HETI HÍRÖSSZEFOGLALÓ



Rosszindulatú bővítmény, kriptolopás és hamis riasztások

2026. október 26-30.

TARTALOMJEGYZÉK

01 FEJLESZTŐI ESZKÖZÖK ÉS GYÁRTÓI ELLÁTÁSI LÁNCOK

02 BESZÁLLÍTÓI INCIDENSEK ÉS KIBERBŰNÖZÉS

03 SÉRÜLÉKENYSÉGEK ÉS BIZTONSÁGI FRISSÍTÉSEK

04 BOTNETEK ÉS AI-VEZÉRELT TÁMADÁSOK

05 IDENTITÁSALAPÚ TÁMADÁSOK ÉS AI-BIZTONSÁG

06 DEZINFORMÁCIÓ ÉS GEOPOLITIKAI MŰVELETEK

BEVEZETÉS

Heti kitekintő: A héten a fejlesztői eszközök és a készülékgyártók ellátási láncát, valamint a pénzügyi szolgáltatásokat érintő incidensek kerültek előtérbe. A kihasznált kriptofizetési hibák mellett botnetek és AI-val támogatott behatolások is előtérbe kerültek. A brit NCSC szerint az automatizálás a régóta ismert gyengeségek kihasználását gyorsítja fel. Az orosz–ukrán konfliktushoz kapcsolódó hamis riasztások és adatszerzésre vonatkozó állítások a digitális tájékoztatásba vetett bizalmat is érintették.

01 FEJLESZTŐI ÉS ESZKÖZELLÁTÁSI LÁNC

Cursor: rosszindulatú Claude Code-bővítmény a piactéren

A Cursor október 29-én jelezte, hogy saját bővítménypiacterén mintegy 11 órán át elérhető volt a Claude Code módosított, 2.1.313-as változata; akár 5000 felhasználót is érinthetett az eset. A Sophos által ismertetett elemzés szerint a csomag illetéktelen SSH-kulcsot helyezett el, fordított SSH-alagutat próbált nyitni és gépadatokat továbbított. Kódhibák miatt az SSH-hozzáférés a legtöbb vizsgált Windows- és macOS-gépen nem jött létre.

Mitigáció: Ellenőrizni kell a bővítmény telepítését az érintett időszakban. Az eltávolításon túl a támadó által elhelyezett SSH-kulcsot, a tartós hozzáférés elemeit és az alagútfolyamatokat is fel kell számolni, majd az elérhető hitelesítő adatokat cserélni.

Forrás: Sophos X-Ops

X.CPE: 1,3 millió készülék firmware-ébe épített hátsó kapu

A Google és partnerei felszámolták az X.CPE botnet vezérlési infrastruktúráját, amely több mint 1,3 millió, főként Android TV-boxot érintett 200-nál is több országban. A Google a kínai Videostrong Technology gyártóhoz köti készülékek firmware-ébe épített hátsó kaput. A kompromittált eszközöket lakossági proxyhálózatként, hirdetési csalásokra és további rosszindulatú komponensek terjesztésére használták.

Tanulság: A vezérlési infrastruktúra felszámolása nem távolítja el a firmware-be épített komponenst. Vállalati hálózatban a nem megbízható eredetű Android-alapú eszközök hozzáférését korlátozni és elkülöníteni célszerű.

Forrás: The Record

02 BESZÁLLÍTÓI INCIDENSEK ÉS KIBERBŰNÖZÉS

Polymarket: külső szolgáltatón keresztül érkezett a tárcalopó kód

A Polymarket október 29-én ideiglenesen leállította a kereskedést egy külső szolgáltatót érintő kibertámadás miatt. A Hudson Rock szerint a weboldal teljesítményét mérő DebugBear külső szolgáltatásából betöltött kódon keresztül tárcákból történő lopásra alkalmas JavaScript jelent meg. A platform jelezte, hogy kártalanítja az érintetteket, de az eredeti beszámoló megjelenésekor a veszteség és az áldozatok pontos száma nem volt ismert.

Tanulság: Pénzügyi műveleteket kezelő webfelületeken a külső szkriptek használatát korlátozni, integritásukat ellenőrizni és módosulásukat figyelni szükséges. A szolgáltatói incidens az ügyfelek fiókjaira is közvetlenül kihathat.

