식 등의 사후 조치가 필요하다.

랜섬웨어 공격이 발생했다는 것은 공격자가 네트워크 내에 침입해 모든 준비를 끝냈다는 의미다. 따라서 피해 기업은 사건 조사를 위해 평균 9개월 간의 로그 데이터를 검토해야 하는데, 수개월 간의 로그를 저장한 기업은 그리 많지 않다. 또한 동종 업계나 관련 업체에 특정 취약점으로 인한 보안 사고 소식이 전파되면, 보안 담당자는 해당 취약점이 자사에 미치는 영향에 대해 즉각적으로 파악해 업데이트해야 한다.

또한 기업이 랜섬웨어에 감염되면 보안 담당자는 확산을 막기 위해 최선을 다해 노력한다.

그림 | APT 공격 단계별 공격 기술



하지만 이런 노력이 일회성으로 끝나면 아무런 소용이 없다.

랜섬웨어는 드러난 공격 형태일 뿐, 유입, 감염, 전파, 실행, 은닉 등의 공격 단계는 APT의 그것과 같기 때문에 APT 방어 전략으로 접근해야 한다. APT의 공격 단계별 징후 및 행위를 기존 EPP로는 탐지할 수 없듯이 랜섬웨어 공격 또한 마찬가지다.

<그림>은 마이터 어택(MITRE ATT&CK)에서 정리한 공격 단계다. 초기 접근부터 파괴에 이르기까지 총 12단계에 걸쳐 있는데, 각 단계별로 공격자들이 사용할 수 있는 기술은 아주 다양하다. 이를 한두 개의 자동화된 도구로 방어한다는 것은 불가능에 가깝다.

APT 대처 수단으로 등장한 EDR

기존 시그니처 기반의 보안 솔루션의 한계를 극복하고 APT 공격의 대처 수단으로 등장한 것이 엔드포인트 탐지 및 대응(Endpoint Detection & Response, EDR)이다.

EDR은 네트워크 상의 최종 사용자 기기에서 의심스러운 활동과 행동을 탐지하고 인식된 위협을 자동으로 차단하도록 대응하고, 추가 조사를 위해 포렌식 데이터를 저장하는 보안 도구다. EDR 플랫폼은 자동화된 프로세스나 인간의 개입을 통해 엔드포인트에서 발생하는 모든 것, 즉 프로세스, DLL로의 변경, 레지스트리 설정, 파일 및 네트워크 활동 등에서 위협을 인식하거나 대응할 수 있는 데이터 집합과 분석을 결합한다.

2013년에 등장한 비교적 새로운 개념인 EDR은 기존의 보안 도구를 통합한 EPP(Endpoint Protection Platforms)와 비교되기도 한다. 시그니처 기반의 EPP는 본질적으로 예방의 성격을 띄고 있는데 비해, EDR은 구성 변경부터 시작 또는 삭제된 프로세스, 접근, 복사 또는 유출되는 파일에 이르기까지 엔드포인트에서 발생하는 모든 활동을 모니터링하면서 보안 담당자에게 일정 수준의 자동 대응과 함께 초동조치를 제공하는 것을 목표로 한다.

EDR의 동작 방식은 일반적으로 최종 사용자 기기에 설치된 에이전트를 통해 세밀한 모든 활동을 모니터링하면서 내부 또는 클라우드에 있는 중앙 집중식 서버로 정보를 전송한다. 서버는 자동으로 문제를 탐지해 이를 수정하거나 보안 직원에게 경고를 보낼 수 있으며, 또한 보안팀이 모니터링하는 대시보드를 통해 정보를 제공한다.

EDR 개념을 처음 소개한 가트너는 EDR 솔루션이 제공해야 하는 주요 기능을 다음과 같이

정리했다.

우선 의심스러운 활동에 대한 탐지 기능이다. 이는 EDR의 핵심으로, 어떤 일이 언제부터 잘못되고 있는지를 파악할 수 있다. 지능형 공격 차단 기능은 위협이 탐지되는 즉시 퇴치 작업을 시작한다. 경고 분류와 필터링 기능은 보안 담당자의 '경고 피로'를 극복하는 데 중요하다. EDR은 잠재적인 경고 신호를 분류할 수 있으며, 사람의 주의를 필요로 하는 경고를 구분한다. 여러 공격 방식이 다방면에서 한 번에 밀려올 때, 다중위협보호 기능은 랜섬웨어와 악성코드를 동시에 차단할 수 있다. 위협 사냥 및 사건 대응 기능을 통해 보안 담당자는 잠재적인 공격을 찾아내는 포렌식 데이터를 조사한다.

