2026 március 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 márciusában a kiberfenyegetési helyzetképet elsősorban a geopolitikai feszültségek, különösen a közel-keleti konfliktusokhoz kapcsolódó állami és félállami kiberműveletek határozták meg. Az iráni kötődésű szereplők – köztük a Seedworm, a Handala Hack Team és más proxy csoportok – izraeli és amerikai célpontok ellen folytattak kémkedési, adathalászati és információs-pszichológiai műveleteket, miközben az orosz, kínai és észak-koreai APT-csoportok is aktívak maradhattak Európában, Ukrajnában, illetve más stratégiai térségekben is. A hónap általános képe alapján a támadók fő célja továbbra sem kizárólag a közvetlen rombolás volt, hanem a tartós hozzáférés megszerzése, az adatlopás, a reputációs nyomásgyakorlás és a kritikus ellátási láncok megfigyelése.

Technikai szinten a fenyegetési környezet egyre kifinomultabbá vált: a támadók legitim alkalmazások trójai változatait, DLL sideloadingot, memóriában futó backdoorokat, felhőszolgáltatásokon keresztüli C2-kommunikációt, valamint célzott spearphishing kampányokat alkalmaztak. Az izraeli „Red Alert" alkalmazás kompromittálása, a kínai APT-k telekommunikációs és IoT-célzásai, az orosz Pawn Storm és Sednit műveletei, valamint a Konni és az OceanLotus kampányai azt mutatják, hogy az állami hátterű szereplők egyszerre célozzák a lakossági, a vállalati és a védelmi szektort. Ezzel párhuzamosan a káros kódok és a zsarolóvírusok terjedése is erősödött: Magyarországon a mirai és a qsnatch fertőzések növekedtek, nemzetközi szinten pedig a Qilin megőrizte vezető szerepét, miközben a LockBit visszatérése és több új szereplő aktivitásnövekedése is érzékelhető volt.

A helyzetet tovább súlyosbította, hogy a támadások jelentős része továbbra is ismert, de sok helyen javítatlan sérülékenységekre épült, beleértve régebbi és újonnan aktívan kihasznált hibákat is. Az ICS/SCADA és OT-környezetek különösen érzékenynek bizonyultak: az internet felől elérhető ipari vezérlők, a sérülékeny épületautomatizálási

és folyamatirányítási rendszerek, valamint a kritikus infrastruktúrák digitalizációja miatt az IT–OT határ tovább mosódott el. Elmondható, hogy egy emelkedő fenyegetettségi szintű időszakot mutatott az elmúlt időszak, ahol a szervezetek számára a gyors javításkezelés, a hálózati szegmentáció, a hitelesítési kontrollok megerősítése és a célzott adathalász támadások elleni felkészültség vált a legfontosabb védekezési prioritássá.

Káros kódok és zsarolóvírusok

APT csoportok

A 2026 márciusi kiberfenyegetési környezetet a közel-keleti geopolitikai feszültségek és az ehhez kapcsolódó állami hátterű műveletek dominálták. Az iráni kötődésű fenyegetési szereplők, mint a Seedworm (MuddyWater) és a Handala Hack Team, összehangolt kémkampányokat és dezinformációs műveleteket folytattak izraeli és amerikai kormányzati szervek, valamint olyan stratégiai haditechnikai vállalatok ellen, minta Lockheed Martin. Ezen akciók során kifinomult technikákat alkalmaztak, beleértve a legitim alkalmazások (például a Red Alert riasztórendszer) trójai változatainak terjesztését, valamint adathalászaton alapuló hitelesítőadat-lopást és kártékony hátsó kapuk (backdoorok) telepítését. Az iráni APT aktivitásról hosszabban olvashat a Havi vendégszektor elemzés: amerikai és izraeli kritikus infrastruktúra célpontok elemzésben.

Ezzel párhuzamosan az Európai Unió területén is jelentős támadási hullámot észleltek, amelyet az orosz Pawn Storm (BlueDelta), a kínai Flax Typhoon és az iráni Emennet Pasargad csoportok vezényeltek. Ezek a műveletek kritikus infrastruktúrákat, IoT-eszközöket és védelmi ellátási láncokat céloztak meg, gyakran olyan friss sebezhetőségeket kihasználva, mint a CVE-2026-21509 és a CVE-2026-21513. Az EU Tanácsa válaszul több kínai és iráni szervezetet is szankciós listára tett, mivel bizonyítottá vált részvételük az állami szintű kiberkémkedésben és a közösségi szolgáltatások elleni destruktív tevékenységekben.

Izrael

Ismeretlen támadók – feltételezhetően az APT-C-23 (Desert Falcons) Gázai csoporthoz köthető szereplők – az izraeli lakosság körében népszerű „Red Alert" rakétariasztási alkalmazást használták fel kifinomult mobilkémprogram terjesztésére. A támadás során a felhasználók hitelesnek tűnő, de hamisított SMS-értesítéseket kaptak, amelyek egy rosszindulatú frissítés letöltésére buzdították őket. A trójai falóként működő alkalmazás megőrizte eredeti funkcióit, miközben a háttérben több mint 20 kockázatos jogosultságot szerzett meg, lehetővé téve az SMS-ek, kontaktlisták, pontos helyadatok és eszközfiókok folyamatos figyelését és kinyerését. A kémprogram egy speciális betöltő

(loader) egységet használt, amely megkerülte az Android biztonsági ellenőrzéseit és aláírás-hitelesítési folyamatait, miközben kódobfuszkációval (a programkód szándékos összekuszálásával) és többrétegű titkosítással próbálta elrejteni a vezérlőszerverrel (C2) folytatott kommunikációját. Az összegyűjtött adatokat a szoftver helyben tárolta, majd szakaszosan továbbította a támadók szervereire, különös figyelmet fordítva a telepített alkalmazások listázására és a felhasználó tartózkodási helyére alapozott eseményvezérelt adatgyűjtésre.[1]

