Hunting Lateral Movement in Windows Infrastructure v2

Teymur Kheirkhabarov

Who Am I

- Senior SOC Analyst @Kaspersky Lab
- SibSAU (Krasnoyarsk) graduate
- Ex- Infosec dept. head
- Ex- Infosec admin
- Ex- System admin
- Infosecurity conferences speaker: PHDays, ZeroNigths
- Twitter @HeirhabarovT
- www.linkedin.com/in/teymur-kheirkhabarov-73490867/

What are we going to talk about

- Different ways to launch executables remotely by using compromised credentials and operating system functionality;