

2026 október havi CTI riport

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet havi rendszerességgel ad ki fenyegetéselemzést, mely összefoglalja a kibertér globális, valamint magyarországi helyzetét. A riport megismerése megfelelő támpontot adhat az olvasó számára, hogy szervezete milyen IT biztonsági kihívásokkal nézhet szembe a közeli jövőben.



Helyzetkép

A 2026. októberi kiberbiztonsági helyzetképet a célzott kibertámadások, az állami hátterű APT-csoportok aktivitása, a zsarolóvírus-csoportok közötti átrendeződés, valamint az új és ismert sérülékenységek fokozódó kihasználása határozta meg. A jelentés bemutatja a nemzetközi és hazai káros kód trendek alakulását, a meghatározó fenyegetési csoportok tevékenységét, valamint az ipari vezérlőrendszereket és kritikus infrastruktúrákat érintő sérülékenységeket és kiemelt biztonsági eseményeket. Részletesebben foglalkozik az ICS/SCADA és OT-környezetekben azonosított biztonsági hiányosságokkal, az érintett gyártók

termékeivel, illetve a franciaországi szupermarketek hűtésvezérlő rendszereit érintő támadássorozattal. A saját hálózati monitoringrendszerünk augusztus és október közötti adatai alapján áttekintjük az internet felől elérhető szolgáltatások ellen irányuló felderítési és kihasználási kísérleteket, különös tekintettel az októberben kiugró aktivitást mutató PHP/php2shell sérülékenységekre, valamint a Drupal, Grafana, Vite és PHPUnit rendszereket érintő támadási próbálkozásokra. Az ágazati elemzés az egészségügy, a közigazgatás, a pénzügyi szektor és a turizmus fenyegetettségi sajátosságait és a megfigyelt változásokat is ismerteti. A sérülékenységi helyzetkép kitér az októberben megjelent CVE-k számának rekordmértékű növekedésére, az aktívan kihasznált hibákra, valamint a hálózati peremeszközöket és távoli hozzáférési megoldásokat érintő jelentősebb biztonsági problémákra. Végezetül a honeypot-rendszerek forgalomelemzése alapján bemutatjuk a támadói infrastruktúra földrajzi átrendeződésének egyik kiemelkedő példáját, a Bulgáriából érkező káros forgalom jelentős növekedését, valamint az ehhez kapcsolódó hálózati és szolgáltatói változásokat.

APT csoportok

A Kaspersky 2026. október 29-i jelentése szerint egy ismeretlen APT-csoport a NetamLoader nevű, korábban nem dokumentált kártevőkeretrendszert alkalmazta egy ázsiai kormányzati felhasználásra fejlesztett Windows 10-rendszer ellen, feltehetően szoftverellátásilánc-támadás keretében.

A Cisco Talos 2026. október 8-i jelentése szerint az UAT-11985 APT-csoport tajvani kutatóintézetek munkatársait célzó adathalász-kampányt folytatott, amelyben hamis Google Forms-hivatkozásokat és rosszindulatú QR-kódokat alkalmazott. A támadók közbeékelődéses (AitM) adathalász-technikával szerezték meg az áldozatok Google-fiókjainak hitelesítő adatait és munkamenet-tokenjeit, lehetővé téve a fiókok átvételét a többtényezős hitelesítés (MFA) ellenére is.

Általános káros kód trendek

A Symantec Threat Hunter Team jelentése szerint az APT28 (Swallowtail, Fancy Bear) orosz kötődésű kiberkémkedési csoport több NATO-tagország szervezeteit támadta, többek között a Hookedge hátsóajtó alkalmazásával. A támadók rosszindulatú Word-

dokumentumokon keresztül jutottak be a rendszerekbe, majd SSH-alagutak segítségével tartós hálózati hozzáférést alakítottak ki, miközben NTLM-hitelesítési adatokat próbáltak megszerezni és belső hálózati felderítést végeztek. A támadás során egy korábban ismeretlen, memóriában futó kód végrehajtására alkalmas betöltőprogramot is alkalmaztak, azonban az esetleges adatlopás mértéke nem ismert.

