HETI HÍRÖSSZEFOGLALÓ



Kihasznált peremeszköz-hibáktól az AI-vezérelt behatolásokig

2026. október 26-30.

TARTALOMJEGYZÉK

01 AKTÍVAN KIHASZNÁLT SÉRÜLÉKENYSÉGEK

02 AI A TÁMADÓI OLDALON

03 ÁLLAMI HÁTTERŰ ÉS FEJLESZTŐKET CÉLZÓ MŰVELETEK

04 NAGY LÉPTÉKŰ ADATSZIVÁRGÁSOK

05 BESZÁLLÍTÓI, SZOLGÁLTATÓI ÉS KÖZSZOLGÁLTATÁSI INCIDENSEK

BEVEZETÉS

Heti kitekintő: A heti válogatásban a hálózati peremeszközök kihasználása és az AI támadói felhasználása kap kiemelt szerepet. A Cisco egy aktívan kihasznált SSL VPN-hibát javított, a Dream pedig olyan támadási láncot tárt fel, amely PAN-OS-tűzfalakról az Active Directory felderítéséig vezetett. Az AI többféle szerepben jelenik meg: eszközfejlesztési segítségként, műveletтervezőként és autonóm végrehajtóként. A szolgáltatói incidensek adatlopást és közszolgáltatási kiesést is okoztak.

01 AKTÍVAN KIHASZNÁLT SÉRÜLÉKENYSÉGEK

Cisco: aktívan kihasznált SSL VPN-hiba okozhat szolgáltatásleállást

A Cisco október 28-án javította a Secure Firewall ASA és FTD szoftver CVE-2026-76418 azonosítójú, 8,6-os CVSS-pontszámú hibáját, amelyet októberben már aktívan kihasználtak. Hitelesítés nélküli támadó speciálisan összeállított kéréssel újraindíthatja az eszközt. A sérülékenységhez elérhető SSL VPN-belépési szolgáltatás és az érintett kapcsolatprofilban beállított másodlagos hitelesítés szükséges; sikeres VPN-bejelentkezés nem kell.

Mitigáció: A javított kiadás telepítése szükséges. Átmeneti mérsékléskénti a Cisco a kapcsolatprofillista letiltását vagy a másodlagos hitelesítés eltávolítását írja le, az alapértelmezett profil beállításától függően. Utóbbi csökkenti a VPN védelmét, ezért a módosítás hatását előzetesen értékelni kell; a konfigurációs intézkedés nem helyettesíti a frissítést.

Forrás: Cisco | BleepingComputer

PHP2Shell és Fragnesia: PAN-OS-tűzfalaktól az Active Directoryig

A Dream szerint egy feltételezetten kínai kötődésű támadó saját PHP2Shell-exploitot (CVE-2026-109618, CVE-2026-109619) kapcsolt össze a Fragnesia Linux-kernelhibával (CVE-2026-46300). A lánccal 25 PAN-OS-tűzfalon és kezelőszerveren szerzett rootjogosultságot; a kezdeti hozzáféréstől a tartós webshellig negyedóránál rövidebb idő telt el. Egy amerikai kormányzati kötődésű környezetben visszafejtette az LDAP-szolgáltatásfiók jelszavát, és felderítette a tartomány felhasználóit és csoportjait. A további tartományi támadások sikerét nem tudták megállapítani.

Mitigáció: Az érintett PAN-OS-verziókhoz kiadott gyártói javításokat telepíteni kell, és korlátozni kell a kezelőfelületek elérhetőségét. Kompromittálódás gyanújakor webshell-eket, a /etc/pam.d/su módosítását és tartós hálózati alagutakat is keresni kell; az érintett szolgáltatásfiókok hitelesítő adatait cserélni szükséges.

Forrás: Dream

Node2Shell: nyilvános PoC-ra épülő kihasználási kísérletet észleltek

Az ELLIO október 26-án egy CVE-2026-111497 Brotli-hibára épülő, Node.js 24.22.0 rendszert célzó támadási kísérletet rögzített. A támadó a nyilvános PoC elemeihez saját ROP-láncot, vagyis meglévő kódrészleteket összekapcsoló végrehajtási láncot illesztett. Ez a kutatók ötven tesztjében egyszer sem eredményezett parancsértelmező-hozzáférést, miközben saját exploitjuk ugyanazon a rendszeren működött. A sikertelen kódfuttatási kísérletek is összeomlaszthatják a folyamatot.

