2026 július 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

2026 júliusában a kiberfenyegetettségi környezetet a támadási aktivitás általános erősödése, a célzott műveletek összetettebbé válása és az automatizált támadási módszerek térnyerése jellemezte. A fenyegető szereplők egyre nagyobb figyelmet fordítottak a kritikus infrastruktúrák, az ipari és irányítástechnikai környezetek, valamint az internet felől közvetlenül elérhető rendszerek támadására. A kockázatot tovább növelte, hogy egyes műveletekben már nem csupán a kezdeti hozzáférés megszerzése és az információk gyűjtése jelentett célt, hanem a kompromittált

rendszerek működésének, adatainak és biztonsági funkcióinak befolyásolása is. Ezzel párhuzamosan a károskódok és zsarolóvírusok aktivitása is fokozódott, miközben a támadók egyre változatosabb technológiai környezeteket, többek között mobil, felhő és fejlesztői rendszereket vettek célba. A sérülékenységek kiemelt szerepet játszottak a kezdeti hozzáférés megszerzésében, különösen az internet felől elérhető eszközök, vállalati alkalmazások és menedzsmentrendszerek esetében. A telemetriai adatok az automatizált támadási kísérletek jelentős növekedését mutatták, amelyben a botnetek és más tömeges támadási infrastruktúrák is meghatározó szerepet töltöttek be. Mindeközben a mesterséges intelligenciával támogatott technikák megjelenése tovább növelte a támadások gyorsaságát és alkalmazkodóképességét. A hazai környezetben szintén erősödő károskód és zsarolóvírus-aktivitás volt megfigyelhető.

Káros kódok és zsarolóvírusok

APT csoportok

2026 júliusában több, állami hátterű APT-csoporthoz köthető kampány is kritikus és stratégiai jelentőségű informatikai rendszereket célzott. Iráni kötődésű szereplők internet felől közvetlenül elérhető Rockwell Automation/Allen-Bradley, Schneider Electric és Siemens programozható logikai vezérlőket (PLC) kompromittáltak a 44818, 2222, 102 és 502 ipari protokollportokon, valamint SSH-n keresztül elérhető modemeket támadtak. A támadók legitim mérnöki szoftverekkel letöltötték, módosították, majd visszatöltötték a PLC-projekteket, miközben a normál vezérlési logikát részben megtartva manipulálták a biztonsági határértékeket, riasztási és leállítási funkciókat, valamint a HMI- és SCADA-rendszereken megjelenő adatokat, ami működési zavarokat és pénzügyi veszteséget okozott. A Laundry Bear néven követett, orosz állami érdekekhez kötött APT a Zimbra Collaboration Suite CVE-2025-66376 sérülékenységét kihasználó, felhasználói interakciót nem igénylő „zero-click” támadásokkal kompromittált postafiókokat. A megnyitott e-mailekbe ágyazott JavaScript-kód többek között levelezési adatokat, jelszavakat, névjegyzékeket és kétfaktoros hitelesítési tokeneket próbált megszerezni. A Lazarushoz kapcsolt APT-C-26 eszköztára is fejlődött: a KKernel.exe komponens több szintű billentyűzetnaplózást, Windows-szolgáltatáson alapuló perzisztenciát és automatikus

folyamat-újraindítást biztosít, miközben a meglévő távoli megfigyelési keretrendszerrel együtt képernyőtartalmak és felhasználói bevitelek tartós megfigyelését teszi lehetővé.

Általános káros kód trendek

Az időszak fenyegetési eseményei az Android-eszközök, a felhős infrastruktúrák és a fejlesztői környezetek elleni támadások fejlődését mutatják. A RedHook mobilkártevő az Android Wireless ADB és az Akadálymentesítési Szolgáltatás engedélyeivel visszaélve rootolás nélkül képes shell (UID 2000) jogosultságot szerezni, majd Shizuku-alapú komponensekkel parancsokat végrehajtani, biztonsági beállításokat módosítani, alkalmazásokat kezelni és RAT-funkciókon keresztül adatokat lopni. A JadePuffer zsarolóvírus-műveletben a kutatók egy autonóm, LLM-alapú AI-ügynök alkalmazását azonosították, amely a Langflow CVE-2025-3248 sérülékenységének kihasználásától kezdve a hitelesítőadat-gyűjtésen, perzisztencia kialakításán és oldalirányú mozgáson át a Nacos-konfigurációk titkosításáig önállóan hajtotta végre és a hibákhoz dinamikusan igazította a támadási láncot. Emellett kompromittált npm-csomagokon keresztül fejlesztői környezeteket célzó ellátásilánc-támadást is feltártak, amely a VS Code tasks.json automatikus folderOpen végrehajtását, fontfájlnak álcázott JavaScriptet és blokklánc-tranzakciókba rejtett „dead drop” információkat alkalmazott. A végső, többplatformos Python-infostealer böngészőadatok, kriptotárcák, jelszókezelők, SSH-kulcsok, valamint fejlesztői és felhős hitelesítő adatok megszerzésére törekedett, így a fertőzött munkaállomások további kódtárak és felhőszolgáltatások kompromittálásának kiindulópontjává válhatnak.