Az ukrán kiberbiztonsági hatóságok szerint több orosz kötődésű fenyegetési csoport célzott támadásokat hajtott végre Android- és iOS-alapú mobileszközök ellen, kémkedési és adatlopási céllal. A támadók a DarkSword exploitkészlettel kompromittált weboldalakon keresztül használtak ki iOS és Safari-sérülékenységeket, míg az UAC-0244 és UAC-0263 csoportok hamis weboldalakon terjesztették a CamelSpy és BTMOB kártevőket. A rosszindulatú eszközök lehetővé tették a hitelesítő adatok, üzenetek, híváselőzmények és helyadatok megszerzését, valamint egyes esetekben a fertőzött készülékek távoli vezérlését.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. A jelenlegi trendek alapján az első három kártevő stagnálást mutat, emelkedő tendenciát látunk a Socks Escort, Ranbyus és Andromeda és Avalanche káros kódok elterjedtségében.

Káros kód	Trend
BADBOX 2.0	↔
IPIDEA	↔
Vo1d(2)	↔
Socks Escort	↑
Popcorn Time	↔
NetNut	↓
Ranbyus	↑
Andromeda	↑
Avalanche	↑
Tinba	↓

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. októberi adatok alapján egy nagyobb átrendeződés történt a sikeres támadások alapján. A Gentlemen csoport átvette a legsikeresebb helyet, illetve új csoportként jelent meg a n0n illetve a Boba, akik megtöbbszörözték a támadásaik számát.

Típus	Trend
Gentlemen	↑
Quilin	↓
n0n	↑
INC	↓
Boba	↑
Akira	↓
Lockbit	↑
Emperador	↑
Everest	↑
Safepay	↓

2. ábra: Top 10 zsarolóvírus trendadata

ICS/SCADA

A fejezet a kritikus infrastruktúrákat és az ipari környezeteket érintő, kiemelt kiberbiztonsági sérülékenységeket és fenyegetési eseményeket mutatja be. Áttekinti a kiber-fizikai peremeszközök és IIoT-rendszerek, az ipari kommunikációs és hálózatfelügyeleti megoldások, valamint a folyamatvezérlési és gyártásirányítási rendszerek sérülékenységeit, különös tekintettel az érintett termékekre, a kihasználás lehetséges következményeire és a gyártók által javasolt javításokra, illetve kockázatcsökkentő intézkedésekre. Emellett kitér a mérnöki munkaállomásokhoz és a fizikai biztonsági rendszerekhez kapcsolódó kockázatokra, végül pedig egy kiemelt, több európai ország kiskereskedelmi üzleteit érintő támadássorozaton keresztül szemlélteti az ipari és üzemi vezérlőrendszerek kompromittálásának valós működési és gazdasági következményeit.

Kiber-fizikai peremeszközök és IIoT rendszerek

Két Siemens termék, a Siemens Industrial Edge Device Kit és a Siemens Industrial Edge Devices ugyanazt a hibatípust érinti. Mindkét esetben több útvonalbejárási (path traversal) sérülékenység teszi lehetővé, hogy egy hitelesített, távoli támadó belső, érzékeny információkhoz férjen hozzá. A Siemens új verziókat adott ki az érintett eszközök egy részéhez, a javítással még nem rendelkező termékekhez pedig külön kockázatcsökkentő intézkedéseket javasol.

A Kiloview E3 NDI Encoder 1.30 előtti firmware-verzióiban kilenc CVE-azonosító szerepel. A hibatípusok között van operációsrendszer-parancsbeszúrás, hiányzó hitelesítés kritikus funkcióknál, elégtelen munkamenet-lejárat, útvonalbejárás, NULL-mutató-hivatkozás és beégetett hitelesítő adatok használata. A tanácsadó szerint a sikeres kihasználás az eszköz teljes átvételét teszi lehetővé. Az érintett ágazatok a kommunikáció és az informatika, a gyártó székhelye Kína.

