E-BOOK

랜섬웨어를 예방할 수 없는 5가지 이유

NetApp

목차

5 수익성이 있기 때문

4 저렴하기 때문

3 효과가 입증되었기 때문

2 ROI 실현이 빠르기 때문

1 사람은 신뢰할 수 없기 때문

제로 트러스트 랜섬웨어 방지

수년간 눈에 띄는 랜섬웨어 공격의 수와 감염에 따른 심각한 결과를 고려했을 때 예방 방법의 완성도가 높아져야만 랜섬웨어가 머지않아 완전히 근절될 것으로 보일지도 모릅니다.

한때 널리 퍼졌던 익스플로잇 키트 위협, 즉 당시 보안 팀의 엄청난 골칫거리였던 악명 높은 Angler 등을 떠올려 보십시오. 이러한 익스플로잇 키트는 연구원들의 부단한 예방 노력 덕분에 거의 잊히게 되었습니다.

하지만 랜섬웨어는 여전히 도처에 있고 완전한 랜섬웨어 예방은 사실상 불가능합니다. 왜 그런지 이유를 살펴보겠습니다.

5

수익성이 있기 때문

공격에 성공하면 엄청난 보상이 따르므로 공격자는 그 어느 때보다 적극적입니다. 미국, 캐나다, 유럽에서 여러 조직이 지불한 평균 금품은 2019년 미화 115,123달러에서 2020년 312,493달러로, 전년 대비 171% 증가했습니다. 2021년 회계연도 1분기의 평균 금액은 850,000달러였습니다. 2019년 이후에는 랜섬웨어 관련 사고가 65% 증가했습니다. 공격 빈도는 계속해서 증가할 것으로 보이며, 2031년쯤에는 11초가 아닌 2초마다 공격이 발생할 것으로 추정됩니다. 랜섬웨어 공격은 점점 더 흔해질 것입니다. 이와 같은 수치로 미루어보아 랜섬웨어가 범죄 활동에 계속 빈번하게 악용되는 이유를 쉽게 알 수 있습니다.

그리고 조직에서는 법집행기관의 권고를 따르지 않고 금품을 계속해서 지급하고 있습니다. 기업에서 데이터를 보호하려는 것은 당연한 일이지만, 비즈니스 운영 중단으로 인한 비용이 금품 자체보다 높은 경우가 많다 보니 금품을 지불하는 일이 비용 효율성 면에서 최선인 경우가 다반사입니다.

4

저렴하기 때문

다른 한편으로는 랜섬웨어 공격을 시행하는 데 드는 자기 부담 비용은 낮습니다. 오늘날 공격자는 얼마 안 되는 금액으로 프리팹 랜섬웨어 키트를 구매할 수 있습니다. 키트에는 공격을 배포하고 이를 바탕으로 수익을 내는 데 필요한 암호화 서비스, 페이로드 드롭퍼, 난독화 툴 등 모든 것이 포함되어 있습니다. 일반적인 서비스형 랜섬웨어(RaaS) 가입비는 월별 100달러가 약간 넘은 금액으로 시작합니다. 더 복잡하고 강력한 버전은 수천 달러가 들 수 있지만, 잠재적인 보상도 증가합니다. 공격자가 서비스를 최대한 활용할 수 있도록 돕는 지원 플랜도 포함됩니다.

3

효과가 입증되었기 때문

랜섬웨어는 수익성 높은 사업입니다. 어두운 방에서 후드티를 입고 있는 해커를 상상하는 고정관념은 버리십시오. 랜섬웨어는 여느 기업 파트너 프로그램에 비견되는 정교한 네트워크입니다. 최근 RaaS 사례인 DarkSide는 2020년 8월 초에 처음 발견되었고 11월쯤에 RaaS 배포 모델로 전환되었습니다. 신고된 사고에 따르면 데이터 잠금을 해제하는 키를 제공하는 대가로 요구하는 일반적인 금액은 20만 달러에서 200만 달러 사이입니다. DarkSide 랜섬웨어 운영자는 많은 대가를 받을 뿐 아니라 수익성 높은 대규모 기업에서 돈을 받고 수익금을 자선 기부까지 하면서 '정의의 사도'를 자처하기도 합니다. 유출 사이트 기반 보고서에 따르면 현재까지 90명 이상의 희생자가 DarkSide로 피해를 본 것으로 나타났습니다. 현재 총 2TB 이상의 도난당한 데이터가 DarkSide 사이트에 호스팅되어 있어서 인센티브가 추가로 지급될 것으로 보입니다.

