

Odvrácená strana bezpečnosti

Petr Medonos

whoami

- 7 let ve společnosti Etnetera
- konzultace DBA, performance
- ofenzivní bezpečnost
- CEH, RHCE, M102, M202

[@PetrMedonos](#)

[\[in\] PetrMedonos](#)



Sociální techniky

- sociální sítě
- helpdesk
- flash disky
- Teensy
- využití chyb aplikace

```
..#####..#####..#####  
..##.....##.##.....##...  
..##.....##.....##...  
..#####..#####.....##...  
.....##.##.....##...  
..##.....##.##.....##...  
..#####..#####.....##...  
[---] The Social-Engineer Toolkit (SET)  
[---] Created by: David Kennedy (ReL1K)  
[---] Version: 6.1.2  
[---] Codename: 'Midnight'  
[---] Follow us on Twitter: @TrustedSec  
[---] Follow me on Twitter: @HackingDave  
[---] Homepage: https://www.trustedsec.com  
  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
Join us on irc.freenode.net in channel #setoolkit  
  
The Social-Engineer Toolkit is a product of TrustedSec  
  
Visit: https://www.trustedsec.com  
  
Select from the menu:  
  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
  
set>
```

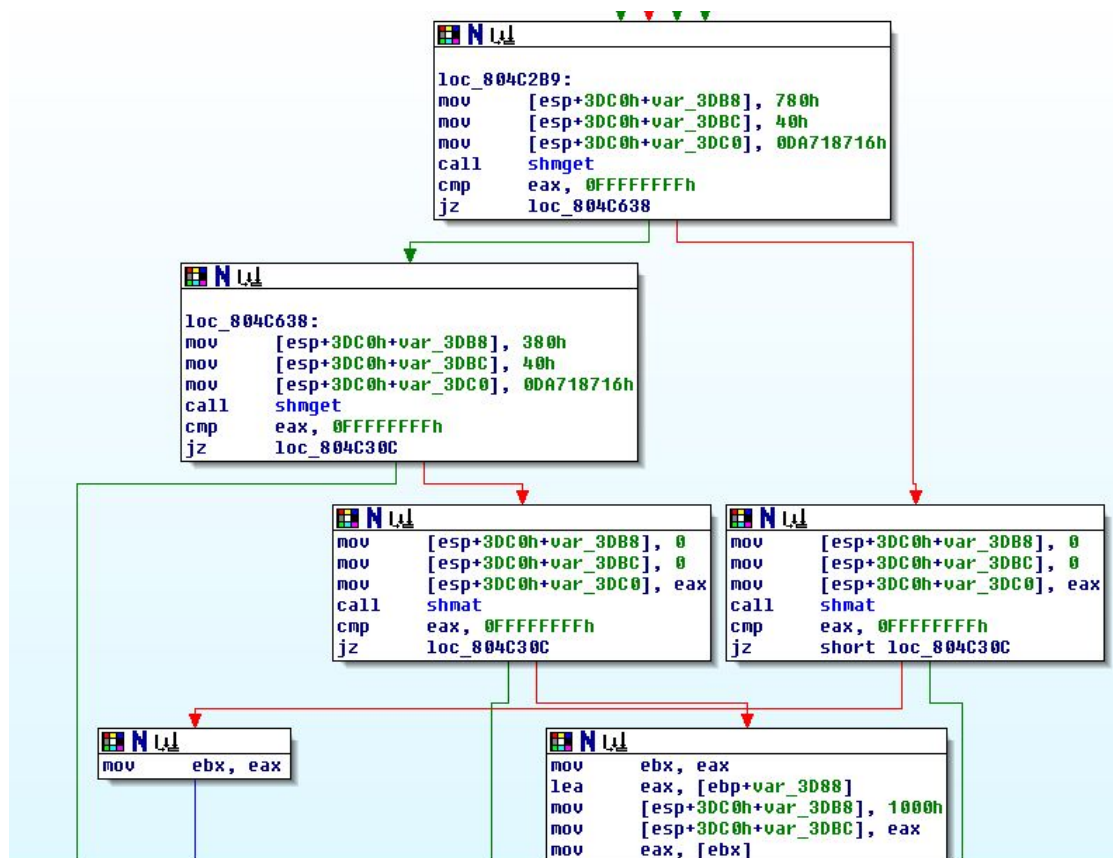
Administrační nástroje



- Powershell
- WMI
- Psexec
- VB scripty
- standardní nástroje => nezachytitelné antivirem!

Malware

- brute-force hesel k administrátorským účtům
- dešifrování za běhu
- podmíněná aktivace



Současná rizika

- Big Data
- marketingová a UX rozhodnutí
- Dropbox
- (D)DoS útoky
- chybí validace bezpečnostních nastavení

=> penetrační testování

=> školení zaměstnanců proti SE



Děkuji za pozornost!