A Guangzhou Juan IoT Technology EseeCloud esetében a sikeres kihasználás az IP-kamerák feletti irányítás megszerzését teszi lehetővé. A sérülékenységek beégetett hitelesítő adatok használatát, objektumattribútumok nem megfelelően ellenőrzött módosítását és megfigyelhető válaszeltéréseket jelentenek. Az érintett ágazatok az energetika, a kommunikáció, a közlekedés, a pénzügyi szolgáltatások, valamint a kormányzati szolgáltatások és létesítmények. A gyártó székhelye Kína.

A Monta monta.app négy CVE-azonosítót tartalmaz (CVE-2026-95102, CVE-2026-97363, CVE-2026-97212, CVE-2026-93474), és a tanácsadó szerint az alkalmazás minden verziója érintett. A sikeres kihasználás jogosulatlan adminisztrátori irányítást adhat a töltőállomások felett, illetve szolgáltatásmegtagadással megzavarhatja a töltési szolgáltatást. Az érintett ágazatok az energetika és a közlekedés, a gyártó székhelye Hollandia.

Ipari kommunikációs csatornák és hálózatfelügyelet

Az EPICS Base sérülékenységeinek kihasználásával a támadó szolgáltatásmegtagadást okozhat, memóriát sérthet meg, érzékeny információt szerezhet, és akár tetszőleges kódot is végrehajthat. Az érintett ágazat a kritikus gyártás.

A Grid Protection Alliance openPDC (2.9.477 és 2.9.482 alatti verziók) és openHistorian (2.8.580 és 2.8.585 alatti verziók) termékeiben öt közös CVE szerepel. Az openPDC Docker-képfájlja egy további, hatodik azonosítót (CVE-2026-105278) is tartalmaz. A hibatípusok megbízhatatlan adatok deszerializálása, hiányzó hitelesítés kritikus funkciónál, szerveroldali kéréshamisítás (SSRF), beégetett hitelesítő adatok és külsőleg vezérelt bemenet alapján történő osztály- vagy kódválasztás. Az érintett ágazat az energetika, a gyártó székhelye az Egyesült Államok.

A Savannah lwIP SMTP kliensében puffertúlcsordulás található. A tanácsadó szerint ez az érintett eszköz összeomlását okozhatja, a túlcsordulás pedig távoli kódfuttatást is lehetővé tehet. Az érintett ágazatok az energetika és a víz- és szennyvízrendszerek, a gyártó székhelye Svédország.

A J4Care dcm4che sérülékenységei lehetővé teszik tárolt orvosi képek törlését, betegadatok kiszivárogtatását, hamisított vizsgálatok beszúrását, betegrekordok átrendelését és fájlok felülírását, továbbá szolgáltatásmegtagadást. A hibatípusok hiányzó jogosultságellenőrzés, végtelen ciklus, nem hatékony algoritmikus komplexitás és hiányzó hitelesítés. Az érintett ágazat az egészségügy és a közegészségügy, a gyártó székhelye Ausztria. A tanácsadó orvosi (ICSMA) besorolású.

Folyamatvezérlési és gyártásirányítási környezetek

A Siemens SIMATIC S7-1500 eszközök webszerverében található sérülékenységek lehetővé teszik, hogy a támadó rosszindulatú kódot futtasson egy jogosult felhasználó böngészőmunkamenetében, és a felhasználó jogosultságainak keretein belül PLC-műveleteket hajtson végre. A Siemens javításokat készít elő, a javítással még nem rendelkező termékekhez pedig kockázatcsökkentő intézkedéseket javasol. Az érintett ágazatok a kritikus gyártás, a közlekedés, az energetika, az egészségügy, a pénzügyi

szolgáltatások, valamint a kormányzati szolgáltatások és létesítmények. A gyártó székhelye Németország.

A SIMATIC S7-1500 TM MFP (V1.1.1) és a SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP (V3.1.7 firmware, a SIPLUS változattal együtt) esetében a sérülékenységek a további GNU/Linux alrendszert érintik. Mindkét termékhez a Siemens javításokat készít elő, és átmeneti kockázatcsökkentő intézkedéseket javasol.

