2026 február 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 februárjában a globális kiberfenyegetettségi környezet egyértelmű módszertani szintlépést mutatott, amelyet elsősorban a mesterséges intelligencia operatív integrációja határozott meg a támadási lánc teljes spektrumában. Az államilag támogatott APT-csoportok – különösen kínai, iráni és észak-koreai szereplők – az MI-t már nem csupán kísérleti eszközként, hanem a célpontfelderítéstől és social engineeringtől kezdve a sérülékenységek elemzésén és kártékony kód generálásán át a támadások automatizálásáig alkalmazzák. Ennek egyik látványos példája az úgynevezett „ágens alapú" malware-megközelítés, amely futás közben generált kóddal és fájlmentes működéssel jelentősen megnehezíti a hagyományos védelmi rendszerek detektálását. A geopolitikai hátterű kiberkémkedési műveletek mellett továbbra is aktívak a klasszikus támadási formák, mint például a spear-phishing, a supply-chain támadások és a legitim rendszergazdai eszközökkel való visszaélés. Ugyanakkor mindeközben a zsarolóvírus-ökoszisztéma stabilan magas aktivitást mutat. Magyarországon is megfigyelhető a banki trójaiak, információlopó kártevők és Android-alapú fenyegetések növekedése, ami jól illeszkedik a nemzetközi trendekhez, és rávilágít arra, hogy a modern kibertámadások egyre inkább a felhasználói bizalom, a legitim infrastruktúrák és az automatizált támadási technikák kombinációjára épülnek.

A CISA ICS advisory-k számos ipari és kritikus infrastruktúra-szektort érintettek. A jelentések főként ipari vezérlőrendszerekre (ICS), SCADA megoldásokra, hálózati és kommunikációs eszközökre, CCTV rendszerekre, ipari IoT berendezésekre, valamint energiaszektorhoz kapcsolódó rendszerekre (pl. EV-töltési platformok, hűtésvezérlés) vonatkoztak.

A kritikus besorolású sérülékenységek többsége távolról kihasználható (pl. remote code execution, autentikáció megkerülése, parancsinjektálás, jogosultság-kiterjesztés), amelyek megfelelő védelem hiányában veszélyeztethetik az ipari folyamatok rendelkezésre állását és integritását.

Az advisories alapján az OT/ICS környezetekben továbbra is magas a hálózaton keresztül kihasználható kritikus sérülékenységek aránya, és ez az utóbbi hónapokhoz képest növekvő trendet mutat. A leírás több olyan súlyos biztonsági problémára utal különböző rendszerekben, amelyek lehetővé tehették a támadók számára az eszközök feletti jogosulatlan irányítást, érzékeny funkciók elérését, illetve akár távoli kódfuttatást vagy szolgáltatáskiesést is. Az ilyen sérülékenységek különösen kockázatosak olyan környezetekben, ahol a rendszerek működése vagy a fizikai biztonság ezekre a technológiákra épül.

Az európai kritikus infrastruktúrák, különösen az energia - és közműszektor, egyre nagyobb kiberbiztonsági kockázatoknak vannak kitéve. A rendszerek digitalizációja, az ipari irányítástechnikai és informatikai környezetek egyre szorosabb összekapcsolása növeli a működés hatékonyságát, ugyanakkor új sérülékenységeket is teremt, amelyeket a támadók egyre kifinomultabb módszerekkel igyekeznek kihasználni. A közelmúlt eseményei is jól mutatják, hogy mind az ipari irányítórendszereket, mind a vállalati informatikai infrastruktúrát érintő támadások képesek megzavarni az energetikai szervezetek működését jelentős üzemeltetési és biztonsági kockázatot teremtve.

Káros kódok és zsarolóvírusok

APT csoportok

2026 februárjában a kiberfenyegetettségi kép módszertani szintlépést mutatott, amelyet elsősorban a mesterséges intelligencia (MI) teljes körű operatív integrációja dominált a támadási folyamat minden szakaszában. A trendek egyértelmű elmozdulást jeleznek a dinamikusan, futás közben generált kódokat alkalmazó „ágens alapú" kártevők felé, amelyek fájlmentes működésükkel és a biztonsági szoftverek kijátszására alkalmas automatizált technikákkal rendkívül nehezen detektálhatóvá teszik a behatolást.

