

Ransomware Facts

Ransomware: A form of malware that targets critical data and systems for the purpose of extortion. Once active on a victim's network, it encrypts and holds hostage critical sensitive data by withholding the decryption key until payment is made. The ransom demand is usually accompanied by a countdown clock and the cybercriminal usually requires payment in bitcoin or another anonymous form of payment.

According to the FBI, victims in the United States have paid more than **\$209 million** in ransom payments in the first three months of this year compared with **\$25 million** in all of 2015. -FBI

<https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise>



2016

First 3 months

 = \$25 million



2015

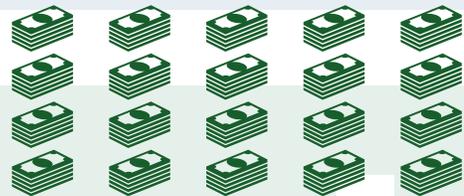
The ransom demands vary greatly but averages about **\$500** for individuals and **\$10,000** for businesses. -Symantec

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf



Individual

 = \$500



Business

More than
4,000
ransomware attacks have occurred daily on average, since January 1, 2016.

-US CERT

<https://www.us-cert.gov/security-publications/Ransomware>

This is a
300%
increase over the approximately 1,000 attacks per day seen in 2015.

-US CERT

<https://www.us-cert.gov/security-publications/Ransomware>

Beazley Breach Insights handled **86** ransomware attacks during the first six months of 2016, after seeing only **43** in the entire 2015 calendar year.

<https://www.beazley.com/Documents/2016/201607-Beazley-Breach-Insights.pdf>

Basic Ransomware Defenses

Educate all staff on risks and defensive email and web usage

Limit write capability to file servers where possible

Make regular offline backups

Use web and email security protection

Maintain strong and up to date endpoint protection

Immediately disconnect any device suspected of being infected