Kína

A kínai állami háttérrel rendelkező UAT-9244 (más néven Famous Sparrow vagy Tropic Trooper) APT-csoport 2024 óta szisztematikusan támadja Dél-Amerika telekommunikációs infrastruktúráját, Windows és Linux alapú rendszereket egyaránt kompromittálva. A támadássorozat során a fenyegetési szereplő DLL sideloading technikát alkalmaz, amelynek lényege, hogy egy legitim futtatható állományt (wsprint.exe) használva kényszeríti ki a kártékony kód (BugSplatRc64.dll) betöltését, elkerülve ezzel a hagyományos biztonsági szoftverek detekcióját. A végső célpont a TernDoor backdoor, amely a memóriába ágyazva fut, majd a regisztrációs adatbázis (Registry) és ütemezett feladatok segítségével biztosítja a tartós jelenlétet a fertőzött hálózaton. A csoport továbbá beveti a PeerTime nevű, BitTorrent protokollt használó ELF-alapú kártevőt, valamint a GoLang nyelven írt BruteEntry implantátumot, amely a kompromittált hálózati eszközöket (edge devices) bázisállomásokká (ORB - operational relay box) alakítja, hogy onnan távolról vezérelve brute-force (nyers erejű) támadásokat indítson SSH, Postgres és Tomcat szolgáltatások ellen.[2]

Az Európai Unió Tanácsa 2026 márciusában szankciókat léptetett életbe kínai és iráni entitások ellen, amelyek kritikus infrastruktúrák elleni támadásokban és dezinformációs műveletekben vettek részt. A büntetőintézkedések érintik a kínai Integrity Technology Group vállalatot, amely a Flax Typhoon (RedJuliett) APT-csoportot támogatta egy több mint 65 000 Internet of Things (IoT) eszközt – azaz hálózatba kapcsolt okoseszközt – érintő botnet kiépítésében az EU területén. Szintén szankciós listára került az i-SOON (Anxun

[1] https://www.acronis.com/en/tru/posts/mobile-spyware-campaign-impersonates-israels-red-alert-rocket-warning-system/#OUUtO6exPJ
[2] https://blog.talosintelligence.com/uat-9244/

Information Technology) két alapítója, akik „hacking-for-hire" (bérhackelés) szolgáltatás keretében kínáltak hozzáférést bizalmas állami adatokhoz és kulcsfontosságú rendszerekhez. Az iráni vonalon az Emennet Pasargad (Haywire Kitten) csoportot nevesítették, amely a francia Charlie Hebdo magazintól ellopott adatok dark weben történő értékesítése mellett a 2024-es párizsi olimpián digitális óriásplakátok kompromittálásával terjesztett álhíreket, valamint korábban szavazói adatbázisokhoz való hozzáféréssel próbált beavatkozni választási folyamatokba. Az EU döntése értelmében az érintettek vagyonát befagyasztották, valamint utazási és tranzakciós tilalmat rendeltek el velük szemben a tagállamok területén.[3]

Oroszország

Az orosz kötődésű Sednit (más néven BlueDelta) APT-csoport 2025 és 2026 között folytatott kémkampánya során az ukrán katonai állományt vette célba, egyedi fejlesztésű kártevők és módosított keretrendszerek alkalmazásával. A műveletek alapját a SlimAgent nevű kémprogram adta, amely a korábbi hírhedt Xagent kódbázisára épülve képes billentyűleütések naplózására, képernyőképek készítésére és a vágólap adatainak ellopására. Ezzel párhuzamosan a támadók bevetették a BeardShell implantátumot is, amely egy .NET futtatókörnyezetben hajt végre PowerShell parancsokat, és legitim felhőszolgáltatásokon (például Icedrive) keresztül tartja a kapcsolatot a vezérlőszerverrel (C2), megnehezítve a hálózati forgalom elemzését. A csoport az elemzések szerint a nyílt forráskódú Covenant keretrendszert is saját igényeihez igazította, egyedi azonosító generálási módszerekkel és felhőalapú kommunikációs protokollokkal egészítve ki azt. A legutóbbi, 2026 januári incidensek során a Sednit már célzott adathalászattal (spearphishing) terjesztette eszközeit, kihasználva a Microsoft Office termékekben azonosított CVE-2026-21509 számú kritikus sebezhetőséget.[4]

Az orosz kötődésű Pawn Storm (más néven BlueDelta) APT-csoport jelenleg is zajló kiberkémkedési kampányt folytat Ukrajna és a közép-kelet-európai szövetséges államok védelmi célú ellátási láncai ellen, a „PRISMEX" elnevezésű kártevőcsaládot használva. A támadók két kritikus sebezhetőséget használnak ki: a Microsoft Office OLE biztonsági funkcióit megkerülő CVE-2026-21509-et, valamint a Windows MSHTML védelmét érintő

[3] https://www.reuters.com/world/china/eu-sanctions-chinese-iranian-companies-cyber-attacks-2026-03-16/
[4] https://www.welivesecurity.com/en/eset-research/sednit-reloaded-back-trenches/

CVE-2026-21513-at. A fertőzési lánc katonai logisztikai témájú adathalász levelekkel indul, amelyek megnyitása után a rendszer távoli WebDAV szerverekhez csatlakozik kártékony állományok letöltése céljából. A PRISMEX moduláris felépítése során a csoport steganográfiát – képekbe rejtett adatátvitelt – alkalmaz, ahol egy speciális algoritmus segítségével bontják ki a kártékony kódot PNG fájlokból, majd a memóriában futtatják azt. A támadás végső fázisában a módosított Covenant keretrendszer és a Filen.io felhőszolgáltatás segítségével építenek ki vezérlőszerver-kommunikációt (C2), amely lehetővé teszi a távoli parancsvégrehajtást és a bizalmas katonai adatok szivárogtatását.[5]

Észak-korea

A Genians legfrissebb jelentése szerint az észak-koreai kötődésű Konni APT-csoport egy többlépcsős adathalász kampányt indított, amely során kompromittált KakaoTalk fiókokat használnak fel a kártevők továbbterjesztésére. A támadás kezdeti fázisában a csoport hivatalosnak tűnő, észak-koreai emberi jogi előadói kinevezésnek álcázott spearphishing e-maileket küld ki, amelyek egy kártékony LNK (parancsikon) fájlt tartalmaznak. Az LNK futtatása PowerShell-parancsokat indít el, amelyek távoli vezérlőszerverekről (C2) töltenek le payloadokat, biztosítva a támadóknak a távoli hozzáférést és a rendszerszintű perzisztenciát ütemezett feladatok segítségével.

