S teroristy se (ne)vyjednává

Radomír Orkáč

Když to nejmíň čekáte...

- **Majitel firmy:**
  - *„Máme napadený server, asi je vše zašifrované, včetně záloh...“*
  - cenik150306095123.txt.id-72330MJP2.cry
  - HOW TO DECODE FILES.H.txt

****
ATTENTION!! Changing the file name makes the restore process impossible!
****

Your data is encrypted.

To receive a program of decoding, You need to pay ~ $ 750 and You need to send
the personal code 72330MJP2 to the email address tom.anderson@india.com, DE_CODER@mail2tor.com, scryptx@meta.ua

Then you will receive all the necessary instructions.

Attempts to decipher independently will not lead to anything, except irretrievable loss of information.

We respond to all emails, if there is no answer within 10 hours, duplicate your letter other email services. If you did not receive the answer from the after-cited email for more than 48 hours (and only in this case!),

Download Tor Browser from here: https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar http://5akvz3kp6qbqmpoo.onion/

Thank you for your attention and have a good day.

****
ATTENTION!!! Changing the file name makes the restore process impossible!
****

Vyjednávat nebo nevyjednávat?

- **M. Zeman:** S teroristy se nevyjednává, s teroristy se bojuje.
- **A. Šándor:** S teroristy musíme vyjednávat, je to jediná cesta [1].
- **ESET:** Platbou výkupného podporujete zločin [2].
- **FBI:** S teroristy vyjednává každý stát, snad kromě Rusů [3].

  ...

- **Majitel firmy:** Jestli je to opravdu zašifrované, firmu položím...

Příběh se šťastným koncem

- **Oběť:** *Lets make a deal*
  - 26. června 2017 10:39
  - Thank you for cooperation:)
- **Útočníci (+6 min):** *RE: Lets make a deal*
  - *Tom Anderson <tom.anderson@india.com>*
  - *"Проживальский Пётр" <scryptx@meta.ua>*
  - The cost of decrypting your data is 0.31 BTC
    - (26.6. 2017) 0.31 BTC = 18 830 Kč

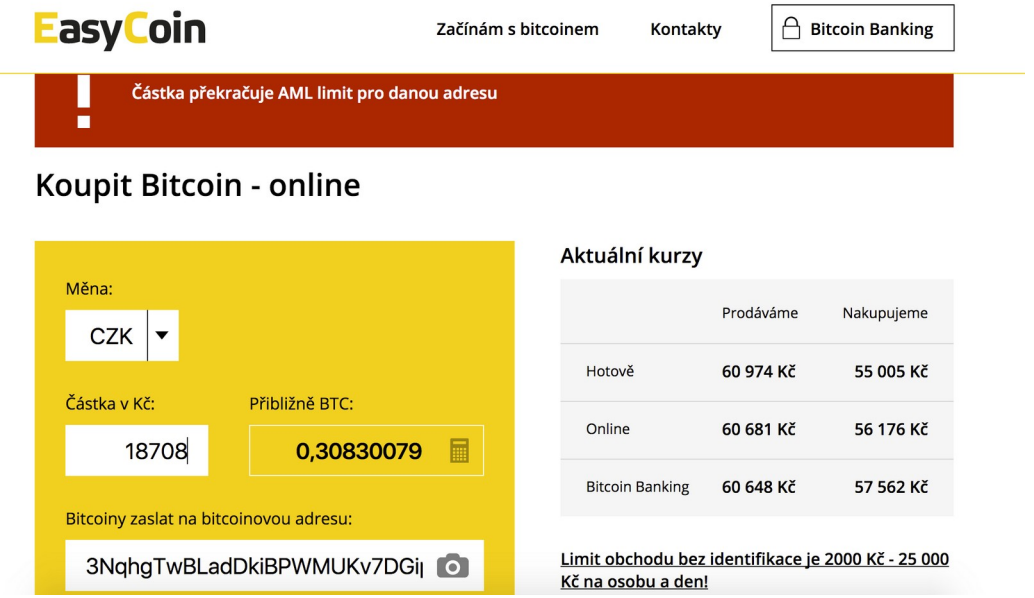
Příběh se štastným koncem

- **Oběť (+5 min):** *How to decrypt?*
  - *Will you send me a decrypt tool?*
- **Útočníci (+13 min):** *RE: How to decrypt?*
  - *I'll send the program for decryption.*
- **Oběť (+10 min):** *RE RE: How to decrypt?*
  - *Could you decrypt this txt file?*
- **Útočníci (+6 min):** *RE RE: How to decrypt?*
  - *We send 10 lines.*

