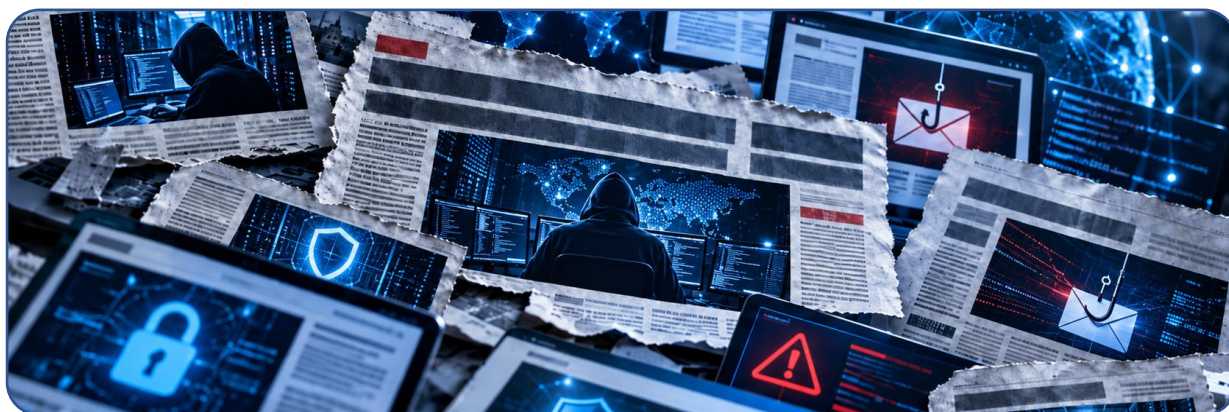


HETI HÍRÖSSZEFOGLALÓ



Kihasznált sérülékenységektől a reklámokon át terjesztett kémprogramokig

2026. október 12-16.

TARTALOMJEGYZÉK

- 01 VÁLLALATI INFRASTRUKTÚRA ÉS KIHASZNÁLT SÉRÜLÉKENYSÉGEK**
- 02 CÉLZOTT KÉMKEDÉS ÉS AI-VAL TÁMOGATOTT TÁMADÁSOK**
- 03 SZOLGÁLTATÁSMEGTAGADÁS, HACKTIVIZMUS ÉS FIZIKAI SZABOTÁZS**
- 04 ADATLOPÁS ÉS BESZÁLLÍTÓI INCIDENSEK**
- 05 ÁLDOZATOKAT CÉLZÓ CSALÁS**

BEVEZETÉS

A hét beszámolója a központi menedzsmentrendszerek és az AI-platformok sérülékenységeire, valamint a célzott megfigyelés új módszereire irányították a figyelmet. Egy FortiManager kompromittálása több mint ötszáz tűzfal konfigurációját érintette, a Langflow sérülékenységét célzó kihasználási kísérleteket pedig honeypot rendszerekben észlelték. Kutatók reklámok megjelenítésével indított, kattintást nem igénylő kémprogram-fertőzéseket is igazoltak. A szolgáltatáskiesések, valamint a japán Burger Kinget érintő nagyszabású adatlopás egyaránt rávilágítanak az üzletmenet-folytonosságot és az ügyfeladatok biztonságát fenyegető kockázatokra.

01 ÁLLAMI HÁTTERŰ ÉS CÉLZOTT MŰVELETEK

Fortinet: központi menedzsentrendszeren át támadtak egy távközlési szolgáltatót

A Unit 42 egy 2024 szeptemberében kezdődött behatolás vizsgálatát ismertette: a CL-STA-0954 szereplő a FortiManager CVE-2024-47575 hibáján keresztül több mint 500 FortiGate tűzfal konfigurációját és titkosítási adatait szerezte meg. Később a FortiOS CVE-2025-61624 sérülékenységet is kihasználta, és telepítette a memóriában működő PEERSTITCH kártevőt. Az ügyfelek hálózataiba történő behatolást a vizsgálat nem igazolta.