A Hitachi Energy RTU500 tanácsadóját a gyártó a Dragos által jelentett megállapítások nyomán tette közzé. A jelentett hibák a támogatását már megszüntetett RTU500 CMU 9.x firmware-t érintik. A gyártó szerint a jelenleg támogatott verziókat nem érintik, a 11.x és korábbi, életciklusuk végére ért verziók esetében viszont valószínű az érintettség. Mivel ezek már nem kapnak biztonsági frissítést, a Hitachi Energy a jelenleg támogatott firmware-verzióra való frissítést javasolja, és mélységi védelmi intézkedéseket ajánl.

A Mitsubishi Electric és a Mitsubishi Electric Iconics Digital Solutions termékeinél (GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32 és BizViz) a sérülékenységek tetszőleges kód végrehajtását (CVE-2023-4863), hitelesítés megkerülését (CVE-2026-16436 és CVE-2026-16437) és tetszőleges műveletek végrehajtását (CVE-2026-16438) tehetik lehetővé. A következmény információkiszivárgás, információ módosítása, megsemmisítése vagy törlése, illetve szolgáltatásmegtagadás lehet.

Mérnöki munkaállomások és fizikai biztonsági zónák

Az Armatura One egy webalapú, integrált biztonsági és személyazonosság-kezelő platform. Tanácsadója (ICSA-26-274-01) öt CVE-azonosítót tartalmaz (CVE-2023-46604 és CVE-2026-94591–94594), az összesített CVSS-pontszám 9,8, a besorolás kritikus. A sikeres kihasználás jogosulatlan adatbázis-hozzáférést, a legmagasabb jogosultsági szinten végrehajtott tetszőleges kódfuttatást vagy a fizikai beléptetőrendszer feletti irányítás megszerzését teszi lehetővé. Az érintett verziók a 4.7.2 alatti Armatura One és a 4.6.1 alatti amerikai változat, a gyártó frissítést adott ki. Az érintett ágazatok a kommunikáció, a kritikus gyártás, az energetika és a közlekedés.

A Siemens RUGGEDCOM CROSSBOW Station Access Controller (SAC) beépített SQLite komponensében több sérülékenység van. A tanácsadó szerint ezek

tetszőleges kód végrehajtását, szolgáltatásmegtagadást vagy érzékeny információ megszerzését teszik lehetővé. A Siemens új verziót adott ki, és a legfrissebb verzióra való frissítést javasolja.

Kiemelt fenyegetési esemény

Október 11-ről 12-re virradóra ismeretlen támadók illetéktelen hozzáférést szereztek hűtésvezérlőkhöz, és olvasztási üzemmódba állították őket. Emiatt mintegy 700 francia szupermarketben kellett kidobni a megromlott élelmiszert, a hőmérséklet több beszámoló szerint akár 50 °C-ra emelkedett, és egyes esetekben tűz is keletkezett. Az érintett vezérlők zömmel a Danfoss támogatásukat már nem kapó AK-SM 800 és AK-SC 355 típusai voltak. A behatolás módját a források nem erősítették meg, a sérülékeny szoftververziókról és az alapértelmezett jelszavak használatáról csak feltételezések szólnak.

A második hullám jelentésünk elkészültéig zajlott le, november 1–2-án legalább tíz további európai országban mintegy 100–115 üzletet érintett.

Saját hálózati monitoringon (EWS) alapuló CTI helyzetkép

A nemzetközi ICS/SCADA fenyegetési kép mellett a saját hálózati monitoring rendszerünk augusztus–október közötti adatai azt mutatják, hogy a vizsgált ágazatok magasabb súlyosságú fenyegetési képét továbbra is elsősorban az internet felől elérhető webalkalmazások, webszerverek és hálózati szolgáltatások sérülékenységeinek felderítése és kihasználási kísérletei határozták meg. Októberben ugyanakkor jelentősen átrendeződött a fenyegetési profil: új, rendkívül nagy volumenű PHP/php2shell exploitminták jelentek meg, miközben több korábban is megfigyelt webes sérülékenység aktivitása eltérő irányban változott.