가시성은 EDR의 모든 기능과 관련된 중요한 개념이다. EDR은 의심스러운 활동을 추적하기 위해 모든 엔드포인트 간의 연결내역을 볼 수 있어야 하며, EDR이 보는 모든 것을 이해하기 쉽도록 서로 다른 출처의 데이터를 일관성 있게 통합한다. 다른 도구와의 통합 기능은 EDR의 효과를 최대한으로 확장하게 해준다.

즉, EDR 플랫폼이 제공하는 가시성과 통합 데이터 접근은 기존 보안 도구가 좀 더 효과적으로 동작하도록 한다.

태생적 한계를 안고 있는 초기 EDR 솔루션

최근 공격자는 단순히 바이러스나 악성코드를 심는 것이 아니라 다양한 공격 방식으로 접근하고 있다. 예를 들어, 공격자는 기본적으로 이상 징후를 보이는 프로세스를 이용하지 않고, 운영체제에서 제공하는 프로그램이나 오픈소스, 깃허브(GitHub)에서 다운로드 받을 수 있는 일반적인 프로그램의 기능을 활용해 침투하고 확산한다. 또한 목표 기업에 구축된 수많은 소프트웨어나 네트워크 제품, 하드웨어의 취약점에 맞춰 공격하기도 한다.

기업이 공격을 탐지했다 하더라도 즉각 대응하기가 어렵다. 감염을 탐지했다면 초기 감염과 감염 경로를 확인해야 하지만, 이를 파악하지 못해 조치를 취할 수 없는 경우가 많았다. 또한 확산은 자동적으로 진행되기 때문에 감염 확산 속도가 대응 속도보다 빠를 수밖에 없다.

사실 기존 EDR 솔루션은 태생적인 한계를 안고 있다. 초기 EDR 솔루션이 기존 안티바이러스 업체가 기능 개선을 통해 확장하다 보니 자체 보안 인텔리전스를 사용하는 경우가 많다. 인텔리전스의 범위가 좁다는 한계를 극복하기 위해 공급업체는 기업 고객의 메모리, 프

로세스 정보 등을 공급업체의 중앙 서버에 보내 분석한다. 이 후, 분석 결과를 기업의 엔드포인트나 EDR 시스템에 인텔리전스로 추가하는 방식을 취하게 되는데, 이 때 가져올 수 있는 기업 고객의 정보 또한 제한적이다. 기업 고객의 데이터를 과도하게 수집해 문제가 된 경우도 있었다.

따라서 기업은 여러 공격 단계에 걸쳐 완성되는 APT 및 랜섬웨어 공격에 대한 적극적인 대처 방법이 필요하며, 제한된 인텔리전스와 데이터 분석의 한계를 극복해야 하는 과제를 안게 됐다. 최근 기업은 하나의 공급업체에서 제공하는 인텔리전스에 의존하기보다는 여러 곳의 인텔리전스를 조합해 활용하고 있다.

태니엄 EDR, 엔드포인트 정보를 빠르고 가시성 있게 제공

태니엄(Tanium)은 다양하고 수많은 엔드포인트에서 발생하는 정보를 실시간으로 수집하여 해당 정보의 가시성을 높여 보안 관리자나 시스템에 제공한다. 또한 사건 발생 시 각 엔드포인트 정보를 신속히 파악 및 제어할 수 있도록 해 기업의 대응 시간을 획기적으로 줄일 수 있다.

태니엄은 기업 고객에서 이미 구축된 보안 솔루션이나 네트워크 장비, 기존에 구독하던 인텔리전스 등과 연계해 사용할 수 있다는 장점을 갖고 있다. 또한 자체 탐지 기법 외에도 다양한 외부 IoC(Indicators of Compromise)를 활용한 탐지, 분석이 뛰어나며, 다양한 정보를 다양한 단계에서, 다양한 형식으로 가시화할 수 있다.