Kiemelt

A Google Fenyegetéskutató Csoportja (GTIG) 2026. februári jelentése szerint az államilag támogatott kínai, észak-koreai és iráni hekkercsoportok (APT) szintet léptek a Gemini mesterséges intelligencia (MI) operatív használatában, és azt már nem csupán kísérleti jelleggel, hanem a támadási folyamat minden szakaszában alkalmazzák. Az iráni APT42 (más néven, Mint Sandstorm) a Gemini segítségével finomítja a célzott közösségi manipulációs (social engineering) technikáit: az áldozatok életrajza alapján hiteles profilokat és családi üzeneteket generál, valamint a nyelvi korlátok leküzdésére fordítást és kulturális kontextus-elemzést végez. Ezzel párhuzamosan az észak-koreai UNC2970 csoport nyílt forráskódú hírszerzésre (OSINT) és védelmi szektorbeli célpontok részletes profilozására használja az MI-t, míg a kínai szereplők (például az APT31) a sebezhetőségek automatizált elemzésére és az amerikai védelmi rendszerek kijátszását célzó teszttervek kidolgozására fókuszálnak. A jelentés külön kiemeli a „HONESTCUE" nevű új malware-családot, amely közvetlenül a Gemini API-ját hívja meg futás közben, hogy dinamikusan generált C# kódot kapjon a támadás második szakaszához, ami a kártevőt fájlmentessé (fileless) és a hagyományos vírusirtók számára rendkívül nehezen detektálhatóvá teszi. Ez az „ágens alapú" megközelítés lehetővé teszi a támadók számára, hogy a manuális adatgyűjtést és kódírást automatizálva, a korábbinál sokkal gyorsabban és nagyobb léptékben hajtsanak végre komplex infiltrációs műveleteket.[1]

[1] https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use

Irán

Az iráni Hírszerzési és Biztonsági Minisztériumhoz (MOIS) kötött MuddyWater (vagy GreenGolf) kibercsoport 2019 és 2026 közötti műveletei rávilágítanak a közel-keleti és európai kormányzati, diplomáciai és távközlési szektor elleni módszeres kémtevékenységre. A csoport elsődleges behatolási módszere a célzott adathalászat (spear-phishing), amely során megtévesztő Microsoft Word dokumentumokkal veszik rá a felhasználókat kártékony makrók futtatására. A támadók technikai evolúciója jól nyomon követhető: míg a korai kampányok PowerShell-alapú hátsó kapukat (backdoor) használtak, a későbbi szakaszban áttértek a legitim távfelügyeleti eszközök (RMM), mint a Syncro vagy az Atera visszaélésszerű használatára, amelyekkel észrevétlenül biztosítanak állandó rendszergazdai hozzáférést a kompromittált hálózatokhoz. A legfrissebb, 2026-os jelentések már modern, Rust nyelven írt kártevőket azonosítottak, amelyek rejtett form-objektumokból bontják ki magukat, és titkosított csatornákon keresztül kommunikálnak a vezérlőszerverrel (C2). Ez a stratégia, amely ötvözi a hivatalos diplomáciai arculattal visszaélő pszichológiai manipulációt a digitálisan aláírt, legitim szoftverek telepítésével, jelentősen megnehezíti a hagyományos védelmi rendszerek számára a támadás detektálását és a folyamatos adatgyűjtés megakadályozását.[2]

