Akamai Enterprise Security Suite로 랜섬웨어 킬 체인 무력화

목차

서론

Akamai 기업 보안 솔루션을 사용하여 킬 체인의 다양한 단계에서 랜섬웨어 차단

오늘날 기업이 직면한 가장 큰 보안 위협 중 하나는 디바이스의 중요한 파일을 암호화하여 사용할 수 없도록 만드는 멀웨어의 한 형태인 랜섬웨어입니다. 멀웨어 운영자는 파일을 원래 데이터로 복원할 수 있는 암호 해독 키나 소프트웨어의 대가로 몸값을 요구합니다. 최근 몇 년 동안, 랜섬웨어 범죄 그룹의 전략은 피해자의 데이터를 공개적으로 유포하거나 다크 웹에서 판매하겠다고 협박하여 데이터를 탈취함으로써 추가적인 영향력을 행사하는 것으로 진화했습니다.

이러한 종류의 공격을 방어하려면 랜섬웨어 그룹이 목표를 달성하기 위해 어떤 방식으로 운영되는지 이해해야 합니다. 이 백서가 바로 그 작업에 도움이 될 것입니다.

랜섬웨어 킬 체인의 이해

랜섬웨어 공격은 복잡합니다. 시스템 침입은 시작에 불과합니다. 공격자는 피해를 극대화하기 위해 암호화를 시작하기 전에 악성 페이로드를 네트워크 전체에 퍼뜨려야 합니다. 한 대의 컴퓨터만 암호화된다면 공격자들은 금품을 요구할 만한 충분한 영향력을 갖지 못하게 될 것입니다. 랜섬웨어 공격이 성공하려면 공격자는 네트워크 자산을 탐색하고 측면으로 이동하는 등 다양한 단계를 수행해야 합니다. 이러한 단계를 흔히 랜섬웨어 킬 체인이라고 합니다.

이 체인의 각 단계에는 탐지 및 방어를 위한 많은 기회가 있습니다. Akamai 기업 보안 제품군으로 네트워크를 미리 준비하면 공격표면을 줄일 수 있으며, 랜섬웨어 공격을 받았다는 사실을 인지하기도 전에 피해를 완화하고 억제하는 데 도움이 됩니다. 이 백서에서는 Akamai Guardicore Segmentation, Enterprise Application Access, Secure Internet Access를 사용하여 킬 체인의 여러 단계에 걸쳐 랜섬웨어 활동을 탐지하고 차단하는 방법을 자세히 설명합니다.

초기 접속
공격자가 외부에서 내부 네트워크에 침입하는 공격의 첫 번째 단계

탐색
공격자가 네트워크 내부의 중요 자산을 탐색하기 위해 사용하는 방법

측면 이동
공격자가 네트워크 전반으로 확산되어 추가 자산을 감염시키는 단계

명령 및 제어
공격자가 감염된 자산에 정보와 명령을 전송하기 위해 네트워크에 통신 채널을 유지하는 다양한 방법

탈취
공격자가 은밀한 방식으로 탈취한 민감한 데이터를 유출하기 위해 사용하는 방법

초기 접속

모든 기업에는 인터넷과 연결되는 수많은 인터페이스가 있습니다. 공격자는 네트워크에 접근하기 위해 이러한 인터페이스를 악용하려고 합니다. Akamai를 사용하면 이러한 인터페이스를 원활하게 보호하고 공격자가 네트워크에 접근하지 못하도록 차단할 수 있습니다.

인터넷 기반 서버 보호

Secure Internet Access 페이로드 분석 기능을 사용하여 인터넷 기반 서버를 공격으로부터 보호하세요

Kaspersky에 따르면, 공격자가 초기 접속 권한을 얻기 위해 사용하는 가장 일반적인 방법은 패치되지 않은 시스템에서 인터넷 기반 애플리케이션의 원데이 취약점을 악용하는 것입니다. Log4Shell(CVE-2021-44228)과 ProxyLogon(CVE-2021-26855) 같은 취약점은 오늘날에도 여전히 네트워크를 침해하고 랜섬웨어를 배포하기 위해 악용되고 있습니다.

