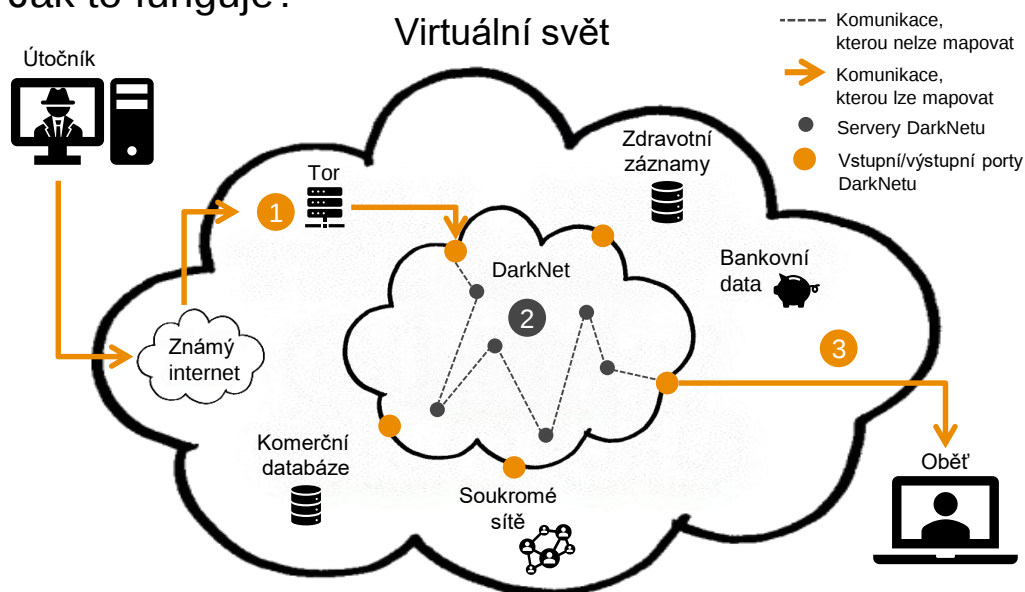


DarkNet

Věděli jste, že veřejná část internetu tvoří pouze 4 % celého virtuálního prostředí? Co tvoří ty ostatní části? Máte představu, odkud přichází známé kybernetické útoky? Stejně jako v reálném světě existuje podsvětí, i část internetu obsahuje obdobné místo, kde probíhají ilegální aktivity.

Jak to funguje?



Útočník se připojí na DarkNet pomocí speciálního internetového prohlížeče Tor (The Onion Router) 1 přes vstupní porty, které jsou lokalizovány různě po světě. Tam končí záznam, který lze mapovat. 2 Komunikace poté probíhá přes servery a jejich porty v DarkNetu, jejichž komunikační cesty nelze sledovat. 3 Komunikace začne být stopovatelná opět na výstupním portu z DarkNetu, s odlišnou lokalizací než vstupní port, a je směrována na oběť. Odlišná lokalizace vstupních a výstupních portů v praxi znamená, že útočník dle záznamů z logů pochází např. z Ruska, ale v praxi to může být kolega sedící vedle Vás.

Co si může útočník objednat?

- Účty s hesly (\$160/bankovní účet)
- Ransomware as a service (\$120/měsíc)
- DDoS útoky (\$10/hodinu)
- Různé typy malware (\$150/aplikace)



To nejdůležitější na závěr.

Stay Secure! Určitě se nezkoušejte pokoušet o přihlášení na DarkNet. Jedná se o ilegální aktivitu, za kterou můžete být stíháni dle trestního zákoníku.

Jak vám můžeme pomoci?

Pokud máte nějaké dotazy ohledně tohoto vydání, neváhejte se na mne obrátit. Rád vám poradím i v dalších oblastech kybernetické bezpečnosti.

Cyber
& Privacy



Oddělení IT Bezpečnosti