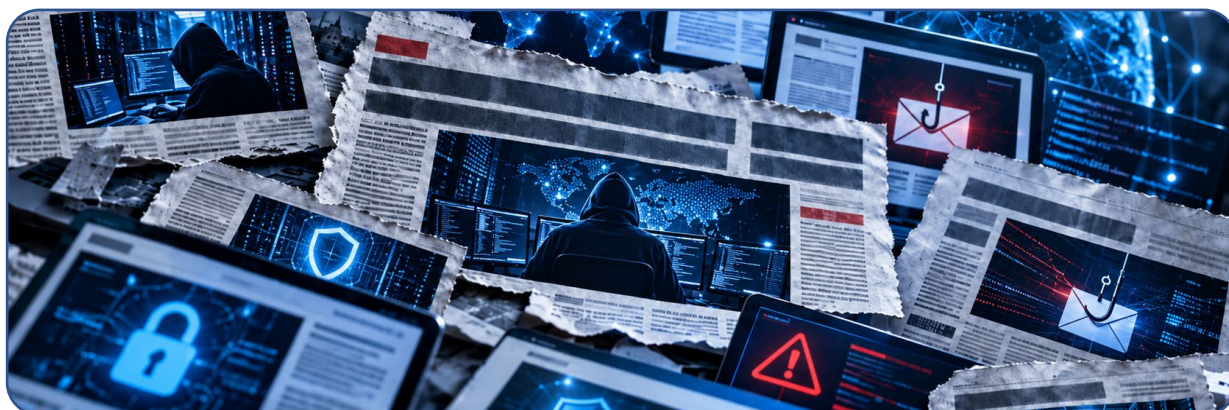


HETI HÍRÖSSZEFOGLALÓ



Jogosulatlan HTTPS-tanúsítványoktól a nemzetközi kiberműveletek felszámolásáig

2026. október 05-10.

TARTALOMJEGYZÉK

- 01 ÁLLAMI HÁTTÉRŰ ÉS CÉLZOTT MŰVELETEK**
- 02 A BIZALMI INFRASTRUKTÚRA ELLENI TÁMADÁSOK**
- 03 SOCIAL ENGINEERING ÉS TÁVOLI HOZZÁFÉRÉS**
- 04 ZSAROLÓVÍRUS ÉS NAGY LÉPTÉKŰ ADATSZIVÁRGÁS**
- 05 BŰNÜLDÖZÉS ÉS SZAKPOLITIKA**

BEVEZETÉS

A héten több esemény a digitális bizalmi infrastruktúra és a beszállítói láncok sérülékenységeire mutatott rá. Három országhód szerinti legfelső szintű domain infrastruktúrájának kompromittálásával jogosulatlan HTTPS-tanúsítványokat szereztek, miközben kutatók már értékesítés előtt fertőzött Android-készülékeket azonosítottak. Egy nemzetközi hatósági akcióban a Flax Typhoonhoz köthető infrastruktúra egy részét is lefoglalták. A célzott adathalász kampányok és a SharePoint-sérülékenységek kihasználása mellett kiemelt figyelmet kapott a dán CPR-nyilvántartás mintegy 8,8 millió személy adatait érintő incidense.

01 ÁLLAMI HÁTTERŰ ÉS CÉLZOTT MŰVELETEK

Flax Typhoon: nemzetközi akcióban foglalták le a kínai vállalat eszközeit

Az FBI és az amerikai igazságügyi minisztérium hét domaint foglalt le, amelyek a pekingi Integrity Technology Group két eszközét – a MicroScan sérülékenységvizsgálót és a FishHub adathalász és támadástámogató platformot – szolgálták ki. A hatóságok szerint a cég szerződéses kapcsolatban áll a kínai állammal, eszközeit pedig a Flax Typhoon néven ismert kampányban használták. Ezzel párhuzamosan tíz ügynökség hét országból 58 oldalas [közös közleményt](#) adott ki.

Tanulság: A nemzetközi közlemény IoC-eket és technikai leírásokat közöl, többek között Exchange-rendszereket célzó jelszópróbálgatásról és Active Directory-hitelesítő adatok gyűjtéséről. A közzétett indikátorok alapján visszamenőleges vizsgálat indokolt; a lefoglalt domainek nem jelentik a támadóeszközök megszűnését.

Forrás: [The Record](#)

TA419: amerikai AI-szakpolitikai szakértőket céloznak megsemmisítéssel

A Proofpoint szerint a Kínához köthető TA419 júliusban több hitelesítőadat-halász kampányt futtatott: ismert közigazdászokat és AI-szakpolitikusokat – köztük a Fehér Ház tudománypolitikai hivatalának egy korábbi vezetőjét – megsemmisítve célzott agytrösztökben, egyetemeken és ügyvédi irodákban dolgozó szakértőket; februárban egy Anthropic-munkatárs nevében is küldtek levelet. Az első üzenet ártalmatlan, a követő levél rövidített linken át egy módosított Frameless BitB AiTM-készlethez vezet, amely munkamenetsütit is lop.