Kína

A Silver Fox APT csoport egyik alcsoportja 2026 eleje óta szisztematikus támadássorozatot folytat tajvani szervezetek ellen, adózási és e-számlázási témájú adathalász kampányokkal terjesztve a „Winos 4.0" (vagy ValleyRat) nevű távoli hozzáférést biztosító trójai programot. A támadók két fő módszert alkalmaznak a bejutáshoz: az első esetben kártékony parancsikonokat (.LNK) és obfuszkált szkripteket használnak a detektálás elkerülésére, míg a második variánsban a tajvani Pénzügyminisztérium nevével visszaélve, legitim alkalmazások mellé csomagolt kártékony DLL-fájlokkal (DLL sideloading) tévesztik meg a védelmi rendszereket. Ez utóbbi módszer során a kártékony kód egy megbízható folyamat környezetében fut le, kihasználva a Windows fájlkeresési mechanizmusait. [3]

A TeamT5 kiberbiztonsági vállalat 2024 február végén megerősítette, hogy a saját fejlesztésű ThreatSonar zsarolóprogram-ellenes szoftverében felfedezett CVE-2024-7694

[2] https://www.genians.co.kr/
[3] https://www.fortinet.com/blog/threat-research/massive-winos-40-campaigns-target-taiwan

azonosítójú sérülékenységet már 2024-ben célzott támadásokhoz használták fel. Ez a biztonsági hiba egy úgynevezett korlátozás nélküli fájlfeltöltési sebezhetőség, amely lehetővé teszi, hogy egy adminisztrátori jogosultsággal rendelkező támadó kártékony állományokat juttasson a szerverre, és ott tetszőleges parancsokat hajtson végre (arbitrary command execution). A TeamT5 elemzése szerint a támadássorozat mögött kínai állami hátterű csoportok, név szerint a Slime57 (más néven UNC4841) és a Slime62 állnak, akik egy kiterjedt ellátási lánc elleni támadás (supply-chain attack) keretében, több száz főként tajvani kompromittált eszközön keresztül maszkírozták tevékenységüket. Bár a gyártó szerint a sérülékeny verziókat már kivezettek és az érintett szervezeteket értesítették, az amerikai CISA (Cybersecurity and Infrastructure Security Agency) a sebezhetőséget felvette a ténylegesen kihasznált hibák listájára (KEV Catalog), hangsúlyozva a kockázat súlyosságát a magas profilú célpontok számára.[4]

Az UNC3886 néven hivatkozott, Kínához köthető APT csoport kiberkémkedési kampányt indított Szingapúr telekommunikációs szektora ellen, jelentette be a Szingapúri Kiberbiztonsági Ügynökség (CSA). Az Ügynökség és az Infocomm Media Development Authority (IMDA) közös védelmi hadműveletet (CYBER GUARDIAN) kezdeményezett a telekommunikációs szektor védelme érdekében. A vizsgálatok szerint az UNC3886 már 2025 júliusa óta hajt végre célzott támadási kampányokat Szingapúr négy legnagyobb telekommunikációs vállalata, az M1, a SIMBA Telecom, a Singtel és a StarHub ellen. A támadások során jellemzően hálózati eszközök és virtualizációs technológiák nulladik napi sérülékenységeit használják ki. A kiberbűnözői csoport célpontjai között leginkább az amerikai és ázsiai védelmi, technológiai és telekommunikációs szektorok szerepelnek.[5]

Dél-Korea

Az AhnLab 2026. februári jelentése szerint észak-koreai kötődésű fenyegető csoportok összehangolt kiberbiztonsági műveleteket hajtottak végre dél-koreai célpontok ellen, elsősorban adathalász e-mail alapú támadásokkal (spearphishing). A támadók megtévesztő Windows parancsikon-fájlokat (LNK) használtak, amelyek legitim dokumentumoknak álcázva ágyaztak be kártékony PowerShell parancsokat az áldozatok rendszereibe való bejutáshoz. Az elemzés két fő támadási típust azonosított:

[4] https://www.securityweek.com/cisa-hackers-exploiting-vulnerability-in-product-of-taiwan-security-firm-teamt5/
[5] https://nki.gov.hu/it-biztonsag/hirek/szingapuri-telekommunikacios-vallalatokat-vett-celba-egy-kinahoz-kotheto-apt-csoport/

az első esetben a PowerShell egy külső URL-ről töltött le további kártékony programokat, miközben a Windows beépített adatátviteli eszközét, a curl.exe fájlt átnevezve próbálta elkerülni a védelmi szoftverek detektálását, majd egy automatizálási szkriptnyelv (AutoIt) segítségével fájlkezelési és parancsvégrehajtási jogokat szerzett. A második módszernél GitHub vagy Google Drive tárhelyekről töltöttek le egy kártékony HTA (HTML alkalmazás) fájlt, amely egy adatlopó szoftvert (infostealer) és egy memóriában futó hátsó kaput (backdoor) telepített, lehetővé téve a rendszerinformációk, virtuális eszközök és bizalmas állományok folyamatos kinyerését, valamint a távoli irányítást a Windows Feladatütemezőjébe rögzített állandósítási technika révén.[6]

Általános káros kód trendek

Az NKI által közétett közzétett rendszeres IT-biztonsági hírek alapján a támadók egyre gyakrabban váltják fel a hagyományos szoftversebezhetőségek kihasználását olyan kifinomult pszichológiai manipulációval és ellátásilánc-alapú technikákkal, amelyek a felhasználói bizalomra és a legitim infrastruktúrákra építenek. A jelentések szerint mind a macOS, mind a Windows és Android rendszerek célponttá váltak: a támadók kompromittált hirdetési fiókokkal (például Google Ads), hamis állásajánlatokkal, trójai jellegű böngészőbővítményekkel vagy akár mesterséges intelligenciával támogatott kártevőkkel (mint a PromptSpy) próbálnak érzékeny adatokat, kriptovaluta-tárcákat és vállalati hitelesítő adatokat megszerezni. A védekezés kulcsa a technikai integritásellenőrzésen túl a fokozott éberség: elengedhetetlen a szoftverek kizárólag hivatalos forrásból történő beszerzése, a böngészőbővítmények minimalizálása, valamint a gyanús, interakciót igénylő (például terminálparancsok futtatására buzdító) megkeresések kritikus kezelése, mivel a támadók már olyan népszerű eszközök frissítési mechanizmusait is képesek eltéríteni, mint a Notepad++ vagy különféle fejlesztői könyvtárak.

[6] https://asec.ahnlab.com/en/

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Februárban hasonlóan az előző hónapban tapasztalt emelkedés folyatódott a banki trójai fertőzések, valamint az információ lopást végző kártevők számában, továbbá a nemzetközi trendeknek megfelelően hazánkban is igen elterjedtek az Android kártevők is.

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

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

A 2026 februárjára vonatkozó fenyegetettségi adatok alapján a sikeres zsarolóvírus-támadások (ransomware) száma stagnálást mutat, ami ugyan a növekedési ütem lassulását jelzi, de továbbra is magas szintű kockázatot jelent a szervezetek számára. A kiberbűnözői csoportok közül a Quilin őrizte meg piacvezető pozícióját, azonban mellettük markáns aktivitásnövekedés tapasztalható a LockBit és a Dragon Force részéről.

Szektoranalízis

A februárban megismert információk szerint a zsarolóvírus-csoportok elsősorban az IT, gyártó, ipari szektort, egészségügyet, jogi, valamint építési, szektort vették célba. A legtöbb incidens az Amerikai Egyesült Államokban történt, ugyanakkor Európa, illetve Közép-Európa továbbra is érintett: Magyarországról, Ausztriából, Romániából, Lengyelországból, Csehországból is jelentettek ilyen eseményeket.