2

ROI 실현이 빠르기 때문

랜섬웨어가 아주 매력적인 또 다른 이유는 보통 이메일 첨부 파일, 악성 URL, 안전하지 않은 원격 데스크탑 프로토콜, 악성 광고('멀버타이징') 등을 통해 조직 내부로 침입한 후 빠르게 이동한다는 점입니다. 네트워크를 검사하여 파일을 찾은 다음 콘텐츠를 암호화하고 금품을 요구합니다. 안타깝게도 암호화 프로세스가 시작된 후에는 실행 취소할 수 있는 방법이 거의 없습니다. 그리고 공격자가 데이터를 암호화하기 전에 훔칠 수 있는 새로운 방법이 급속도로 생겨났습니다. 2021년 5월 미국 동부 해안의 연료 45%를 공급하는 Colonial Pipeline이 랜섬웨어 공격을 받았습니다. DarkSide 또는 관련 집단의 공격을 받은 것입니다. DarkSide는 Colonial Pipeline의 컴퓨터 시스템을 잠갔을 뿐 아니라 100GB 이상의 회사 데이터도 훔쳤습니다. 이 데이터 도난 사건은 DarkSide가 희생자를 이중으로 갈취한다는 것을 보여 줍니다. 영향을 받은 컴퓨터의 잠금을 해제하기 위한 돈을 요구할 뿐 아니라 희생자가 지불하지 않으면 도난당한 데이터를 공개적으로 유출하겠다고 위협하면서 입수한 데이터에 대해서도 금액을 요구합니다.

1

사람은 신뢰할 수 없기 때문

지금까지 랜섬웨어가 매우 널리 퍼진 이유는 살펴봤지만, 랜섬웨어를 예방하는 방법은 전혀 다루지 않았습니다. 향상된 패치 방역을 통해 상당수의 공격을 예방할 수 있다는 것도 사실이지만 완전한 예방이 불가능한 주된 이유는 사람 때문입니다.

직원은 조직에 결코 의도적으로 해를 가하진 않을 거라고 생각하실 겁니다. 하지만 랜섬웨어 감염이 계속해서 발생하는 이유는 직원이 악성 링크 및 이메일 또는 피싱 시도로 인한 위험에 항상 주의를 기울이지는 않기 때문입니다.

