AUTODESK

The risks of downloading pirated software

Understand the hidden dangers of malware for you and your business

WHAT is malware?

Malware is often hidden in pirated software and is specifically designed to disrupt, damage or gain unauthorized access to a computer system.

WHO creates malware?

Cybercriminals, who can be individuals or groups of people who use technology to commit malicious activities.

WHY is malware dangerous?

Once in your computer system, it can access money, critical data, documents, financial information and everything that is valuable to you, your employees and your company.

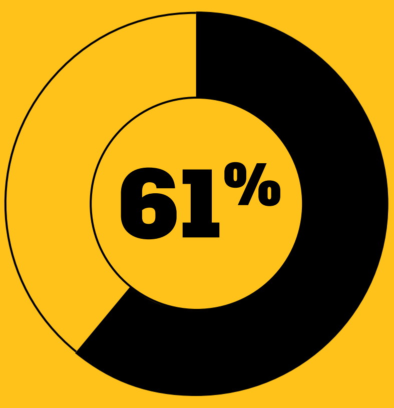
Each malware attack can cost a company $2.4 million on average and can take up to 50 days to resolve.

Source: BSA - Global Software Survey

$2.4 million

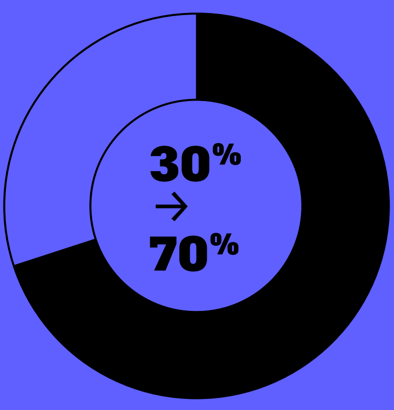
61% of organizations experienced a ransomware attack that led to disruption of business operations in 2020.

Source: Mimecast



Between 30% and 70% of pirated versions of Autodesk's top software are infected with malicious malware. Is this a risk you are willing to take?

Source: Autodesk Keygen Weaponization Research, April 2021



The Malware Journey

There are as many malware journeys as there are users. Here's an example of what can happen in a company with a well intentioned but unaware employee who just wants to get the job done.

1 THE NEED

An employee finds the perfect Autodesk product to use for a job with a tight deadline. Knowing that the approval process for a new license is long and that access to internal servers is limited, **the employee looks for an easier way to get access to the software**.

2 THE OPPORTUNITY

The employee finds a free version online through a quick search. The website looks legitimate and they are excited to be saving time and money with this deal. The employee hits download without hesitation.

3 THE OUTBREAK

The software is infected with malware (between 30% and 70% of pirated software contains malware) that starts to spread throughout the company's network. Meanwhile, the employee keeps working with the software, experiencing a few minor performance issues.

4 THE ATTACK

In the background, the malware spreads quickly and its behavior depends on the malware type:

→ It can be silent, work behind the scenes and collect confidential data.

→ It can ask the user to download a plug-in or to update the software, which will most likely infect their computer and files with additional malware.

→ It can block access to files and information, demanding ransom.

5 THE CONSEQUENCES

The malware in pirated Autodesk Software can cause major disruption and irreversible consequences throughout an organization, such as:

→ Design theft
→ Client list theft
→ Financial data theft
→ Confidential work leaked before public release dates

Be Aware of Malware Types

Trojan

Disguises itself as legitimate software and creates backdoor access to a user's files to seek financial gains through data and file destruction or ransom.

PUA (Potentially Unwanted Applications)

They target search engines or anti-virus programs to cause damage to the user's computer or affect software performance.

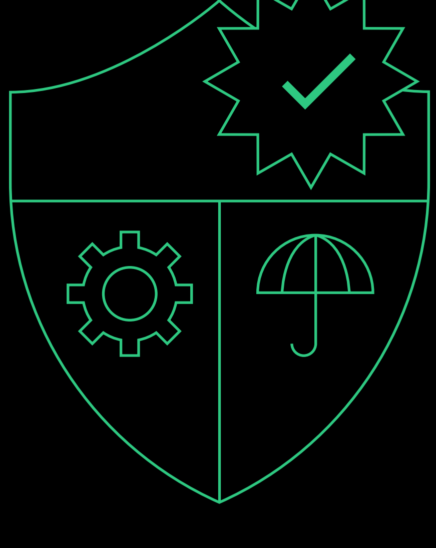
Ransomware

First, they block your software and files. Then they contact you directly and ask for a ransom to get them back

Keygens, or key-generators, are most commonly weaponized to elicit financial data from the affected user. This is often done through the use of Trojans or PUAs. Roughly 90% of all pirated key-generators are weaponized with malware.

Source: Autodesk Keygen Weaponization Research, April 2021

HOW can you protect your company against malware?



STEP 1 **Purchase genuine software from a reliable source**

Knowing that between 30% and 70% of Autodesk software downloads from untrusted sources are infected with malicious malware, purchasing your software from Autodesk or an authorized reseller is the first step in protecting your company and your employees.

STEP 2 **Conduct proper maintenance regularly**

Software asset management (SAM) involves the optimization, maintenance and disposal of software within your organization. It involves keeping only the software you need and updating it.

STEP 3 **Install proper anti-virus software and run regular checks**

Not all anti-virus software are created equal as they don't always detect malware in a computer or within an organization. According to a recent study conducted by the Autodesk Threat Intelligence team, the average detection rate across 72 anti-virus vendors was 28%. That being said, you should run anti-virus regularly to keep everything in order.

AUTODESK

Visit **www.autodesk.com**