Zsarolóvírus-csoportok havi aktivitási trendje

2026 februárjában a fertőzési számokat nézve továbbra is a Qilin bizonyult a legsikeresebb zsarolóvírus-csoportnak, viszont aktivitásban a LockBit csoportot emelnénk ki, hiszen az előző hónaphoz képest több mint háromszor annyi sikeres támadást hajtottak végre. A 2019-es alapítása óta aktív LockBit zsarolóvírus-csoport az elmúlt években a kiberbűnözői ökoszisztéma egyik legmeghatározóbb szereplőjévé vált, folyamatosan fejlesztve kártékony szoftvereit a 2.0-s, majd 2022 júniusában a 3.0-s verzióig. A csoport működési modellje az úgynevezett kettős zsarolásra épül, ahol nemcsak titkosítják az áldozat adatait, hanem azok nyilvánosságra hozatalával is fenyegetnek egy dedikált kiszivárogtató portálon, miközben a váltságdíj kifizetésére a hagyományos Bitcoin és Monero mellett már a Zcash kriptovalutát is elfogadják. A LockBit 3.0-val bevezetett újítások tovább fokozták a nyomást az áldozatokon, mivel lehetővé tették a fizetési határidő pénzért történő meghosszabbítását, az adatok végleges megsemmisítésének megvásárlását, sőt, akár külső harmadik felek számára is felkínálták a lopott adatok megvételét még azok publikálása előtt.

Típus	Trend
Qilin	↔
Gentlemen	↑
Play	↑
Akira	↓
CL0P	↓
LockBit	↑
Dragon Force	↑
INC	↓
NightSpire	↑
Sinobi	↓

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

A sikeres zsarolóvírus-támadások során a támadók több ismert sérülékenységet is kihasználnak, elsősorban azért, mert a szoftverek rendszeres frissítései rendszeresen elmaradnak, így ezen hibák kihasználása különösen egyszerű. A leggyakrabban felismert sebezhetőségek a Veeam Backup & Replication-t érintő CVE-2023-27532, a CVE-2020-1472 (Zerologon), valamint a Apache log4j-t érintő 2021-44228 (Log4Shell).

ICS/SCADA

2026 februárjában a CISA ICS advisory publikációi széles ipari és infrastruktúra-szektort érintettek, főleg ipari vezérlőrendszereket, SCADA megoldásokat, valamint hálózati és kommunikációs eszközöket, CCTV rendszereket, ipari IoT berendezéseket, és energiaszektorhoz kapcsolódó EV-töltési platformokat és hűtésvezérlő rendszereket érintettek. A kritikus besorolás jellemzően távolról kihasználható sebezhetőségekre utal, (pl. remote code execution, autentikáció megkerülés, parancsinjektálás vagy jogosultság-kiterjesztés), amelyek megfelelő védelem hiányában közvetlenül veszélyeztethetik az ipari folyamatok rendelkezésre állását és integritását. A publikált advisories egyértelműen jelzik, hogy az OT/ICS környezetekben továbbra is magas a hálózaton keresztül kihasználható, kritikus kockázatú sérülékenységek aránya, amely az utóbbi hónapok tükrében ez növekedést mutat.

- Avation Light Engine Pro[7]
- RISS SRL MOMA Seismic Station[8]
- Synectix LAN 232 TRIO[9]
- TP-Link Systems Inc. VIGI Series IP Camera[10]
- Mitsubishi Electric MELSEC iQ-R Series[11]
- Ilevia EVE X1 Server[12]
- Hitachi Energy XMC20[13]
- Hitachi Energy FOX61x[14]
- ZLAN Information Technology Co. ZLAN5143D[15]

[7] https://www.cisa.gov/news-events/ics-advisories/icsa-26-034-02
[8] https://www.cisa.gov/news-events/ics-advisories/icsa-26-034-03
[9] https://www.cisa.gov/news-events/ics-advisories/icsa-26-034-04
[10] https://www.cisa.gov/news-events/ics-advisories/icsa-26-036-01
[11] https://www.cisa.gov/news-events/ics-advisories/icsa-26-036-02
[12] https://www.cisa.gov/news-events/ics-advisories/icsa-26-036-04
[13] https://www.cisa.gov/news-events/ics-advisories/icsa-26-036-05
[14] https://www.cisa.gov/news-events/ics-advisories/icsa-26-036-06
[15] https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-02

