2026 április 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 havi CTI jelentés fókuszában továbbra is a fejlett, célzott kibertámadások és a zsarolóvírus-kampányok állnak, különös tekintettel az állami kötődésű APT csoportok aktivitására. A jelentés kitér az iráni és más geopolitikai hátterű szereplők módszereire, például a módosított Tor-kliensekkel végzett rejtett hozzáférésre, az ICS/SCADA környezetek kompromittálására, valamint a BYOVD technikák terjedésére, amelyekkel a támadók legitim, de sérülékeny drivereket használnak a védelmi rendszerek megkerülésére. Emellett hangsúlyos szerepet kapnak az ipari infrastruktúrákat érő fenyegetések, különösen az energia-, víz- és automatizálási rendszerek elleni támadások.

A jelentés részletes áttekintést ad a globális és hazai károskódtrendekről, beleértve az aktuálisan legaktívabb malware és ransomware csoportokat, valamint azok trendváltozásait. Kiemelten foglalkozik a zsarolóvírus-ökoszisztéma átrendeződésével, az újonnan erősödő csoportokkal és az általuk kihasznált sérülékenységekkel. A dokumentum bemutatja a legfontosabb CVE-ket, köztük VPN, virtualizációs, backup és peremvédelmi rendszereket érintő hibákat, amelyek kritikus belépési pontot biztosíthatnak vállalati környezetek kompromittálásához.

Külön fejezet foglalkozik az egészségügyi szektort érő kibertámadásokkal, ahol a ransomware incidensek mellett az adatlopásos és kettős zsarolási kampányok is meghatározó trendként jelennek meg. A jelentés ismerteti a nemzetközi és hazai incidensek működési és üzleti hatásait, beleértve a betegellátást, az egészségügyi informatikai rendszereket és a beszállítói láncokat érintő következményeket.

Káros kódok és zsarolóvírusok

APT csoportok

A Sandworm (APT-C-13) néven ismert fenyegetési csoport áprilisban kifinomult adathalász kampányt folytatott[1], amelynek célja a kritikus infrastruktúrák és diplomáciai szervek hálózatába való rejtett behatolás. A támadók zsarolóprogramok helyett tartós hozzáférésre törekednek: a fertőzési lánc során egy módosított Tor-klienst telepítenek, amely rejtett szolgáltatásként (hidden service) működik, így az áldozat belső hálózati szolgáltatásait – például az SSH, SMB és RDP protokollokat – kívülről is elérhetővé teszik a támadók számára. Ez a módszer megkerüli a hagyományos tűzfalakat, mivel a forgalmat legális TCP-adatfolyamnak álcázzák, lehetővé téve a hosszú távú kémkedést és az adatszivárogtatást.

Az iráni kötődésű szereplők az internetre közvetlenül csatlakozó programozható logikai vezérlők (PLC) ellen indítottak támadásokat[2]. A támadók nem használnak hagyományos kártékony kódokat, hanem legális mérnöki szoftverekkel (például Rockwell Automation Studio 5000) csatlakoznak a nem megfelelően szegmentált eszközökhöz az ipari protokollokon (EtherNet/IP, Modbus) keresztül. A behatolók módosítják a vezérlési logikát és hamisítják a SCADA/HMI felületeken megjelenő adatokat, ami közvetlen üzemzavart és fizikai kockázatokat idézhet elő az ipari környezetekben.

A Dragon Breath csoport pedig egy kritikus sebezhetőséget kihasználva az úgynevezett BYOVD (Bring Your Own Vulnerable Driver) technikát alkalmazta, hogy megkerülhessen EDR (Endpoint Detection and Response) rendszereket[3]. A támadás során egy érvényes Microsoft WHQL aláírással rendelkező kernel drivert (dragoncore_k.sys) telepítenek a célrendszerekre. Mivel a driver aláírása hiteles, az operációs rendszer betölti azt, a támadók pedig kernel szintű jogosultságokat szerezve képesek leállítani a védelmi szoftvereket, például a Microsoft Defender-t, és megkerülni a PPL (Protected Process Light) folyamatvédelmet.

