CYBERSECURITY
maxvalor
Heimdal™ Security Alliance Partner

18. hét

WEEKLY CYBER NEWS

Espresso mellé (1-3 perces)

Több mint 90 000 ip címen még mindig aktív a plugx. A Sekoia kiberbiztonsági cég jelentése szerint a több mint 90 000 egyedi IP címhez tartozó rendszer még mindig fertőzött egy PlugX féregváltozattal, amely fertőzött USB meghajtókon keresztül terjed.
forrás: nki

Ha ilyen eszközön tárolja az adatait, minden fájl a rosszindulatú emberek kezében landolhat. Magyarországon is jelen vannak azok a tárolók, amelyek támogatás híján már nem védettek a nemrég felfedezett támadási lehetőségekkel szemben. A rosszindulatú felek aktívan ki is használják ezt.
forrás: hvg

Az ukraina ellen célzottan irányított támadás 7 éves ms office bugot használt ki. Egy hét éves MS Office sérülékenységet használt ki az Ukrajnát Cobalt Strike-kal támadó hacker kampány.
forrás: nki

A német hadsereg ennél nagyobb bakit már el sem követhetett volna. A német haderő több mint hatezer, köztük titkosított online konferenciájának adatai váltak hozzáférhetővé az interneten.
forrás: index

Felltörték a Dropbox sign-t. A DropBox felhőalapú tárolási szolgáltató cég szerint hackerek behatoltak a DropBox Sign eSignature platform termelési rendszereibe és hozzáférést szereztek a hitelesítési tokenekhez, MFA kulcsokhoz, kódolt jelszavakhoz és ügyféladatokhoz.
forrás: nki

Cappuccino mellé (3-5 perces)

Akár 100 millió amerikai állampolgár is érintett lehet a kibertámadásban. Két hónappal azután, hogy hackerek betörtek a Change Healthcare rendszerébe, ellopva és titkosítva a cég adatait, még mindig nem világos, hány amerikait érintett a kibertámadás.
forrás: itbusiness

A változás több ezer céget érint, jobb, ha időben felkészülnek rá. Systems direktíva második változatát, a NIS 2-t, amelynek célja a kiberbiztonsági képességek egységesítése és az unióban működő szervezetek védelmének megerősítése. A vállalatoknak – ahogy más európai országokban – Magyarországon is fel kell készülniük az új követelményekre.
forrás: index

Bajban lehet, aki bedőlt ennek az átverésnek – milliók adatait lopták el. Már a mesterséges intelligenciára alapuló szolgáltatások nevével is visszaélnek a támadók, egy milliós követőbázissal rendelkező Facebook-oldalt is felhasználtak erre – a cél a kártevők telepítése volt az áldozatok gépére.
forrás: hvg

A mobilja mikrofonján is hallgatózhat ez az új androidos vírus, ami teljes hozzáférést ad másoknak a telefonjához. Chrome-frissítésnek álcázza magát, de valójában egy rendkívül veszélyes vírus bukkant fel, ami tálcán kínál mindent, ami egy okostelefonon fellelhető.
forrás: hvg

Biztonságos jelszavakat használ? A Hive Systems jelszótáblázatának 2024-es frissítésének köszönhetően, most megtudhatja, hogy átlagosan mennyi idő alatt tudnak feltörni brute force támadással különböző erősségű jelszavakat.
forrás: hive systems

Feliratkozom az új hírcsatornára!

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