"101036";"Plyšový medvěd 80 cm tmavě hnědý";"1";"4,00";"ks";"21,00";"577,69";"479,00";"409,09";"519,92";"0,00";"0,00";"";"Krásný plyšový medvěd nesmí chybět v žádném dětském pokojíčku!...

Příběh se šťastným koncem

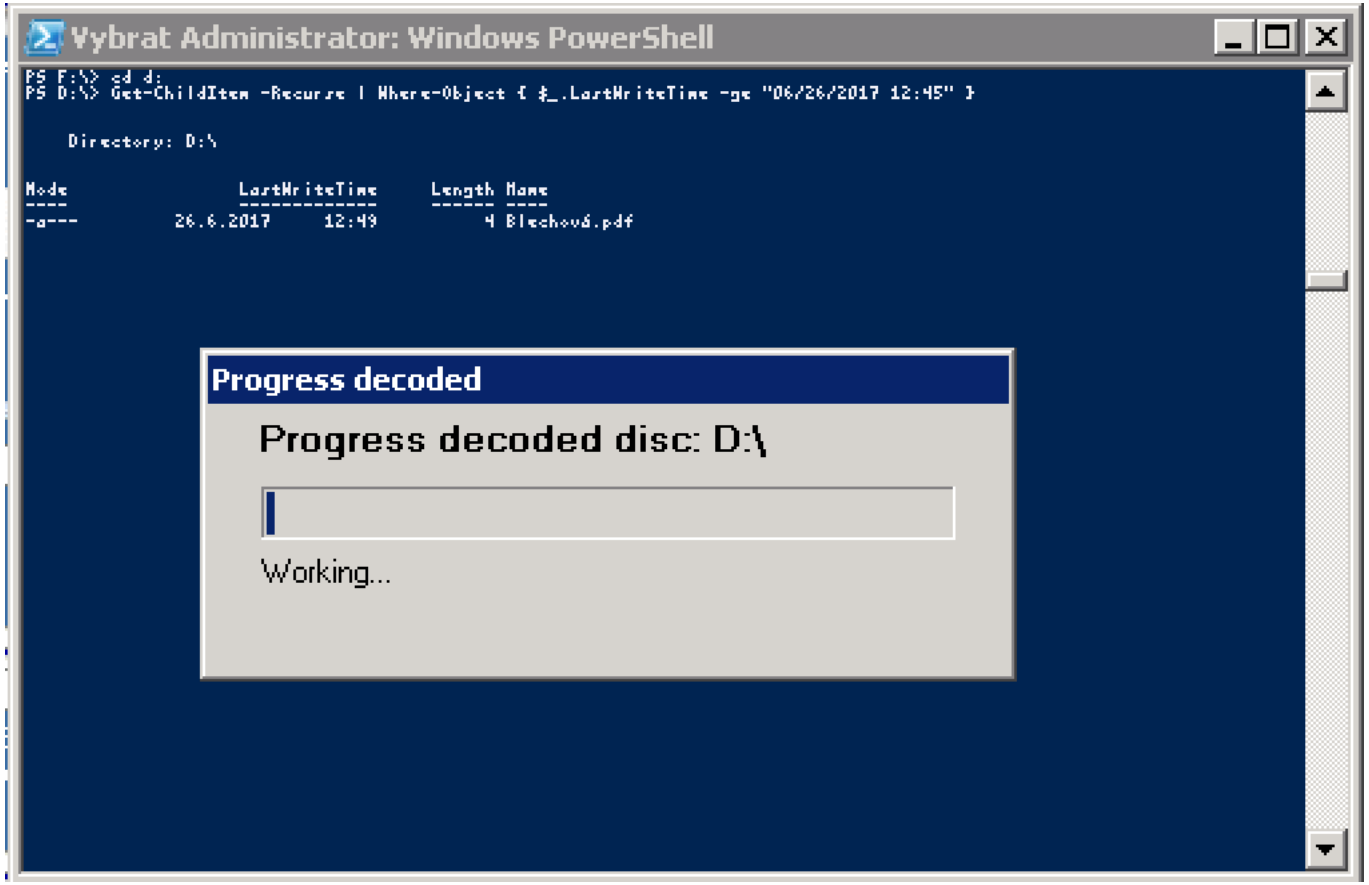
- **Oběť (+46 min):** *AML limit?*
  - *The amount exceeds the AML limit for that address. If you send me the decryptor than I promise to pay you in future.*
- **Útočníci (+7 min):** *RE: AML limit?*
  - *You can divide the translation into …*