A hónap legmarkánsabb új jelenségét a CVE-2026-109618 sérülékenységhez kapcsolódó php2shell figyelmeztetések jelentették. Az aktivitás rövid idő alatt kiugró szintre emelkedett, és továbbra is nagy mennyiségben, folyamatosan megfigyelhető. A jelenség különösen a pénzügyi szektor fenyegetési képét határozta meg, de kisebb mértékben a többi vizsgált ágazatban is jelen volt. A megfigyelések alapján ez nem

egyszeri kiugrásként, hanem tartósan fennálló PHP-alapú exploitációs fókuszként értékelhető, amelynek további alakulása a következő hónapokban is kiemelt figyelmet érdemel.

A php2shell aktivitás mellett az októberi háttérfenyegetettség több ponton is erősödött. A szeptemberben visszatérő Drupal CVE-2014-3704 SQL injection és Grafana CVE-2021-43798 path traversal aktivitás októberben tovább emelkedett, ezért ezek már nem egyszeri havi kiugrásként, hanem folytatódó exploitációs fókuszként értelmezhetők. Jelentősen megerősödtek egyes általános SQL injection minták is. A fájl és könyvtárfelderítési aktivitás a szeptemberi visszaesés után részben ismét emelkedett, de továbbra sem érte el a nyár végi kiugró szintet.

A Vite CVE-2025-30208 sérülékenységéhez kapcsolódó aktivitás a szeptemberi mérséklődés után ismét erősödött, és továbbra is a legfontosabb webalkalmazás-sérülékenységek között maradt. Emellett egy másik Vite fájlolvasási sérülékenység, a CVE-2025-31486 is hangsúlyosabbá vált, így a Vite-hoz kapcsolódó fenyegetési kép már nem egyetlen CVE-re korlátozódik. Ezzel szemben a Log4Shell az augusztusi magas aktivitás óta lefelé tartó tendenciát mutat, bár továbbra is rendszeresen megfigyelhető. A PHPUnit CVE-2017-9841 a szeptemberi visszaesés után ismét erősödött, megerősítve azt a hosszabb távú mintát, hogy bizonyos régi és jól automatizálható sérülékenységek az aktuális exploitációs fókuszok változása mellett sem tűnnek el. A nyári időszakban jelentős Cisco ASA/Firepower aktivitás ugyanakkor októberre már nem tartozott a meghatározó fenyegetések közé.

Ágazati helyzetkép

Egészségügy

Októberi fenyegetési képe több szempontból eltért a korábbi hónapoktól. A PHP/php2shell aktivitás itt is megjelent, ugyanakkor az ágazati összképet egy új, kiugró volumenű X-Forwarded-For: localhost hunting jelzés is jelentősen befolyásolta. Ezzel párhuzamosan a MITRE ATT&CK Network Boundary Bridging technika hirtelen hangsúlyosabbá vált. A jelenlegi adatok alapján ezt azonban nem indokolt valódi defense-evasion trendként értelmezni, mivel nem ismert, hogy a jelzések mekkora része kapcsolódik legitim proxy-, reverse proxy- vagy alkalmazásforgalomhoz. Emiatt

ez egyelőre elsősorban további vizsgálatot igénylő hálózati mintának tekinthető. A hagyományos webes exploitációs rétegben a Vite aktivitása mérséklődött, miközben a PHPUnit a szeptemberi visszaesés után ismét erősödött. A kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó forgalom továbbra is alapvetően stabil háttérjelenséget mutat.

Közigazgatás

Továbbra is a legszélesebb technológiai támadási spektrumot mutatta, és a szeptemberben megkezdődött erősödés októberben több területen folytatódott. A php2shell-jelzések mellett jelentősen emelkedett az SQL injection aktivitás, tovább erősödött a Drupal és Grafana sérülékenységek kihasználására irányuló forgalom, miközben a PHP local file inclusion és a fájlfelderítési minták is tartósan jelen maradtak. A kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó forgalom immár több hónapja emelkedő tendenciát mutat. A webshellhez kapcsolódó malware-jelzések szintén erősödtek, volumenük ugyan továbbra is alacsonyabb az általános exploitációs aktivitásnál, technikailag azonban jól illeszkednek az ágazat széles szerveroldali támadási profiljához.