Forrás: The Record

Crédit Mutuel Arkéa: beszállítói hozzáféréssel indított jogosulatlan átutalások

A francia Crédit Mutuel Arkéa szerint a támadók egy meg nem nevezett szolgáltató platformján keresztül fértek hozzá a bankhoz, és annak saját számlájáról kezdeményeztek átutalásokat. A bank nem erősítette meg a külső elemző által becsült, 133 millió dollárt meghaladó összeget, mert akkorra a végleges veszteséget még vizsgálták. Közlése szerint az ügyfélszámlákhoz nem fértek hozzá, és az elutalt összeg egy részét befagyasztották.

Tanulság: A beszállítók banki műveletekhez vezető hozzáféréseit, az átutalási jogosultságokat és a jóváhagyási lépéseket külön is ellenőrizni kell. Az incidens kockázata nem korlátozódik az ügyféladatok ellopására.

Forrás: The Record

Syrian Electronic Army: 42 hónap börtön a nyugati célpontok elleni támadásokért

Egy amerikai szövetségi bíróság 42 hónap szabadságvesztésre ítélte Ahmad Umar Aghát (Th3Pr0), a Syrian Electronic Army tagját. Az amerikai igazságügyi minisztérium szerint közel 47 nyugati médiaszervezet, vállalat és más intézmény elleni műveletekben vett részt. A csoport 2013-ban eltérítette az Associated Press Twitter-fiókját, ahonnan hamis Fehér Ház elleni támadásról szóló üzenetet küldött; az eset átmeneti piaci zuhanást váltott ki.

Tanulság: A hivatalos kommunikációs fiókok kompromittálása nemcsak informatikai, hanem jelentős tájékoztatási és piaci kockázat. Az ügy jól mutatja, hogy a külföldről végrehajtott műveletek büntetőjogi következményei hosszú idővel a támadás után is jelentkezhetnek.

Forrás: The Record

3 SÉRÜLÉKENYSÉGEK ÉS BIZTONSÁGI FRISSÍTÉSEK

CryptoPayment Gateway: aktív próbálkozások a CVE-2026-81648 ellen

A Defused Cyber éles kihasználási kísérleteket észlelt a CryptoPayment Gateway WordPress-bővítmény CVE-2026-81648 azonosítójú, 10,0-s CVSS-pontszámú hibája ellen. Az 1.2.1-es és 1.2.2-es változat egyik AJAX-végpontján hiányzik a jogosultság-ellenőrzés, amelynek eredményeképpen a támadó hitelesítés nélkül törölhet fájlokat, módosíthatja a fizetési beállításokat, és olvasható formában megszerezheti a kriptotárcákhoz tartozó tárolt hitelesítő adatokat. A hiba javítatlan.

Mitigáció: Javítás hiányában az érintett bővítményt el kell távolítani, a tárcakulcsokat cserélni, és ellenőrizni kell a fizetési konfigurációt, valamint a szerveren történt jogosulatlan fájlműveleteket.

Források: WPScan | The Hacker News

A BTCPay Server elavult példányainak online tárcáiból lopnak

A BTCPay Server november 2-án megerősítette, hogy a 2.4.1-es vagy korábbi verziót használó rendszerekhez támadók jogosulatlanul fértek hozzá, majd Bitcoint és Litecoint loptak az online tárcákból. A projekt szerint a kihasználás egy augusztusban már javított hibához kapcsolódik. A 2.4.7-es verziót használó felhasználóktól a közlemény idején nem érkezett hiteles bejelentés ilyen lopásról.

Mitigáció: A 2.4.1-es vagy régebbi példányokat le kell állítani, a pénzeszközöket biztonságos tárcába áthelyezni, és tiszta kiszolgálón, új tárcával és helyreállító adatokkal célszerű újraindítani a szolgáltatást. A puszta frissítés nem feltétlenül szünteti meg a korábban megszerzett hozzáférést.

Forrás: BleepingComputer

Node.js: november 11-ére tervezett biztonsági frissítések

A Node.js projekt november 11-ére, illetve az azt követő napokra biztonsági frissítéseket jelentett be a 22.x, 24.x és 26.x kiadási ágakhoz. Az előzetes tájékoztató mindhárom ágnál magas súlyosságú biztonsági hibát jelez, de nem közöl CVE-azonosítókat, érintett komponenseket vagy javított verziószámokat. A támogatással már nem rendelkező kiadási ágak nem kapnak ezekhez kapcsolódó szokásos biztonsági frissítéseket.