Mitigáció: Frissíteni kell a Node.js 22.23.4, 24.22.1 vagy 26.12.1 kiadására, illetve rendszerkönyvtárat használó telepítésnél a Brotli megfelelő csomagjára. A kitettség a nem megbízható Brotli-adatok kibontásához kapcsolódik, akár bejövő kérések, akár letöltött válaszok feldolgozásakor. Az ismétlődő összeomlásokat és a memóriamentések hozzáférési jogosultságait is vizsgálni kell.

Forrás: ELLIO

02 AI A TÁMADÓI OLDALON

AI-támogatott támadások: identitásszolgáltatók és japán szervezetek a célkeresztben

A Wiz szerint egy Storm-0940-hez kapcsolható támadó ARTEX-alapú AI-eszközökkel próbálta megkerülni IT- és szoftvergyártók hitelesítését, és hozzáférni ügyféladataikhoz; a kísérletek többsége sikertelen volt. A TrendAI japán célpontokat érintő vizsgálata az autonóm végrehajtástól az ember által irányított tervezésen át az eszközfejlesztésig azonosított AI-használatot. A célba vétel nem minden esetben vezetett sikeres behatoláshoz.

Mitigáció: A Wiz IoC-ket és naplómintákat is közölt. Az adathalászattal szemben ellenálló többtényezős hitelesítés és a feltételes hozzáférés mellett figyelni kell a több fiókot érintő, összehangolt sikertelen bejelentkezéseket, különösen, ha azokat sikeres belépés követi. Az automatizált próbálkozások blokkolás után perceken belül más IP-címekről is folytatódhatnak.

Forrás: Wiz | TrendAI

Skynet: mások nyelvi modelljeit használja jogosulatlanul egy támadóügynök

A Symantec AI-honeypotja rögzítette egy „Skynet” nevű támadóügynök teljes utasításkészletét. A módszer az LLMjacking: az ügynök hitelesítés nélkül elérhető vagy lopott kulccsal használható AI-végpontokat – önálló modellkiszolgálókat, AI-átjárókat, MCP-kiszolgálókat – keres, majd az áldozat modelljével terveztet és hajtat végre támadásokat, az áldozat költségére. Az ötrétegű utasításkészlet a modell biztonsági korlátainak megkerülését célozza, 74 támadóeszköz definícióját tartalmazza, és akár 100 000 műveleti lépést is engedélyez emberi jóváhagyás nélkül. A rögzített utasításkészlet önmagában nem bizonyítja a felsorolt támadások sikeres végrehajtását.

Mitigáció: A támadás a nem megfelelően védett AI-szolgáltatások hozzáférését használja ki. Az LLM API-kat és az MCP-kiszolgálókat hitelesítéssel kell védeni, az API-kulcsokat rendszeresen cserélni, a modellhasználat és a kapcsolódó költségek szokatlan növekedésére pedig riasztást kell beállítani. Az eszközöket használó AI-ügynökök jogosultságait és kimenő hálózati hozzáférését is korlátozni kell.

Forrás: Symantec

BUGSTER: korlátozott szakértelemmel is többféle támadást végzett AI-támogatással

A Unit 42 egy BUGSTER néven követett, pénzügyi motivációjú szereplő környezetét vizsgálta, aki a Hermes ügynökkeretrendszert és a DeepSeek V4 modellt használta hitelesítőadat-lopáshoz, adatbázis-kiszivárogtatáshoz, VoIP-csalás tervezéséhez, Wi-Fi-jelszavak töréséhez és C2-műveletekhez. A célpontok főként indiai szervezetek voltak; egy egyetem MongoDB-adatbázisából egy több mint 5 200 személyes adatot tartalmazó rekordot loptak el. A kutatók szerint a szereplő egyszerű eszközöket használt, és végig AI-generált szkriptekre támaszkodott.

Tanulság: Az AI részletes útmutatással és kódgenerálással csökkentheti egyes támadások végrehajtásának szakértelemigényét. A kutatók szerint a szereplő olyan tevékenységeket is végre tudott hajtani, amelyekhez korábban valószínűleg nem rendelkezett elegendő tudással.