Mitigáció: A javítások mellett kompromittálás esetén a megszerzett hitelesítő adatokat, kulcsokat és tanúsítványokat is cserélni kell. Vizsgálandók a szokatlan auto-script konfigurációk és a gyártó által közölt memóriabeli indikátorok.

Forrás: [Unit 42](#)

Langflow: hitelesítés után kód futtatást enged az MCP-konfiguráció hibája

A Langflow CVE-2026-105740 sérülékenysége (CVSS 9,9) az MCP-kiszolgálók stdio-konfigurációján keresztül tesz lehetővé távoli kód futtatást. Egy egyszerű felhasználói fiókkal megadott parancs ellenőrzés nélkül, a Langflow folyamatának jogosultságaival fut le a kiszolgálólista lekérésekor. A Previdian szeptember 19. óta észlelt kihasználási kísérleteket csapdarendszerében; ezekből az éles rendszereken végrehajtott, sikeres támadások száma nem állapítható meg.

Mitigáció: A hiba az 1.9.0-s kiadásban javított. Telepítsék a megfelelő biztonsági frissítéseket, korlátozzák a hálózati hozzáférést, és ellenőrizzék az MCP-kiszolgálók beállításait, valamint a hitelesítési naplókat.

Forrás: [Previdian](#) | [The Hacker News](#)

02 CÉLZOTT KÉMKEDÉS ÉS AI-VAL TÁMOGATOTT TÁMADÁSOK

C2Agent: nyelvi modell irányítja a fertőzött gépen végzett műveleteket

A Unit 42 által azonosított C2Agent Windows-kártevő egy nagy nyelvi modellre bízta a támadói cél eléréséhez szükséges műveletek kiválasztását, majd végrehajtja azokat a fertőzött gépen. A Go nyelven írt eszköz MCP-kapcsolatokat és feladatspecifikus utasításokat használ; parancsfuttatásra, felderítésre és adatkimentésre képes. Egyes változatai a célpont gépén már telepített AI-fejlesztőeszközöket is bevonhatják.

Mitigáció: Figyelni kell az AI-fejlesztőeszközök szokatlan háttérfolyamatait, parancsfuttatását és hálózati kapcsolatait; az ismert kártevőminták és C2-indikátorok alapján célzott vizsgálat végezhető.

Forrás: [Unit 42](#) | [PolySwarm](#)

Reklámokkal terjesztett kémprogram: a fertőzéshez kattintás sem szükséges

A Citizen Lab technikai bizonyítékokkal támasztotta alá, hogy az Al Jazeera eszközeit célzott online hirdetések keresztül fertőzték meg a Candiru kémprogramjával. A Discover-Tech infrastruktúrája a reklám megjelenésekor kódot töltött be a kiválasztott célpont eszközére, felhasználói kattintás nélkül. Kormányzati és nemzetközi szervezetek hálózatain is megjelentek ilyen hirdetések, de ez önmagában nem bizonyít sikeres fertőzést.

Tanulság: A kattintások kerülése ennél a módszernél nem elegendő. A hirdetési infrastruktúrához kapcsolódó forgalom vizsgálata és a közzétett támadói indikátorok keresése is szükséges lehet.

Forrás: [The Record](#)

Kimsuky: ukrán szakértőket céloznak háborús információért

A Genians szerint az észak-koreai Kimsuky az Operation GitPower kampány részeként ukrán diplomáciai és biztonságpolitikai szakértőket célzott. Hamis konferenciameghívásokkal és kutatási együttműködés ígéretével építettek bizalmat, majd rosszindulatú dokumentumokat és hivatkozásokat küldtek. A kutatók szerint a cél a háborúról, az észak-koreai veszteségekről és a hadifoglyokról szóló információgyűjtés lehetett; a megfigyelt támadási kísérletek többsége sikertelen volt.

Védekezés: A szakmai meghívásokat a szervező ismert elérhetőségén, külön csatornán kell ellenőrizni. A valós rendezvényadatok és az ártalmatlan első levél nem igazolják a később érkező fájlok megbízhatóságát.

