DON'T BE BLACKMAILED!

How you can defend against a RANSOMWARE ATTACK?

WHAT IS THE RANSOMWARE?

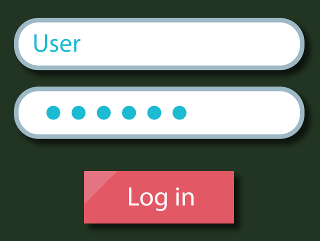
Ransomware is a malicious software what's goal is to take hostage your personal data stored on your IT devices, keeping them unavailable until you pay the demanded ransom.

WAYS OF INFECTION

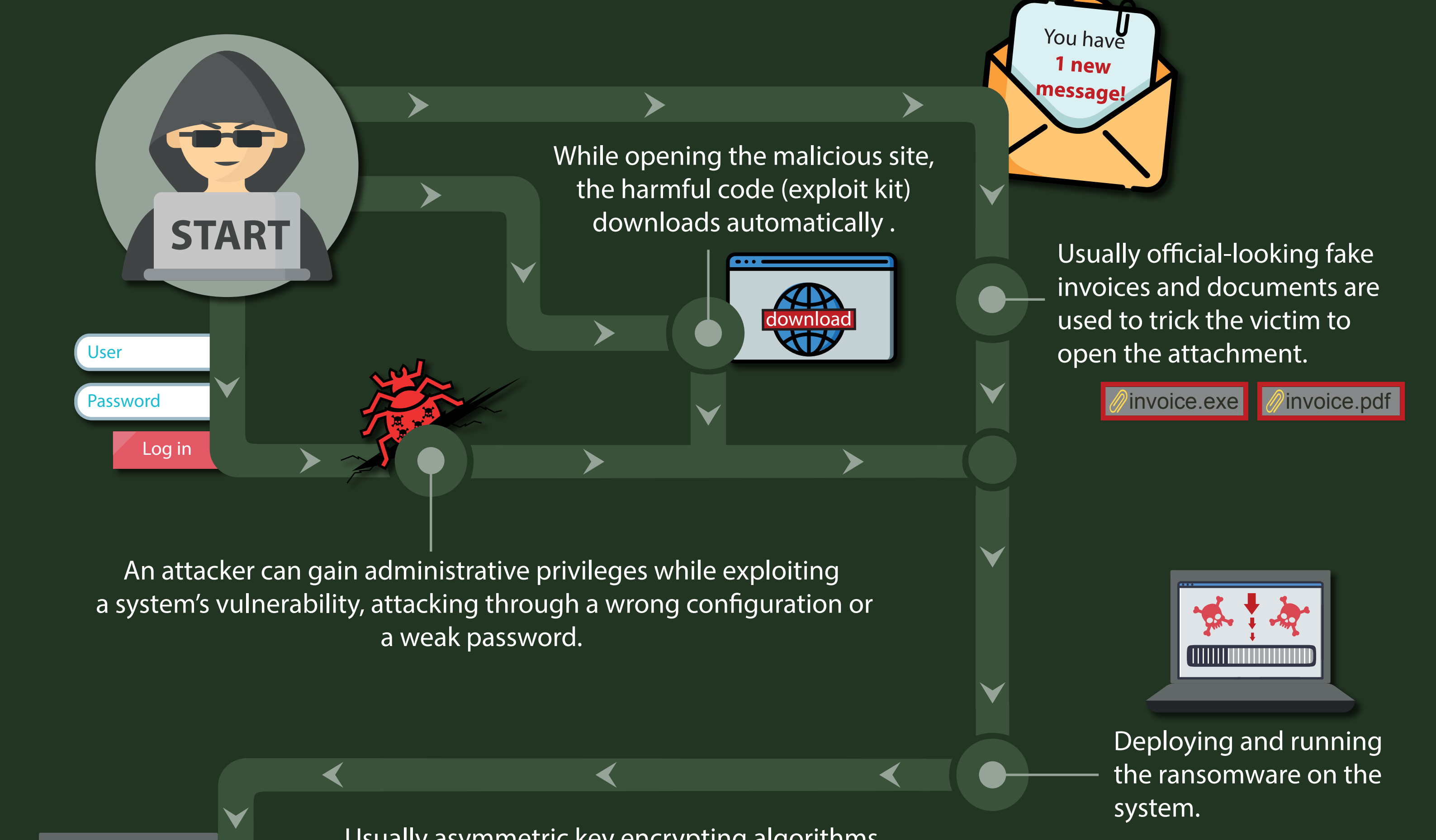
infected e-mail attachments

malicious websites

exploit of a vulnerability, a wrong configuration or the user's lack of attention, negligence



The attackers' goal is to infect the targeted system.