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 Popcorn Time, ismételten a 10 legtöbbet észlelt káros kód között található a SmokeLoader, Nymaim, valamint az Avalanche.

Káros kód	Trend
BADBOX 2.0	↔
IPIDEA	↔
Vo1d(2)	↔
Popcorn Time	↑
SmokeLoader	↑
Socks Escort	↓
Randybus	↑
Andromeda	↓
Nymaim	↑
Avalanche	↑

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. júliusi adatok alapján a Gentlemen csoport aktivitása tovább növekedett, miközben több új csoport, mint a Global Secret, CRPx0, Krybit is bekerült a legtöbb fertőzést végrehajtó csoportok közé.

Típus	Trend
Gentlemen	↑
Qilin	↓
Dragon Force	↔
INC	↑
Safepay	↔
Global Secret	↑
CRPx0	↑
Krybit	↑
Akira	↓
Everest	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

A vizsgált időszak adatai alapján megállapítható, hogy a vizsgált időszakban, a felderített zsarolóvírus-támadások néhány sebezhetőség kihasználásával valósultak meg, melyek technikai szempontból az alábbi három fő kategóriába sorolhatók:

- Kezdeti hozzáférés és hálózati átjárók kompromittálása: A támadók továbbra is elsősorban az internet felől elérhető hálózati eszközöket és távoli hozzáférési szolgáltatásokat veszik célba. Kiemelkedő kockázatot jelentenek a Citrix NetScaler sérülékenységei (CVE-2023-3519, CVE-2023-4966 – Citrix Bleed).
- Alkalmazás-alapú sebezhetőségek és távoli kódvégrehajtás (RCE): A támadók továbbra is előszeretettel használják ki a kritikus szerveralkalmazások távoli kódfuttatást lehetővé tevő hibáit. Gyakran visszaélnek a Fortinet FortiManager (CVE-2023-48788) sérülékenységeivel a szerverek feletti teljes ellenőrzés megszerzése érdekében.
- Hitelesítés megkerülése és érzékeny adatok megszerzése: A külső elérésű rendszerek és adatkezelő megoldások sebezhetőségei továbbra is fontos belépési pontot jelentenek. A Veeam Backup & Replication (CVE-2023-27532) révén a támadók titkosított hitelesítő adatokat szerezhetnek meg.

ICS/SCADA

A vizsgált időszakban keletkezett sérülékenységek jól szemléltetik, hogy az OT/ICS és IoT környezetek különböző rétegeiben jelentkező biztonsági problémák egyaránt veszélyeztethetik az ipari és kritikus infrastruktúrák működését.

Kiber-fizikai peremeszközök és IIoT rendszerek

A Gardyn IoT Hub sérülékenysége az IoT-alapú automatizációs rendszerek, míg a Hydro-Québec Le Circuit Électrique töltőállomás-háttérrendszer hibája az elektromos járműtöltő infrastruktúrák biztonsági kockázataira hívja fel a figyelmet. A Tycon Systems TPDIN-Monitor-WEB2 sérülékenysége a távoli monitoring és felügyeleti eszközök kompromittálása jogosulatlan hozzáférést,

konfigurációmódosítást és további támadások kiindulópontját jelentheti. A Siemens SIDIS Secured SmartPlug esetében az intelligens energiaelosztási környezetek biztonsága kerül előtérbe, ahol a támadók érzékeny konfigurációs adatokhoz és hálózati információkhoz juthatnak.

Ipari kommunikációs csatornák és hálózatfelügyelet

A Siemens SINEC OS, az ABB T-MAC Plus, a Rockwell Automation 1715-AENTR EtherNet/IP Adapter, valamint a Panduit IntraVUE sérülékenységei az ipari hálózatok menedzsmentjét, kommunikációját és láthatóságát érintik. Ezeknek a rendszereknek a kompromittálása lehetővé teheti a hálózati konfigurációk módosítását, az EtherNet/IP kommunikáció megzavarását, jogosulatlan vezérlési parancsok továbbítását, illetve az infrastruktúra feltérképezését, elősegítve a laterális mozgást és további célzott támadásokat.