인터넷 기반 서버로 들어오는 모든 웹 트래픽을 모니터링하고, 이 트래픽을 분석하여 악성이거나 비정상적인 활동을 식별하고 차단하도록 Enterprise Threat Protector를 설정할 수 있습니다.

피싱 URL 차단

Enterprise Threat Protector의 URL 검사 기능을 사용하여 피싱 시도를 탐지하고 차단하세요

피싱은 네트워크에 침입하는 매우 일반적인 방법입니다. 공격자는 종종 악성 첨부 파일이나 인증정보를 도용하도록 설계된 가짜 로그인 페이지로 연결되는 링크가 포함된 이메일을 보냅니다. 엔드포인트에서 Enterprise Threat Protector 클라이언트를 사용하면 사용자가 클릭하는 각 URL을 실시간으로 스캔하여 악성이나 비정상적인 링크를 식별하고 차단할 수 있습니다.

VPN 공격표면 감소

Enterprise Application Access를 사용하여 안전한 애플리케이션 전용 VPN 접속을 활성화하고 외부 공격표면을 줄이세요

원격 근무를 포함하는 오늘날의 하이브리드 업무 환경에서는 사용자가 VPN을 사용하여 기업 네트워크에 로그인하도록 허용하는 것이 점점 더 보편화되고 있습니다. 공격자들이 여기에 적응하면서 이 기회를 악용하여 내부 네트워크에 접속하기 시작했습니다. 공격자는 직원의 개인용 컴퓨터를 공격하여 VPN 인증정보를 감염시킨 다음 이를 통해 내부 네트워크에 접속하는 경우가 종종 있습니다. 어떤 경우에는 공격자가 취약한 서버를 표적으로 삼아 인증정보를 유출하기도 합니다. 2022년 11월, 공격자들은 Fortinet VPN 서버의 취약점을 악용하여 초기 접속 권한을 획득한 후 전체 네트워크에 랜섬웨어를 확산시켰습니다.

Enterprise Application Access을 사용하면 네트워크에 대한 애플리케이션별 역할 기반 접속을 허용하여 이러한 리스크를 크게 줄일 수 있습니다. 즉, 기존 VPN처럼 사용자에게 전체 네트워크에 대한 전체 접속 권한을 부여하지 않고 지정된 애플리케이션에 대한 제한된 접속만 허용합니다. 이렇게 하면 공격자가 사용자의 인증정보를 감염시키고 MFA 보호 기능을 우회하더라도 네트워크에 접속할 수 없으며 제한된 애플리케이션 세트에만 접속할 수 있습니다.

명령 및 제어

C2(Command and Control) 서버 차단

Akamai Secure Internet Access를 사용하여 알려진 멀웨어 C2(Command and Control) 서버를 차단하세요

일반적인 멀웨어, 특히 랜섬웨어는 명령을 전송하고 감염된 자산에서 정보를 검색하기 위해 외부 C2 서버와 통신해야 합니다. Akamai의 방대한 통신 데이터를 분석하여 랜섬웨어 및 멀웨어 C2 도메인을 모니터링하고 새롭게 진화하는 캠페인을 추적할 수 있습니다. Enterprise Threat Protector 클라이언트를 사용하면 전체 DNS 통신을 실시간으로 모니터링하고 악성 도메인과의 통신을 차단하여 멀웨어가 제대로 실행되지 않도록 하여 공격자의 목표 달성을 저지할 수 있습니다.

탐색

공격자는 네트워크에 침입하면 측면 이동을 시작하기 전에 네트워크 구조를 파악하기 위해 추가 자산을 식별하려고 시도합니다. 이 과정에서 Akamai Guardicore Segmentation이 감지할 수 있는 내부 통신이 발생하는 경우가 많습니다.