- Siemens COMOS[16]
- Siemens SINEC OS[17]
- Airleader Master[18]
- Honeywell HIB2PI and HDZ Series CCTV Cameras (Update A)[19]
- Jinan USR IOT Technology Limited (PUSR) USR-W610[20]
- InSAT MasterSCADA BUK-TS[21]
- Gardyn Home Kit[22]
- Johnson Controls, Inc. Frick Controls Quantum HD[23]
- CloudCharge cloudcharge.se[24]
- EV2GO ev2go.io[25]
- SWITCH EV swtchenergy.com[26]
- EV Energy ev.energy[27]
- Mobility46 mobility46.se[28]
- Copeland XWEB and XWEB Pro[29]
- Chargemap chargemap.com[30]

Legkiemelkedőbb esetek közé tartozott a Honeywell HIB2PI és HDZ sorozatú CCTV kamerákat érintő kritikus sérülékenység, amely lehetővé tette, hogy a támadó, jogosulatlanul módosíthassa a jelszó-visszaállításhoz tartozó e-mail címet, ezáltal teljes

[16] https://www.cisa.gov/news-events/ics-advisories/icsa-26-043-03
[17] https://www.cisa.gov/news-events/ics-advisories/icsa-26-043-06
[18] https://www.cisa.gov/news-events/ics-advisories/icsa-26-043-10
[19] https://www.cisa.gov/news-events/ics-advisories/icsa-26-048-04
[20] https://www.cisa.gov/news-events/ics-advisories/icsa-26-050-03
[21] https://www.cisa.gov/news-events/ics-advisories/icsa-26-055-01
[22] https://www.cisa.gov/news-events/ics-advisories/icsa-26-055-03
[23] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-01
[24] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-03
[25] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-04
[26] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-06
[27] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-07
[28] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-08
[29] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-10
[30] https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-05

hozzáférést szerezhessen az eszközök felett, beleértve az élő kameraképek és beállítások kezelését is. Szintén jelentőségteljes volt a Siemens COMOS ipari mérnöki szoftverben azonosított sebezhetőség, amely bizonyos körülmények között távoli kódfuttatást vagy szolgáltatásmegtagadást tehetett lehetővé, potenciálisan veszélyeztetve az ipari környezetek zavartalan működését. A TP-Link VIGI sorozatú IP kamerák esetében is kritikus biztonsági hibákat jelentettek, amelyek kihasználása révén a támadók jogosulatlan hozzáférést szerezhettek az eszközökhöz, ami különös kockázatot jelent olyan infrastruktúráknál, ahol ezek a rendszerek fizikai biztonsági megfigyelésre szolgálnak.

Sérülékenységek

Sérülékenység publikálások az NKI weboldalán február hónapban (kritikus)	Sérülékenység publikálások a CISA KEV katalógusában[31] február hónapban
CVE-2026-1281	CVE-2021-39935
CVE-2025-11953	CVE-2025-64328
CVE-2019-19006	CVE-2019-19006
CVE-2025-40551	CVE-2025-40551
CVE-2025-15467	CVE-2025-11953
CVE-2026-25049	CVE-2026-24423
CVE-2026-24423	CVE-2026-21525
CVE-2025-26385	CVE-2026-21510
CVE-2026-1340	CVE-2026-21533
CVE-2024-43468	CVE-2026-21519
CVE-2025-15556	CVE-2026-21514
CVE-2025-40536	CVE-2026-20700
CVE-2026-1731	CVE-2024-43468
CVE-2020-7796	CVE-2025-15556
CVE-2021-22175	CVE-2025-40536
CVE-2026-22769	CVE-2026-1731
CVE-2026-1731	CVE-2020-7796
CVE-2025-40538	CVE-2024-7694
CVE-2025-40539	CVE-2008-0015
CVE-2025-40540	CVE-2026-2441
CVE-2026-20127	CVE-2021-22175
	CVE-2026-22769
	CVE-2025-49113
	CVE-2025-68461
	CVE-2026-25108
	CVE-2022-20775
	CVE-2026-20127

