AUTODESK

불법 복제 소프트웨어를 다운로드하는데 따르는 위험

자신과 비즈니스에 미치는 맬웨어의 숨겨진 위험 이해

무엇

맬웨어란?

맬웨어는 불법 복제 소프트웨어에 숨겨져 있는 경우가 많고, 컴퓨터 시스템을 손상시키거나 시스템에 지장을 주거나 무단으로 액세스하기 위해 특별히 설계되었습니다.

누구

맬웨어를 만드는 사람은?

사이버 범죄자로, 기술을 활용해 악의적인 행동을 하는 개인이나 집단일 수 있습니다.

이유

맬웨어는 왜 위험한가요?

일단 컴퓨터 시스템에 침투하면 자금, 중요한 데이터, 문서, 재무 정보는 물론, 해당 컴퓨터 사용자 본인과 직원, 회사에 중요한 모든 사항에 액세스할 수 있습니다.

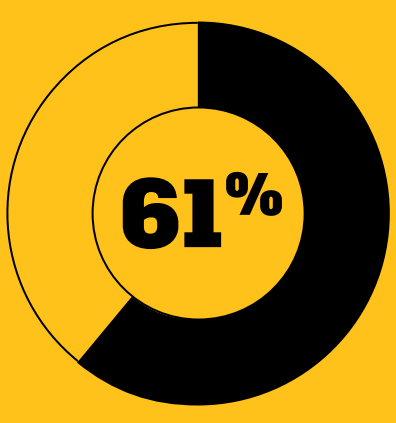
각각의 맬웨어 공격은 회사에 평균 240만 달러의 손해를 끼칠 수 있으며 해결하는 데 최대 50일이 걸릴 수 있습니다.

출처: BSA - 글로벌 소프트웨어 설문 조사

240만 달러

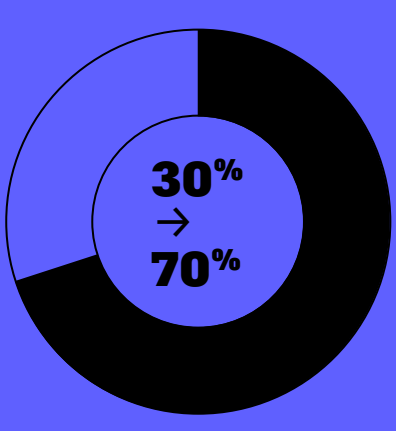
2020년에 조직의 61%가 비즈니스 운영 중단을 야기하는 랜섬웨어 공격을 경험했습니다.

출처: Mimecast



주요 오토데스크 소프트웨어의 불법 복제 버전의 30%~70%는 악성 맬웨어에 감염되어 있습니다. 이 위험을 기꺼이 감수하시겠습니까?

출처: Autodesk Keygen Weaponization Research, 2021년 4월



맬웨어 여정

세상에는 사용자만큼이나 많은 맬웨어 여정이 있습니다. 다음은 그저 작업을 완료하고 싶었던, 의도는 좋았지만 잘 알지 못하는 직원으로 인해 회사에 어떤 일이 일어날 수 있는지를 보여주는 예입니다.

1 필요

한 직원이 기한이 촉박한 작업에 사용하기에 완벽한 오토데스크 제품을 찾고 있습니다. 신규 라이선스 구입에 대한 승인 절차는 길고 내부 서버에 대한 액세스가 제한되어 있다는 것을 알고 있는 이 직원은 소프트웨어를 이용할 수 있는 더 쉬운 방법을 찾고 있습니다.

2 기회

직원이 간단한 검색을 통해 온라인에서 무료 버전을 발견합니다. 웹 사이트는 합법적인 것으로 보이며 이 무료 버전을 사용하면 시간과 비용을 절약할 수 있다는 사실이 마음에 듭니다. 직원은 망설이지 않고 다운로드를 누릅니다.

3 발생

소프트웨어가 맬웨어에 감염되어 있고(불법 복제 소프트웨어의 30%~70%에 맬웨어가 포함되어 있음), 맬웨어가 회사 네트워크 전체에 퍼지기 시작합니다. 그동안 직원은 이 소프트웨어로 계속 작업하고 몇 가지의 사소한 성능 문제를 겪습니다.

