MANDIANT®

솔루션 소개서

Mandiant Managed Defense를 통한 랜섬웨어 위협 방어 전략

이점

- **주요 경보 확인**
  전문가를 통해 환경 전반에 걸쳐 기술 경보를 모니터링하고 식별, 조사 및 우선순위를 지정할 수 있습니다. 이에 따라 우선순위로 지정되는 경보의 수가 줄어들고, 각각의 경보에 풍부한 컨텍스트 정보를 함께 제공합니다.
- **숨겨진 공격자 적출**
  MITRE ATT&CK 프레임워크에 매핑된 선제적 위협 헌팅으로 숨겨진 침해 및 잠재적인 사이버 공격을 감지합니다.
- **신속한 공격 차단 및 대응**
  Managed Defense 전문가들은 Mandiant 침해 사고 대응 담당자 및 보안 분석가들의 종합적인 지식과 경험을 통해 공격에 대한 대응을 지원합니다.
- **보안 담당자의 역량 향상**
  Mandiant의 지정된 보안 전문가팀은 보안 담당자들을 교육하고 자문을 제공하며, 함께 협력하여 사이버 보안 지식을 전달하고 기업의 보안 환경을 깊이 있게 이해합니다.
- **보안 수준 강화**
  Threat Intelligence를 통해 명확한 근거를 기반으로 지속적인 보안성 점검을 진행하고 권고 사항을 제시하여 보안 태세를 강화합니다.

2017년부터 랜섬웨어 공격 빈도와 심각도가 급속도로 증가해 왔습니다. 숙련된 공격자들은 초기에는 다소 번거로운 방법으로 데이터 암호화와 데이터 노출에 대한 공격을 결합한 복잡하고 여러 단계로 구성된 공격을 진행해 왔습니다. 이와 동시에, 이런 공격자들은 멀웨어를 널리 퍼뜨리는 일에서부터 도시 전체를 비롯한 특정 기업과 산업을 표적으로 삼는 일까지 공격의 범위를 확장했습니다. 오늘날 랜섬웨어 공격으로 야기되는 총 비용은 수백만 달러 규모로 오를 수 있습니다.

이처럼 위협이 진화하자, 많은 조직은 대응 속도를 높이기 위해 잠재적인 랜섬웨어 방지 전술을 평가하고, 개발 및 고도화하게 되었습니다. Mandiant Managed Defense와 같은 효과적인 관리형 탐지 및 대응(Managed Detection and Response, MDR) 기술은 APT 그룹에 의해 전략적으로 배포되는 랜섬웨어와 같은 공격에 대한 위험성을 완화하고 소속된 조직의 임원진에게 보안 시스템이 잘 작동하고 있음을 확신시켜 줄 수 있습니다. 조직 내에서 이러한 역량을 갖추는 데는 시간과 리소스가 필요합니다.

Managed Defense를 통한 랜섬웨어 차단

수준 높은 랜섬웨어 전술과 위협에 직면하고 있는 조직을 대상으로, Managed Defense는 매일 명확한 목적을 가지고 위협해 오는 공격자들에 대응하고 이들의 공격을 방어해 내는 전문가들이 지원을 해 드립니다.

모든 위협 경로에서 중대한 위협 확인

랜섬웨어를 이용하려는 공격자들은 원격 데스크톱 프로토콜, 악성 링크나 첨부파일이 포함된 스피어 피싱 이메일 또는 악성 웹사이트 방문 시 악성코드가 다운로드되는 '드라이브 바이 다운로드' 등 다양한 경로를 통해 피해자의 환경에 진입할 수 있습니다. 침해 후, 공격 목적을 달성하기 위해 이러한 공격자들은 핵심 시스템과 데이터를 찾아냅니다.

대부분의 조직에서는 수많은 엔드포인트부터 오늘날 급속하게 확장되는 네트워크 경계에 이르기까지 기업 인프라 전반에 대한 가시성과 제어력을 확보하는 것이 침해 당한 후의 치밀한 공격을 발견하는 데 매우 중요합니다. Managed Defense는 엔드포인트뿐 아니라 네트워크 전체에 대한 가시성을 확보하여 이상 행동을 탐지하고 조사를 진행할 주요 경보의 우선순위를 정합니다. 또한 Mandiant 전문가들은 이메일 정보를 통해 새로운 공격자 동향과 랜섬웨어 전달 메커니즘을 확인할 수 있습니다.

