Kybernetické incidenty pohledem NÚKIB - duben 2023

12.5.2023 - | Národní úřad pro kybernetickou a informační bezpečnost

Počet kybernetických incidentů se po březnovém rekordním nárůstu způsobeném DDoS útoky vrátil do průměrných hodnot posledního roku. Nejčastěji evidovaným typem incidentů byly incidenty, které vyústily v nedostupnost služeb.

V dubnu pokračoval trend intenzivních phishingových kampaní proti strategickým vládním cílům v zemích NATO, včetně ČR. Tyto aktivity, při kterých je využíván nový malware MQsTTang, jsou spojovány se skupinou Mustang Panda. Kampani se věnujeme také v rubrice: Technika měsíce. Útočníci při ní použili neobvyklý způsob komunikace mezi jejich řídícím serverem a kompromitovanou stanicí oběti. Komunikaci posílali skrze protokol MQTT, který se používá pro správu IoT zařízení. To je odlišuje od dalších aktérů. Obecně tato technika v MITRE matici spadá pod Application Layer Protocol.

Celý dokument naleznete zde: https://www.nukib.cz/download/publikace/vyzkum/Kybernetické incidenty pohledem NUKIB - duben 2023.pdf

http://www.nukib.cz/cs/infoservis/aktuality/1958-kyberneticke-incidenty-pohledem-nukib-duben-2023