4 공격

백그라운드에서 맬웨어가 빠르게 확산되며, 그 동작은 맬웨어 유형에 따라 다릅니다.

→ 조용하게 이면에서 작동하면서 기밀 데이터를 수집합니다.

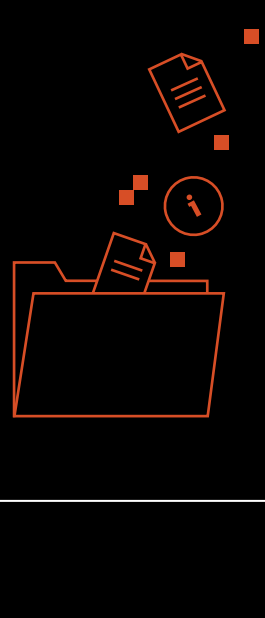
→ 사용자에게 플러그인을 다운로드하거나 소프트웨어를 다운로드하라고 요청할 수 있으며 이로 인해 컴퓨터와 파일이 또 다른 맬웨어에 추가로 감염될 가능성이 높습니다.

→ 파일 및 정보에 대한 액세스를 차단하고 랜섬을 요구합니다.

5 결과

불법 복제된 오토데스크 소프트웨어에 포함된 맬웨어는 조직 전반에서 다음과 같은 중대한 중단과 되돌릴 수 없는 결과를 초래할 수 있습니다.

→ 설계 도난
→ 고객 목록 도난
→ 재무 데이터 도난
→ 공개 릴리즈 날짜 전에 기밀 작업 누출



맬웨어 유형 알기

트로이 목마

합법적인 소프트웨어로 가장해 사용자의 파일에 대한 백도어 액세스를 만들어 데이터 및 파일 파손을 통한 금전적 이득을 챙기거나 랜섬을 요구합니다.

PUA

(Potentially Unwanted Applications: 잠재적 유해 응용프로그램)

검색 엔진이나 바이러스 백신 프로그램을 겨냥해 사용자 컴퓨터에 손상을 입히거나 소프트웨어 성능에 영향을 미칩니다.

랜섬웨어

먼저, 랜섬웨어는 소프트웨어 및 파일을 차단합니다. 그런 다음 직접 연락해서 소프트웨어와 파일을 다시 찾고 싶다면 랜섬을 지불하라고 요구합니다.

Keygen, 즉 키 생성기는 영향을 받는 사용자로부터 재무 데이터를 끌어내기 위해 가장 많이 무기화됩니다. 이는 트로이 목마 또는 PUA 사용을 통해 이루어지는 경우가 많습니다. 모든 불법 복제 키 생성기의 약 90%는 맬웨어로 무기화되어 있습니다.

출처: Autodesk Keygen Weaponization Research, 2021년 4월

방법

맬웨어로부터 회사를 어떻게 보호할 수 있을까요?

1단계

신뢰할 수 있는 소스에서 정품 소프트웨어 구매

신뢰할 수 없는 소스에서 다운로드하는 오토데스크 소프트웨어의 30%~70%는 악성 맬웨어에 감염되어 있다는 것을 인지하고 오토데스크나 공인협력업체로부터 소프트웨어를 구매하는 것이 회사와 직원을 보호하는 첫 걸음입니다.

2단계

주기적으로 적절한 유지 관리 수행

소프트웨어 자산 관리(SAM)에는 조직 내 소프트웨어의 최적화, 유지 관리 및 폐기가 포함됩니다. 이 과정에서는 필요한 소프트웨어만 유지하고 이를 업데이트해야 합니다.

3단계

적절한 바이러스 백신 소프트웨어를 설치하고 정기 검사 실행

바이러스 백신 소프트웨어가 컴퓨터나 조직 내에서 맬웨어를 항상 감지하는 것은 아니듯이 모든 바이러스 백신 소프트웨어가 동일하게 제작되는 것은 아닙니다. 오토데스크 위협 인텔리전스 팀이 최근 실시한 연구에 따르면 72개 바이러스 백신 공급업체의 평균 감지율은 28%였습니다. 하지만 모든 것이 순조롭게 돌아가도록 하기 위해서는 주기적으로 바이러스 백신을 실행해야 합니다.