RANSOMWARE

An increasing number of organizations were affected by encryption ransomware last year. This nasty form of malware encrypts, or locks, your files, then demands a monetary ransom for their return. In 2015, over 750,000 computers were infected by ransomware. So, how does a ransomware attack happen?

Did you know?

In 2015, Ransomware was found on the computers of over 750,000 users.

1. Distribution

Ransomware is typically distributed in phishing emails. Large and small organizations are increasingly being targeted by these attacks.

2. Engagement

The recipient, unaware of the scam, engages with the email by downloading a file attachment or following a link to a malicious site hosting the malware.

Ransomware is often distributed by executable/script files (.js or .exe) or macro-enabled Word documents (.docm).

3. Infection

The computer is infected and important files are encrypted. Any connected devices, including a backup drive, may also be affected. At this point, any personal or company information stored on your computer or network may be compromised.

4. Ransom

The attacker reveals itself to the user. At this point, files are nearly impossible to recover, and a ransom of $150-1000 (USD) is demanded.

Ransomware attackers have gone so far as to set up "support" teams to facilitate the payment process. If a payment is not received quickly, the price goes up.

5. End Game

In most cases, unless the recipient has access to an unaffected backup, they may feel their only option is to pay the ransom or lose the files.

Ransomware attacks rose 26 percent in the last quarter of 2015.

What can you do to stop this?

Say "no" to Unsolicited Files

Never download a file you were not expecting. If you know the sender, you can verify the attachment with a quick phone call.

Keep Regular Backups

Back your files up regularly. Don't forget to disconnect your backup from your computer when not in use!

Keep Macros Disabled

If a document tells you to enable Office macros, do not do it. This allows attackers to access your computer.

Keep Software Updated

Ransomware can also be distributed through vulnerable software. Update software often to patch security holes.

The best time to stop a ransomware attack is before it happens.

Ransomware can quickly infect an entire network, so remember to report any suspicious activity to keep our organization safe and secure.

https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/
https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html
http://phishme.com/ransomware-rising-criakl-osx-others/

PHISHME

Copyright © 2016, PhishMe, Inc. All rights reserved.
The PhishMe name and logo are trademarks of PhishMe, Inc. in the United States and other countries.