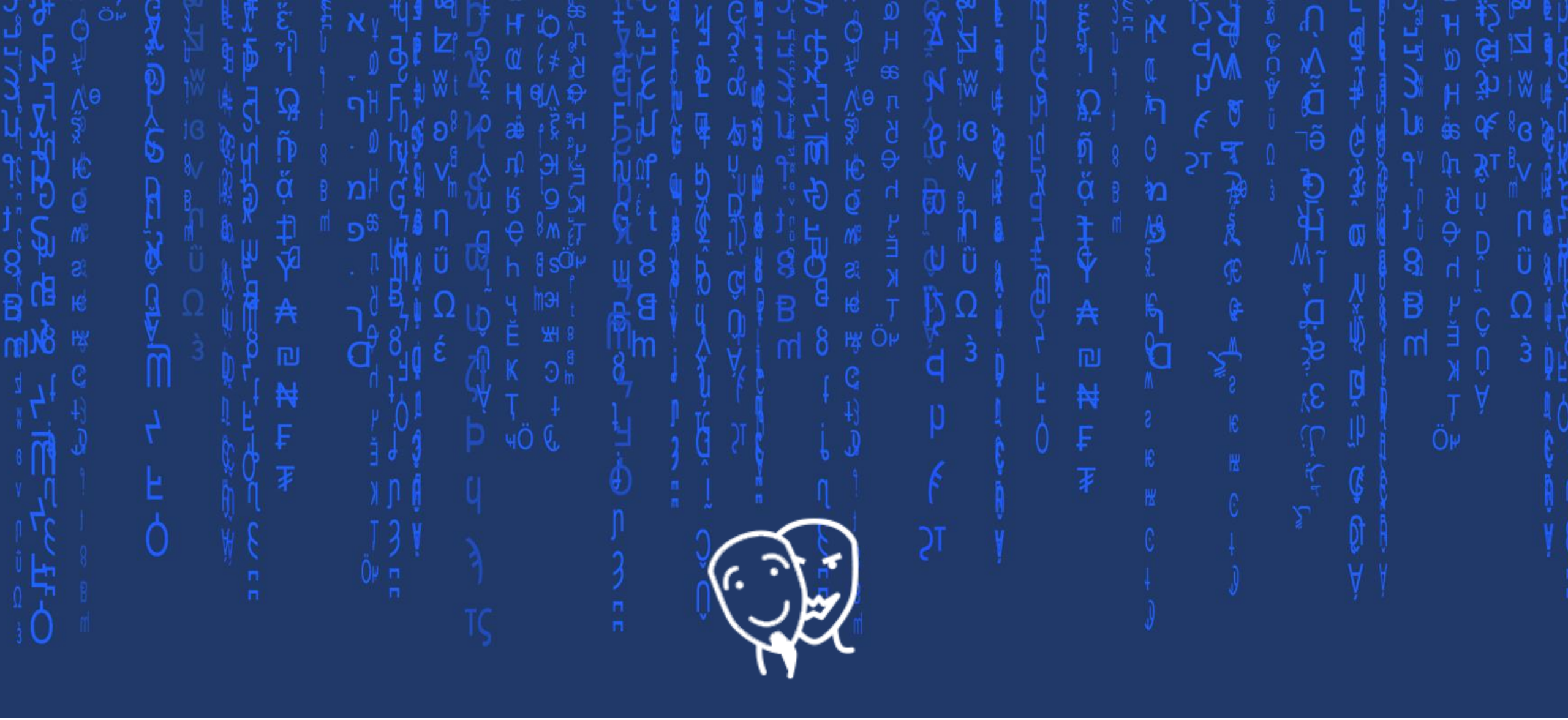
Cybersecurity workshop III

Milan Kyselica

Head of Offensive Dept. IstroSec

MODERUJE: Mario Minarovský, CREDIBILIS



„Turla“

Turla

- Turla používa sofistikované techniky a nástroje na infikovanie, skrývanie a ovládanie svojich obetí, vrátane zneužitia satelitnej komunikácie, vytvárania falošných digitálnych certifikátov, využívania rootkitov a backdoorov
- Turla je považovaná za jednu z najstarších a najdlhšie pôsobiacich kybernetických hrozieb, ktorá má korene v 90. rokoch minulého storočia. Jej pôvod je nejasný, ale niektoré zdroje naznačujú, že má spojenie s Ruskom
- Turla sa neustále prispôsobuje a vyvíja, aby sa vyhla odhaleniu a zvýšila svoju účinnosť. V posledných rokoch bola Turla zodpovedná za niekoľko vysoko profilových útokov, napríklad na ministerstvo zahraničných vecí Nemecka, armádu Francúzska, Európsku organizáciu pre jadrový výskum (CERN) a ďalšie

Scénar Turla

- Turla je podozrivý balík trojanov, ktorý je považovaný za produkt ruskej vládnej agentúry.
- Začína stiahnutím škodlivej phishingovej prílohy vo forme skriptu VBS, ktorý modifikuje kľúče registra a vytvorí proces, ktorý nainštaluje zadné vrátka Epic, ktoré komunikujú s C&C serverom a prijímajú príkazy na vykonanie na infikovanom systéme
- Ďalej sa snaží dostať do viacerých počítačov v sieti, získať viac práv, zobrať si dôležité informácie a odoslať ich.

CREDIBILIS

LIVE

CREDIBILIS

Ďakujeme za pozornosť.

CREDIBILIS

www.credibilis.sk