A sikeres behatolást követően a csoport az áldozat KakaoTalk üzenetküldő alkalmazásához is hozzáfér, majd a kontaktlistáról választott másodlagos célpontoknak küld tovább észak-koreai videótartalmaknak álcázott kártékony fájlokat. Ez a másodlagos terjesztési módszer egy legális AutoIt bináris segítségével futtat le egy PDF-nek álcázott szkriptet (APDNHFU.pdf), amely az „EndRAT" kártevőhöz hasonló funkciókat kínál, beleértve a távoli parancsvégrehajtást és az adatszivárogtatást. A Konni továbbá moduláris jelleggel egyéb RAT (Remote Access Trojan) típusú kártevőket is telepít – például az „RftRAT"-ot és a „RemcosRAT"-ot –, amelyeket rejtett könyvtárakban (ProgramData, Public) tárol, és titkosított konfigurációkkal, valamint billentyűnaplózási (keylogging) funkciókkal lát el a hosszú távú jelenlét és az elemzések elkerülése érdekében.[6]

[5] https://www.trendmicro.com/en_us/research/26/c/pawn-storm-targets-govt-infra.html
[6] https://cybersecuritynews.com/konni-apt-hijacks-kakaotalk-accounts/

Vietnám

A vietnámi kötődésű OceanLotus (más néven APT32) kiberkémcsoport 2025 második fele óta szisztematikusan támadja a kínai védelmi, diplomáciai és szakpolitikai szektorokat, aktuális politikai témákat használva csaliként az adathalász kampányaiban. A támadók ZIP-archívumokba ágyazott IMG lemezképfájlokon keresztül juttatják el a kártevőket, amelyekben LNK (parancsikon) fájlok indítják el a többlépcsős fertőzési láncot. A technikai elemzés szerint a csoport DLL hijacking (dinamikus könyvtárak eltérítése) technikát és MST-transzformációs fájlokat alkalmaz, hogy a háttérben, a felhasználó számára észrevétlenül telepítsen egy Rust nyelven írt távoli vezérlő (backdoor) programot. Ez a memóriában futó kártevő teljes kontrollt biztosít a fertőzött rendszerek felett, lehetővé téve a távoli parancsvégrehajtást, fájlok ellopását és további rosszindulatú kódok letöltését HTTP-alapú vezérlőszervereken (C2) keresztül, miközben a perzisztenciát a Windows regisztrációs adatbázisának Run kulcsaival garantálja.[7]

Általános káros kód trendek

A legfrissebb NKI oldalán elérhető hírek alapján a fenyegetési szereplők, mint az orosz Star Blizzard, már szerveroldali szűréssel észlelik az áldozat eszközét, hogy célzottan iPhone-specifikus támadókódokat juttassanak célba. Ezzel párhuzamosan megjelent a VoidStealer, amely a világon elsőként hardveres töréspontok segítségével, közvetlenül a memóriából nyeri ki a böngészők titkosítási főkulcsait, megkerülve a Chrome legújabb védelmi vonalait. A lakossági szektorban a Steam platformján terjedő kártékony játékok, míg a szakmai körökben a népszerű fejlesztői eszközöket (pl. Claude Code) utánzó, hamisított weboldalak és a ClickFix technika jelentenek kritikus kockázatot, ahol legitim Windows-segédprogramok (pl. finger.exe) segítségével telepítenek információlopókat és távoli hozzáférést biztosító backdoorokat.

[7] https://www.antiy.net/p/analysis-of-oceanlotus-organizations-targeted-phishing-attacks-against-key-targets-in-china/

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Márciusban erős trendemelkedés látható a mirai illetve a qsnatch fertőzési számaiban, a TOP3 legsikeresebb kártevő viszont továbbra sem változott.

Káros kód	Trend
Vextrio	↔
BADBOX 2.0	↔
Vo1d(2)	↔
Randybus	↔
mirai	↑
Nymaim	↓
Ngioweb	↓
Tiny Banker	↓
SmokeLoader	↓
gsnatc	↑

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

A 2026 márciusi fenyegetettségi adatok alapján a sikeres zsarolóvírus-támadások számának emelkedése szoros összefüggésbe hozható a geopolitikai feszültségek és katonai konfliktusok során megfigyelt kibertevékenységgel.

Szektoranalízis

A 2026. márciusi adatok a zsarolóvírus-aktivitás erősödését mutatják az előző hónaphoz képest. A támadások elsődleges célpontjaivá a gyártó-, az építő- és az ipari szektor, valamint az egészségügyi és jogi szolgáltatók váltak. Európában Franciaország vált a leginkább érintett országgá 36 regisztrált támadással, megelőzve Németországot és az Egyesült Királyságot. A közép-európai régióban Ausztria, Csehország és Lengyelország területén is átlagon felüli fenyegetettséget mértek.

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. márciusi adatok alapján a Qilin zsarolóvírus-csoport megőrizte piacvezető szerepét, és az elért sikeres támadásainak száma folyamatos emelkedést mutat. Ez a tendencia a csoport technikai stabilitását és a partnerhálózatuk hatékonyságát igazolja, miközben továbbra is a kettős zsarolás módszerével kényszerítik térdre az áldozataikat. A statisztikák szerint a legnépszerűbb zsarolóvírus-családok tevékenysége általános növekedési pályán mozog, azonban kiemelendő a LockBit visszatérése, illetve több új csoport megjelenése is amelyek az előző időszakhoz képest jelentős mértékben növelni tudták sikeres műveleteiknek intenzitását.

Típus	Trend
Qilin	↔
Gentlemen	↔
Akira	↔
LockBit	↑
NightSpire	↔
ALP-001	↑
Coinbase Cartel	↑
Gunra	↑
Dragon Force	↔
APT73	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

A zsarolóvírus-csoportok támadási stratégiájának alapkövét továbbra is a jól ismert, kritikus javítatlan sebezhetőségek jelentik, amelyek segítségével a támadók behatolhatnak a hálózatokba, kiterjeszthetik jogosultságaikat, vagy távoli kódvégrehajtást érhetnek el. A tapasztalatok azt mutatják,hogy a kiberbűnözők előszeretettel támaszkodnak a régebbi, de széles körben elterjedt hibákra, mivel sok szervezetnél a biztonsági frissítések telepítése továbbra is elmarad a fenyegetések ütemétől.