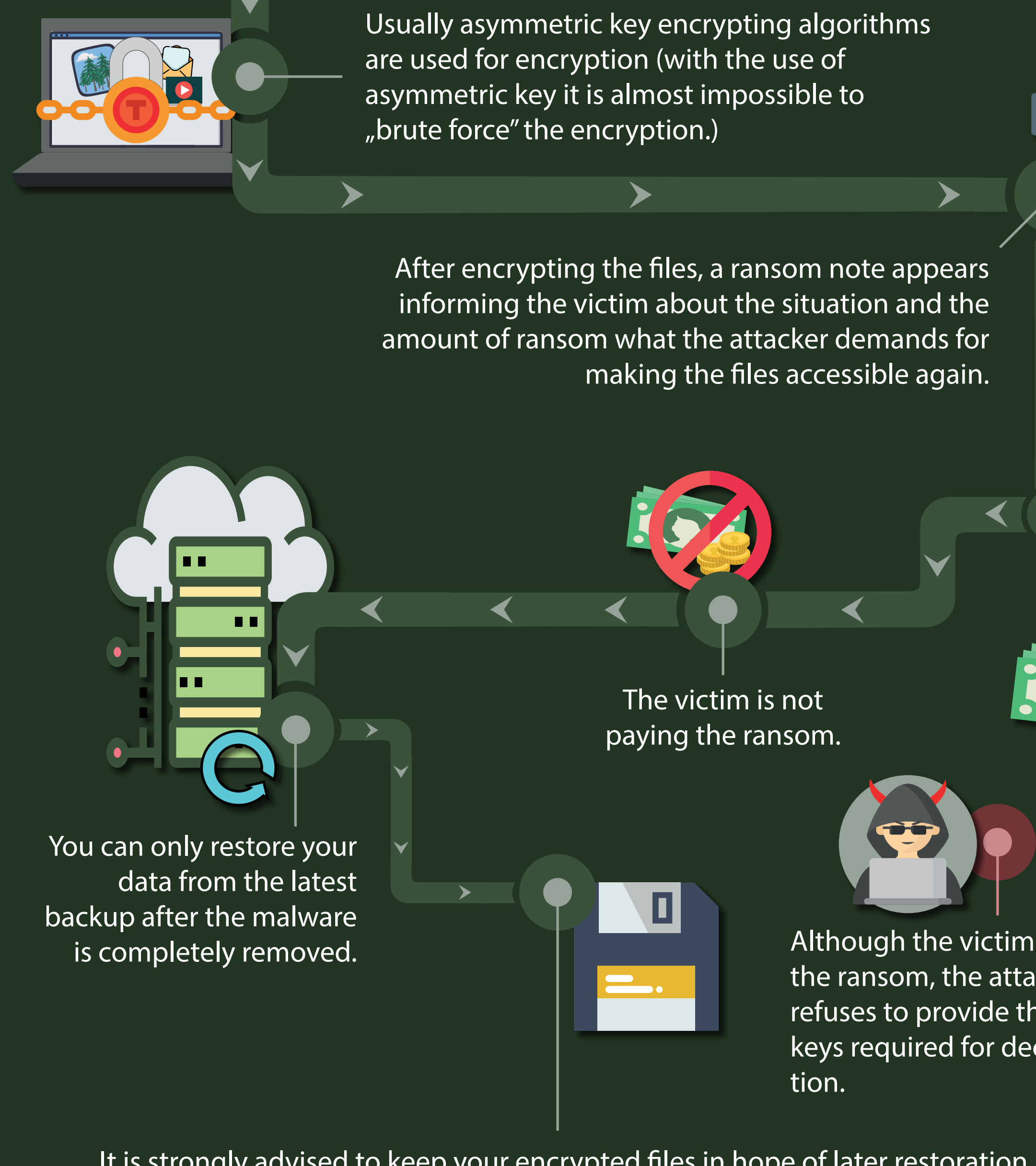


While opening the malicious site, the harmful code (exploit kit) downloads automatically .