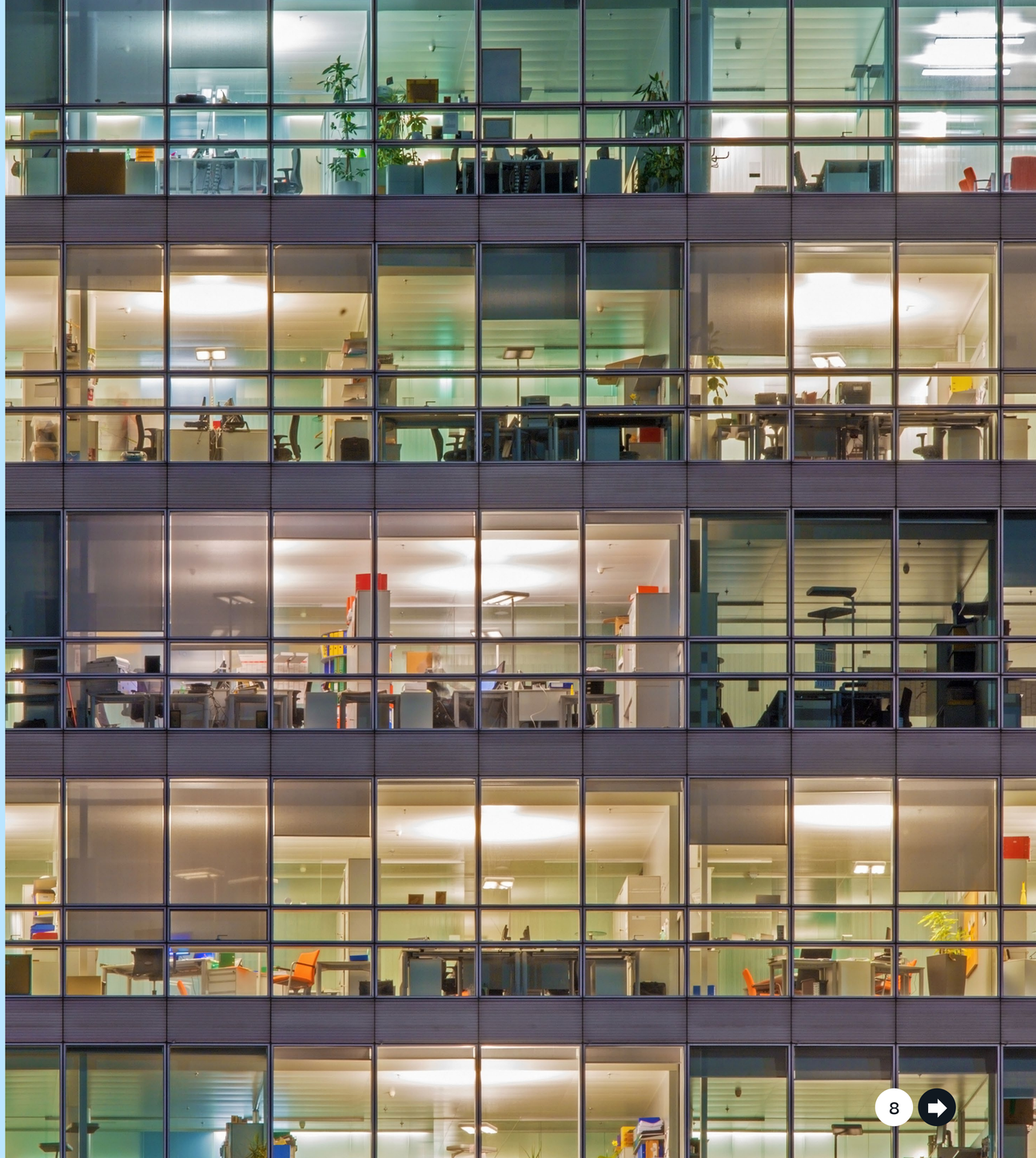
이 글을 읽는 많은 분이 정기적인 필수 보안 인식 컴퓨터 기반 교육에 익숙할지도 모르겠습니다. 교육은 아무리 해도 지나치지 않지만, 보안 인식이 아주 높은 직원일지라도 링크를 클릭하거나 이메일을 열 때 순간적으로 판단력이 흐려질 수 있습니다. 그리고 직원의 실질적인 업무 수행을 과도하게 제한하는 보안 정책이 없는 한 이러한 판단 실수는 피할 수 없습니다. 몇 분, 몇 시간이 아니라 몇 초 이내에 실수를 감지해야 하기 때문입니다.

제로 트러스트 랜섬웨어 방지

랜섬웨어를 예방할 수 없다면 랜섬웨어로부터 어떻게 보호할 수 있을까요?

직원은 업무를 수행하기 위해 랜섬웨어가 하듯이 데이터에 액세스해야 하므로 직원이 공격 벡터가 됩니다. 데이터 액세스를 제한하는 정책과 역할이 도움이 될 수 있지만 너무 많으면 생산성을 저해할 수 있습니다.

조기 감지, 사용자 행동 분석, 의심스러운 패턴 발생 시 자동화된 작업이 몇 초 이내에 이루어져야 합니다.



NetApp® Cloud Insights는 Cloud Secure라는 기능을 통해 이러한 유형의 감지를 제공합니다. Cloud Secure를 사용하면 활동을 모니터링하고, 이상 징후를 감지하며, 대응을 자동화할 수 있습니다.

- **사용자 활동 모니터링**
  위반 사항을 정확히 파악하기 위해 온프레미스 및 하이브리드 클라우드 환경의 모든 사용자 활동을 캡처하여 분석합니다. 고객 환경의 VM에 설치된 가벼운 상태 비저장 데이터 수집기 에이전트를 사용하여 데이터를 수집합니다. 이러한 데이터에는 자체 데이터 센터나 클라우드에 있는 NetApp ONTAP® 스토리지의 사용자 파일 활동과 Active Directory 및 LDAP 서버의 사용자 데이터도 포함됩니다.

