GOPAS
POCITACOVA.SKOLA.CZ

GENERÁLNÍ PARTNER:

Deloitte.

Credentials Guard, BitLocker, UEFI Secure Boot, UAC, Remote Credentials Guard, ATA, Shielded VMs, ...

vs.

(un)safe behavior

HACKERFest2017

Ing. Ondřej Ševeček | GOPAS a.s.
ondrej@sevecek.com | www.sevecek.com
MCSM:Directory | MVP:Security | CEH | CISA | CISM | CHFI

Buzzwords

- Credential guard
- Secure Boot
- BitLocker
- Remote Credentials Guard
- UAC
- Shielded VMs
- ATA, antimalware, heuristics, ...

Scenario

- Corporate desktop computers and/or notebooks
- With everything
  - users are (not) local administrators
  - UEFI secure boot
  - BitLocker with TPM
  - Credentials Guard
  - UAC
- happily using Domain Admins credentials

Privilege escalation to local Administrators

- Hardware keylogger/spy-camera
- Software keylogger under limited user
- Machine reinstallation
  - connect to domain
  - without connecting to domain

SSO injection

- why would it try hacking the local computer with UAC?

- testing applications under strong accounts
  - locally
  - remotely
  - Kerberos delegation

SSO hell

- Kerberos protocol transition

Shielded VMs

- are really only shielded

Message

- no technology can protect you definitely

- behave safely (learn what you do)
  - never use strong accounts against weak computers
  - never give sensitive data to unknown hosters
  - Kerberos authentication
    - Enter-PSSession, mstsc /RestrictedAdmin
  - disable Kerberos delegation on sensitive accounts
  - disable Add computer to domain
  - require safe UAC prompts
  - ...

- incidents always happen
  - isolate with separated accounts and responsibilities
  - isolate with Windows Firewall

Incidents

- incidents cannot be resolved if not contained
  - resetting krbtgt is not enough :-)

Dávejte si pozor!!
Děkuji za pozornost

GOC175 - Security internals
GOC172 - Kerberos
GOC169 - ISO 2700x

www.**hackerfest**.cz
www.**gopas**.cz