A zsarolóvírus-akciók során leggyakrabban kihasznált sebezhetőségek technikai szempontból három fő kategóriába sorolhatók:

- A Log4Shell (CVE-2021-44228) és a Spring4Shell (CVE-2022-22965) továbbra is a legveszélyesebb belépési pontok közé tartoznak, mivel a Java-alapú alkalmazásokon keresztül teljes szerverkontrollt biztosítanak a támadóknak. Hasonlóan kritikus a BlueKeep (CVE-2019-0708), amely a régebbi Windows rendszerek távoli asztali elérését (RDP) támadja, lehetőséget adva a kártevők gyors, hálózaton belüli önsokszorosítására.
- A Zerologon (CVE-2020-1472) és a CVE-2018-8453 segítségével a támadók egyszerű felhasználói jogosultságról tartományi adminisztrátori szintre emelhetik magukat, ami elengedhetetlen a zsarolóvírusok teljes hálózatra kiterjedő telepítéséhez. A legújabb kritikus hiba, a CVE-2024-1709 (ConnectWise ScreenConnect) pedig a hitelesítés teljes megkerülését teszi lehetővé, közvetlen utat nyitva a távoli elérésű eszközök feletti átvételhez.
- A CVE-2019-11510 (Pulse Secure VPN) továbbra is népszerű módszer a kezdeti hozzáférés megszerzésére, mivel a javítatlan VPN-átjárókon keresztül a támadók tiszta szöveges jelszavakhoz és aktív munkamenet-kulcsokhoz férhetnek hozzá, észrevétlenül bejutva a vállalati belső hálózatokba.

Ezen sebezhetőségek kombinált alkalmazása lehetővé teszi a zsarolóvírus-csoportok számára, hogy a behatolást követően pillanatok alatt kompromittálják a teljes IT-infrastruktúrát, megbénítva az üzletmenetet és előkészítve a terepet a váltságdíj-követeléseknek.

ICS/SCADA

2026 márciusában Európára vonatkozóan az ICS/SCADA kiberbiztonsági helyzete több, egymással összefüggő dimenzió mentén írható le: konkrét incidensek, aktív fenyegetési trendek, technológiai sérülékenységek, valamint szabályozási és stratégiai változások. Ezek együtt egy egyértelműen romló, de egyre tudatosabb kezelt fenyegetési környezetet rajzolnak ki.

Az egyik legfrissebb, Európához közvetlenül köthető esemény a 2026. március 24-én észlelt kibertámadás volt az Európai Bizottság ellen.[8] A támadás felhőinfrastruktúrát érintette, amely a publikus webes szolgáltatásokat (Európa platform) szolgálja ki. Bár a belső rendszerek nem sérültek, és a szolgáltatás nem állt le, az első vizsgálatok szerint adatlopás történt, akár több száz gigabájtnyi érzékeny adattal. Ez az incidens mutatja, hogy az EU intézményi és digitális infrastruktúrája – amely számos kritikus szolgáltatást koordinál – célpont, és az IT-OT határ egyre inkább elmosódni látszik.

Közvetlenebbül az ICS/SCADA környezetet érintő fejlemény, hogy márciusban publikált kutatások szerint továbbra is jelentős számú ipari vezérlőeszköz (OT/ICS) marad közvetlenül internere kötve, ami súlyos kockázatot jelenthet. A Team Cymru jelentése kiemeli, hogy ezek az eszközök aktívan célpontjai nemzetállami támadóknak és több ezer egyedi IP-címen detektáltak célzott aktivitást. Ez különösen kritikus az energiahálózatok és alállomások esetében (pl.: RTU-k), ahol a kompromittálás fizikai hatásokkal járhat. Ezzel párhuzamosan a támadási felszín tovább bővülhet: egyes jelentések szerint globális (és részben Európát is érintő) ipari és közlekedési rendszerek ellen. 2026 márciusában jelentősen nőtt a zavarás és a spoofing jellegű támadások száma, például műholdas navigációs rendszerek ellen, amelyek kulcsszerepet játszanak a tengeri és logisztikai infrastruktúrában. Ez közvetetten ICS-kockázattal járhat, mivel a modern ipari rendszerek egyre inkább külső adatforrásokra támaszkodnak.

[8] https://nki.gov.hu/it-biztonsag/hirek/ujabb-kibertamadas-erte-az-europai-bizottsagot/

Március hónapban érintett ipari és IoT rendszerek listája:

- Labkotec LID-3300IP[9]
- Mobiliti e-mobi.hu[10]
- ePower epower.ie [11]
- Everon OCPP Backends [12]
- Apeman Cameras[13]
- Lantronix EDS3000PS and EDS5000[14]
- Honeywell IQ4x BMS Controller (Update A)[15]
- Siemens RUGGEDCOM APE1808 Devices[16]
- Siemens SIMATIC[17]
- CODESYS in Festo Automation Suite[18]
- Schneider Electric SCADAPack and RemoteConnect[19]
- CTEK Chargeportal [20]
- IGL-Technologies eParking.fi [21]
- Automated Logic WebCTRL Premium Server [22]
- Pharos Controls Mosaic Show Controller[23]
- Schneider Electric Plant iT/Brewmaxx [24]
- WAGO GmbH & Co. KG Industrial Managed Switches [25]
- PTC Windchill Product Lifecycle Management
- Anritsu Remote Spectrum Monitor
- PX4 Autopilot

[9] https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-05
[10] https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-06
[11] https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-07
[12] https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-08
[13] https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-01
[14] https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-02
[15] https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-03
[16] https://www.cisa.gov/news-events/ics-advisories/icsa-26-071-02
[17] https://www.cisa.gov/news-events/ics-advisories/icsa-26-071-04
[18] https://www.cisa.gov/news-events/ics-advisories/icsa-26-076-01
[19] https://www.cisa.gov/news-events/ics-advisories/icsa-26-076-02
[20] https://www.cisa.gov/news-events/ics-advisories/icsa-26-078-06
[21] https://www.cisa.gov/news-events/ics-advisories/icsa-26-078-07
[22] https://www.cisa.gov/news-events/ics-advisories/icsa-26-078-08
[23] https://www.cisa.gov/news-events/ics-advisories/icsa-26-083-01
[24] https://www.cisa.gov/news-events/ics-advisories/icsa-26-083-03
[25] https://www.cisa.gov/news-events/ics-advisories/icsa-26-085-01

- PTC Windchill Product Lifecycle Management[26]
- Anritsu Remote Spectrum Monitor[27]
- PX4 Autopilot[28]

A fenti listán található ipari és OT/ICS környezetben használt megoldás is szerepel, amelyek közül különösen relevánsnak a SCADA/BMS rendszerekhez és ipari hálózati eszközökhöz kapcsolódó technológiák, mint például a Schneider Electric SCADAPAck és EcoStruxure megoldásai, valamint a WAGO ipari menedzsment switchei. Mindemellett a CODSESYS alapú vezérlési környezetek és a Honeywell BMS kontrollerei szintén kiemelt kockázatot hordoznak, mivel széles körben alkalmazzák őket épületautomatizásában és ipari folyamatirányításban.