[1] https://www.ctfiot.com/306024.html
[2] https://www.ic3.gov/CSA/2026/260407.pdf
[3] https://ransom-isac.org/blog/dragonbreath-dragon-in-the-kernel/

Általános káros kód trendek

A legfrissebb NKI oldalán elérhető hírek alapján a GlassWorm v2 kampány során rosszindulatú Visual Studio Code bővítményekkel fertőzik meg a fejlesztők munkaállomásait, ahol a kártékony funkciókat gyakran csak egy későbbi frissítés aktiválja, megkerülve ezzel a kezdeti ellenőrzéseket. A Cisco tűzfalakat érintő Firestarter backdoor rávilágít arra, hogy a szoftveres javítás önmagában nem garantálja a biztonságot: a kártevő a rendszerindítási folyamat manipulálásával képes túlélni a frissítéseket, így a fertőzött eszközök teljes újratelepítése (re-imaging) válik szükségessé. Az ellátási láncok elleni támadások a tartalomkezelő rendszereket is elérték, ahol az EssentialPlugin WordPress-bővítményekbe épített vezérlőszerver-alapú (C2) hátsó kapu több mint harminc népszerű kiegészítőt kompromittált, lehetőséget adva távoli kódfuttatásra és a konfigurációs fájlok módosítására.

A Silver Fox APT csoport legújabb kampánya során a Dragon Breath csoporthoz hasonlóan a kifinomult „Bring Your Own Vulnerable Driver" (BYOVD) technikát alkalmazza, amelynek lényege, hogy egy legális, de sebezhető kerneldrivert (jelen esetben a wnBios állományt) kényszerít a rendszerre. Ez a módszer azért különösen veszélyes, mert a kernel szintű hozzáférés révén a támadók közvetlenül a fizikai memóriába írhatnak, és hatástalaníthatják a telepített védelmi szoftvereket, mielőtt azok észlelnék a ValleyRAT trójai vírus jelenlétét. Hasonló műveleti sebességre és precizitásra törekszik a Medusa zsarolóvírus-csoport is, amely a frissen publikált sérülékenységeket akár órákon belül kihasználja a kettős zsarolási stratégia – az adatok egyidejű ellopása és titkosítása – megvalósításához. A fenyegetettség ellensúlyozására a Google Drive egy új, mesterséges intelligencia alapú védelmi funkciót vezetett be, amely a zsarolóvírusokra jellemző tömeges és gyanús fájlmódosítások észlelésekor azonnal leállítja a felhőalapú szinkronizációt, megakadályozva ezzel a felhőben tárolt adatok fertőződését és segítve a gyors helyreállítást.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Áprilisban megjelent a kártékony proxyhálózatot jelző IPIDEA illetve a Matsnu kártékony kód. Fertőzési számaiban, a TOP3 legsikeresebb kártevő viszont továbbra sem változott.

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

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

Kiemelt esemény, magyarországi támadások

Kiemelt eseménynek tekinthető az áprilisban bekövetkezett, a MediaWorks Magyarország ellen elkövetett kibertámadás, amelyet a WordLeaks zsarolócsoport vállalt magára. Mivel azonban egyelőre nem érhetők el konkrét információk, nem tudni, hogy zsarolóvírusos támadás vagy más jellegű hackertevékenység állhatott-e az eset mögött.

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. áprilisi adatok alapján a Qilin zsarolóvírus-csoport megőrizte piacvezető szerepét, viszont az elért sikeres támadásainak száma csökkenést mutat az előző hónaphoz képest. A többi zsarolóvírus tekintetében viszont erős átrendeződés látható: nagymértékű trendemelkedés látható, a Coinbase, Payouts King esetében, új elemként bekerült a listába a Krybit és a SchrodingerCat. Nem volt nagy jelenléte viszont a Play, CL0P variánsoknak, melyek az elmúlt hónapokban eddig jelentős aktivitást mutattak.

Típus	Trend
Qilin	↔
Gentlemen	↔
Dragon Force	↑
Akira	↔
Coinbase	↑
INC	↑
LockBit	↓
Payouts King	↑
Krybit	↑
SchrodingerCat	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

Az április hónapban monitorozott zsarolóvírus-akciók során leggyakrabban kihasznált sebezhetőségek technikai szempontból elsősorban a biztonsági mentési rendszerek, virtualizációs platformok, VPN- és tűzfaleszközök, valamint távoli hozzáférési szolgáltatások kompromittálásához kapcsolódnak.