네트워크 스캔 파악

> Akamai Guardicore Segmentation 탐지기를 사용하여 의심스러운 네트워크 스캔을 파악하세요

공격자가 네트워크 탐색에 사용하는 일반적인 방법 중 하나는 포트 스캔을 사용하여 네트워크 서비스를 파악하는 것이며, 많은 랜섬웨어 그룹이 오픈 소스 네트워크 스캐너를 사용하는 것으로 나타났습니다. LockBit 3.0 랜섬웨어와 관련된 최근의 CISA Advisory에 따르면, 한 그룹이 "SoftPerfect Network Scanner"를 사용하여 포트 스캐닝을 하고 있는 것으로 나타났습니다. 또 다른 예로, Nokoyawa 랜섬웨어 그룹이 네트워크를 탐색하여 SQL 서버의 민감한 데이터에 접속하는 것이 관찰되었습니다.

Akamai Guardicore Segmentation은 네트워크의 모든 통신을 모니터링하여 이러한 스캔을 식별하고 경고하는 탐지기가 내장되어 있으므로 멀웨어 확산이 시작되기 전에 차단할 수 있습니다.

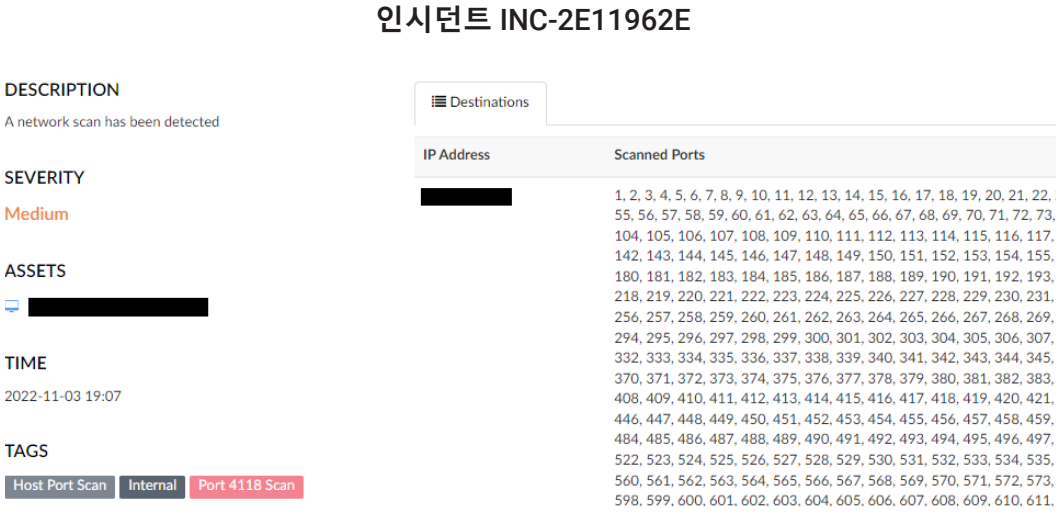
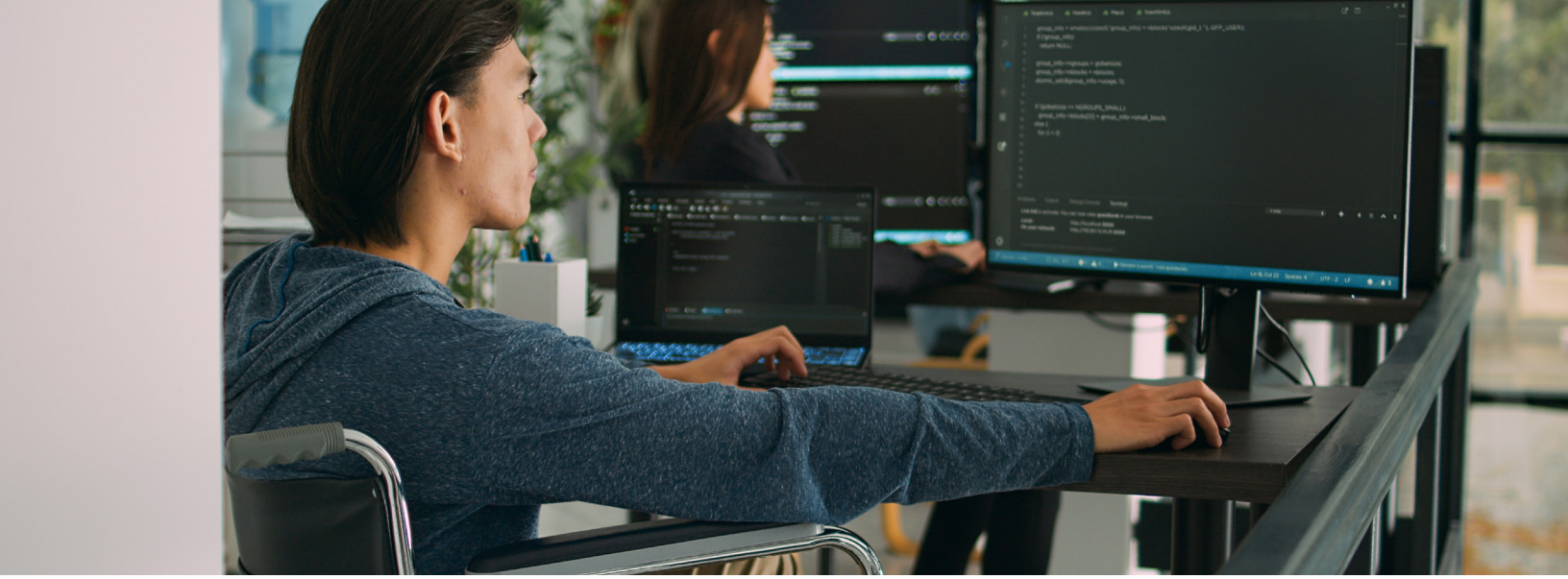


