ENJOY SAFER TECHNOLOGY™

Globální vývoj kybernetických hrozeb za Q3 1. část

Ve třetím čtvrtletí letošního roku ubylo po celém světě masových hrozeb, jakými jsou phishing či spyware.

Ubylo detekcí webových hrozeb. Jejich pokles **souvisí se zánikem malwaru** na dvou nejaktivnějších doménách, které útočníci využívali - **adobviewe[.]club a fingahvf[.]top.**

O pětinu klesly detekce mobilního malware pro platformu Android.

Podobně jako ve druhém čtvrtletí **rostl v červenci a srpnu objem e-mailových hrozeb.**

V případě phishingových e-mailů **zneužívali útočníci nejčastěji renomé logistické společnosti DHL.**

Výrazně přibylo útoků na služby využívající RDP

Firmy i nadále využívají ve zvýšené míře různé nástroje umožňující práci na dálku. **Jedním z nejběžnějších je protokol vzdálené správy, RDP.**

Útoků na něj v minulém čtvrtletí přibylo o 140 %. Běžným scénářem, jak takovýto útok uskutečnit, je tzv. brute-force.

Brute-force útok je postup, kdy útočník typicky pomocí velké sítě infikovaných počítačů hádá přístupové údaje.

Ransomware útoky na nemocnice pokračují

Detekce ransomware ve třetím čtvrtletí klesly o 20 %. Jako většinový vektor šíření byl využit škodlivý e-mail. V polovině těchto útoků analytici detekovali ransomware WannaCry.

Vážným rizikem je i nadále ransomware Ryuk, který je často používán při útocích na zdravotnická zařízení po celém světě. **V Česku se objevil na přelomu roku například v nemocnici v Benešově.**

Zdroj: ESET Threat Report Q3/2020.