- CVE-2023-27532 és a CVE-2024-40711 a Veeam Backup & Replication rendszereket érintő kritikus sérülékenységek, amelyek különösen veszélyesek zsarolóvírus-támadások esetén, mivel a támadók hozzáférhetnek a mentési infrastruktúrához, illetve jogosulatlan távoli kódfuttatást hajthatnak végre. Ez lehetővé teheti a biztonsági mentések törlését vagy manipulálását, jelentősen növelve a váltságdíjfizetés kikényszerítésének esélyét.
- CVE-2021-21972 a VMware vCenter Server sérülékenysége, amely hálózati hozzáférés esetén távoli kódfuttatást tehet lehetővé a vCenter kiszolgálón. Mivel

a virtualizációs környezetek gyakran teljes szerverparkokat kezelnek, egy sikeres támadás gyorsan kiterjedhet több üzletkritikus rendszerre is.

- CVE-2020-3259 és a CVE-2023-20269 Cisco ASA/FTD eszközöket érintő sérülékenységek, amelyek a VPN- és peremvédelmi infrastruktúrákon keresztül jelenthetnek kockázatot. Ezek kihasználása érzékeny információk kiszivárgásához, illetve jogosulatlan VPN-hozzáférési kísérletek támogatásához vezethet.
- CVE-2024-40766 a SonicWall SonicOS hozzáférés-kezelési hibája, amely jogosulatlan erőforrás-hozzáférést és bizonyos esetekben tűzfaleszközök leállását okozhatja, ezáltal kezdeti behatolási pontként szolgálhat támadói csoportok számára.
- CVE-2021-27876 a Veritas Backup Exec hitelesítési mechanizmusát érintő sérülékenység, amely jogosulatlan hozzáférést és adatkezelési műveletek végrehajtását teheti lehetővé a mentési környezetben.

Ezen sérülékenységek közös jellemzője, hogy a támadók számára közvetlen hozzáférést biztosíthatnak a vállalati infrastruktúra kulcselemeihez: a mentésekhez, virtualizációs rendszerekhez, VPN-kapukhoz és tűzfalakhoz. Kombinált kihasználásuk lehetővé teheti a gyors oldalirányú mozgást, a biztonsági mentések semlegesítését, majd a teljes IT-környezet titkosítását, jelentősen fokozva a zsarolóvírus-támadások üzleti hatását.

ICS/SCADA

2026 áprilisában kiemelt ICS/SCADA esemény, hogy a CISA, FBI és NSA közös figyelmeztetése szerint iráni kötődésű szereplők több kritikus infrastruktúra-szektorban különösen víz, szennyvíz és energetikai környezetekben, internetkapcsolattal rendelkező PLC-ket és HMI/SCADA rendszereket próbáltak kompromittálni, kiemelten Rockwell Automation / Allen-Bradley eszközöket.[4] A szakértői elemzés szerint a támadások célja nem pusztán hozzáférésszerzés volt, hanem operatív folyamatok manipulálása, projektfájlok módosítása és szolgáltatáskimaradások előidézése is.
A hónap során jelentős figyelmet kapott a víz és energiagazdálkodási iparágban a több

[4] https://www.techradar.com/pro/security/us-agencies-warn-iranian-hackers-are-targeting-american-critical-infrastructure-causing-disruptive-effects-within-the-united-states

mint 100 országban 7700 közüzemi szolgáltatóval kapcsolatban álló Itron IT rendszerébe történ behatolás, mely a gyártó szerint nem érintette az ügyfelek adatait, viszont nem is volt hajlandó elárulni, mely rendszereit érintette a támadás. Megemlítendő, hogy a CISA elindította a „CI Fortify" kezdeményezést[5], amelynek célja, hogy a kritikus infrastruktúra szereplők kibertámadások idején is képesek legyenek működni akár internet és telekommunikációs kapcsolatok nélkül is. A kezdeményezés az OT-hálózatok szegmentálását, a külső függőségek leválasztását, valamint az izolált működés és helyreállítás képességének fejlesztését hangsúlyozza, reagálva többek között a kínai Volt Typhoon kampány és más állami hátterű OT-fenyegetések tanulságaira.[6]

A hónapban a CISA által publikált kritikus ICS sebezhetőségek:

- Hitachi Energy Ellipse[7]
- Contemporary Controls BASC 20T[8]
- Horner Automation Cscape and XL4, XL7 PLC[9]
- Anviz Multiple Products[10]
- AVEVA Pipeline Simulation[11]
- Siemens SCALANCE[12]
- Silex Technology SD-330AC and AMC Manager[13]
- SenseLive X3050[14]
- Carlson Software VASCO-B GNSS Receiver[15]
- Milesight Cameras[16]

