

Ransomware

Ran·som·ware | noun

A type of malicious software designed to encrypt or block access to a computer system or files until a sum of money is paid.

What's the price tag?

209M

Amount ransomware victims paid out in Q1 2016 (SRC. FBI).

70%

Enterprise ransomware victims paid up.

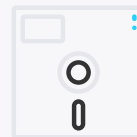
25%

Paid between \$20,000 USD and \$40,000 USD.



BITCOIN

Bitcoin is the #1 payment medium in ransomware attacks, namely because of the anonymity and difficulty to trace transactions.



WHEN DID IT STARTED?

Dec 11, 1989

20,000 envelopes containing 5 1/4" floppy disks loaded with the first known ransomware ('aids') were mailed.

Who are the targets?



Victims

Individuals, business, hospitals, schools, government agencies.



Channels

Email or websites; sometimes directly to the system via backdoors.



Systems

Notoriously Windows, but recently broadened to Linux, OS X, and even Android devices.

What happens to the system?



Files or systems are locked.



Files or systems are encrypted.



The victim has an average of **72 hours** to pay the ransom.



Or... files are deleted.



OUT TO MAKE A PROFIT

Attackers are out to make a profit, so ransomware victims are chosen by their likelihood to pay. Attackers often launch the attacks broadly—the more targets, the better chance of making money.

What can you do to prevent it?

Back your systems up often

If you have a recent backup, you can restore your system and avoid paying or losing your files.

Install endpoint security

Make sure your endpoint security has zero-day threat prevention to protect against ransomware variations.

Follow security best practices for web

Don't click on links/open attachments in suspicious-looking emails or click on ads on untrusted sites.

What can you do if you get hit?

Alert law officials

With any ransom activity, law officials should be notified.

Isolate the system

Take the machine offline so attackers can't use it to access other machines on the network.

Don't pay

You may hear different opinions on this, but if you pay, attackers will only be encouraged - plus you may not get your files back and be a repeat target.

Remediate

Run endpoint security software to find and remove the ransomware. If it cannot detect it, wipe your machine.

Restore

Restore your files or system back to the last known good copy



For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com