Folyamatvezérlési és gyártásirányítási környezetek

A Siemens Opcenter X és az OpenPLC v3 sérülékenységei közvetlenül érintik a gyártásirányítási (MES) és folyamatvezérlési környezeteket. Egy sikeres támadás lehetőséget biztosíthat gyártási adatok és folyamatok manipulálására, jogosulatlan PLC-programfeltöltésre, vezérlési logika módosítására, valamint a termelési folyamatok befolyásolására, ami az üzemeltetési és üzleti működésre egyaránt jelentős hatással lehet.

Mérnöki Munkaállomások (EWS) és Fizikai Biztonsági Zónák

A Siemens CADRA sérülékenysége a mérnöki tervezési környezetekben tárolt konfigurációs és rendszerinformációk védelmének fontosságát hangsúlyozza. A Johnson Controls C-CURE 9000 és a Victor Application Server sérülékenységei a fizikai biztonsági rendszereket érintik, amelyek kompromittálása nemcsak informatikai, hanem fizikai biztonsági következményekkel is járhat, például jogosulatlan belépés vagy a szervezeti védelmi képességek gyengítése révén.

Kiemelt fenyegetési esemény

Kiemelt jelentőségű esemény volt a Minnesota államban bekövetkezett koordinált kibertámadás, amely során több mint harminc helyi víziközmű informatikai és OT/SCADA környezetét érte összehangolt támadássorozat. Az FBI és a CISA vizsgálata szerint a támadók több vízellátó rendszer felügyeleti és vezérlési infrastruktúrájához szereztek jogosulatlan hozzáférést. Az amerikai hatóságok értékelése alapján az iráni kötődésű fenyegető szereplők egyre inkább a kritikus infrastruktúrák – különösen a vízügyi, energetikai és ipari OT/ICS környezetek – működésének megzavarására törekednek. A támadások már nem csupán információgyűjtésre vagy kezdeti hozzáférés megszerzésére irányulnak, hanem a PLC-programlogika módosítására, a HMI/SCADA felületeken megjelenített adatok manipulálására, valamint a biztonsági és védelmi funkciók befolyásolására is kiterjednek.

Sérülékenységek

A vizsgált időszakban nyilvánosságra hozott és aktívan kihasznált kritikus sérülékenységek alapján továbbra is meghatározó trend, hogy a támadók elsődleges célpontjai a széles körben alkalmazott vállalati infrastruktúra-elemek, webes alkalmazások, együttműködési és menedzsmentplatformok, valamint hálózati és biztonsági megoldások. A 2026. júliusi időszakban kiemelt jelentőségű sérülékenységek érintették többek között a WordPress, Microsoft SharePoint, React Server Components, SonicWall SMA1000, Check Point SmartConsole, Oracle E-Business Suite, Adobe ColdFusion, Langflow és Joomla! szoftvereket. Az érintett termékek köre jól mutatja, hogy a sérülékenységek a vállalati IT-infrastruktúra több, egymással összekapcsolódó rétegét érintik, így egyetlen kritikus komponens kompromittálása további rendszerek és szolgáltatások veszélyeztetéséhez is vezethet.

A hónap egyik legjelentősebb sérülékenységi eseménysorozatát a WordPress CVE-2026-60137 és CVE-2026-63030 azonosítójú hibái jelentették. A két sérülékenység együttes kihasználása hitelesítés nélküli támadó számára SQL injection, majd távoli kódfuttatás lehetőségét biztosíthatja. Mindkét sérülékenység bekerült a CISA Known

Exploited Vulnerabilities (KEV) katalógusába, és a Vulnerability-Lookup júliusi jelentése alapján a hónap leggyakrabban észlelt sérülékenységei között szerepeltek. A kockázatot tovább növeli, hogy a támadáshoz nem szükséges felhasználói interakció, így az internet felől elérhető WordPress-alapú rendszerek automatizált támadási kampányok célpontjává válhatnak.

Kiemelt kockázatot jelentettek a Microsoft SharePoint sérülékenységei is. Július folyamán több SharePoint Server hibát is felvettek a KEV katalógusba, köztük a CVE-2026-45659, CVE-2026-56164, CVE-2026-58644 és CVE-2026-50522 azonosítókkal rendelkező sérülékenységeket. Az érintett hibák között nem megbízható adatok deszerializálásával, illetve hitelesítéssel kapcsolatos sérülékenységek találhatók, amelyek kihasználása megfelelő körülmények között távoli kódfuttatáshoz vagy jogosulatlan hozzáféréshez vezethet. A SharePoint vállalati dokumentumkezelési és együttműködési környezetben betöltött szerepe miatt ezen rendszerek kompromittálása különösen jelentős kockázatot jelenthet, mivel a támadók érzékeny üzleti dokumentumokhoz férhetnek hozzá, illetve további belső rendszerek ellen hajthatnak végre oldalirányú mozgást.