어제까지 필요 없었던 정보가, 새로운 공격 기법의 출현으로 오늘은 필요한 정보가 될 수 있다. 때문에 분산된 다수의 엔드포인트 기기에서 원하는 정보를 실시간으로 수집할 수 있다는 점은 태니엄의 차별화된 장점 가운데 하나다. 뿐만 아니라 태니엄은 파악된 징후를 가진 엔드포인트에 대해 실시간으로 조치(삭제/변경/업데이트 등)할 수 있다.

태니엄은 담당자가 레지스트리에 있는 정보를 수집해 분석하는데 문제가 없다. 예를 들어, 특정 PC에 있는 폴더의 파일을 가져다가 확인하는 데 제약이 없다는 의미다. 태니엄은 기본적으로 현재 데이터뿐만 아니라 과거 데이터 이벤트를 30일, 60일, 90일 등 설정에 따라 조회할 수 있다. 때문에 30일 전에 이상한 징후를 보였던 프로세스가 현재 공격에 나섰다 하더라도 30일 전, 혹은 그 이전에 있었던 전후 맥락을 파악할 수 있다는 것이다.

사후 조치 측면에서 실시간이 중요한 이유

태니엄은 탐지 단계뿐만 아니라 대응 단계에서도 강점을 갖고 있다. 기존 EDR이 '탐지(Detection)'에는 효과적이지만 '대응(Response)'에는 효과가 떨어진다는 한계를 극복한 것이다.

예를 들어, 협력업체에서 감염 사례를 발견하거나, 혹은 동종 업계에서 특정 취약점을 이용한 위협이 발견됐다면, 자사의 엔드포인트에는 유사한 위협이 없는지 파악하고 조치를 해야 한다. 하지만 전국에 설치된 수천 대의 엔드포인트 기기에 특정 문자열, 레지스트리 특정 값, 호스트 파일의 특정 내용을 짧은 시간 안에 파악하는 것은 불가능에 가깝다. 또한 마이크로소프트 오피스의 특정 버전에 취약점이 발견된 경우, 한두 시간 내에 업데이트할 수 있는 솔루션은 없다. 현실적으로 특정 업데이트를 하기 위해서는 1주일 정도 순차적으로 작업해야 한다.

특히 포렌식 측면에서 일단 사고가 발생했다면 공격자는 9개월 또는 그 이상을 내부 네트워크에 잠복해 있었다는 점이 감안했을 때, 수개월 이전의 로그 데이터가 필요하지만 앞서 언급했듯이 일부 기업을 제외하고 수개월 간의 로그 데이터를 저장하는 곳은 거의 없다.

기업은 기간과 상관없이 엔드포인트 기기의 로그 데이터를 확보하는 것이 중요하다. 또한 엔드포인트에 저장된 수개월치의 로그를 제대로 분석하기 위해서는 지역과 기기의 수에 관계없이 실시간 조회가 가능해야 의미가 있다.

태니엄은 엔드포인트에 저장된 로그데이터와 함께 기존 보안 장비의 위협 정보와 네트워

크 상의 로그 이벤트, 다양한 인텔리전스 서비스들을 상호 연관 관계를 통해 보안 관리자에 제공한다. 또한 자동화를 통해 영향을 받은 엔드포인트 기기를 격리하거나, 악성코드를 제거할 수 있으며, 좀 더 강력하게는 해당 기기를 꺼버리는 등의 다양한 방식으로 대응할 수 있다.