Pénzügy

Ezt a hónapot egyértelműen a php2shell aktivitás határozta meg, amely a korábbiakhoz képest új és kiugró exploitációs fókuszt jelent.
A háttérben ugyanakkor a korábban kialakult sérülékenységvezérelt profil továbbra is megfigyelhető. A Vite aktivitása a szeptemberi visszaesés után ismét erősödött, és az újabb Vite fájlolvasási sérülékenység is elsősorban ebben az ágazatban jelent meg. A Log4Shell lefelé tartó tendenciája folytatódott, miközben újabb Drupalhoz kapcsolódó SQL injection minták is megjelentek. A WordPress-felderítés továbbra is jelen van, bár a korábbi hónapokhoz képest mérséklődött. Változatlan sajátosság, hogy a pénzügyi adatokban továbbra sem jelennek meg a kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó összesített találatok, így ez már több hónapon át fennálló ágazati eltérésnek tekinthető.

Turizmus

Októberben az eddig viszonylag keskeny webes exploitációs profiljához képest egyértelmű kiszélesedést mutatott. A Vite aktivitása tovább erősödött, de ennél fontosabb változás a React Server Components, JavaScript prototype pollution és sandbox escape jellegű próbálkozások növekedése. Ez a React/JavaScript irány nem kizárólag októberi kiugrás: az elmúlt három hónapban fokozatos erősödés figyelhető meg, amely októberre már markáns ágazati sajátossággá vált. Amennyiben ez a következő hónapban is fennmarad, már önálló CTI-profilváltozásként lesz értékelhető. Emellett a PHP-hoz kapcsolódó sérülékenységi aktivitás is erősödött, miközben a kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó aktivitás fokozatosan csökkenő tendenciát mutat.

Sérülékenységek

2026 októberében 17 097 CVE jelent meg a CVE List v5 forrásból, ami az előző hónaphoz képest 14,3 százalékos növekedést jelentett, így már a harmadik egymást követő hónapban dőlt meg a rekord. A sérülékenységekhez kapcsolódó megfigyelések száma 20,3 százalékkal emelkedett. Miközben az általános észlelések száma jelentősen nőtt, a nyilvános proof-of-concept kódokhoz és a kihasználási tevékenységhez kapcsolódó megfigyelések száma csökkent.

A hónap egyik meghatározó témája a PHP2Shell néven ismertté vált két PHP-sérülékenység, a CVE-2026-109618 és a CVE-2026-109619 volt. A hibák az október 21-i koordinált közzététele előtt kiszivárogtak, és együttesen 1773 megfigyelést kaptak. A Previdian és a Shadowserver honeypotjai már a közzététel napján kihasználási próbálkozásokat észleltek. Ettől elkülönítendő a Security Affairs október 23-i közlése, amely szerint sikeres kihasználás ekkor még nem volt megerősítve: a honeypotokat érő próbálkozások önmagukban nem igazolják éles rendszerek sikeres kompromittálását. Október 21-én összesen 3537 megfigyelést rögzítettek, köztük 245 kihasználásra utaló észlelést, míg a hónap többi napján ez utóbbi érték legfeljebb 119 volt.

Szintén kiemelt figyelmet kaptak a távoli hozzáférést biztosító és a hálózati peremen működő eszközök sérülékenységei. Az Ivanti Connect Secure három hibája került be

a CISA ismerten kihasznált sérülékenységeket nyilvántartó KEV-katalógusába. Az egyikhez kapcsolódó kihasználást a CIRCL már négy nappal a CVE nyilvános közzététele előtt megerősítette. A hónap további érintett termékei között szerepelt a NetScaler, a FortiMail, a BeyondTrust, a PAN-OS, a Cisco ASA és az Arista VeloCloud. Októberben összesen 204 különböző sérülékenység került be legalább egy, a jelentésben nyomon követett KEV-katalógusba.