Mitigáció: Az eredethez kötött, adathalászatnak ellenálló hitelesítési módszerek, például a FIDO2-alapú hozzáférési kulcsok jelentősen csökkenthetik a leírt közbeékelődéses adathalászat eredményességét, de önmagukban nem védenek minden munkamenet-eltérítési módszer ellen. A rövidített linkeket tartalmazó szakmai megkereséseket másik csatornán is ellenőrizni kell. A Proofpoint kompromittálódási indikátorokat is közölt.

Forrás: [Proofpoint](#) | [Undercode News](#)

Blinder Tunnel: hamis állásinterjúval az iraki kritikus infrastruktúra ellen

A Unit 42 szerint egy nagy bizonyossággal Iránhoz köthető szereplő (CL-STA-1178) a dubaji repülőtér IT-részlegének adta ki magát, és trójaivá tett Visual Studio kódolási feladatot küldött egy iraki kritikus infrastruktúrában dolgozó szoftvermérnöknek. A .csproj build-fájl AppDomainManager-eltérítést és DLL sideloadingot indít, majd telepíti a ShelbyLoader V2 betöltőt és a ShelbyC2 V2 távoli hozzáférési eszközt. A vezérlés GitHub-tárolókon és -issue-kon keresztül működik.

Mitigáció: Az ismeretlen eredetű fejlesztői feladatokat csak elkülönített, ellenőrzött környezetben szabad futtatni. Indokolt az msbuild.exe szokatlan gyermekfolyamatainak, valamint a GitHub API-val kommunikáló, nem megszokott folyamatoknak a vizsgálata.

Forrás: [Unit 42](#)

02 A BIZALMI INFRASTRUKTÚRA ELLENI TÁMADÁSOK

ccTLD-infrastruktúra kompromittálása: jogosulatlan HTTPS-tanúsítványok Google-domainekre

Támadók a .gh, .sl és .as országkód szerinti legfelső szintű domainek (ccTLD-k) infrastruktúráját kompromittálták. Az irányadó DNS-rekordok módosításával jogosulatlan HTTPS-tanúsítványokat szereztek Google- és más szervezetek domainjeire. A Google szerint nincs ok feltételezni, hogy a tanúsítványkibocsátók hibáztak volna, és saját rendszereit sem kompromittálták. A Chrome CRLSets segítségével blokkolta az azonosított tanúsítványokat, továbbá együttműködött a kibocsátókkal azok visszavonásában.

Mitigáció: A szervezeteknek érdemes folyamatosan figyelniük a Certificate Transparency naplókat a teljes domainportfólióra, ideértve a parkolt és regionális domainneveket is. Korlátozó CAA-rekordok és – ahol támogatott – ACME-fiókhoz kötött kibocsátási szabályok alkalmazása ajánlott. Ezek aktív DNS-eltérítés alatt nem nyújtanak teljes védelmet, de az ellenőrzés helyreállítása után csökkenthetik az újabb jogosulatlan kibocsátás kockázatát.

Forrás: [Google Chrome Security](#)

03 SOCIAL ENGINEERING ÉS TÁVOLI HOZZÁFÉRÉS

ASOS: egyetlen megszerzett munkavállalói fiókból ügyféladat-szivárgás

A brit ASOS megerősítette, hogy egy támadó megbízható kapcsolatnak adva ki magát megszerezte egy munkatárs bejelentkezési adatait, majd ezekkel harmadik feles platformokon tárolt adatokhoz fért hozzá. Nevek és elérhetőségek kerülhettek ki; fizetési adat és fiókjelszó nem. Az eset október 6-án vált nyilvánossá, amikor az ASOS saját alkalmazásán keresztül push-üzenet került kiküldésre a vásárlóknak, amelyben a magát Xuanye Groupnak nevező támadó követelt kapcsolatfelvételt.

Tanulság: A közlések szerint az ASOS-fiókok jelszavai és a fizetési adatok nem voltak érintettek. A megszerzett nevek és elérhetőségek ugyanakkor célzott adathalász támadásokhoz használhatók, ezért az ASOS nevében érkező megkereséseket fokozott óvatossággal kell kezelni. Szervezeti oldalon a külső ügyfélkommunikációs platformok hozzáférési jogosultságainak szigorú kezelése indokolt.

Forrás: [The Record](#) | [BleepingComputer](#)

MSP360 és ScreenConnect: két legitim távfelügyeleti eszköz egy támadási láncban

A Microsoft olyan adathalász kampányokat figyelt meg, amelyekben meghívónak, PDF-nek vagy szoftverfrissítésnek álcázott, valódi és aláírt MSP360 RMM-telepítő érkezik. A UAC-jóváhagyás után az eszköz szolgáltatásként települ, majd PowerShell-lel csendben feltelepít egy ConnectWise ScreenConnect-klienst is, így a támadónak két, egymástól független távoli hozzáférése marad. Sérülékenységet egyik termékben sem használtak ki; a visszaélés a legitim működésre épül.

