stealing passwords ☠ avoiding detections + multifactor authentication ? not stealing anything ☺

Ondřej Ševeček |
ondrej@sevecek.com |
www.sevecek.com

26. – 28. september 2022

#ntk22

Notes

- proofs-of-concept only
  - by design problems only
- privileged person on insecure environment
  - + extortion inside-job
  - + CyberArk protected enterprise
  - + banking app developers
- full antimalware protection
  - tested with Defender, Symantec, F-Secure, Eset, Avast, Kaspersky

No ☠ new things included

- yet everybody behaves like they are safe

Fake GUI

- full screen app

Software keyloggers

- principles
- detection avoidance
- vectors

Clipboard

- interconnecting the whole world of RDPs, TeamViewers or VNCs

Password managers

- many different passwords +
- complexity +
- remembering nothing +
- typing nothing +
- encrypted database +
- MFA available +

User simulations

- sometimes a bit slower but you can always display some fake UI ☺

MFA

- in browsers
- in OS