Forrás: Unit 42

3 Állami hátterű és fejlesztőket célzó műveletek

KeyDrift: titkosítási kulcsok megszerzésére képes kártevő SD-WAN-vezérlőkön

A Cisco Talos szerint az UAT-11473 a Catalyst SD-WAN-vezérlők CVE-2026-20127 hitelesítésmegkerülési hibáját kihasználva telepítette a KeyDrift kártevő-keretrendszert. A legitim vezérlőfolyamatokba ágyazódó komponensek visszafejtett vezérlőforgalmat figyelnek meg, és titkosítási kulcsanyagot gyűjtenek. A célpontok között űr- és műholdas szolgáltatók, védelmi és repülőgépipari cégek, valamint szakpolitikai kutatóintézetek szerepeltek. A Talos nagy bizonyossággal jelentős infrastruktúra-átfedést állapított meg a Volt Typhoon Silent Train hálózatával; ez önmagában nem azonosítja a két szereplőt.

Mitigáció: Telepíteni kell a gyártói javításokat, követni az SD-WAN-rendszerek megerősítésére kiadott útmutatót, és keresni a kompromittálódás jeleit. Illetéktelen tevékenység észlelésekor incidenskezelést kell indítani, a kulcsanyag érintettségét pedig a gyártó támogatásával felmérni. A sérülékenység javítása önmagában nem távolítja el a már telepített kártevőt.

Forrás: Cisco Talos

Belarusz csoportok: egyre inkább orosz prioritásokat szolgálnak ki

Az ESET szerint a belarusz kötődésű csoportok műveletei egyre inkább Oroszország ukrajnai hírszerzési prioritásait tükrözik. Május végén a GhostWriter adattörlő kártevőt vetett be egy szállítmányozást támogató ukrán gyártó ellen – ez az első ilyen pusztító támadás, amelyet az ESET belarusz kötődésű csoporttól Európában dokumentált. A kutatók nem tudták eldönteni, hogy a cél a rombolás vagy a kémkedés nyomainak eltüntetése volt.

Tanulság: Az ESET értékelése szerint az eset precedenst teremthet: a kutatók szerint más belarusz kötődésű állami csoportok is bevethetnek adattörlő kártevőt a közeljövőben. Az ESET emellett az észak-koreai Ukrajna-fókusz erősödését is látja, köztük drónok iránti érdeklődést, de a közvetlen orosz háborús támogatásra kevésbé meggyőző a bizonyíték.

Forrás: The Record

sol-live: VS Code-beállításba rejtett hátsó kapu állásinterjús feladatban

A SlowMist egy sol-live nevű GitHub-tárolót elemzett, amely Solidity-interjúfeladatnak adja ki magát. A .vscode/settings.json fájlba rejtett parancs távoli szkriptet tölt le és futtat, amikor a felhasználó elindítja a projekt saját terminálkonfigurációját; a files.exclude szabály ráadásul elrejti a .vscode könyvtárat a VS Code fájlfájában. A kártevő képes böngészők bejelentkezési adatbázisainak,

tárcakiegészítők adatainak és macOS Keychain-fájloknak a gyűjtésére, fájlok feltöltésére, távoli parancsfuttatásra és a vágólap figyelésére. A SlowMist nyolc hasonló tárolót is azonosított.

Mitigáció: Ismeretlen projekt megnyitása előtt át kell nézni a .vscode/settings.json fájlt és a terminálindítási paramétereket, a feladatokat pedig elkülönített környezetben kell futtatni. Gyanú esetén a gépet izolálni kell, a kriptoeszközöket megbízható eszköz használatával új tárcába áthelyezni, és a kapcsolódó hitelesítő adatokat cserélni.

Forrás: SlowMist

4 Nagy léptékű adatszivárgások

So-net és plala: 2,59 millió előfizetői rekord került ki

A Sony Network Communications október 27-én közölte, hogy a So-net internetszolgáltatás tagsági adatbázisát illetéktelen hozzáférés érte. A behatolás október 19-én történt, az illetéktelen hozzáférést a vállalat október 23-án igazolta, és 24-én állapította meg a kiszivárgott adatok körét. Összesen 2 585 481 rekord érintett: 2 141 986 So-net- és 443 495 plala S csomaghoz tartozó tagsági adat, névvel, telefonszámmal, e-mail-címmel, felhasználói azonosítóval, születési dátummal, nemmel és internetkapcsolati azonosítóval. Az érintett So-net-ügyfelek egy részénél összesen 54 401 e-mail-cím és a hozzájuk tartozó jelszó is kiszivárgott; emellett 16 bankszámla adatai is érintettek. Az október 29-én frissített közlemény hét, jelszó-visszaállításhoz kiadott értesítés adatainak kiszivárgását is jelzi.

Mitigáció: A cég október 27-én biztonsági intézkedésként alaphelyzetbe állította az érintett e-mail-jelszavakat, ezeket újra be kell állítani. Aki ugyanazt a jelszót máshol is használta, ott is cserélje le. A szolgáltató nevében érkező, adategyeztetést kérő levelekre, SMS-ekre és hívásokra fokozottan érdemes figyelni.