Kiemelt figyelemmel lehetünk a Siemens SIMATIC platform közelmúltban előforduló sérülékenységire, mivel széles körben alkalmazzák kritikus infrastruktúrákban, beleértve a gyártást, energetikát és közműszolgáltatásokat. A rendszerhez kapcsolódóan több, magas súlyosságú sérülékenység került publikálásra, amelyek egy része távoli kódfuttatást vagy hitelesítési mechanizmusok megkerülését is lehetővé teheti, különösen nem megfelelően szegmentált hálózati környezetben. A jelentős európai telepített bázis, a patching folyamatok gyakori késedelme, valamint az OT környezetekben jellemző hosszú életciklus miatt a SIMATIC rendszerek továbbra is vonzó célpontot jelenthetnek a célzott támadások számára, így indokolt ezek fokozott monitorozása és sérülékenységkezelése egyaránt.

Lényegében elmondható, hogy Európában az ICS/SCADA biztonság jelenleg egy átmeneti fázisban van, a fenyegetések gyorsabban fejlődnek, mint a védekezési gyakorlatok, ugyanakkor a szabályozás és a tudatosság most kezd felzárkózni ehhez az élethelyzethez.

[26] https://www.cisa.gov/news-events/ics-advisories/icsa-26-085-03
[27] https://www.cisa.gov/news-events/ics-advisories/icsa-26-090-01
[28] https://www.cisa.gov/news-events/ics-advisories/icsa-26-090-02

Sérülékenységek

Sérülékenység publikálások az NKI weboldalán március hónapban (kritikus)	Sérülékenység publikálások a CISA KEV katalógusában [29]március hónapban
CVE-2026-21902	CVE-2026-22719
CVE-2025-13942	CVE-2026-21385
CVE-2026-1670	CVE-2017-7921
CVE-2026-28289	CVE-2021-22681
CVE-2017-7921	CVE-2023-43000
CVE-2021-22681	CVE-2021-30952
CVE-2025-26399	CVE-2023-41974
CVE-2026-23813	CVE-2021-22054
CVE-2026-20131	CVE-2025-26399
CVE-2026-21992	CVE-2026-1603
CVE-2025-54068	CVE-2025-68613
CVE-2026-33017	CVE-2026-3910
CVE-2026-4681	CVE-2026-3909
CVE-2026-21643	CVE-2025-47813
CVE-2025-53521	CVE-2025-66376
CVE-2026-3055	CVE-2026-20963
	CVE-2026-20131
	CVE-2025-32432
	CVE-2025-54068
	CVE-2025-43510
	CVE-2025-43520
	CVE-2025-31277
	CVE-2026-33017
	CVE-2026-33634
	CVE-2025-53521
	CVE-2026-3055

3. ábra: Márciusi összegző táblázat az NKI által publikált kritikus sérülékenységekből, illetve a CISA KEV katalógusából

[29] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

A 2026 márciusában azonosított, aktívan kihasznált sérülékenységek közül a CVE-2026-22719, a CVE-2026-21385 és a CVE-2025-54068 egyaránt kiemelt kockázatot jelentenek, különösen kritikus rendszereket üzemeltető infrastruktúrák számára, ugyanakkor eltérő szerepet töltenek be a támadási láncokban. Mindhárom sérülékenység magas súlyossági besorolással rendelkezik, és szerepelnek a CISA Known Exploited Vulnerabilityes (KEV) katalógusában, ami megerősíti, hogy azokat valós támadások során is kihasználják.

A CVE-2026-22719 elsősorban egy gyorsan aktívan kihasznált, kezdeti hozzáférést biztosító sérülékenységként értelmezhető, amely alkalmas lehet peremvédelmi rendszerek megkerülésére és a hálózatba történő elsődleges behatolásra. Ezzel szemben a CVE-2026-21385 egy szélesebb körben elterjedt, több támadói eszköztárba integrált sérülékenység, amely különösen alkalmas lehet jogosultságkiterjesztésre vagy laterális mozgás támogatására, ezáltal elősegítve a támadók mélyebb beágyazódását a célzott környezetekben. A CVE-2025-54068 esetében a fő kockázatot az jelenti, hogy egy régebbi, de továbbra is aktívan kihasznált sérülékenységről van szó, amely különösen a nehezen frissíthető, legacy rendszereket tartalmazó környezetekben – például ipari vagy IT infrastruktúrákban – biztosíthat tartós hozzáférést és perzisztenciát a támadók számára.

A fent említettek közül, két sérülékenység együttes kihasználása egy jól ismert támadási mintázatot rajzol ki: a VMware Aria Operations sérülékenység révén történő kezdeti kompromittációt követően a Laravel Livewire Code Injection sérülékenység stabil perzisztenciát és hosszabb távú jelenlétet tehet lehetővé. Ez a kombináció különösen veszélyes lehet a kritikus infrastruktúrák esetében, ahol a heterogén, részben legacy rendszerek és az IT-OT konvergencia miatt egy sikeres támadás hatása jelentősen kiterjedhet az üzletmentre és a fizikai folyamatokra is.

Ennek megfelelően ezen sérülékenysége során kiemelten fontos a javítások prioritásalapú telepítése, a hálózati szegmentáció erősítése, valamint a detekciós és válaszadási képességek folyamatos fejlesztése.

A Nemzeti Kiberbiztonsági Intézet (NKI) hivatalos oldalán elérhető riasztások alapján a kritikus sérülékenységek közül 3 esetében is készült riasztás:

- CVE-2025-53521[30]
- CVE-2026-21262, CVE-2026-26127 [31]

Ezek közül kiemelkedik a CVE-2025-53521, amely az F5 BIG IP Access Policy Manager (APM) komponensét érinti, és egy hitelesítés nélkül kihasználható, kritikus (CVSS 9.3) távoli kódfuttatást lehetővé tevő sérülékenység, amelyet a támadók már aktívan alkalmaznak valós környezetben.

4. ábra: a fent említett sebezhetőséget (CVE-2025-53521) érintő kibertámadások /az érintett sebezhetőséghez köthető összes kibertámadási és kiberbűnözői kihasználási hivatkozás összesített megjelenítését szemlélteti

Emellett a Microsoft havi biztonsági frissítései kapcsán több tucat sérülékenység került javításra, köztük két nulladik napi (zero-day) hiba: a CVE-2026-21262 (CVSS 8.8), amely jogosultságkiterjesztést tesz lehetővé SQL Server környezetben, valamint a CVE-2026-26127 (CVSS 7.5), ami szolgáltatásmegtagadásos (DoS) támadások végrehajtására ad lehetőséget .NET alapú rendszerek ellen. A riasztások alapján ezek a sérülékenységek különösen veszélyesek széles körű elterjedésük, aktív kihasználhatóságuk és kritikus rendszereket érintő hatásuk miatt, ezért minden esetben

[30] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-f5-big-ip-access-policy-manager-termeket-erinto-serulekenysegrol/
[31] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-termekeket-erinto-serulekenysegekrol-2026-marcius/

a biztonsági frissítések haladéktalan telepítése és az érintett rendszerek fokozott ellenőrzése javasolt.

