UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

TLP:CLEAR

Týždenná správa csirt.upjs.sk
15.10.2024 – 30.10.2024

TLP:CLEAR

Vypracoval: csirt.upjs.sk

Microsoft: Školy každý týždeň zápasia s tisíckami kybernetických útokov (USA)

Microsoft upozorňuje, že vzdelávacie inštitúcie, ako sú základné a stredné školy, univerzity, čelia každý týždeň tisíckam kybernetických útokov. Sektor vzdelávania je jednou z najzraniteľnejších oblastí a hackeri sa snažia využiť slabé miesta v zabezpečení. Cieľom útokov sú často citlivé informácie študentov a zamestnancov, čo môže viesť k zneužitiu osobných údajov. Problémom sú aj používatelia — niektorí už vo veku od 6 rokov — ktorí sú príliš mladí na to, aby vedeli o bezpečných návykoch v kybernetickej bezpečnostoi.

Google varuje, že uBlock Origin a ďalšie rozšírenia môžu byť čoskoro deaktivované

Google varuje, že rozšírenia ako uBlock Origin a ďalšie môžu byť čoskoro deaktivované. Dôvodom sú nové obmedzenia v rámci Manifest V3, ktorý výrazne mení spôsob fungovania rozšírení v prehliadači Chrome. Manifest V3 obmedzuje prístup rozšírení k niektorým funkciám, čo môže znamenať koniec pre populárne blokovače reklám a ďalšie bezpečnostné nástroje. Mnohí používatelia sú znepokojení, pretože tieto zmeny môžu výrazne ovplyvniť ochranu súkromia a bezpečnosť pri surfovaní na internete. Google tvrdí, že zmeny sú zamerané na zvýšenie bezpečnosti a výkonu, ale komunita vývojárov a používateľov to považuje za krok späť v oblasti ochrany súkromia.

FBI vytvára falošnú kryptomenu, aby odhalila rozšírenú manipuláciu s kryptomenami

FBI vytvorilo falošnú kryptomenu na odhalenie kybernetických zločincov. Tento krok bol súčasťou zložitej operácie, ktorej cieľom bolo infiltrovať čierny trh a získať informácie o nezákonných aktivitách. Použitím tejto falošnej kryptomeny sa FBI podarilo identifikovať a zatknúť viacero jednotlivcov zapojených do prania špinavých peňazí a iných kriminálnych aktivít.

American Water vypína systémy po kybernetickom útoku

Americká vodárenská spoločnosť sa stala obeťou kybernetického útoku, ktorý narušil ich systémy a spôsobil výpadky služieb. Útočníci získali prístup k citlivým údajom, čo spôsobilo značné obavy ohľadom ochrany infraštruktúry kritických služieb. Spoločnosť spolupracuje s odborníkmi na kybernetickú bezpečnosť a orgánmi činnými v trestnom konaní, aby minimalizovala škody a zabezpečila svoje systémy pred ďalšími útokmi.

Výskumníci odhaľujú malvér Hijack Loader pomocou ukradnutých certifikátov na podpisovanie kódu

Výskumníci odhalili nový kybernetický nástroj s názvom Hijack Loader, ktorý útočníkom umožňuje infikovať systémy malvérom. Hijack Loader je pokročilý a flexibilný nástroj, ktorý dokáže prenášať rôzne druhy malvéru vrátane trojanov a ransomware. Útočníci využívajú Hijack Loader na obchádzanie bezpečnostných mechanizmov, ako sú antivírusové riešenia a firewally, pričom aplikujú techniky ako dynamická injekcia kódu, obfuskácia a vyhýbanie sa detekcii pomocou analýzy správania. Týmto spôsobom dokážu infiltrovať cieľové systémy a infraštruktúru, pričom cieľom sú najmä podniky a organizácie.