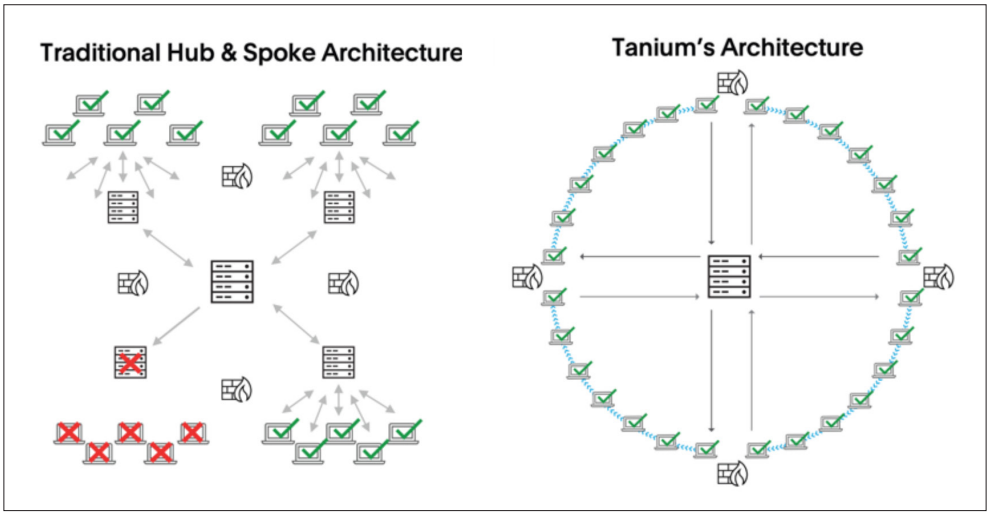
리니어 체인 아키텍처 통해 실시간 분석

태니엄이 수많은 엔드포인트에 담긴 로그데이터를 실시간으로 분석하고 대응할 수 있는 것은 태니엄의 리니어 체인 아키텍처(Linear Chain Architecture) 덕분이다.

일반적으로 많이 사용하는 아키텍처는 허브 및 스포크 아키텍처(Hub & Spoke Architecture)로, 다수의 엔드포인트가 서버와 통신하는 구조를 가지고 있다. 이 아키텍처는 중앙 위치에서 보안 정책을 적용하는 등의 제어 측면에서는 효과적이지만, 많은 문제점을 안고 있다. 예를 들어, 대규모로 분산된 환경에서는 각 지역마다, 엔드포인트 수가 많아질수록 연계 서버 또한 더 많이 필요하기 때문에 엄청난 인프라 비용과 관리 문제가 대두된다. 또한 연계 노드에서 장애가 발생하면 해당 연계 노드와 통신하는 모든 엔드포인트가 동시에 장애가 발생할 수 있는 위험을 안고 있다. 뿐만 아니라 한 서버에 많은 엔드포인트가 동시에 통신하면 서비스에도 부하가 발생한다.

태니엄의 리니어 체인 아키텍처는 하나의 네트워크 내에 단 몇 대의 엔드포인트만 서버와 통신하기 때문에 서버에서 발생할 수 있는 트래픽 부하나 성능 문제를 획기적으로 줄일 수 있다. 또한 서버와 통신한 몇 대의 엔드포인트가 다른 엔드포인트와 체인을 유지하고 있기

그림 | 전통적인 허브 및 스포크 아키텍처와 태니엄의 리니어 체인 아키텍처



때문에 엔드포인트의 성능 문제도 줄일 수 있다. 태니엄은 자동적으로 최적화된 통신을 유지하는 아키텍처를 통해 부분적으로 장애가 발생하더라도 자동적으로 복구되며, 엔드포인트에 대한 실시간 제어 능력을 확보할 수 있다.

실제 보안 위협에 대응하는 시나리오

최근 공격은 굉장히 진화되고 교묘해지면서 오피스 매크로를 활용해 침투하는 형태가 많이 발생하고 있다. 2020년 11월 말, '국세청 전자세금 계산서 발급 메일 안내'로 위장한 피싱 메일이 불특정 다수를 대상으로 유포됐다.

국세청을 사칭한 악성 피싱 메일은 1년 전부터 꾸준히 발생했던 악성 위협 형태로, 기존에는 워드 파일이었다가 최근에는 파워포인트 파일로 변화하고, 암호화된 zip 파일 형태로 들어오는 경우도 있다. 이렇게 공격자는 좀 더 교묘한 방법으로 사용자들이 메일을 받았을 때 파일을 열어보지 않을 수 없도록 진화하고 있다.

사용자가 첨부 파일을 열면, 실제 매크로가 동작하면서 경고 문구가 뜨긴 하지만, 대부분의 사용자는 국세청에서 보낸 메일이기 때문에 확인만 하고 넘어가는 경향이 있다. 사용자 클릭 한 번으로 공격자는 엔드포인트에 악성코드를 심고 추가적인 악성 행위를 할 수 있는 기반을 마련한 셈이다.