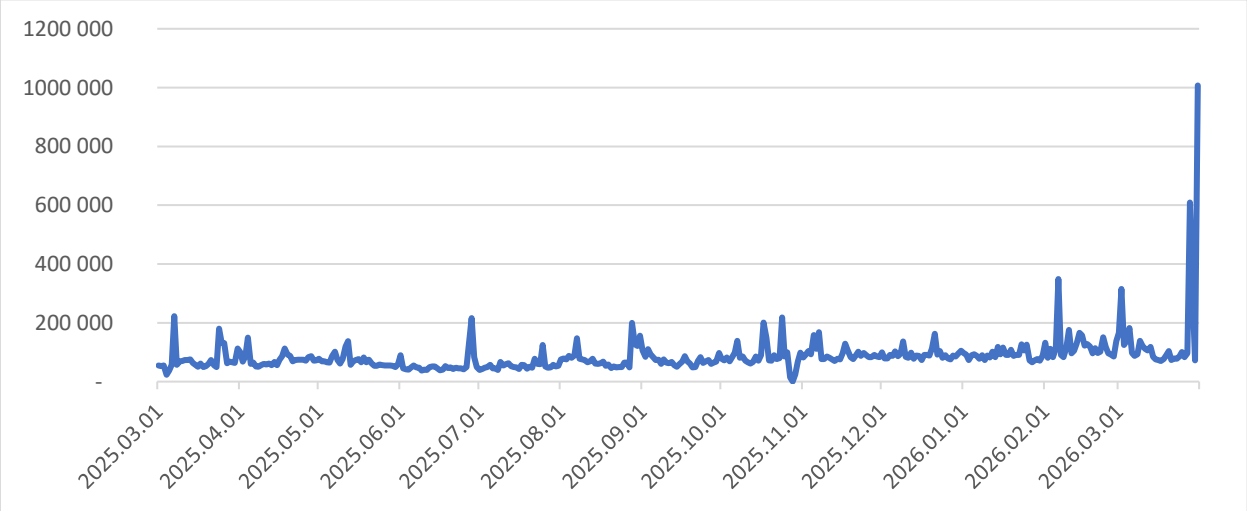
Honeypot forgalom elemzése

A Honeypot szenzoraira érkező események között kifejezetten érdekes indikátor lehet a támadás forrásának megtekintése. Habár a proxy-k, VPN-ek és Tor kijáratok világában a geolokáció érdektelenné válik, a bennük felfedezhető trendváltozások és a mögöttes adatok már más fényben tüntetnek fel eseményeket. Március hónapban ugyanis a forrás országok vizsgálata során az Egyesült Államok messzemenőleg dominált.

Egyesült Államok	4,577,557
Franciaország	1,043,624
Hollandia	974,690
Kína	962,902
India	689,764

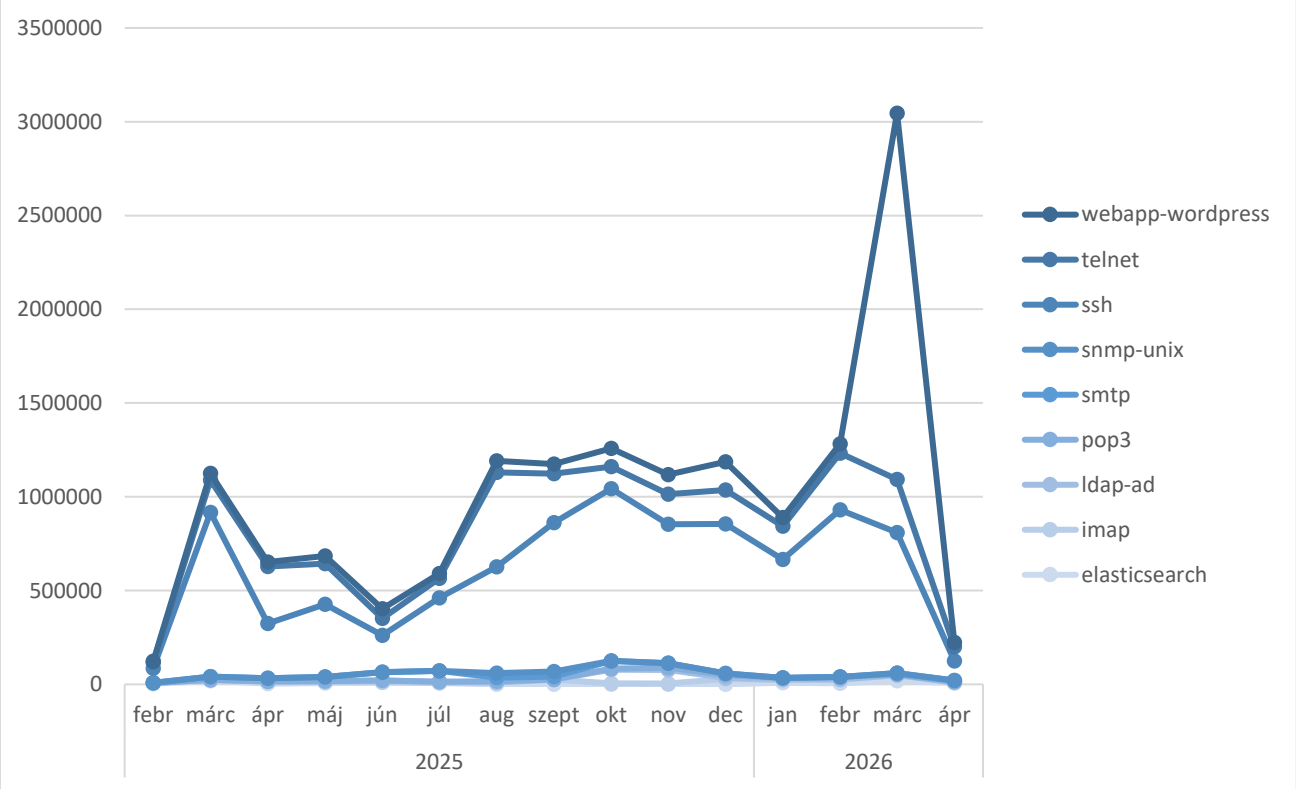
5. ábra: A Top 5 támadói ország március hónapban.