랜섬웨어 위협 패턴 인지

랜섬웨어 공격자의 공격 전술, 기법 및 절차에 대한 전문 지식을 보유하고 있는 숙련된 분석가들과의 협력이 과거 그 어느 때보다 중요해졌습니다. 랜섬웨어 공격자들이 공격 목표를 달성하려면 먼저 공격을 위한 발판을 다진 후 공격 대상의 환경에 접속하여 연결 상태를 유지해야 합니다. 예를 들어, Mandiant 전문가들은 MAZE 공격자들이 피해자의 네트워크를 통해 내부망 내 이동 후 많은 서버와 워크스테이션에 페이로드를 설치했다는 사실을 확인했습니다. 그 후 이 그룹은 액세스를 할 수 있게 되고, 권한을 상승시키고, 침투한 네트워크상 이동이 자유로워졌습니다.

2019년에 Mandiant가 발견한 바에 따르면, 침해 사고 대응 고객 중에서 APT 위협 그룹이 전략적으로 배포한 랜섬웨어의 경우 랜섬웨어 배포 전 평균 공격 지속 시간이 72일이었습니다. 또한 Managed Defense 고객들은 APT 위협 그룹이 주도한 랜섬웨어의 표적이 되었지만 거의 대부분의 경우, 랜섬웨어가 배포되기 전에 탐지되었고 피해를 완화시킬 수 있었습니다. 이를 통해 전략적으로 배포된 랜섬웨어의 평균 공격 지속 시간을 72일에서 24시간 이내로 줄일 수 있었습니다(그림 1).

그림 1.

Managed Defense는 2019년 랜섬웨어 공격 지속 시간을 대폭 줄였습니다.

전략적으로 배포되는 랜섬웨어 공격을 탐지하려면 우선 숨어있는 공격자들을 색출해 내야 합니다. 하지만 많은 조직들은 과거와 현재 공격 행위에 대한 전문 지식을 가지고 위협 헌팅을 할 수 있는 전문 인력이 없습니다. Managed Defense 위협 헌팅팀은 최상의 사이버 위협 인텔리전스와 침해 사고 대응에 대한 고유한 경험을 기반으로 전략적 랜섬웨어 위협을 탐지해 내고 있습니다.

위협에 대한 사전 대응

전략적 랜섬웨어는 매우 빠르게 감염시키고 암호화할 수 있기 때문에 신속하고 효과적으로 대응해야 합니다. 최근의 랜섬웨어 공격은 그 양상이 매우 다양합니다. 따라서 보안팀은 공격 활동의 전체 범위를 파악하고 이를 철저하게 관리해야 합니다. Managed Defense는 24시간 모니터링하고 경보 발생에 대한 우선순위를 지정하여 Mandiant 전문가를 통해 신속하게 파악하고 조사합니다.

Managed Defense는 15년이 넘는 대형 침해 사고에 대응한 경험을 기반으로 신속하게 평가하고 위협을 방어합니다. Managed Defense 컨설턴트는 Mandiant 침해 사고 대응 전문가들과 협력하여 네트워크상의 공격자 활동을 탐지하고 저지합니다. 이러한 신속한 대응 활동 덕분에 98%의 경우는 일반적으로 발생하는 침해 사고 대응 비용을 모두 지출하지 않아도 됩니다. Managed Defense의 조사 결과는 인사이트를 포함하여 보안 담당자와 협력하여 도출하고 Managed Defense 포털을 통해 상세 보고서를 제공합니다.

위협적인 랜섬웨어를 찾아내어 대응하는 데 Mandiant Managed Defense를 통해 어떻게 해결할 수 있는지를 **www.fireeye.com/managed-defense**에서 확인해 보세요.

FireEye Korea
서울특별시 강남구 테헤란로 507 WeWork 빌딩
12층 112호
02-6959-4017
korea.info@fireeye.com

Mandiant 솔루션 소개
Mandiant 솔루션은 세계 최고의 Threat Intelligence와 최일선에서 수집된 전문 지식을 지속적인 보안 검증 기능과 통합하여 조직이 보안 효과를 높이고 비즈니스 위험을 줄이는 데 필요한 툴을 제공합니다.

MANDIANT®