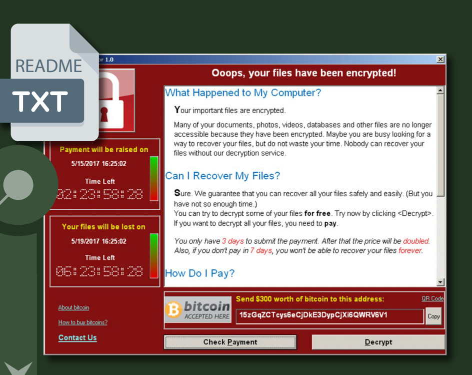
Usually official-looking fake invoices and documents are used to trick the victim to open the attachment.

An attacker can gain administrative privileges while exploiting a system's vulnerability, attacking through a wrong configuration or a weak password.

Deploying and running the ransomware on the system.



Usually asymmetric key encrypting algorithms are used for encryption (with the use of asymmetric key it is almost impossible to „brute force" the encryption.)



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

About bitcoin
How to buy bitcoins?
Contact Us

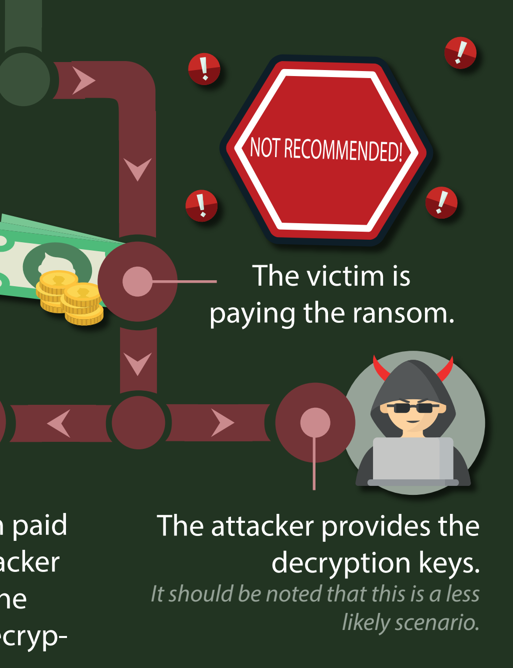
bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address: QR Code

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1 Copy

Check Payment | Decrypt

After encrypting the files, a ransom note appears informing the victim about the situation and the amount of ransom what the attacker demands for making the files accessible again.



The victim is not paying the ransom.

The victim is paying the ransom.

You can only restore your data from the latest backup after the malware is completely removed.

Although the victim paid the ransom, the attacker refuses to provide the keys required for decryption.

The attacker provides the decryption keys. *It should be noted that this is a less likely scenario.*

It is strongly advised to keep your encrypted files in hope of later restoration. Ransomware developers make mistakes, that – if you are lucky – can be used to gain control over your files again. Sometimes even the attacker itself publish the decryption keys. You never know.

HOW TO DEFEND YOURSELF

USER

- Always install the latest security updates and patches.
- Use antivirus products and update the virus definition database regularly.
- Regularly make security backup of your files . If possible, keep the backup on a removable media (e.g. an external hard drive). Keep at least 3 copy of your backup.
- Never open the e-mail attachments coming from an unknown person. Be especially careful with archive files or those having double extensions (e.g. .doc.exe).
- Enable „Controlled folder access".

ADMINISTRATOR

- Audit open ports and services. Those found unnecessary, should be closed. For the rest, change the default port numbers and use logging.
- Disable external access to common TCP and UDP ports (only allow connections from specified IP addresses for a limited group of users).
- Disable remote admin ports used to manage networks. If required, use VPN.
- Regularly patch perimeter devices' software and update blacklists.
- Periodically audit user privileges. (Suspend inactive, unwanted users, minimize the number of users having remote access rights.)
- Use strict password policy: if possible, use multi-factor authentication (MFA).

IF TROUBLE HAS ALREADY OCCURRED...

- Disconnect the device from the network, as soon as possible.
- Stop all internal file sharing and external services.
- Perform a clean install on all infected workstations.
- Don't connect removable media as the infection may spread further.
- After the investigation is over, don't forget to take the appropriate measures to prevent such incidents.

nki.gov.hu
csirt@nki.gov.hu

NATIONAL CYBER SECURITY CENTER HUNGARY