A tény, hogy az Egyesült Államok első helyen végez támadói országok listáján nem, hordoz magában sok meglepetést. Az USA digitális infrastruktúrában fejlett ország, amely rengeteg elérhető hoszting szolgáltatással rendelkezik, illetve a nagy technológiai vállalatok többsége is innen eredeztethető. Azonban, ha mélyebben megtekintjük az adatokat egy drasztikus változás nyomait figyelhetjük meg, ugyanis az előző hónapokhoz képest 44-76%-os növekedést regisztráltunk.



6. ábra: Az Egyesült Államokból származó események számának változása

Ha közelebbről is megvizsgáljuk támadásokat felfedezhetjük, hogy az érintett csapda protokollok között március egyedisége a megnövekedett Wordpress elleni incidensek voltak. A webapp csapda egy karbantartás alatt álló admin felületet szimulál. Az ide érkező támadási kísérleteket általában brute force jogosultságszerzés, szkennelés vagy DoS jellegű próbálkozások jellemzik.



6. ábra: Hálózati forgalom változása szolgáltatásonként

A hónapra fókuszálva a beérkező adatok alapján több ütemű, egy forráshoz tartozó támadást fedezhetünk fel. Nem kevesebb mint 1.8 millió bejegyzés keletkezett egy Google felhőszolgáltatásaihoz köthető domaintől. Az elsőre valid crawler programnak tűnő forgalom azonban egy perzisztens automatizált támadást rejt, amely többféle módon próbál jogosultságot szerezni a Wordpress oldalhoz alapvető felhasználónév-jelszó párosok és hibák kihasználásával.

Havi vendégszektor elemzés: amerikai és izraeli kritikus infrastruktúra célpontok

A 2026. február 28-át követő időszak kiberdimenzióját elsősorban a pro-iráni hacktivista aktivitás gyors felfutása jellemezte az amerikai–izraeli csapásokat követően. A rendelkezésre álló Insikt - anyagok alapján több, egymással összehangoltnak tűnő műveletet és felelősségvállalást figyeltek meg, különösen izraeli civil, média - és kommunikációs célpontokkal kapcsolatban. Ugyanakkor a korai szakaszban megjelent állítások túlnyomó része nem nyert független megerősítést, ezért az első hetek aktivitása inkább mobilizációs és információs-pszichológiai hullámként, semmint bizonyítottan nagy volumenű, technikailag sikeres romboló kampányként értékelhető. Az iráni internetkapcsolat jelentős visszaesését például az elemzések inkább kormányzati lekapcsolásként, mintsem külső kibertámadás következményeként kezelték, még annak ellenére is, hogy párhuzamosan az amerikai és izraeli műveletek érzékelhető zavarokat okoztak az iráni központosított kiberirányítási struktúrában és hálózati infrastruktúrában.

Az Irán körüli geopolitikai feszültségek eszkalációja jelentős növekedést eredményezett a közel-keleti kormányzati és diplomáciai célpontok elleni, állami támogatású adathalász kampányokban. A támadók kompromittált hivatalos e-mail infrastruktúrát és kontextus-specifikus social engineering technikákat alkalmaznak a hitelesség növelésére, miközben fejlett eszköztárat használnak (pl. OWA credential harvesting oldalak, tracking pixelek, Rust-alapú backdoorok .NET loaderen keresztül). Egyes aktorok kifinomult célzási mechanizmusokat (pl. geofencing) és hosszú távú bizalomépítésre épülő támadási láncokat alkalmaznak a hitelesítő adatok megszerzése és a hozzáférés fenntartása érdekében.[32]

Az időszak egyik legerősebben alátámasztott incidense a Handala nevű, Iránhoz köthető hacktivista csoporthoz kapcsolható Stryker-támadás volt 2026. márciusában. A több forrásban is visszatérő információk szerint a támadás jelentős működési zavart okozott az amerikai orvostechnológiai (medtech) vállalat globális hálózataiban, miközben

[32] https://www.proofpoint.com/us/blog/threat-insight/iran-conflict-drives-heightened-espionage-activity-against-middle-east-targets

a csoport a műveletet nyíltan megtorlásként keretezte az amerikai–izraeli csapásokra válaszul. Bár az elkövetők által hangoztatott, megszerzett adatmennyiségre és egyes részletekre vonatkozó állítások propagandisztikus elemeket is tartalmazhattak, maga az incidens ténye és az üzleti fennakadás több ponton is megerősítést nyert. Ez az eset az adott időszak leginkább validált, konfliktushoz köthető kiberműveletként kezelhető, különösen annak fényében, hogy más, nagy volumenűnek beállított akciók – például a Lockheed Martin elleni, 375 TB adatlopásra vonatkozó APT IRAN claim[33] – hitelessége erősen megkérdőjelezhetőnek bizonyult.

Említésre méltó még Kash Patel személyes e-mailfiókjának 2026. március vége körüli kompromittálását[34], amelyet több forrás iráni kötődésű szereplőkhöz, köztük a Handala Hack Teamhez kapcsol. Az incidenshez nyilvános kiszivárogtatás is társult, amely során személyes dokumentumok, levelezések és egyéb érzékeny adatok kerültek publikálásra, amit az amerikai Igazságügyi Minisztérium is megerősített. Ez arra utal, hogy a művelet elsődleges célja nem infrastruktúra-rombolás, hanem reputációs és pszichológiai nyomásgyakorlás lehetett. Az eset jól illeszkedik abba a mintázatba, amelyben magas láthatóságú személyek és szimbolikus célpontok válnak a konfliktus cyberfrontjának részévé, és ahol az adatszivárogtatás, a doxing és a médiavisszhang generálása kiemelt szerepet kap.

A következő hitelesebben alátámasztott trend az amerikai kritikus infrastruktúra elleni iráni kötődésű OT/PLC-célzás volt 2026. áprilisa elején. Az erre vonatkozó anyagok szerint internet felől elérhető PLC-ket és más ipari vezérlőrendszereket céloztak, különösen a víz-, szennyvíz-, energia- és egyéb kritikus infrastruktúra-szektorokban. Kiemelten érintettek voltak a Unitronics Vision Series típusú eszközök, amelyek kompromittálása demonstrálta, hogy a fizikai folyamatokat vezérlő rendszerek továbbra is elsődleges célpontot jelentenek. Az összkép ugyanakkor azt mutatja, hogy ez inkább folyamatos kampánytrendként, nem pedig egyetlen kiugró incidensként értelmezhető.