  Cloud Secure는 사용자별 행동 모델을 구축하여 사용자 행동의 이상 징후를 감지합니다. 이 행동 모델에서 사용자 활동의 비정상적인 변화를 감지한 후 행동 패턴을 분석하여 위협이 랜섬웨어인지 아니면 악의적인 사용자인지 여부를 판단합니다. 이 행동 모델 덕분에 불필요한 거짓 양성 오류가 줄어듭니다.

- **이상 징후 감지 및 잠재적 공격 파악**
  오늘날의 정교한 랜섬웨어와 맬웨어는 무작위 확장명과 파일 이름을 사용하므로 서명 기반(차단 목록) 솔루션으로 감지해도 효과가 없습니다. Cloud Secure는 고급 머신 러닝 알고리즘을 사용하여 비정상적인 데이터 활동을 밝혀내고 잠재적 공격을 감지합니다. 이러한 접근 방식 덕분에 정확한 실시간 감지가 가능하며 불필요한 허위 감지는 줄어듭니다.

- **대응 정책 자동화**
  Cloud Secure는 잠재적인 랜섬웨어 공격을 알리고 여러 개의 자동 대응 정책을 제공하여 공격으로부터 데이터를 보호합니다.

  비정상적인 행동을 감지하면 NetApp Snapshot™ 복사본을 생성합니다. 복구를 빠르게 진행하면서도 거짓 양성 오류로 인한 운영 중단 가능성을 제한할 수 있도록 데이터가 보호됩니다.

사용자의 데이터 액세스 차단:
- 비정상적인 (읽기/쓰기) 사용자 행동이 감지되는 경우
- 비정상적인 파일 삭제 행동이 감지되는 경우

Cloud Secure는 세부적인 액세스 감사를 제공하므로 관리자가 손상된 데이터와 함께 공격 출처를 신속하게 파악하여 빠르게 수정하고 복구할 수 있습니다.

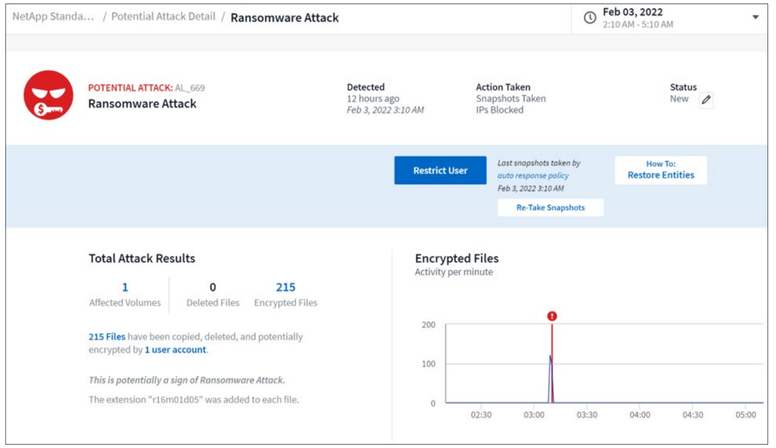


그림 1) 랜섬웨어 공격을 보여 주는 Cloud Secure 대시보드

Cloud Secure에 관해 더 알고 싶다면, 30일 무료 평가판을 신청하십시오. 자세히 알아보고 무료 평가판을 시작하십시오.

NetApp

NetApp 정보

평범함으로 가득한 세상에서 NetApp은 특별함을 선사합니다. NetApp은 귀사가 데이터를 최대한 활용할 수 있도록 돕는다는 한 가지 목표에 주력하고 있습니다. NetApp은 귀사에서 사용 중인 엔터프라이즈급 데이터 서비스를 클라우드로 전환하고, 클라우드의 유연성을 데이터 센터에 제공합니다. 업계 최고 수준의 NetApp 솔루션은 다양한 고객 환경과 세계 최대의 퍼블릭 클라우드에서 작동합니다.

클라우드 주도형 데이터 중심 소프트웨어 회사인 NetApp만이 고유한 Data Fabric을 배포하고, 클라우드를 단순화하고 연결하며, 언제 어디서나 원하는 사람에게 원하는 데이터와 서비스, 애플리케이션을 안전하게 제공하도록 지원할 수 있습니다.