A webes és alkalmazási rétegben további kiemelt kockázatot jelentett a CVE-2025-55182, amely a React Server Components működését érinti. Bár a sérülékenységet már korábban publikálták, 2026 júliusában továbbra is jelentős kihasználási aktivitás volt megfigyelhető, és a sérülékenység a CISA KEV katalógusában is szerepel. A hiba előhitelesítés nélküli távoli kódfuttatás lehetőségét biztosíthatja, ezért különösen veszélyes azokban a környezetekben, ahol a React Server Components internet felől elérhető alkalmazásokban kerül alkalmazásra. A sérülékenység jól példázza, hogy egy korábban publikált hiba a javítások elmaradása esetén hosszabb időn keresztül is releváns támadási vektort jelenthet.

A hálózati és biztonsági infrastruktúrát érintő sérülékenységek közül kiemelkednek a SonicWall SMA1000 CVE-2026-15409 és CVE-2026-15410, valamint a Check Point SmartConsole CVE-2026-16232 azonosítójú hibái. A SonicWall sérülékenységei SSRF-hez, illetve kódbefecskendezéshez kapcsolódnak, míg a Check Point SmartConsole esetében hitelesítés-megkerülési probléma teszi lehetővé a biztonsági környezet jogosulatlan befolyásolását. A biztonsági és hálózatvédelmi eszközök kompromittálása kiemelt jelentőségű, mivel a támadók nem csupán egyetlen

végpontot vagy alkalmazást veszélyeztethetnek, hanem hozzáférést szerezhetnek a hálózat védelmi infrastruktúrájához, módosíthatják a biztonsági szabályokat, megkerülhetik a védelmi mechanizmusokat, illetve további támadások előkészítésére használhatják fel a megszerzett hozzáférést.

Az üzleti alkalmazások közül jelentős kockázatot képviselt az Oracle E-Business Suite Payments CVE-2026-46817 sérülékenysége. A hiba jogosultság nélküli támadó számára az alkalmazási környezet kompromittálásának lehetőségét biztosíthatja, ezért különösen veszélyes lehet olyan vállalati környezetekben, ahol az Oracle E-Business Suite pénzügyi, beszerzési vagy egyéb üzleti folyamatokat támogat. Hasonlóan magas kockázatú az Adobe ColdFusion CVE-2026-48282 sérülékenysége, amely kritikus, CVSS 10,0 értékelést kapott, és path traversal problémához kapcsolódik. A sérülékenység esetében a nyilvános interneten elérhető ColdFusion-szerverek különösen veszélyeztetettek lehetnek, mivel az ilyen rendszerek automatizált felderítése és támadása rövid időn belül megkezdődhet a sérülékenység nyilvánosságra kerülését követően.

A júliusi időszakban az AI és automatizálási platformok sérülékenységei is egyre hangsúlyosabbá váltak. A Langflow esetében több olyan sérülékenység is megjelent, amelyek közül a CVE-2026-0770 hitelesítés nélküli távoli kódfuttatást, míg a CVE-2026-55255 jogosulatlan hozzáférést és más felhasználók munkafolyamatainak végrehajtását teheti lehetővé. Az ilyen sérülékenységek különösen relevánsak a gyorsan terjedő AI és workflow-platformok esetében, mivel ezek a rendszerek gyakran érzékeny vállalati adatokhoz, API-kulcsokhoz és belső szolgáltatásokhoz rendelkeznek hozzáféréssel. Egy sikeres kompromittálás ezért nem feltétlenül korlátozódik magára az érintett alkalmazásra, hanem további vállalati erőforrások veszélyeztetésére is lehetőséget teremthet.

A webes tartalomkezelő rendszerek esetében a Joomla! kiegészítőit érintő sérülékenységek jelentettek kiemelt kockázatot. A hónap során több Joomla! komponens, köztük a JoomShaper SP Page Builder, Page Builder CK, iCagenda és Balbooa Forms sérülékenységei is bekerültek a KEV katalógusba. Az érintett hibák között korlátozás nélküli fájlfeltöltést lehetővé tevő sérülékenységek is találhatók, amelyek megfelelő körülmények között PHP-kód végrehajtásához és a webkiszolgáló kompromittálásához vezethetnek. A széles körben használt webes komponensek

esetében a sérülékenységek különösen jelentős kockázatot hordoznak, mivel egyetlen hibás vagy elavult bővítmény nagyszámú, egymástól független weboldalt tehet támadhatóvá.