[5] https://www.cisa.gov/topics/industrial-control-systems/ci-fortify
[6] https://therecord.media/cisa-initiative-aims-for-critical-infrastructure-to-operate-during-cyberattacks
[7] https://www.cisa.gov/news-events/ics-advisories/icsa-26-092-03
[8] https://www.cisa.gov/news-events/ics-advisories/icsa-26-099-01
[9] https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-02
[10] https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-03
[11] https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-04
[12] https://www.cisa.gov/news-events/ics-advisories/icsa-26-111-07
[13] https://www.cisa.gov/news-events/ics-advisories/icsa-26-111-10
[14] https://www.cisa.gov/news-events/ics-advisories/icsa-26-111-12
[15] https://www.cisa.gov/news-events/ics-advisories/icsa-26-113-02
[16] https://www.cisa.gov/news-events/ics-advisories/icsa-26-113-03

- Hangzhou Xiongmai Technology Co., Ltd XM530 IP Camera[17]
- Intrado 911 Emergency Gateway (EGW)[18]
- ABB Edgenius Management Portal[19]

A hónap során számos, európai ipari és energetikai környezetekben széles körben alkalmazott technológia, többek között Siemens, Schneider Electric, ABB, Mitsubishi és AVEVA rendszerek kapcsán jelentek meg magas kockázatú sérülékenységek, amelyek potenciálisan lehetővé tehetik távoli kódfuttatást, jogosultságkiterjesztéstvagy OT-folyamatok manipulációját. Az európai kritikus infrastruktúrákat érintő orosz/proxy aktivitásról szóló hírszerzési és kiberbiztonsági jelentések egyre hangsúlyosabbá válása tovább növelte a kockázatokat, miközben a szakértői közösség mindinkább azt emelte ki, hogy a működési stabilitás, a hálózati szegmentáció és az izolált működési képesség váljon elsődleges prioritássá.[20] A CISA és több OT-biztonsági szereplő szerint az MI alapú támadási képességek gyors fejlődése tovább növeli annak kockázatát, hogy a jövőben automatizált és nagy sebességű kiberműveletek érjék az ipari környezeteket és közműszolgáltatókat.

[17] https://www.cisa.gov/news-events/ics-advisories/icsa-26-113-05
[18] https://www.cisa.gov/news-events/ics-advisories/icsa-26-113-06
[19] https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-03
[20] https://www.securityweek.com/sweden-blames-pro-russian-group-for-cyberattack-last-year-on-its-energy-infrastructure/

Sérülékenységek

2026 áprilisának legfontosabb sebezhetősége a CVE-2026-31431[21] azonosítójú, Linux rendszerek kernelét érintő Copy Fail, melyről az NKI riasztást is adott ki[22]. A sérülékenység sikeres kihasználásával egy alacsony jogosultsági szintű helyi felhasználó vagy folyamat root szintű hozzáférést szerezhet az érintett Linux rendszeren. A sérülékenység önmagában nem távoli belépési hiba, azonban különösen kockázatos olyan környezetekben, ahol a támadó már képes kódot futtatni.

A lista további kiemelt elemei között több peremhálózati biztonsági eszközt és fejlesztői környezetet érintő sérülékenység is szerepelt. A Fortinet FortiClient EMS egyik, CVE-2026-21643[23] azonosítójú SQL-injektálási hibája bekerült a CISA ismerten kihasznált sérülékenységeket tartalmazó KEV-katalógusába[24]. Az Adobe Acrobat Reader CVE-2026-34621[25] azonosítójú prototype pollution sérülékenysége, valamint a GitHub Enterprise Server CVE-2026-3854[26] azonosítójú, git-push parancsbefecskendezést lehetővé tevő hibája szintén a hónap kiemelt sérülékenységei közé tartozott.

Áprilisban az MI, és fejlesztői infrastruktúrákhoz kapcsolódó sérülékenységek is hangsúlyosan megjelentek. A marimo esetében egy hitelesítés nélküli távoli kódfuttatást lehetővé tevő hiba került a KEV-katalógusba, amely egy nem megfelelően védett terminál WebSocketen keresztül volt kihasználható. A Meta React Server Components CVE-2025-55182[27] azonosítójú sérülékenysége továbbra is aktívan kihasznált, kiemelt kockázatú hibának számított.