Források: Sony Network Communications | So-net | ITmedia | NTT Docomo

Koppenhágai Egyetem: 525 ezer ember adata egy tesztkörnyezetből

A Koppenhágai Egyetem október 23-án jelentette be, hogy támadók hozzáfértek az egyik tesztkörnyezetéhez; az esetet október 20-án észlelték. Mintegy 525 ezer ember teljes neve, dán személyi azonosítója (CPR), munkahelyi és magántelefonszáma, valamint privát e-mail-címe érintett. Október 25-én derült ki, hogy mintegy 20 ezer munkatárs és hallgató belépőkártyájának PIN-kódja is illetéktelenekhez kerülhetett – a kódokat lecserélték, és átmenetileg korlátozták egyes kiemelt egyetemi helyszínek fizikai megközelítését.

Tanulság: Az eset a tesztkörnyezetekben tárolt személyes adatok kockázatára is rámutat. Ezekben a környezetekben is az adatok érzékenységéhez igazodó védelemre van szükség; ahol lehetséges, éles személyes adatok helyett szintetikus vagy megfelelően anonimizált tesztadatokat célszerű használni.

Forrás: Koppenhágai Egyetem | BleepingComputer

5 Beszállítói, szolgáltatói és közszolgáltatási incidensek

AfD: a párt saját tárhelyszolgáltatóján keresztül szivárgott ki 345 ezer e-mail-cím

A német AfD október 20-i közleménye szerint szeptemberben támadás érte egyik tárhelyszolgáltatóját, és néhány, többségében évek óta használaton kívüli postafiók tartalmát illetéktelenül lemásolták. A beszámolók a szolgáltatót a párt tulajdonában lévő Alternita Dienstleistungs GmbH-ként azonosítják. A Have I Been Pwned mintegy 345 ezer egyedi e-mail-címet rögzített az állományban; a The Register által idézett oknyomozó beszámoló szeptember 9-re teszi az első észlelést, míg a párt szeptember végi támadásról számol be. A támadás részletes lefolyását hivatalos forrás nem erősítette meg. A párt szerint csak néhány fiókot másoltak le, de elismeri a nagy mennyiségű adat kikerülését.

Tanulság: A 345 ezres szám az egyedi e-mail-címekre vonatkozik, nem a feltört postafiókok számára. A hack-and-leak műveleteknél az adatok nyilvánosságra hozatala tovább növelheti az incidens reputációs és üzleti hatását.

Források: AfD | The Register

Suzuki World: júliusi behatolás, októberi közlemény

A Suzuki kétkerekű üzletága október 14-én jelentette be, hogy a Suzuki World honlapon július 29-én illetéktelen hozzáférést észlelt, amire az oldal lezárásával és a támadási útvonal elvágásával reagált. Az üzemeltető partnerrel és külső szakértőkkel közösen végzett vizsgálat szerint a kapcsolatfelvételi űrlap naplóiban tárolt mintegy 4400, személyes adatokat tartalmazó bejegyzés – név, e-mail-cím, telefonszám, cím és a megkeresés tartalma – kerülhetett illetéktelen kezekbe.

Tanulság: A késedelmes tájékoztatás csökkentheti az érintettek lehetőségét arra, hogy időben felismerjék az adataikkal történő visszaéléseket. A kapcsolatfelvételi űrlapok naplói is tartalmazhatnak személyes adatokat, ezért ezekre is megőrzési időt és törlési szabályokat kell meghatározni.

Források: Suzuki World | Scan NetSecurity

Belga adóhivatal: napokkal a határidő előtt állt le a portál

A belga Szövetségi Pénzügyi Szolgálat október 28-án kibertámadás miatt ideiglenesen elérhetetlenné tette a MyMinfin adóügyi portált. A hatóság közlésekor nem volt adatlopásra utaló jel, de az esetleges adatkitettséget még vizsgálták. Az október 31-i bevallási határidővel érintett adózóknak haladékot ígértek, az új határidőt a hivatkozott beszámoló megjelenéséig nem közölték. A korábbi PHP-riasztással való összefüggést nem igazolták.

Tanulság: A közszolgáltatási incidenskezelésnek a technikai helyreállítás mellett az ügyfelek tájékoztatására, az alternatív ügyintézési lehetőségekre és az érintett határidők kezelésére is ki kell terjednie.

Forrás: The Record