그림 1: Akamai Guardicore Segmentation에서 발생한 네트워크 스캔 인시던트



탐색에 대응한 기만

Akamai Guardicore Segmentation를 사용하여 탐색 시도를 파악하세요

공격자는 네트워크에 침입할 때 네트워크의 구조와 그 안에 있는 다양한 자산에 대한 사전 지식이 없습니다. 이러한 격차를 극복하기 위해 공격자는 "어둠 속에서 탐색"하고 수동으로 방법을 찾아야 합니다. Akamai Guardicore Segmentation은 공격자를 허니팟 서버로 유인하고, 활동을 모니터링하며, 이상 징후가 탐지되면 알림을 보내는 기만 서비스를 사용하여 이를 활용할 수 있습니다.

예를 들어, 공격자가 네트워크에 침입하여 Linux 서버의 SSH 인증정보 무차별 대입 공격을 시도한다고 가정해 보겠습니다. Akamai Guardicore Segmentation은 이러한 이상 징후를 식별하고 공격자를 동적으로 생성된 허니팟으로 이동시킵니다. 허니팟에 들어가면 공격자의 모든 행동이 기록되고 알림이 생성됩니다.

다음은 이러한 알림의 한 예입니다.

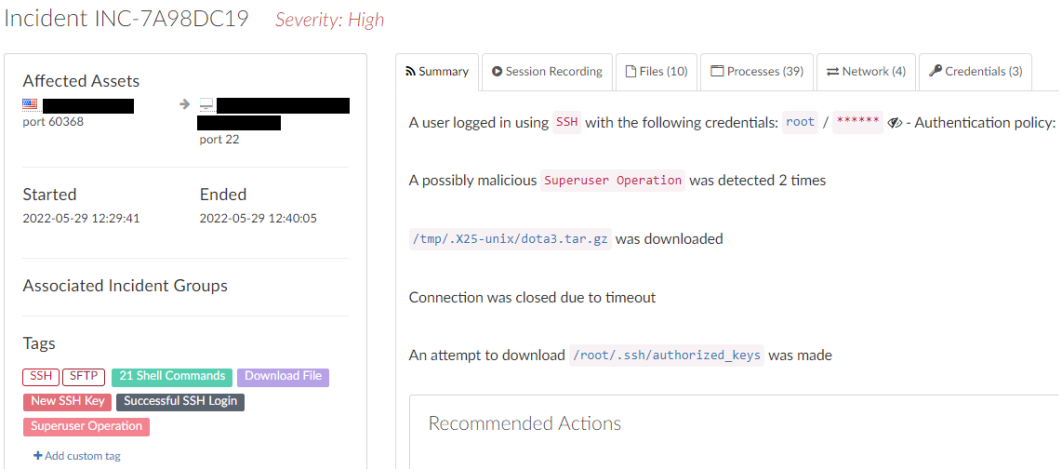


그림 2: Akamai Guardicore Segmentation에서 발생한 기만 인시던트

측면 이동

공격자가 네트워크에 접속하고 토폴로지에 익숙해지면 이를 이용하여 측면 이동을 시도합니다. 최신 랜섬웨어 그룹은 네트워크를 감염시킨 후 최대한 많은 자산을 유출하고 모든 자산을 암호화하기 위해 측면으로 이동합니다. Akamai 기업 보안 제품을 사용하면 측면 이동 가능성을 제한하고 침해 범위를 최소화할 수 있습니다.

의심스러운 호스트 지표 식별

> Akamai Guardicore Segmentation Insight 모듈을 사용하여 다양한 방법으로 의심스러운 호스트 지표를 식별하세요

공격자는 다양한 목표를 달성하기 위해 PowerShell 툴을 사용하며, 그 중 하나는 측면 이동을 수행하는 것입니다. PowerShell 드롭퍼는 매우 일반적이며, 공격자들은 감염된 자산에서 실행하는 첫 번째 코드 조각으로 이를 사용하는 경우가 많습니다. 최근의 Quantum 랜섬웨어 감염은 WMI(Windows Management Instrumentation)를 통해 PowerShell 코드를 실행할 때와 정확히 일치하는 것으로 나타났습니다.