A hónap végén egy kritikus, hosztingkörnyezeteket érintő sérülékenység is nyilvánosságra került. A WebPros cPanel & WHM CVE-2026-41940[28] azonosítójú hibája a bejelentkezési folyamat hitelesítésmegkerülését tette lehetővé, és CVSS 9.8-as súlyossági értéket kapott.

[21] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-31431/
[22] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-linux-rendszereket-erinto-copy-fail-serulekenysegrol/
[23] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-21643/
[24] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2026-21643&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[25] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-34621/
[26] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-3854/
[27] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2025-55182/
[28] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-41940/

A sérülékenység bekerült a CISA KEV-katalógusába is, rendkívül rövid, háromnapos javítási határidővel.

A CISA az ismerten kihasznált sebezhetőségek listájába[29] összesen 30 elem került be áprilisban ezek közül a legfontosabbak, melyek az NKI oldalán is megjelentek:

- CVE-2026-41940: WebPros cPanel & WHM[30]
- CVE-2026-39987: marimo[31]
- CVE-2026-34197: Apache ActiveMQ[32]
- CVE-2026-35616: Fortinet FortiClient EMS[33]
- CVE-2026-34621: Adobe Acrobat & Reader[34]
- CVE-2026-1340: Ivanti Endpoint Manager Mobile (EPMM)[35]
- CVE-2026-32201: Microsoft SharePoint Szerver[36]
- CVE-2026-3502: TrueConf Client[37]
- CVE-2026-5281: Google Chrome[38]

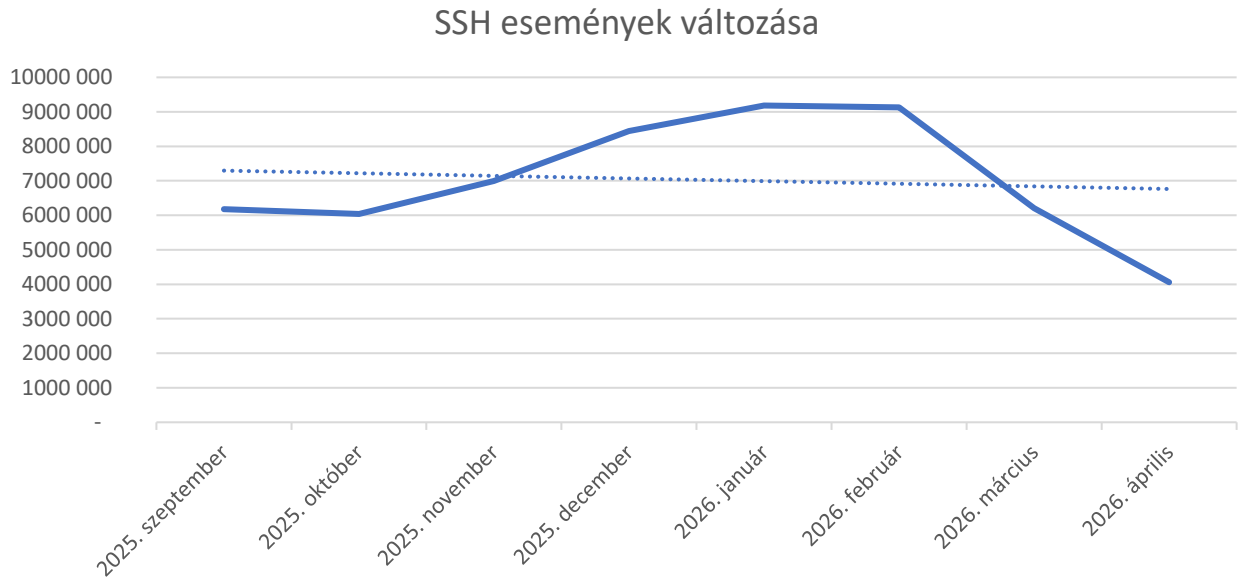
A CISA emellett ismét felhívta a figyelmet több olyan, korábban már ismert sérülékenységre, amelyeket továbbra is aktívan kihasználnak. Ezek közé tartozott a ConnectWise ScreenConnect CVE-2024-1708[39], a SimpleHelp CVE-2024-57726[40] és CVE-2024-57728[41], a Samsung MagicINFO CVE-2024-7399[42], a JetBrains TeamCity

[29] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[30] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-41940/
[31] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-39987/
[32] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-34197/
[33] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-35616/
[34] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-34621/
[35] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-1340/
[36] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-32201/
[37] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-3502/
[38] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-5281/
[39] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2024-1708&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[40] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2024-57726&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[41] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2024-57728+&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[42] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2024-7399&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=

CVE-2024-27199[43], a PaperCut NG CVE-2023-27351[44], valamint a Microsoft Exchange CVE-2023-21529[45] azonosítójú sérülékenysége. Bár a figyelmeztetés régi, ugyanakkor még mindig kihasználható Microsoft Office hibákra is kiterjedt, köztük a CVE-2009-0238[46] és CVE-2012-1854[47] azonosítójú sérülékenységekre.