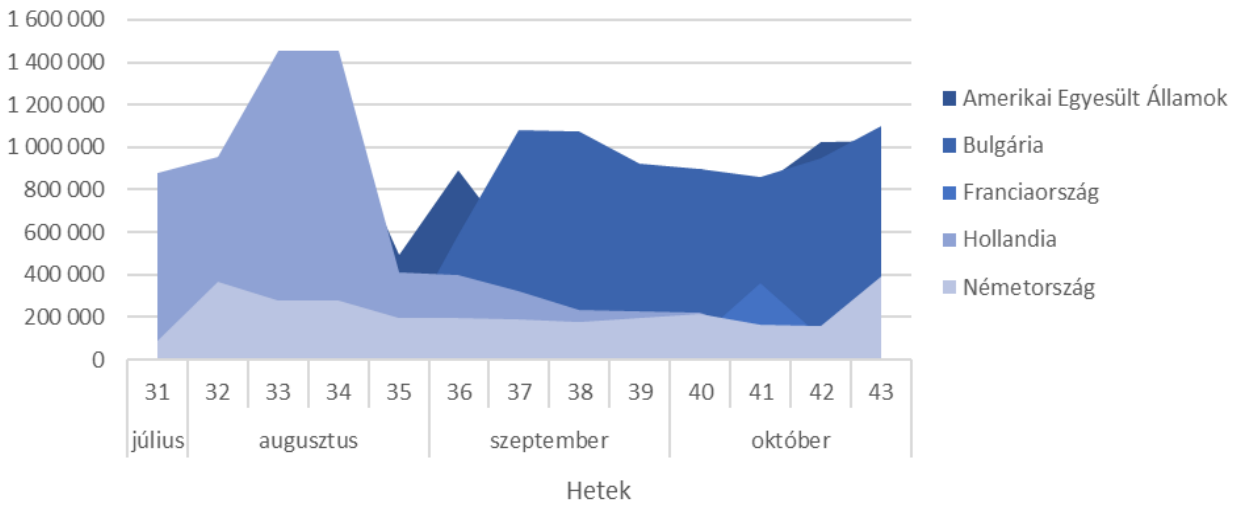
A napi megfigyelések száma október 14-én tetőzött 4751 bejegyzéssel, amit a jelentés a Microsoft javítási ciklusához és az Ivanti közzétételeihez kapcsolt. A BleepingComputer, a SOCRadar és a CrowdStrike korábban idézett beszámolói szerint a Microsoft október 13-i javítócsomagja mintegy 1400 hibát kezelt, köztük az aktívan kihasznált CVE-2026-96951 Windows Shell-sérülékenységet, amelyet a CISA aznap felvett a KEV-katalógusba.

Honeypot forgalom elemzése

Átrendeződő támadói infrastruktúra – A bolgár példa

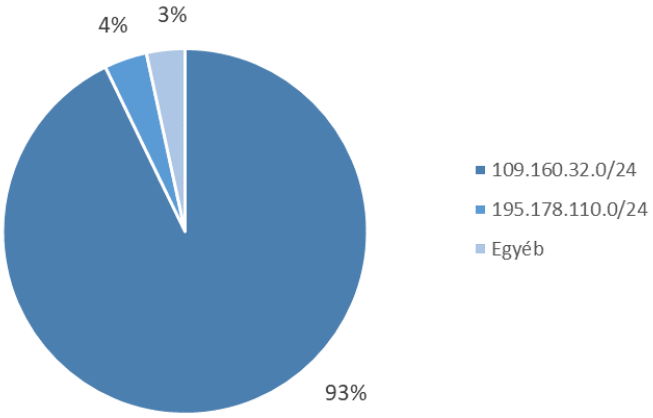
A honeypot rendszerek által azonosított káros forgalmak földrajzi megoszlása általánosságban állandó képet mutat, ugyanakkor időről időre egyes országok aktivitásában drasztikus változások is megfigyelhetők. Jellemzően, olyan országok szoktak események forrása lenni, amelyek jelentős infrastruktúrával rendelkezik mind adatközponti vagy internetszolgáltatói kapacitásban vagy komoly eszközkészletet foglal magába (szerverek, hálózati eszközök, IoT) amelyek kompromitálódási rátája is sokkal magasabb. A hónapok során a GovProbe Honeypot rendszerei irányába folyamatos növekedést tapasztalhattunk a Bulgáriából származó káros forgalmak között, amely októberre már hatalmas különbséggel haladta meg az eddig „vezető” országokat. A változás hátterének vizsgálata során egy konkrét szolgáltatóhoz és IP-tartományhoz kapcsolódó, kiugró aktivitást azonosítottunk.