Forrás: [The Record](#)

3 Szolgáltatásmegtagadás, hacktivizmus és fizikai szabotázs

SkyNet: napokig zavarta támadás a szentpétervári szolgáltatót

A SkyNet internetszolgáltató szerint október 6. óta DDoS-támadás zavarta hálózatát, az online játékokat, a hanghívásokat és a videokonferenciákat is érintve. A BO Team ukrán hackercsoport szeptemberi és októberi támadásokat vállalt magára, és több mint 15 000 hálózati eszköz működésképtelenné tételét állította. A szolgáltató sem ezt, sem a belső rendszereihez való jogosulatlan hozzáférést nem erősítette meg.

Tanulság: A szolgáltató által megerősített DDoS-támadást külön kell kezelni a behatolásról és az eszközök működésképtelenné tételéről szóló, nem igazolt támadói állításoktól.

Forrás: [The Record](#)

Canonical: DDoS-támadás zavarta az Ubuntu webes szolgáltatásait

A Canonical október 8-án tartós DDoS-támadásról számolt be. Az Ubuntu és a Canonical weboldalai mellett a biztonsági közlemények és az API-juk elérésében is fennakadások voltak; a beszámolók valamivel több mint négyórás kiesést említene. A Launchpad, a Snap Store és a csomagtárak működtek. Az elkövető kiléte és a korábbi, szélesebb szolgáltatáskört érintő támadással való kapcsolata nem ismert.

Tanulság: A biztonsági közlemények elérhetetlensége a rájuk épülő automatizált ellenőrzéseket is akadályozhatja, akkor is, ha a szoftvercsomagok továbbra is letölthetők.

Forrás: [SecurityWeek](#) | [Ubunlog](#)

4 Adatlopás és beszállítói incidensek

Burger King Japan: mintegy 11,18 millió tagsági adatrekord szivárgott ki

A Burger King japán üzemeltetője szerint október 2–7. között illetéktelenek fértek hozzá az alkalmazás tagsági adatainak rendszeréhez. Mintegy 11,18 millió rekord került ki, köztük nevek, e-mail-címek, telefonszámok és születési dátumok. Bankkártyaszámot a rendszer nem tárolt; jelszavak kiszivárgását a közlemény idején nem igazolták. A behatolás pontos okát külső szakértők bevonásával vizsgálják.

Védekezés: Az üzemeltető a nevében érkező gyanús e-mailekre, SMS-ekre és telefonhívásokra figyelmeztet; ilyen megkeresésben ne nyissanak meg hivatkozást vagy mellékletet, és ne adjanak meg jelszót.

Források: [Burger King Japan](#)

Housing Ombudsman: beszállítói incidens zavarta az ügykezelést

A brit Housing Ombudsman Service október 13-án közölte, hogy külső szolgáltatójának IT-biztonsági incidense érintette az ügykezelő rendszerét. Az online panaszbeadás kiesése miatt az ügyfeleket telefonos és e-mailes kapcsolattartásra irányították. A szervezet szerint az incidenst megfékeztek; a személyes adatok érintettségét még vizsgálják. Az esetet bejelentették a brit adatvédelmi hatóságnak, az ICO-nak.

Védekezés: A szervezet arra kéri az érintetteket, hogy a váratlan megkeresésekre csak a feladó kilétének ellenőrzése után adjanak meg személyes adatot.

Forrás: [Housing Ombudsman](#) | [BleepingComputer](#)

5 Áldozatokat célzó csalás

Segítség ígéretével csaltak ki pénzt szexuális zsarolás áldozatokról

Az amerikai Szövetségi Kereskedelmi Bizottság (FTC) keresete szerint a Digital Forensics Corporation legalább 60 millió dollárt csalt ki szexuális zsarolás áldozataitól. A cég a megígért segítség helyett állítólag kitalált beszélgetési naplókcal és előre elmentett helyadatokkal hitette el, hogy felderítette a zsarolókat. A bíróság ideiglenesen leállította a működését; az ügyben még nincs végleges döntés.

Tanulság: Figyelmeztető jel, ha egy segítséget ígérő vállalkozás félelemkeltéssel sürgeti a fizetést, vagy lebeszéli az áldozatot a hatóságok megkereséséről.

Forrás: [The Record](#)