Cisco Ransomware Defense: 랜섬웨어 차단

랜섬웨어가 어떤 식으로 접근을 시도하더라도 더 안전하게 보호할 수 있다면? 그러한 보안 제품 및 아키텍처를 제공하는 곳은 Cisco뿐입니다.

개요

파일과 정보는 조직의 근간입니다. 이 정보를 지키고 조직의 생산성을 유지하는 것은 타협할 수 없는 과제입니다.

그러나 랜섬웨어, 즉 개인이나 조직의 컴퓨터에 있는 정보, 이를테면 문서, 사진, 음악을 잠금 상태로 만드는 악성 소프트웨어, 이른바 악성코드가 등장했습니다. 이 파일들을 인질로 잡고 있기 때문에 사용자가 파일을 잠금 해제하고 복구하려면 소위 몸값(ransom)을 지불해야 합니다. 적합한 방어 체계가 없으면 랜섬웨어에 감염되어 펜과 종이로만 업무를 처리해야 할 정도로 심각한 피해를 입을 수 있습니다.

랜섬웨어는 주로 익스플로잇 킷, 맬버타이징(악성코드를 유포할 수 있는 웹 사이트의 감염된 광고), 피싱(신뢰할 수 있는 것으로 위장한 사기성 이메일), 스팸 공격을 통해 유포됩니다. 실제 감염은 누군가가 피싱 이메일의 링크나 첨부 파일을 클릭할 때 시작될 수 있습니다. 자동으로 컴퓨터를 감염시키는 악성 광고를 포함한 사이트에 사용자가 방문할 때도 감염이 일어날 수 있습니다.

Cisco® Ransomware Defense가 있습니다. 이 솔루션은 DNS 레이어부터 엔드포인트, 네트워크, 이메일, 웹까지 포괄하는 계층적 방식으로 랜섬웨어 감염의 위험을 줄입니다. 최고의 가시성과 최강의 랜섬웨어 대응 능력을 접목시키는 아키텍처 차원의 접근 방식으로 통합 방어 체계를 구축합니다.

혜택

- **랜섬웨어 위험을 완화**하여 고객은 비즈니스 운영에 계속 전념
- 위협이 자리 잡기 전에 차단할 수 있는 보안 기술로 **즉각적인 보호 실현**
- DNS 레이어부터 네트워크 및 엔드포인트까지 포괄하는 아키텍처 접근 방식으로 **탁월한 가시성 및 대응력 확보**
- 강력한 네트워크 세그멘테이션으로 **악성코드의 내부 전파 차단**
- 랜섬웨어에 대한 **업계 최고의 Talos 위협 연구 분석 및 인텔리전스 활용**

빠르게 성장하는 강력한 위협

올해는 랜섬웨어의 해입니다. 그리고 랜섬웨어는 수익성이 상당히 높은 것으로 입증되고 있습니다. 랜섬웨어는 역사상 가장 수익성이 높은 악성코드 유형으로 빠르게 자리잡았습니다.

FBI에 따르면 연간 10억 달러 규모의 랜섬웨어 시장이 조성되고 있는 상황입니다. Cisco Talos의 연구를 통해 단일 랜섬웨어 공격으로 연간 최대 6천만 달러의 수익을 올릴 수 있음이 드러났습니다. 랜섬웨어는 TV 프로그램에 등장할 정도로 많은 관심을 받고 있습니다.

공격자들은 풍부한 자금과 동기를 갖고 계속해서 훨씬 더 치명적인 랜섬웨어 개발에 매진합니다. 랜섬웨어가 더 많은 기업 네트워크를 장악하기 위해 자동 전파 기능을 한층 더 활용할 것으로 예상됩니다. 랜섬웨어에 감염되면 사실상 기업의 IT 기능이 1970년대 수준으로 돌아가게 됩니다.

현재 랜섬웨어에 대한 대응은 대개 단일 포인트 제품을 중심으로 전개되고 있습니다. 랜섬웨어가 다양한 감염 벡터를 노리고 있으므로 보다 아키텍처 차원의 접근 방식을 도입할 필요가 있습니다.

이 솔루션 개요에서는 공격자가 사용하는 다양한 공격 벡터와 방법을 다룹니다. 방어자는 이메일 및 웹을 모두 보호하고 인터넷의 악성 인프라에 대한 액세스를 차단하고 엔드포인트로 향하는 모든 랜섬웨어 파일을 차단하고 랜섬웨어에 쓰이는 C&C(Command-and-Control) 콜백을 차단하고, 만일 감염이 일어날 경우 랜섬웨어의 내부 이동을 손쉽게 차단해야 합니다.