Příběh se šťastným koncem

- **Oběť provedla platbu (+35 min)**
  - *26.06.2017 12:37:44*
  - *Platba: -9 105,00 CZK, -9 725,00 CZK*
- **Útočníci (+4 min):** *RE: RE: Lets make a deal*
  - *rename Decrypt.exe.doc to Decrypt.exe and run as administrator.*
- ***Oběť (+27 min)**: Progress bar is not moving*
  - *The progress bar is not moving. Can I find out the information whether process of decrypting is correct?*

Příběh se šťastným koncem



Příběh se šťastným koncem

- **Útočníci (+25 min):** RE: *Progress bar is not moving*
  - *Progress will be in 1-2 minutes of operation of the decoder. Large files decode for a long time.*
- **Oběť (+35 min):** RE RE: *Progress bar is not moving*
  - *Sorry, but there is no progress move during 2 hours. Could you send me decryptor for decrypt selected files? Can I check from command line which files are just decrypted?*
- **Útočník (+26 min):** *RE RE RE: Progress bar is not moving*
  - *Create on the disk d: \ folder "test". (D:\test)*
  - *Copy the files to it for decoding.*
  - *Start the decoder test.exe*

Příběh se šťastným koncem

- **Oběť (+27 hod. 16 min):** Thank you
  - *How did you gain the access? Can you tell me WHICH user had a weak password or there was a SW bug?*
- **Útočník (+8 min):** *RE: Thank you*

admin / admin1
Use complex passwords for user logins via RDP (Remote Desktop). Example of a complex password: bb @ 71H6j070vkX7N
The users you are working with on the system SHOULD NOT be Administrator rights.
Constantly archive your data (databases, documents, etc.). Archives should be on another computer and access to it should only be from the localhost.
To access the server from the "Internet" for guaranteed protection, configure the Firewall in the router or on the server itself, only certain IP addresses will give the maximum protection for you.
Continually update the system.
Check the sfc / scannow system. And turn off the sticking of the keys.

We hope you will be useful.

Příběh se šťastným koncem

- 3NqhgTwBLadDkiBPWMUKv7DGipGXJXzQUB
  - Total Received: 11.46107412 BTC
  - Total Sent: 11.45949486 BTC
- 3QNsTXTVuiowmAdCk38jupi9aVX2A7qC8d
  - Total Received: 0.31434301 BTC
  - Total Sent: 0.31434301 BTC

Zdroj informací

- [1] https://tn.nova.cz/zpravodajstvi/clanek/379087-s-teroristy-musime-vyjednavat-je-to-jedina-cesta-tvrdi-sandor
- [2] https://www.eset.com/cz/blog/hrozby/5-duvodu-proc-neplatit-vykupne-za-ransomware/
- [3] https://zpravy.aktualne.cz/domaci/americane-kritizuji-neco-co-sami-delaji-s-teroristy-vyjednav/r~84c3367ecf4c11e58a2b0025900fea04/