Ezzel párhuzamosan az iráni állami és félállami szereplők működésében is eltolódás figyelhető meg: a központi kiberképességek átmeneti visszaszorulása mellett a hangsúly

[33] https://www.lockheedmartin.com/en-us/careers/why-lm/recruitment-fraud.html#:~:text=Official%20company%20email%20domain:%20@LMCO.com
[34] https://www.reuters.com/world/us/iran-linked-hackers-claim-breach-of-fbi-directors-personal-email-doj-official-2026-03-27/

a félautonóm APT-csoportokra (pl. Charming Kitten, OilRig, MuddyWater/Seedworm) és proxy hálózatokra helyeződött át. Ezek a szereplők továbbra is aktívan alkalmazzák a bevett technikákat – spearphishing kampányok, Microsoft Exchange és VPN-sérülékenységek (pl. CVE-2019-11510) kihasználása[35], RDP-alapú kezdeti hozzáférés, valamint „living-off-the-land" eszközök használata[36], miközben fejlettebb eszközkészletet is bevetnek, beleértve új backdoorokat (pl. Dindoor, Fakeset), legitim tanúsítványokkal aláírt malware-eket és felhőalapú adat-exfiltrációt (pl. Rclone használata)[37].

Az időszak cyberfenyegetettségi képe összetett, hibrid mintázatot mutat: a nagy láthatóságú, gyakran túlzó hacktivista claim-ek mellett valós, de inkább célzott és technikailag kontrollált műveletek zajlanak. A fenyegetés valós és több dimenzióban is alátámasztott (kémkedés, kezdeti hozzáférés, OT-célzás), azonban a nyilvános narratívák által sugallt, széles körű destruktív hatás ebben az időszakban korlátozottabbnak tűnik.

[35] https://blog.polyswarm.io/cyber-strategy-under-fire-iranian-apt-and-proxy-retaliation-risks
[36] https://www.huntress.com/blog/muddywater-attack-chain
[37] https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

Lezárás, védelmi javaslatok

Az NKI (Nemzeti Kiberbiztonsági Intézet) weboldala folyamatosan frissített riasztásokat, sérülékenységi értesítéseket, valamint gyakorlati útmutatókat nyújt a kiberbiztonsági helyzet értelmezéséhez, és hatékony védekezési tanácsokat biztosít különböző szektorok számára. Kiemelten javasoljuk az aktívan kihasználtként megjelölt sebezhetőségeket tartalmazó szoftverek lehető leggyorsabb frissítését.

A vizsgált időszakban tapasztalt eseményekkel kapcsolatban, az látható, hogy továbbra is a pszichológiai manipulációs (social engineering) típusú támadók nagyon népszerűek.

A magát megbízható személynek beállító támadók, hivatalosnak tűnő, de közben káros kódot tartalmazó főként e-mailben küldött dokumentumok, érvénytelen aláírással rendelkező szoftverek ellen a leghatékonyabb védekezés a felhasználói tudatosítás, melynek keretében nagymértékben növelhető az ilyen támadások elleni védekezési képesség.

Javasoljuk a határvédelmi eszközök és szoftverek – például tűzfalak, távoli hozzáférést biztosító megoldások (például MDM rendszerek) valamint az e-mail szűrést végző termékek, ideértve a spamkarantént is - naprakészen tartását. Ezeknek az eszközöknek a kompromittálódása súlyos biztonsági kockázatot jelenthet, mivel az esetleges támadók ezen keresztül könnyen hozzáférhetnek a szervezet belső hálózati szegmenseihez.

A szervezeteknek erősíteniük kell a Zero Trust alapú hozzáférés-kezelést, a többfaktoros hitelesítést és a viselkedéselemzésen alapuló végpontvédelmi (EDR/XDR) megoldásokat, amelyek képesek az anomáliák felismerésére még fájlmentes vagy dinamikusan generált kártevők esetén is. Emellett fontos a felhasználói tudatosság növelése, különösen a spear-phishing és social engineering támadások ellen, valamint a naplózás és a SIEM-alapú folyamatos monitorozás erősítése.

Ipari vezérlőrendszereket üzemeltető partnereink számára kiemelten javasoljuk, hogy kerüljék az internet felőli, védtelen elérések kialakítását. Emellett fontos, hogy rendszeresen ellenőrizzék az érintett eszközök biztonsági frissítéseinek elérhetőségeit, valamint azok telepítését haladéktalanul végezzék el. Ezzel jelentősen csökkenthető a külső fenyegetésekkel szembeni sérülékenység.

Védelmi szempontból a márciusi fenyegetési kép alapján elsődleges prioritás a gyors és kockázatalapú sérülékenységkezelés, különösen a peremvédelmi, VPN-, levelezési, Office-, felhő- és távoli elérésű rendszerek esetében, mivel az APT- és zsarolóvírus-szereplők jellemzően ismert, de javítatlan hibákon keresztül jutnak be, ezzel párhuzamosan elengedhetetlen a többfaktoros hitelesítés széles körű bevezetése, a hitelesítő adatok védelme, a kiemelt fiókok folyamatos monitorozása, valamint a spearphishing és mobilplatformokat célzó támadások elleni felhasználói tudatosság növelése. Kiemelten fontos a hálózati szegmentáció erősítése az IT-, felhő-és OT/ICS-környezetek között, a közvetlenül internet felől elérhető ipari és IoT-eszközök felülvizsgálata, a legitim szolgáltatások mögé rejtett C2-kommunikáció, a DLL sideloading, a PowerShell- és LNK-alapú fertőzési láncok, valamint a memóriában futó implantátumok detektálására alkalmas naplózási és EDR-képességek fejlesztése. A zsarolóvírus-kockázat csökkentése érdekében szükséges a jogosultságok minimalizálása, az adminisztratív hozzáférések szeparálása, a mentések offline vagy immutábilis védelme, a helyreállítás rendszeres tesztelése, továbbá a beszállítói láncok és kritikus partnerek biztonsági ellenőrzése is, mert a jelenlegi trendek azt mutatják, hogy a támadók egyre gyakrabban kombinálják a kémkedési, hozzáférésszerzési, adatszivárogtatási és zsarolási módszereket egyazon műveleten belül.

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