mbc
MANAGED IT SERVICES

RANSOMWARE

WHAT IS IT?

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

HOW CAN IT AFFECT YOUR BUSINESS?

When a user wants to access a file that has been affected, they are blocked and unable to do so creating a severe problem for business' critical data. The system admin who investigates this problem typically finds two files in the directory that indicate the files are taken ransom, and how to pay the ransom to decrypt the files.

Once encrypted the only way to get them back is to restore a recent backup or pay the ransom. These ransoms could vary from $500 within the first deadline and can double if the deadline expires

WHAT YOU NEED TO LOOK FOR?

Attacks are typically carried out using a Trojan that is disguised as a legitimate file. The user is tricked into downloading or opening the email attachment using social engineering tricks. Commonly, the victim receives an email with a password protected ZIP file, DOC or PDFs purported to be from a known contact or your own IT or billing department.

The Ransomware runs when the user opens the attached files, and once on the machine, it starts to encrypt all data files it can find on the PC itself and on any network the PC has access to.

WORK SAFE:

BE CAUTIOUS of emails from senders you don't know, especially those with attached files or with passwords

WHEN IN DOUBT, delete the email

NEVER open odd attachments or links

EVEN IF YOU KNOW THE SENDER, confirm verbally

SEE SOMETHING SUSPECIOUS coming from your own IT department? Always confirm with your manager that this is official communication

AVOID storing data critical files on your local PC

MAKE sure to regularly back up your data