Honeypot forgalom elemzése

A GovPorbe Honeypot adatait megtekintve felismerhetünk egy erős változást június és július eseményei között. Az SSH csapdákon beérkező forgalmak drasztikus 632%-os növekedést tapasztaltunk.

Csapda típusok	Június	Július	Változás
ssh	5 747 881	42 083 792	632%
firewall	9 526 973	7 532 669	-21%
dhcp	2 577 189	2 469 633	-4%
telnet	1 690 620	1 731 779	2%
webapp-wordpress	853 962	566 339	-34%
imap	93 451	147 470	58%

3. ábra: Csapdatípusok megoszlása júniusban és júliusban

A részletesebb vizsgálat alapján azonban a növekedés döntően egy, a hónap közepén jelentkező, kiugró intenzitású eseményhez köthető, amely során körülbelül 36 millió SSH-kapcsolódó esemény érkezett mindössze 14 óra alatt. A forrás IP címek túlnyomó többsége a Hollandiában regisztrált 91.92.0.0/16 hálózathoz tartoznak. A naplófájlok megtekintésekor láthatóvá váltak információ gyűjtési technikák és hozzáférési próbálkozás alapvető hitelesítő adatok használatával. A reputációs vizsgálat tovább erősíti ezt az értékelést. Mind a 31 azonosított forrás IP-címhez kapcsolódott korábbi visszaélési bejelentés az AbuseIPDB adatbázisában, és számos cím esetében kifejezetten SSH brute-force próbálkozások, portszkennelés és egyéb automatizált felderítési tevékenység szerepelt a jelentések között.

Megnövekedett Prometei-aktivitás a júliusi megfigyelésekben

Július folyamán a Prometeihez köthető dropper URL-ek újonnan jelentek meg a telemetriánkban, ráadásul domináns mennyiségben, ami ismét ráirányította a figyelmet erre a régóta ismert, de továbbra is aktív kártevőcsaládra. A Prometei egy moduláris, pénzügyi motivációjú botnet, amely Windows- és Linux-rendszereket egyaránt célba vesz, és egyik fő célja továbbra is a kriptovaluta-bányászat, elsősorban Monero előállítása. Funkcionalitása azonban ennél jóval szélesebb: képes hitelesítő adatok megszerzésére, rendszerfelderítésre, laterális mozgásra, perzisztencia kialakítására, távoli parancsvégrehajtásra, valamint további payloadok telepítésére is. Moduláris felépítése lehetővé teszi, hogy az operátorok a kompromittált rendszereket különböző célokra használják, és a fertőzést sérülékeny szolgáltatásokon vagy megszerzett hitelesítő adatokon keresztül továbbterjesszék.

A GovProbe Honeypot eseményei között júliusban megfigyelt megnövekedett Prometei-indikátorszám különösen figyelemre méltó a kártevő közelmúltbeli újbóli felerősödésének és folyamatos fejlesztésének tükrében. A Palo Alto Networks Unit 42 2025 márciusától jelentős, Linux-rendszereket célzó Prometei-aktivitási hullámot azonosított, amelyben módosított UPX-csomagolást, beágyazott konfigurációs adatokat és fejlettebb detektáláselkerülési technikákat alkalmazó újabb variánsok jelentek meg. A későbbi kutatások további kapcsolódó változatokat tártak fel, ami arra utal, hogy nem pusztán egy régi, statikus payload újbóli terjedéséről, hanem aktívan fejlesztett kártevőcsaládról van szó.

Főbb aktuális jelzések az elmúlt 30 napból:

- A Kaspersky 2026-08-10-én közzétett jelentése szerint a Prometei aktivitása növekedett a 2026 második negyedévére vonatkozó IoT-fenyegetési környezetben, különösen SSH-alapú támadásokban, elsősorban Hollandiában, Németországban és az Egyesült Államokban.
- A Cybereason 2026-07-23-án közzétett jelentése több észak-amerikai incidenskezelési esetet írt le, amelyek Prometei-fertőzéssel függtek össze.

A tevékenységet a Microsoft Exchange sebezhetőségeinek, különösen a CVE-2021-27065 és CVE-2021-26858 kihasználásához kötötték.

- A friss riportok továbbra is a Prometeit többlépcsős Windows és Linux-botnetként írják le, amelyet Monero-bányászatra, hitelesítő adatok ellopására és laterális mozgásra használnak, többek között EternalBlue és BlueKeep technikákkal.

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