A Bulgáriából érkező káros forgalom növekedése már 2026 augusztusában érzékelhető volt, szeptemberben azonban különösen jelentős emelkedést tapasztaltunk. Az augusztusban regisztrált mintegy 1,6 millió eseményhez képest szeptemberben már több mint 3,6 millió eseményt azonosítottunk, ami közel 130%-os növekedést jelent.



3. ábra: Forgalomváltozás országok szerint

A forgalom részletesebb vizsgálata során megállapítottuk, hogy a támadó IP-címek jelentős része a 109.160.32.0/24 tartományhoz köthető, amely jelenleg a bolgár Banatsync SRL (AS198364) hálózatából érhető el. A nyilvánosan elérhető hálózati adatok alapján az érintett IP-tartomány esetében szeptember végén szolgáltatói átrendeződés történt: 2026. szeptember 30-án az AS197170 (TechTies Inc.) hálózatából az AS198364 alá került, miközben a két szolgáltató közötti hálózati kapcsolat fennmaradt. Mivel a káros forgalom növekedése már az átállást megelőzően megkezdődött, a változás nem tekinthető annak közvetlen kiváltó okának, ugyanakkor felveti egy hosszabb ideje zajló infrastruktúra-átszervezés lehetőségét. Független fenyegetésfelderítési megfigyelések szintén jelentős, elsősorban automatizált SSH-jelszópróbálgatásokhoz és rendszerfelderítéshez kapcsolódó aktivitást azonosítottak az érintett tartományban.



4. ábra: Bulgáriából származó események IP tartományainak eloszlása

A káros forgalom növekedésének hátterében több lehetséges magyarázat is állhat. Az egyik ilyen a támadói infrastruktúra szolgáltatók közötti áthelyezése vagy bővítése, amelynek során a támadók újonnan bérelt virtuális szerverekre helyezik át tevékenységüket, akár a korábbi szolgáltatónál alkalmazott korlátozások vagy visszaéléskezelési intézkedések miatt. Szintén elképzelhető, hogy az IP-tartomány átadásával korábban is aktív támadói infrastruktúra került új ASN alá, ami önmagában is megváltoztathatja a szolgáltatókhoz rendelt statisztikákat. További lehetséges tényező a szolgáltató ügyfeleihez tartozó rendszerek kompromittálódása, illetve a támadók számára kedvezőbb üzemeltetési feltételek kihasználása. A rendelkezésre álló információk alapján a hálózati átrendeződés és az összehangolt támadótevékenység közötti kapcsolat felvethető, annak pontos oka azonban egyelőre nem igazolt.

Fontos hangsúlyozni, hogy a bemutatott eset önmagában nem tekinthető rendkívüli jelenségnek, sokkal inkább jól szemlélteti, hogy a támadási forrásországok megoszlását milyen jelentős mértékben befolyásolhatja egy-egy szolgáltató vagy IP-tartomány aktivitásának változása. Hasonló átrendeződések más országok esetében is előfordulhatnak, így egy adott ország támadási statisztikákban történő előretörése nem feltétlenül jelent általános fenyegetettségnövekedést, hanem akár néhány kiemelkedően aktív támadói rendszer működésére is visszavezethető.



Kérdés esetén keressen minket az alábbi elérhetőségeink egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

A riporttal kapcsolatos kérdések esetén:
cyberthreat@nki.gov.hu

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET