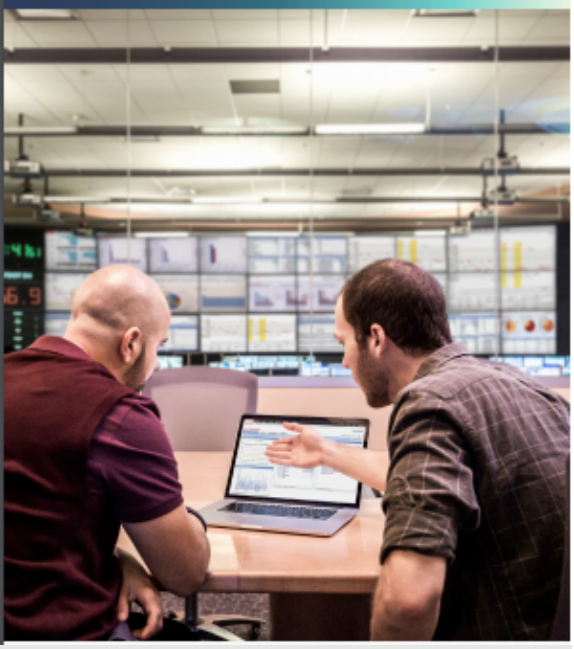
At-a-Glance



Cisco Ransomware Defense

랜섬웨어의 증가

랜섬웨어(Ransomware)는 개인 컴퓨터에 있는 문서, 사진, 음악 등의 정보를 암호화시키는 악성 소프트웨어 또는 악성 프로그램입니다. 따라서 사용자가 비용 즉 요구하는 금액을 지불해야만 파일의 잠금을 해제하고 다시 사용할 수 있습니다.

랜섬웨어는 가장 수익성이 높은 악성 프로그램으로써 빠르게 증가하고 있으며 그 규모가 연간 10억 달러에 이르고 있습니다.

랜섬웨어는 보통 웹이나 이메일을 통해 컴퓨터 또는 네트워크에 침입합니다. 웹사이트에서는 랜섬웨어가 악성 프로그램을 전달할 수 있는 감염된 광고("멀버타이징"이라고 함)를 통해 침투할 수 있습니다.
사용자가 악성 광고가 있는 사이트에 접속하면 악성 프로그램이 자동으로 다운로드되거나 사용자가 익스플로잇 키트로 리디렉션됩니다. 이메일의 경우 랜섬웨어가 피싱 또는 스팸 메시지를 사용하여 공격 기반을 마련합니다.

사용자가 단순히 피싱 또는 스팸 이메일에 있는 링크를 클릭하거나 첨부 파일을 열면 랜섬웨어가 다운로드되고, 해당 '명령 및 제어 (Command and Control)' 서버를 호출합니다.

또한 랜섬웨어는 익스플로잇 키트를 사용하여 시스템을 제어할 수도 있습니다. 익스플로잇 키트는 사용자 시스템의 소프트웨어 취약점을 파악하도록 설계된 소프트웨어 키트입니다. 그리고 나서 취약한 시스템에 랜섬웨어 등 악성코드를 업로드하여 실행합니다.

앞으로는 랜섬웨어는 개별 사용자뿐만 아니라 전체 네트워크를 대상으로 할 것입니다. 새로운 치명적이고 악의적인 광고 기법이 개발됨에 따라 랜섬웨어 개발자들은 네트워크의 보안 침해 기회를 활용하여 일련의 네트워크 폭을 제어함으로써 영향력과 금전을 받을 가능성을 극대화합니다.

보다 효과적인 보안을 통해 랜섬웨어 위험 축소

랜섬웨어가 조직에 침투하는 방법에는 여러 가지가 있으므로, 랜섬웨어 감염 위험을 줄이려면 단일 제품이 아닌 포트폴리오 기반 접근 방식이 필요합니다. 가능하면 랜섬웨어를 사전에 예방하는 것이 최선이며, 시스템에 액세스할 경우에는 탐지하여 억제함으로써 손실을 최소화해야 합니다.

Cisco® Ransomware Defense는 네트워크에서부터 DNS 계층, 이메일 및 엔드포인트까지 아우르는 방어 방식을 통해 비즈니스를 보호합니다. 또한 시스코 보안 아키텍처를 활용하며, 랜섬웨어에 대한 궁극적인 대응을 위해 업계 선두인 Talos 위협 연구소의 지원을 받고 있습니다.

장점

- 위협이 뿌리내리기 전에 차단하는 보안 기법을 통해 랜섬웨어 감염 위험을 낮춥니다.
- 랜섬웨어로부터 즉시 보호하므로 여러분 본연의 업무에 집중할 수 있습니다.
- 계층화된 통합형 방어를 통해 DNS 계층에서부터 네트워크, 엔드포인트에 이르기까지 탁월한 가시성과 대응 능력을 제공합니다.
- 동적 세그먼트화를 통해 랜섬웨어를 네트워크의 제한된 곳에 가둬둡니다.
- Cisco TALOS 보안 인텔리전스 및 연구 그룹이 업계 최고의 인텔리전스를 제공합니다.

"우리는 랜섬웨어의 웹 공격 벡터에서 심각한 위험을 차단하고 인터넷 연결성과 관련된 사용자 경험을 크게 향상시켰습니다."

옥타파마(Octapharma)

랜섬웨어 솔루션은 아래의 구성요소로 구성됩니다.

- Cisco Umbrella가 기업 네트워크 안팎의 시스템을 보호하며, IT 자산이 랜섬웨어 호스팅 악성 사이트에 연결되기 전에 DNS 요청을 차단합니다.
- Cisco의 엔드포인트용AMP(Advanced Malware Protection)는 랜섬웨어 파일이 엔드포인트에 침투하는 것을 차단합니다.
- AMP(Advanced Malware Protection)를 통한 Cisco Email Security는 스팸 및 피싱 이메일과 악성 이메일 첨부 파일, 그리고 URL을 차단합니다. AMP 기술이 엔드포인트에 적용되는 것과 동일하지만 이메일 게이트웨이에도 설치됩니다.
- AMP(Advanced Malware Protection)를 통한 Cisco Firepower 차세대 방화벽과 Threat Grid 샌드박싱 기술이 알려진 위협과 '명령 및 제어(Command and Control)' 콜백을 차단하고 또한 알려지지 않은 악성 프로그램과 위협에 대한 동적 분석을 지원합니다.
- Cisco ISE가 시스코 네트워크를 통해 네트워크를 동적으로 세그먼트화하므로 서비스와 애플리케이션에 대한 액세스를 매우 안전하게 유지하고 랜섬웨어가 다른 곳으로 확산될 수 없도록 합니다.
- Cisco Security Services는 사고 대응 시 즉각 상황을 파악하며, 또한 AMP, NGFW 및 기타 솔루션 제품의 배포를 간소화합니다.

다음 단계

Cisco 영업 담당자에게 연락하여 Cisco Ransomware Defense에 관한 자세한 내용을 파악함으로써 여러분 본연의 업무에 집중하시기 바랍니다.