

INFORMASIE TECHNOLOGIE

INFORMATION TECHNOLOGY

NEW VARIANT OF BIP DHARMA RANSOMWARE FOUND

WHAT IS RANSOMWARE?

Ransomware, for example, CryptoLocker, WannaCry or BIP Dharma, is a type of malware that installs itself on a device, takes files on the device or network storage, encrypts them, and then extorts money from the user to unlock the files. This type of programme can be installed by means of an e-mail attachment, an infected programme or unsafe website with malware installed on it.

The software "kidnaps" your data by encrypting or limiting your access to it and then sending you a message demanding money to regain your access. The only way access is possible again is by acquiring an encryption key from the creator of the ransomware at a fee. However, paying this fee doesn't guarantee that you will have access to your data again, so doing this is a huge risk.

According to Sophos security ransomware is one of the most widespread and damaging threats that internet users face today.



M
falling victim to ransomware.

work somewhere else, preferably off-site. If you do fall for a
your data off-site also protects it from events such as a fire, flood
encrypt your device to ensure that if it ends up in the wrong hands,

If you receive an attachment from someone you don't know. And even if you do know the person, first confirm whether they did send it to you. Just because it's from someone you know, it doesn't mean it's safe. Your colleague or friend's account could have been hacked.

3. Scan attachments

There are tools such as VirusTotal available for scanning attachments to ensure that they are safe to open. VirusTotal is an online scanning tool and can be found at <https://www.virustotal.com/#/home/upload>.

4. Keep Windows updated

Make sure all Windows updates are installed as soon as they come out. Also make sure you update all programmes, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.

5. Security software

Make sure you have some sort of security software installed. If you are unsure whether you have adequate protection on your device, contact us to assess your security.

6. Difficult password

Use hard passwords and never reuse the same password at multiple sites.

[SOURCE: www.sophos.com]

Posted in: [E-mail](#), [Security](#) | | [With 0 comments](#)