Akamai Guardicore Segmentation의 Insight 모듈을 사용하면 예약된 쿼리를 실행하여 모든 자산에 대한 PowerShell 이벤트 로그를 스캔하고 악성 지표가 있는 자산을 레이블링하고 격리할 수 있습니다.

그림 3: 악성 PowerShell을 탐지하기 위한 예약된 Insight 쿼리 만들기

하지만 PowerShell은 하나의 예일 뿐입니다. 예를 들어, 기존 osquery 테이블을 사용하여 다양한 측면 이동 지표를 스캔하는 데 Insight를 활용할 수 있습니다.

- 파일 테이블을 사용하여 이름 또는 해시를 기반으로 멀웨어 파일을 탐지하세요
- 시작 항목 테이블을 사용하여 자산에서 의심스러운 자동 실행 항목을 탐지하세요
- Yara 테이블을 통해 Yara 규칙을 사용하여 자산의 파일을 스캔하여 멀웨어 변종을 탐지하세요

LAN 공격 차단

Akamai Guardicore Segmentation을 사용하여 로컬 네트워크 프로토콜에 대한 공격을 차단하고 탐지하세요

공격자는 네트워크에서 최초 감염자를 만든 후 ARP와 같은 LAN 프로토콜의 취약점을 악용하여 다른 자산을 침해합니다. 이러한 공격은 레이어 2에서 수행되며 이러한 종류의 통신은 방화벽에 도달하지 않기 때문에 기존 방화벽을 사용하면 쉽게 탐지되지 않을 수 있습니다.

Akamai Guardicore Segmentation의 소프트웨어 기반 접근 방식을 사용하면 일반적으로 적용 방화벽에 도달하지 않는 로컬 트래픽까지 포함하여 자산에 출입하는 모든 트래픽을 모니터링하고 차단할 수 있습니다.

관리 포트 제한

Akamai Guardicore Segmentation을 사용하여 프로세스 수준 정책을 생성하고 민감한 포트에 대한 공격표면을 줄이세요

공격자는 일반적으로 네트워크 내부에 침투한 후 인증정보 탈취를 목적으로 감염된 자산에 대해 권한 에스컬레이션을 수행합니다. 공격자는 인증정보를 획득하면 종종 RDP, RPC, SMB, WinRM 같은 관리 프로토콜을 사용하여 네트워크의 모든 자산에 랜섬웨어 페이로드를 실행합니다. 그러나, 관리자가 정상적으로 운영하려면 이러한 포트가 필요하기 때문에 이러한 포트를 완전히 차단하는 옵션은 실행이 불가능한 경우가 많습니다.