고객이 누릴 혜택

Cisco Ransomware Defense는 Cisco 보안 아키텍처의 모든 필수 요소를 통합하여 랜섬웨어 문제를 해결합니다. 모든 요소를 선택하거나 당장 보안 요구사항에 부합하는 구성 요소를 고를 수 있습니다.

Ransomware Defense를 구성하는 요소는 다음과 같습니다.

- Cisco Umbrella - 네트워크에서 떨어진 DNS 레이어에서 위협을 차단합니다.
- Cisco AMP(Advanced Malware Protection) for Endpoints - 악성 랜섬웨어 파일이 엔드포인트에서 실행되지 않도록 합니다.
- Cisco Email Security(클라우드 및 온프레미스) - 피싱 및 스팸 메시지를 통한 랜섬웨어 유포 시도를 차단합니다.

- Advanced Malware Protection - 간편한 라이선스를 통해 이메일 보안 제품에 즉시 추가하여 Cisco 이메일 보안 게이트웨이를 통과하는 미확인 첨부 파일에 대한 정적/동적 분석(샌드박싱)을 실행할 수 있습니다.
- Cisco Firepower™ NGFW(Next-Generation Firewall) - 네트워크를 통과하는 C&C(Command-and-Control) 트래픽 및 악성 파일을 차단합니다.
- Cisco 네트워크 기반 Cisco ISE - 동적으로 네트워크 세그멘테이션을 수행하여 랜섬웨어의 내부 확산을 방지합니다.

Ransomware Defense를 선택한 조직은 자체 네트워크를 활용하여 랜섬웨어 확산을 억제하는 정책을 시행할 수 있습니다. 최악의 경우 랜섬웨어에 감염되더라도 랜섬웨어가 네트워크에서 쉽게 전파될 수 없습니다.

Cisco Security Services는 보안 사고 후 대응 시에 즉각적인 분류 서비스를 제공합니다. AMP, NGFW, 기타 솔루션 제품의 구축도 간소화합니다.

주요 기능

- 랜섬웨어의 네트워크 침투 또는 노트북 컴퓨터로 다운로드 시도 차단
- 최악의 경우 네트워크에 침투한 랜섬웨어 억제

Security Services와 함께 랜섬웨어 퇴치

Cisco Security Services Incident Response 팀은 사고 대응을 위한 대비 서비스를 제공할 뿐 아니라 랜섬웨어 감염 발생 시 사후 사고 대응까지 지원할 수 있습니다.

또한 Cisco Security Integration Services에서 솔루션 레벨의 아키텍처 과제를 해결합니다. AMP for Endpoints, Cisco Firepower NGFW와 같은 솔루션 기술의 구축을 간소화합니다. Cisco 팀은 수준 높은 전문성으로 통합 보안 솔루션을 제공하면서 고객이 필요로 하는 보안 기술을 신속하게 보급하고 그에 따른 불편을 최소화합니다.

더 포괄적인 관점에서는 조직이 랜섬웨어 침투 시 그 피해를 최소화하기 위해 적합한 데이터 백업 기술 및 정책을 갖추는 것도 중요합니다.

"랜섬웨어의 웹 공격 벡터에서 큰 위험을 해결했고 인터넷 연결에 대한 사용자 경험을 크게 향상시켰습니다."

— Octapharma

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital® 파이낸싱을 통해 목표를 달성하는 데 필요한 기술을 습득하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 알아보십시오.

Cisco의 강점

랜섬웨어는 필요하다면 어떤 방법으로든 조직에 대한 침투 경로를 찾아냅니다. 피싱 이메일, 감염된 웹 배너, 스팸 등 다양한 공격 벡터로부터 보호해야 합니다. 랜섬웨어 과제 해결에 필요한 보안 아키텍처를 제공하는 곳은 Cisco뿐입니다. 포인트 제품만으로는 역부족입니다. Cisco 솔루션은 랜섬웨어의 위협을 광범위하게 연구하면서 효과적인 계층적 보호를 가능하게 하는 업계 최고의 Talos Research Group이 뒷받침합니다. Cisco는 랜섬웨어를 차단하고 (언젠가는 겪게 될 일이지만) 허점을 통해 랜섬웨어가 사용자의 네트워크에 침투할 경우 이를 퇴치합니다.

C22-737492-01 08/16