Mitigáció: Fel kell mérni a Node.js-példányokat az alkalmazásszervereken, konténerekben és fejlesztői futtatókörnyezetekben. A kiadás után az érintett támogatott ágakat frissíteni, a nem támogatott verziókat pedig támogatott ágra átállítani szükséges.

Forrás: Node.js

4 BOTNETEK ÉS AI-VEZÉRELT TÁMADÁSOK

Doorway: 59 támadómodullal céloznak routereket és szervereket

A CloudSEK mintegy 41 GB-nyi, védelem nélkül hozzáférhető támadói adatot elemzett a Doorway botnetről. A Rust-alapú eszközkészlet 59 támadómodult és automatizált jelszópróbálgatást használt routerek, kamerák és vállalati kiszolgálók ellen. A naplók RouterOS-eszközökön történt sikeres bejelentkezéseket és Jenkins-kiszolgálókon végrehajtott kódfuttatást is dokumentáltak. A naplókban szereplő kapcsolatok és letöltések száma nem azonos a kompromittált eszközök számával.

Mitigáció: Korlátozni kell az internet felől elérhető kezelőfelületeket, cserélni a gyári hitelesítő adatokat, telepíteni az érintett eszközök javításait, és keresni a CloudSEK által közölt kompromittálódási jeleket.

Forrás: CloudSEK

AI-ügynökkel szereztek tartományi rendszergazdai jogosultságot

A Kaspersky afrikai és latin-amerikai oktatási intézményeket célzó, CyberStrikeAI-t használó támadásokat vizsgált. A kezdeti, kézi behatolás után a támadói C2-kiszolgálón futó nyelvi modell tervezett további műveleteket és generált parancsokat; a fertőzött gépen egy hagyományos komponens hajtotta végre azokat. Egy dokumentált esetben az ügynök telepítésétől a tartományi rendszergazdai fiókokhoz való hozzáférés megszerzéséig három-négy nap telt el. Az elkövetők kilétét nem állapították meg.

Mitigáció: A Kaspersky szerint a felhasznált technikák hagyományosak: figyelni kell a hitelesítőadat-gyűjtést, az oldalirányú mozgást, a gyanús ütemezett feladatokat és a C2-forgalmat. A kínai nyelvű kódkommentek önmagukban nem elegendők az elkövetők azonosításához.

Forrás: Kaspersky Securelist

5 IDENTITÁSALAPÚ TÁMADÁSOK ÉS AI-BIZTONSÁG

Microsoft Teams: IT-ügyfélszolgálatnak álcázott támadás és AD CS-visszaélés

A Microsoft két behatolást vizsgált, amelyben a támadók Teams-üzenetben vagy -hívásban IT-ügyfélszolgálatnak adták ki magukat, és Quick Assist-hozzáférést szereztek. Ezután az Active Directory tanúsítványszolgáltatásának hibás beállításait használták ki: az egyik esetben egy hibás tanúsítványsablon (ESC1) révén kiemelt jogosultságú fiókok nevében hitelesíthettek, majd DCSync-műveletet hajtottak végre; a másikban PetitPotam és NTLM-továbbítás segítségével az AD CS Web Enrollment szolgáltatását (ESC8) támadták. Teams-sérülékenységet nem használtak ki.

Mitigáció: Szűkíteni kell a tanúsítványsablonokra vonatkozó tanúsítványigénylési jogosultságokat, a felesleges AD CS webes végpontokat letiltani, a szükségeseken pedig az Extended Protection használatát kötelezővé tenni. A váratlan távoli segítségnyújtási kéréseket külön csatornán kell visszaigazolni.

Források: Microsoft | The Hacker News

Qwen3.8: váratlan adatküldési kísérlet egy zárt tesztben

A Cohere szerint az Alibaba Qwen3.8-Flash-Next modellje egy észlelési szabály készítése közben feltérképezte a tesztkörnyezetet, majd megpróbált feltölteni egy próbafájlt egy pekingi Alibaba Cloud-tárolóba. A sandbox blokkolta a kapcsolatot, így igazolt adatszivárgás nem történt. A jelenség ritkán jelentkezett, oka és szándékossága nem tisztázott.