Honeypot forgalom elemzése

A GovProbe Honeypot szenzoraira beérkező támadások sosem állandóak, mindig felfedezhetünk valamilyen féle eltérést, változást. Az események figyelemmel követésével megállapíthatunk különböző globális vagy ágazati trendeket. A csapdaszolgáltatásokat érintő támadásokat megvizsgálva feltűnő, hosszútávú csökkenést mutat az SSH csapdákat érintő kísérletek száma. A januári csúcshoz mérten az áprilisi érték csaknem 230% csökkenést mutat és a tendencia fokozatosan esik.



3. ábra: SSH csapdákat érintő események változása (8 hónapos visszatekintés)

[43] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2024-27199&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[44] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2023-27351&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[45] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2023-21529&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[46] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2009-0238&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=
[47] https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search=CVE-2012-1854&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=

Kontextus nélkül könnyen levonhatnánk azt a következtetést, hogy a kibertérben visszaszorulóban vannak a távoli elérést biztosító szolgáltatások elleni támadások. Azonban a mögöttes adatok másról árulkodnak. Az egyes események sikerességére több mérőszámot is fel tudunk állítani köztük belépési kísérletek mennyisége, felhasznált egyedi azonosítók, kiadott parancsok és dropper URL-ek száma.

Ha visszamenőleg megvizsgáljuk az összes eseményt felfedezhetjük, hogy arányaiban megnőtt mind a belépési kísérleteket aránya és a kiadott parancsok aránya is. Ez azt jelenti, hogy a támadók a feltérképezés után, sokkal erősebben próbálkoznak bejutni az adott SSH szolgáltatásra, illetve nagyobb arányban szereznek hozzáférést, majd kihasználva a lehetőségeket valamilyen féle funkciókat is futtatnak.

Hónap	Belépési kísérletek aránya	Kiadott parancsok aránya
2025. szeptember	98%	30%
2025. október	98%	31%
2025. november	93%	25%
2025. december	98%	16%
2026. január	98%	11%
2026. február	72%	17%
2026. március	99%	16%
2026. április	115%	52%

4. ábra: Összehasonlító ábra az SSH kísérleteket érintő belépési kísérletek és az események alatt kiadott parancsok arányáról

Mindezt megerősíti a támadások során elfogott dropper URL-ek száma. A legtöbb esetben a káros kódok bejuttatása linkeken keresztül történik. Gyakori, hogy a botnet kampányok során nagy mennyiségben, széles szórásban próbálják a hálózatukat terjeszteni. Arányaiban nézve azonban ezek igen kis hatásfokkal rendelkeznek. Habár az áprilisi adatok mennyiségükben csökkentek, a kampányok minősége és ezzel együtt sikerességük nagyban nőtt.

Hónap	Dropper URL-ek	Egyedi URL-ek	Arányszám
2025. szeptember	6866	70	0,22
2025. október	20323	101	0,66
2025. november	852	38	0,07
2025. december	6215	53	0,06
2026. január	3427	54	0,04
2026. február	2357	56	0,05
2026. március	5825	56	0,09
2026. április	2107	61	0,61

5. ábra: A támadók által bejuttatott káros kódok letöltésére szolgáló URL-ek mennyisége (összes és egyedi esetek) illetve az összes eseményhez viszonyított korrigált arányszámuk

Hosszabb trendet megtekintve egy fajta átalakulást fedezhetünk fel. A nagy volumenű, szórás jellegű kampányok optimalizáltabbá és kitartóbbá válnak. Habár a zaj csökken fontos, hogy rendszereink védelmét mindig körültekintően kezeljük és frissen tartsuk.

Havi vendégszektor elemzés: egészségügy II.

