CYBERSECURITY
maxvalor
Heimdal™ Security Alliance Partner

44.

WEEKLY CYBER NEWS

Espresso mellé (1-3 perces)

Az OpenText jelentése szerint a kiberbűnözők aktivitásának növekedésére lehet számítani a közelgő események, például az amerikai elnökválasztás körül, ezért a szervezeteknek javasolt fokozniuk biztonsági intézkedéseiket – ideértve a többlépcsős hitelesítést, rendszerfrissítéseket és az MI-alapú felügyeleti megoldások alkalmazását. Tech: Most indul egy kibertámadási hullám az interneten | hvg.hu

A Microsoft valósághű, megtévesztő környezeteket (honeypot tenantokat) hoz létre, hogy adatokat gyűjtsön az adathalász támadókról, feltérképezve azok infrastruktúráját és módszereit, ezzel zavarva és lelassítva tevékenységüket. Az így szerzett információkat más biztonsági csoportok is felhasználhatják hatékonyabb védekezési stratégiák kialakítására. A Microsoft honeypotokkal vizsgál adathalász módszereket | Nemzeti Kibervédelmi Intézet

A Delta Air Lines beperelte a CrowdStrike-ot, miután egy hibás szoftverfrissítésük világszerte üzemzavart okozott, amely több millió ügyfél utazását zavarta meg és 500 millió dollár kárt okozott a légitársaságnak. A CrowdStrike az esetért a Delta elavult IT-infrastruktúráját hibáztatja, míg a Delta a frissítés hiányos tesztelését okolja a károkért. A Delta Air Lines szétperli a repülési káoszt okozó CrowdStrike-ot - AzÜzlet

A Fortinet FortiManager szoftverében talált súlyos sebezhetőséget, a „FortiJump” hibát az UNC5820 csoport már június óta kihasználja, hogy illetéktelen hozzáférést szerezzen több mint 50 szerver konfigurációs adataihoz. A Fortinet azonnal kiadott egy javítást és kárenyhítési útmutatót, hogy megelőzzék a további támadásokat. Hackerek törték fel a Fortinet-et - Portfolio.hu

Az Nemzeti Kibervédelmi Intézet figyelmeztetése szerint iráni kibercsoportok 2023 októbere óta folyamatos támadásokat indítanak kritikus infrastruktúra ellen brute-force, password spraying és "push-bombing" technikákkal, hogy hitelesítő adatokat szerezzenek, amelyeket aztán kiberbűnözői fórumokon értékesítenek. Az FBI és más ügynökségek által kidolgozott jelentés részletes észlelési és védekezési módszereket javasol, hogy a célzott szektorok megvédhessék hálózataikat. [Tájékoztató az iráni kibercsoportok kritikus infrastruktúrát támadó tevékenységéről | Nemzeti Kibervédelmi Intézet]

A hackerek világszerte kihasználják a WordPress oldalak sebezhetőségét, és ártalmatlannak tűnő, rosszindulatú bővítményekkel hamis szoftverfrissítéseket jelenítenek meg, amelyek információlopó programokat telepítenek a látogatók eszközeire. Az új ClickFix kampányban hamis hibaüzenetekkel telepítenek kártékony PowerShell szkripteket, és már több mint 6000 weboldalt vettek célba a GoDaddy jelentése szerint. [Több mint 6000 WordPress weboldalt törtek fel, hogy információlopó bővítményeket telepítsenek | Nemzeti Kibervédelmi Intézet]

A Microsoft digitális védelmi jelentése szerint naponta 600 millió kibertámadás éri ügyfeleiket, beleértve állami és bűnözői támadásokat, amelyek kémkedésre, befolyásolásra és adatlopásra irányulnak. Az SFI keretében a vállalat a mesterséges intelligenciával és automatizált eszközökkel igyekszik megvédeni ügyfeleit és saját rendszerét a növekvő kiberfenyegetésekkel szemben. [Tech: Ön érintett? Naponta 600 000 000-szor akarnak ellopni valamit azoktól, akik a Microsoft programjait használják | hvg.hu]

Egy hacker október 24-én feltörte a 2016-os Bitfinex-hack során lefoglalt pénzeszközöket tartalmazó, amerikai kormány által ellenőrzött tárcát, és 20 millió dollárt utalt át, amelyet pénzmosási műveleteken keresztül próbált tisztára mosni. [Egy hacker feltörte azt a bitcointárcát, amely valószínűleg az Egyesült Államok kormányához tartozik – Kriptoworld]

Feliratkozom az új hírcsatornára!

* A Weekly Cyber News csatornára külön feliratkozás szüksége, kérünk, a gomb megnyomásával jelezd erre irányuló szándékodat! Köszönjük!