All About Ransomware

by reevert

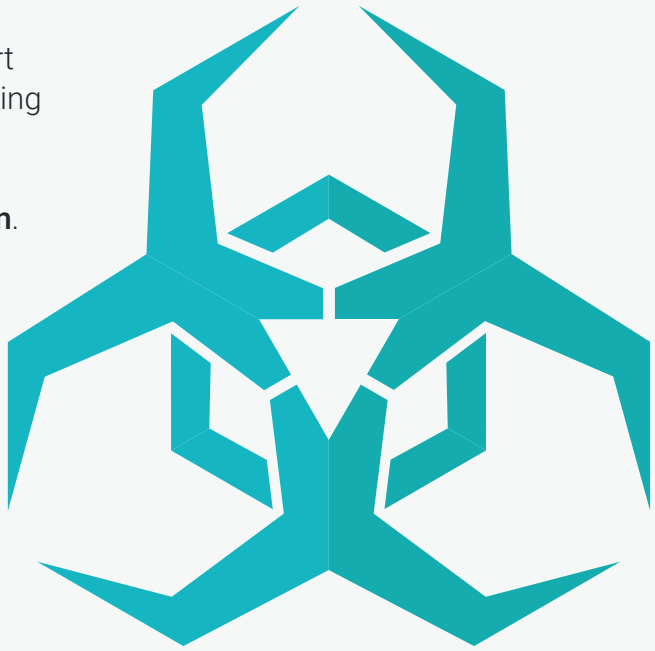
Global annual ransomware damage costs were estimated to reach $5 billion in 2017.

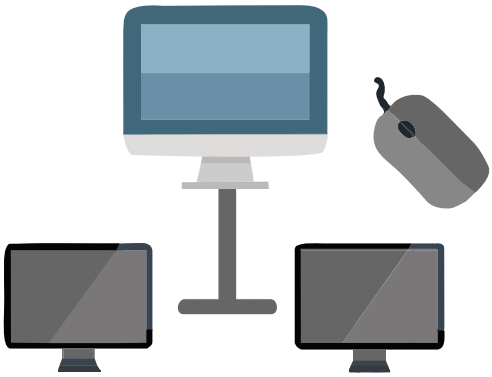
Cybersecurity experts predict ransomware costs will exceed $11.5 billion by the end of 2019*

It is unfortunate how easy it is to become infected with a zero-day ransomware or other viruses even though you may be running a fully-updated anti-virus and/or other type of network security solution on your network. Stay protected with reevert, the hybrid backup & storage solutions to keep your data (and wallet) safe.

1 What is it?

Ransomware is a malicious computer virus that uses encryption to hold user data hostage in an effort to extort users. In most cases, perpetrators make it seem like paying the ransom in exchange for a decryption key is the only method of saving your files. What they don't want you to know is that there is another method: **backup restoration**. A ransomware infection typically starts from a single computer and spreads through the entire network by infecting shared drives, databases and even local backups. However, if your data is backed up properly, you can restore your files in case of an emergency and save your files from further destruction.





2 Who Does It Affect?

Cybercriminals are in this business for the money. Extortionists have narrowed cybercrime down to a science and know exactly who's willing to pay up in exchange for their data. While individuals are still at risk, ransomware crimes are now mostly geared towards businesses and organizations who can't function without their data. Healthcare, manufacturing, service and financial industries are at the top of the attack list.

It only takes one infected computer to take down an entire company. While it may be brought on by only one end user, it's tricky enough to make its way across shared network drives and encrypt anything connected to the infected machine.

3 How Is It Acquired?

Web Pages

Drive-by-downloads are a pathway for malware. It's very important to patch your browser software and keep it up to date, otherwise hackers can use those openings to execute malicious code. Look for http**s**:// to know if the web page you're visiting is secure.

Free Software Downloads

Hackers hiding "cracked" versions of files is a popular way to distribute ransomware since it bypasses firewalls and antivirus programs. If the user directly downloads it, the security measures you've set probably won't catch it.

Email

This is the most common way to acquire ransomware. Ransomware emails will either get you to download a malicious file or send you to a compromised website.

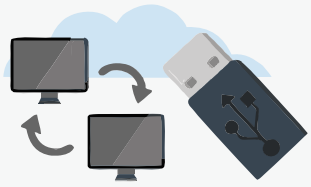
4 How Often Should I Backup My Files?

It is critical that your company or organization maintains regular and current backups in case of an attack. While this process may seem like a daunting one, rest assured knowing your backup files are safe with reevert. Deploy it once and reevert takes care of the rest.

Unlike any other traditional backup systems, reevert take hourly, daily, weekly or monthly and On-Demand snapshots of your data. In case anything bad happens to your data you can recover files by hour intervals or you can rollback your whole filesystem in a matter of seconds. See reevert's features and benefits for more information.

5 Traditional Method vs. reevert

In a traditional environment, you have your file server where users access their files and then you have your backup software that accesses these files and creates your backups. Some firms also add a cloud backup solution on top of this mix to provide off-site backups.



VS

reevert™

- ✗ Restoration from traditional backup media takes time and effort, especially in cases where there is a lot of damage.
- ✗ There are now new strains of ransomware that have the ability to detect and delete your local backups.
- ✗ Having to maintain a file server, a backup software, and an offsite backup solution requires higher licensing costs and increased administration effort.

- ✓ Restoration from local reevert snapshots is blazing fast. With our enterprise subscription, we provide you with 2 image backup licenses.
- ✓ reevert is a cost-effective, intelligent hybrid backup and storage solution that can be managed using an easy to use web interface. It was designed with data loss protection and efficiency in mind.
- ✓ reevert supports Amazon S3, IBM, Google, Wasabi and more to provide highly reliable and cost-effective off-site storage services and durability.

6 Get Your Free 30 Day Trial of reevert

More often than not, ransomware has the power to take over your important files and hold your company's life at risk. Taking preventative measures to ensure you don't lose precious time is crucial.

At the rate that it's been developing at in the past two years alone, it could be just a matter of time before it happens to you. reevert is here to help you prevent & combat the effects of ransomware and keep your business running safely.

Don't wait until it is too late. Download reevert today from our free trial page!

SOURCES & LINKS

Ransomware

Features & Benefits

Why reevert

Free Trial

FAQ

Documentation

* According to Cybersecurity Ventures

brought to you by

reevert™

www.reevert.com