2026 áprilisában tovább erősödött az egészségügyi szektor elleni kibertámadási hullám, amelyet elsősorban ransomware-csoportok domináltak. Q1-hez képest a kockázat súlypontja részben az intézményi támadásokról a kapcsolódó szolgáltatók és technológiai beszállítók felé tolódott, ugyanakkor a közvetlen betegellátást érintő incidensek továbbra is kiemelt fenyegetést jelentettek. A támadók több esetben működési fennakadásokat idéztek elő, beleértve kórházi informatikai rendszerek leállását, betegadatok elérhetetlenné válását, mentőelterelést, gyógyszertári bezárásokat és kezelések halasztását. Az Egyesült Államokban a Signature Healthcare[48] elleni incidens jól mutatta ezt a trendet, a támadás következtében több intézmény kénytelen volt papíralapú működésre átállni, miközben sürgősségi betegirányítási problémák és kemoterápiás kezelések törlése is jelentkezett. Hasonlóan jelentős operatív hatás jelent meg a Mile Bluff Medical Center esetében[49] is, ahol a támadók adattitkosítást hajtottak végre, és ezzel telefonos, illetve informatikai rendszerek kiesését okozták.

A hónap másik meghatározó jellemzője a betegadatok és érzékeny egészségügyi információk elleni kettős zsarolási modell fennmaradása volt. A Caribbean Medical Center áprilisban jelentette[50], hogy egy kibertámadás mintegy 92 000 személyt érintett, miközben a Gentleman Ransomware Group nyilvánosan magára vállalta az incidenst és adatszivárogtatással fenyegetett. Bár a szervezet nem erősítette meg a támadói állításokat, az eset illeszkedik abba a szélesebb extortion-trendbe, amelyben a támadók az operatív kiesés mellett reputációs és szabályozási nyomást is alkalmaznak. Ugyanez a dinamika jelent meg több áprilisi nyílt forrású egészségügyi esetben is, ahol a fenyegetők betegnyilvántartások, intake-formok, biztosítási adatok vagy klinikai dokumentumok kiszivárogtatásával növelték a zsarolási nyomást. A hónap során több további egészségügyi adatvédelmi és ransomware-incidens is napvilágra került, köztük

[48] https://www.techtarget.com/healthtechsecurity/news/366641391/Cyberattack-continues-to-disrupt-operations-at-Signature-Healthcare
[49] https://www.hipaajournal.com/cyberattacks-florida-physician-specialists-mile-bluff-medical-center/
[50] https://beyondmachines.net/event_details/ransomware-and-email-breaches-impact-three-u-s-healthcare-providers-p-c-s-2-n/gD2P6Ple2L

a Minidoka Memorial Hospital, az Advanced Diagnostic Imaging, valamint ausztrál egészségügyi szolgáltatók érintettségével[51].

Európában szintén jelentős incidensek történtek, Hollandiában a ChipSoft egészségügyi szoftverszolgáltatót érte ransomware-támadás[52], amely több kórház elektronikus betegnyilvántartási és betegportál rendszereit érintette. Hasonlóképpen, a Stryker elleni Handala-művelet[53] azt jelezte, hogy a medtech vállalatok is egyre inkább elsődleges célponttá válnak, a rendelkezésre álló források szerint a támadás destruktív komponenseket is tartalmazott, és több ezer eszköz működését is érintette.

A hónap során célzott intrusion-kampányok is érintették a szektort. Az UAC-0247 ukrán egészségügyi intézmények és helyi közigazgatási célpontok elleni tevékenysége arra utalt, hogy a geopolitikai motivációjú fenyegetők továbbra is aktívan használják a phishinget, a credential theftet, a felderítést és a távoli hozzáférést biztosító malware-eket egészségügyi környezetek kompromittálására[54].

[51] https://www.comparitech.com/news/ransomware-roundup-april-2026
[52] https://www.dutchnews.nl/2026/04/patient-medical-data-stolen-in-chipsoft-ransomware-attack
[53] https://www.safestate.com/post/handala-wiper-attack-takes-stryker-offline-across-79-countries
[54] https://babel.ua/en/news/126250-russian-hackers-have-hacked-over-170-mailboxes-of-ukrainian-prosecutors-and-investigators-in-recent-months

A jelentéshez használt forrásink:

Nemzetbiztonsági Szakszolgálat – Nemzeti Kiberbiztonsági Intézet saját üzemeltetésű rendszerei

USA Cybersecurity and Infrastructure Security Agency (CISA)

European Union Agency for Cybersecurity (ENISA)

Computer Incident Response Center Luxembourg (CIRCL)

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