Akamai Guardicore Segmentation를 사용하면 프로세스 수준에서 정책을 적용할 수 있으므로 어떤 프로세스를 민감한 관리 포트를 통해 통신해야 하는지 결정할 수 있습니다. Ansible을 비롯한 많은 관리 프로그램에서 사용되는 WinRM에 대해 알아보겠습니다. 그러나 공격자들이 측면 이동을 수행하기 위해 Evil-WinRM 같은 툴을 사용하여 악용하는 경우도 많습니다. Akamai Guardicore Segmentation을 사용하면 Ansible 프로세스에서 들어오는 WinRM 연결만 허용하고 동일한 포트를 통해 다른 프로세스를 차단하는 정책을 생성할 수 있습니다.

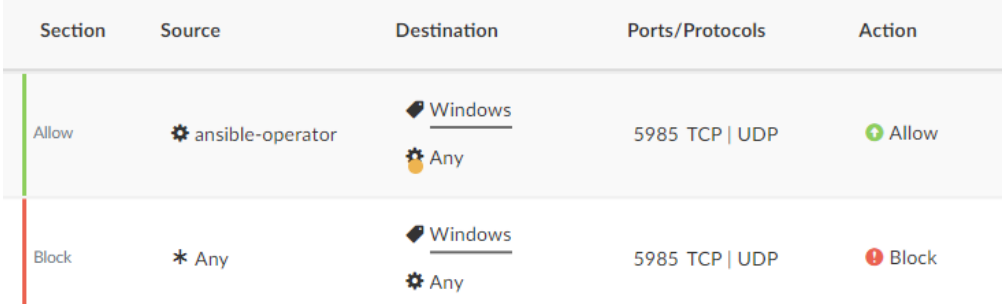


그림 4: WinRM 통신을 제한하는 Akamai Guardicore Segmentation 정책의 예

탈취

최근 몇 년 동안, 공격자들은 피해자로부터 민감한 파일을 탈취하여 추가적인 공격 수단으로 악용하는 전략을 채택했습니다. 공격자는 기업에서 데이터를 유출할 때 네트워크 노이즈에 섞여 들어가려고 하지만, 이 단계에서도 종종 탐지되고 차단될 수 있습니다.

탈취 도메인 차단

> Akamai Guardicore Segmentation을 사용하여 데이터 탈취에 악용될 수 있는 서비스에 대한 접속을 제한하세요

공격자는 네트워크에서 데이터를 유출하기 위해 공개 툴을 사용하는 경우가 많으며, 가장 일반적인 옵션은 MEGA, Dropbox, Google Drive 같은 퍼블릭 호스팅 서비스입니다. 이러한 도메인을 모니터링할 때 어려운 점은 해당 도메인이 일반적으로 네트워크 내에서 합법적으로 사용된다는 것입니다. 예를 들어, 브라우저를 통해 MEGA 도메인에 접속하는 것은 정상적인 것으로 간주될 수 있지만, 여러 공격 그룹에서 데이터 유출을 위해 활발히 사용되고 있는 rclone 유틸리티를 사용하여 접속하는 것은 악성으로 간주됩니다.

Akamai Guardicore Segmentation를 사용하면 해당 툴에 접속할 필요가 없는 모든 엔드포인트에서 해당 도메인을 차단하고 브라우저와 같은 승인된 애플리케이션을 통해서만 접속을 허용함으로써 이러한 툴로 인한 리스크를 최소화할 수 있습니다.

멀티레이어 방어

공격자는 원하는 목표를 달성하기 위해 여러 가지 공격 단계를 거쳐야 합니다. 각 단계는 방어자가 관련 악성 활동을 차단하고 탐지할 기회를 제공합니다. 방어자는 다양한 Akamai 보안 제품을 사용하여 랜섬웨어 킬 체인의 각 단계에서 방어 조치를 취함으로써 공격자의 추적을 차단하고 비정상적인 행동을 탐지할 수 있습니다.

Akamai Guardicore Segmentation에 대한 자세한 내용이 궁금하시거나 개인 맞춤형 제품 데모를 요청하려면 akamai.com/guardicore를 방문하시기 바랍니다.