공격자는 이렇게 이메일을 통한 오피스 매크로 악성코드 공격 방식을 선호한다. 엔드포인트에 대해 직접 악성코드를 심기 위해서는 고도의 기술이 필요하기 때문에 좀 더 쉬운 방법인 이메일 피싱 방법을 택한 것이다.

일단 오피스 매크로가 동작하면 추가적인 악성 페이로드가 실행되는데, 이 때 악성 C&C 서버와 통신하거나 악성 URL로 접근해 악성코드들을 다운로드하는 방식을 취한다.

실제 다운로드되는 악성코드는 RDP(Remote Desktop Protocol)이나 공유 폴더 등을 통해 내부로 전파된다. 전파된 악성코드를 통해 공격자는 랜섬웨어 공격을 하거나, 장기간 은닉하면서 지속적으로 정보를 탈취하는 등의 여러 가지 형태의 공격 형태를 보인다.

기업 입장에서는 단편적인 악성 행위가 아닌 특정 목적으로 자사를 표적으로 장기간 내부에 머무르면서 정보를 수집하고 취약한 엔드포인트를 정찰해 이동하는 공격 형태가 더 위험할 수 있다. 기업은 이런 은밀한 공격에 대해 최우선 순위로 탐지하고 대응해야 한다. 그

리고 공격이 발생한 이후에는 공격 흔적들을 분석하는 포렌식이 무엇보다 중요하다.

태니엄은 기본적으로 다양한 자체 행위기반 탐지 기법인 시그널을 통해 실시간으로 탐지하거나, 경고하는 기능을 제공한다. 또한 필요한 경우, 엔드포인트에 직접 접속해 그동안 저장했던 데이터를 통해 연관 관계를 분석할 수 있는 포렌식에 가까운 분석을 할 수 있다. 물론 악의적인 프로세스에 대해 전사적으로 실시간 차단하거나 삭제, 또는 레지스트리에 대해 수정, 조치를 하는 등 굉장히 유연한 보안 대응 프로세스를 제공한다.

특히 이런 악성코드가 내부 수평 이동(Lateral Movement)을 통해 전파되는 활동에 대해서도 탐지, 대응할 수 있으며, 태니엄뿐만 아니라 기존 솔루션들과 연계해 유연한 보안을 할 수 있는 기능을 제공하고 있다.

고도화된 공격을 태니엄으로 대비

앞서 언급했듯이 특수한 목적으로 장기적이고 고도화된 방식으로 은밀히 침투하는 공격에 대해서는 어떠한 솔루션으로도 100% 방어하기는 어렵다. 그리고 기업 내 모든 엔드포인트의 원하는 요구사항을 모두 맞추는, 100% 보안율을 달성하는 것도 불가능하다. 이 때문에 기업은 여러가지 상황들을 조합해 전후 맥락을 파악하며 장기적이고 고도화된 공격에 대해 탐지하는 것이 중요하다.

하지만 대부분의 EDR 솔루션은 이런 정보에 대해 단편적인 데이터만으로 판단할 수밖에 없다. 수많은 데이터를 실제 중앙 서버로 옮기는 데에는 엔드포인트 자체에도 부담이 되지만, 네트워크 트래픽 면에서도 부하가 심하다. 이와 함께 해당 정보를 저장하고 관리하는 것도 어려운 게 현실이다. 이 문제는 비단 탐지만 아니라 대응 측면에서도 영향을 미친다.

태니엄은 관리자의 설정에 따라 짧게는 3개월, 길게는 1년까지 엔드포인트에서 발생한 세밀한 데이터를 엔드포인트 자체에 저장해 두고 리니어 체인 아키텍처를 통해 실시간으로 저장된 데이터를 서버에 불러와 분석하거나, 엔드포인트에 직접 접속해 분석할 수도 있다.

지난 10년 동안 발생한 대대적인 침해 사고의 상당수에서 보안업체는 모두 사고를 탐지했다고 주장하지만, 정작 피해 기업은 제대로 대응하지 못했다. 경고가 과도하게 많은 경우, 경고가 없는 것과 마찬가지 상황이 연출되는 것이다. 강력하다고 주장하는 솔루션은 많지만 실제 솔루션의 효과는 전적으로 이를 사용하는 보안 팀에 의해 좌우된다.