Mitigáció: A szervezeteknek nyilván kell tartaniuk az engedélyezett RMM-eszközöket, és alkalmazásvezérléssel (például AppLocker vagy WDAC használatával) korlátozniuk kell a nem engedélyezett szoftverek futtatását. Emellett célszerű riasztást beállítani új ScreenConnect-szolgáltatás létrehozására, valamint arra, ha egy gyanús állomány megnyitását rövid időn belül távoli hozzáférést biztosító eszköz telepítése vagy elindítása követi.

Forrás: [Microsoft](#)

04 ZSAROLÓVÍRUS ÉS NAGY LÉPTÉKŰ ADATSZIVÁRGÁS

Warlock: továbbra is kihasználják a SharePoint-sérülékenységeket

A Symantec szerint a Longlegs (más néven Storm-2603) néven követett, Kínához köthető csoport az elmúlt két hónapban legalább négy szervezetet támadott meg portugál és spanyol nyelvterületen: két kritikus infrastruktúra-üzemeltetőt (egy vízművet és egy távközlési szolgáltatót), egy regionális önkormányzatot és egy egyetemet. A belépő továbbra is a javítatlan, helyben üzemeltetett SharePoint: webshell a LAYOUTS könyvtárba, majd az ASP.NET machine key ellopása aláírt kérések hamisításához.

Mitigáció: A SharePoint ToolShell-javításait telepíteni kell, a már kompromittált farmokon pedig a gépkulcs (machine key) cseréje is szükséges. Figyelní kell a K7RKScan sérülékeny illesztőprogram betöltésére és a SYSVOL megosztásból induló, nem adminisztratív műveletekre.

Források: [Symantec](#) / [Security.com](#) | [SecurityWeek](#)

Dánia: 8,8 millió nyilvántartott személy adataihoz férhettek hozzá

A dán hatóságok október 5-én közölték, hogy illetéktelenek egy magánvállalat jogszerű CPR-lekérdezési jogosultságával visszaélve mintegy 8,8 millió nyilvántartott személy adataihoz férhettek hozzá, köztük nevekhez, címekhez és CPR-azonosítókhoz. A nyilvántartás az elhunytak és az országból elköltözöttek adatait is tartalmazza, ezért az érintett rekordok száma nem azonos Dánia jelenlegi lakosságával. A hozzáférést megszüntették; a visszaélés pontos módja a rendelkezésre álló tájékoztatásból nem állapítható meg.

Tanulság: A külső szervezeteknek kiadott jogosultságokat rendszeresen felül kell vizsgálni. A nagy volumenű vagy szokatlan lekérdezések észlelése és korlátozása csökkentheti az ilyen visszaélések kockázatát.

Forrás: [CyberInsider](#)

05 BŰNÜLDÖZÉS ÉS SZAKPOLITIKA

Qilin: Oszakában fogták el, Németországnak adták ki a gyanúsítottat

A CyPro beszámolója szerint a japán hatóságok Oszakában őrizetbe vettek egy 28 éves orosz állampolgárt, akit a Qilin zsarolóvírus-csoporthoz kötnek, majd október 2-án átadták Németországnak. A német eljárás egy logisztikai vállalatot ért zsarolóvírusos támadáshoz kapcsolódik. A gyanúsított szerepére és a kiadatási eljárás jogi sajátosságaira vonatkozó részletekhez további elsődleges hatósági megerősítés szükséges.

Tanulság: Az eset jól mutatja, hogy a határokon átnyúló bűnüldözési együttműködés fontos a zsarolóvírusos ügyek felderítésében. Egy gyanúsított elfogása önmagában nem jelenti a teljes csoport működésének megszűnését.

Forrás: [CyPro](#)

„Putyin-adó”: becslés az orosz ellenséges tevékenység brit gazdasági költségéről

Graeme Downie brit parlamenti képviselő és Dominic Reed elemzése évi 2–2,5 milliárd fontra becsüli az Oroszországhoz köthető kibertámadások, szabotázs és kritikus infrastruktúrát érintő fenyegetések brit gazdasági költségét. Az összeg nem közvetlenül mért kár, hanem feltételezéseken alapuló becslés. Egyik fontos összetevője az a feltevés, hogy a brit vállalkozások 14,7 milliárd fontos kiberbűnözési veszteségének 10 százaléka Oroszországhoz köthető, azonban ezt nem egyedi incidensek bizonyított attribúciója alapján határozták meg.

Tanulság: A jelentés a közvetlen helyreállítási költségeken túl az ellenséges állami tevékenység szélesebb gazdasági hatásainak mérését sürgeti. A becslést ezért nem szabad igazolt veszteségadatként értelmezni.

Forrás: [The Record](#)