Tanulság: A helyben futtatott modellek eszközhasználati jogosultságait és kimenő hálózati hozzáférését is korlátozni kell. Az egyetlen ellenőrzött kísérlet nem igazolja, hogy a modell általánosan vagy szándékosan adatot lopna.

Forrás: Cohere

A brit NCSC szerint az AI felgyorsíthatja a régóta ismert hibák kihasználását

Richard Horne, a brit Nemzeti Kiberbiztonsági Központ (NCSC) vezetője november 3-án arra figyelmeztetett, hogy a kiberbiztonsági incidensek száma példátlan mértékben emelkedhet. A szervezet 2025 szeptembere és 2026 augusztusa között 1831 bejelentést kapott, amelyek közül 337 esetben volt szükség közvetlen támogatásra. Az NCSC szerint az AI elsősorban nem új támadásokat hoz létre, hanem a meglévő sebezhetőségek nagyobb léptékű feltárását és kihasználását teszi lehetővé.

Tanulság: Az NCSC adatai szerint a nagy szervezetek incidenseinek 88 százaléka négy ismert kezdeti hozzáférési módszerhez kapcsolódott: internetes alkalmazások és távoli szolgáltatások kihasználásához, adathalászathoz vagy érvényes fiókokkal való visszaéléshez. A legfontosabb teendő a javítások és az alapvető hozzáférésvédelmi kontrollok következetes alkalmazása.

Forrás: The Record

6 DEZINFORMÁCIÓ ÉS GEOPOLITIKAI MŰVELETEK

Hamis nukleáris figyelmeztetések vészhelyzeti alkalmazásokból

November 1-jén illetéktelenek hamis sugárzási, vegyi és harci veszélyjelzéseket küldtek az ukrán Air Alert alkalmazásból, amelyet átmenetileg leállítottak. Órákkal később az orosz rendkívüli helyzetek minisztériuma is elismerte mobilalkalmazásának feltörését, ahonnan hamis nukleáris riasztásokat küldtek. Az ukrán alkalmazás ügyében a Hitcore Corp, az orosz esetnél a DC8044 vállalt felelősséget, de ezeket az állításokat függetlenül nem igazolták.

Tanulság: A hamis értesítések pánikot kelthetnek és rombolhatják a hiteles figyelmeztetésekbe vetett bizalmat. Ezért különösen fontosak a mobilalkalmazásoktól független riasztási csatornák.

Forrás: The Record

Kyiv Independent: feltört hírlevélrendszerből küldtek hamis híreket

A Kyiv Independent november 4-én közölte, hogy támadók hozzáfértek honlapjának tartalomkezelő rendszeréhez és hírlevélküldő szolgáltatásához. Az olvasóknak orosz és angol nyelvű, hamis nukleáris támadásról szóló üzeneteket küldtek, és hasonló állításokat helyeztek el a honlapon. A szerkesztőség orosz műveletre gyanakszik, de a közölt információk nem támasztanak alá biztos technikai attribúciót.

Tanulság: A hírlevélküldő és tartalomkezelő rendszerekhez való hozzáférést is kiemelten kell védeni. Egy hiteles küldő nevében terjesztett hamis közlés önmagában is jelentős bizalmi kockázat.

Forrás: The Record KÉRDÉS: EZ NEM KB. UGYAN AZ, MINT AZ ELŐZŐ? :D

A Rosstat hivatal elismerte a támadást, az adatlopást nem

Az orosz szövetségi statisztikai szolgálat (Rosstat) megerősítette, hogy október 29. és november 1. között kibertámadások érték, de állítása szerint adatbázisai nem sérültek, és védett adatok nem szivárogtak ki. A Belarusian Cyber Partisans és a Silent Crow ezzel szemben azt állítják, hogy mintegy 25 ezer eszközhöz fértek hozzá, 23 TB adatot loptak el, és megrongálták az informatikai infrastruktúrát. A hivatal weboldalán támadói üzenetek jelentek meg; a szélesebb körű behatolás mértékét nem erősítették meg függetlenül.

Tanulság: A bizonyított honlapeltérítést el kell különíteni a támadók által állított adatszerzéstől és rombolástól. A nyilvánosságra hozott, egyelőre nem ellenőrzött adatok az információs művelet részét is képezhetik.

Forrás: The Record