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

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

Egy magas (CVSS 7.7) besorolású sérülékenység emelkedett ki a február havi sérülékenységek közül, amely a Notepad++ szövegszerkesztő frissítési mechanizmusát érintette a 8.8.9 előtti verziókban. A hiba a WinGUp frissítő komponensben található, amely nem végzett megfelelő kriptográfiai integritás-ellenőrzést a letöltött frissítési metaadatok és telepítőcsomagok esetében. Ennek következtében egy támadó (például hálózati forgalom elfogásával vagy átirányításával) képes lehet frissítési folyamat manipulálására, és egy rosszindulatú telepítőt letölteni, majd futtatni a felhasználó rendszerén. Sikeres kihasználás esetén tetszőleges kód futtatását eredményezheti a felhasználó jogosultságaival, ami az érintett rendszerek kompromittálódásához vezethet. A sérülékenységet aktív támadások során is megfigyelték, ezért bekerült a Cybersecurity and Infrastructure Security Agency ismerten kihasznált sérülékenységek katalógusába. A probléma a Notepad++ 8.8.9 vagy az annál újabb verzióra történő frissítéssel kezelhető, amely már megfelelő aláírás ellenőrzést és integritásvédelmet alkalmaz a frissítések során.

Másik kiemelten fontos sérülékenység, amely kritikus besorolást kapott, a CVE-2019-19006 (CVSS 9.8). A Sangoma FreePBX rendszereket érintő kritikus hibát a hatóságok aktívan kihasznált sérülékenységként azonosították, és szintén felkerült a CISA KEV katalógusába.

A hiba egy nem megfelelő hitelesítési/hozzáférés-ellenőrzési mechnizmusból ered, amely lehetővé teszi, hogy egy távoli, hitelesítetlen támadó megkerülje a bejelentkezési folyamatot, és admin szintű hozzáférést szerezzen a FreePBX webes felületéhez. Sikeres kihasználás esetén a támadók így módosíthatják a telefonrendszer konfigurációját, hozzáférhetnek hívásnaplókhoz és felhasználói adatokhoz, valamint olyan rosszindulatú komponenseket telepíthetnek a rendszerbe, mint a webshell. A februári biztonsági jelentések alapján a sérülékenységet más FreePBX-hibákkal együtt támadási láncokban is alkalmazták, ezért a szervezetek számára is kritikus a sérülékeny verziók frissítése, az adminisztrációs felület hozzáférésének korlátozása, valamint kompromittáltság jeleinek ellenőrzése.

Honeypot forgalom elemzése

Az utóbbi évtizedet nagyban meghatározták a botnet jellegű kiber akciók. A tömegesen terjeszthető viszonylag nagy hatásfokkal működő Mirai típusú káros kódok megjelenése 2016-ra vezethető vissza. Ez az időszak nagyban rávilágított az internetre kihelyezett eszközök (IoT) nagy hibájára: az eszközeink biztonságának hiánya nagy kitettségnek helyez ki mindenkit. Az alapértelmezett jelszavak, elhanyagolt biztonsági frissítések bárhonnan elérhető nyitott szolgáltatások lehetővé tették a Mirai gyors térnyerését. Azóta a malware család több variánsal bővült, köztük a Satori, Moobot, Mukashi, és Soni, amelyek specializálódtak különböző sérülékenységekre és IoT eszközökre. A Nemzeti Kiberbiztonsági Intézet Honeypot adatait megtekintve is magasan a Mirai alapú káros kódok dominanciáját állapíthatjuk meg a globális trendek között.

A botnetek megfertőzött kliensek hálózatából állnak, amelyeknek különböző funkciók kiszolgálására képesek. Mindezek között talán a legszámottevőbb a DDoS avagy szolgáltatásmegtagadási képességek. A több ezer, de akár millió feletti megfertőzött kliensekből álló botnetek összehangolt hálózati támadást tudnak végrehajtani különböző célpontok ellen. Február hónapban a GovProbe Honeypot rendszer több alkalommal is elfogott ilyen jellegű PPS DDoS károskódokat.

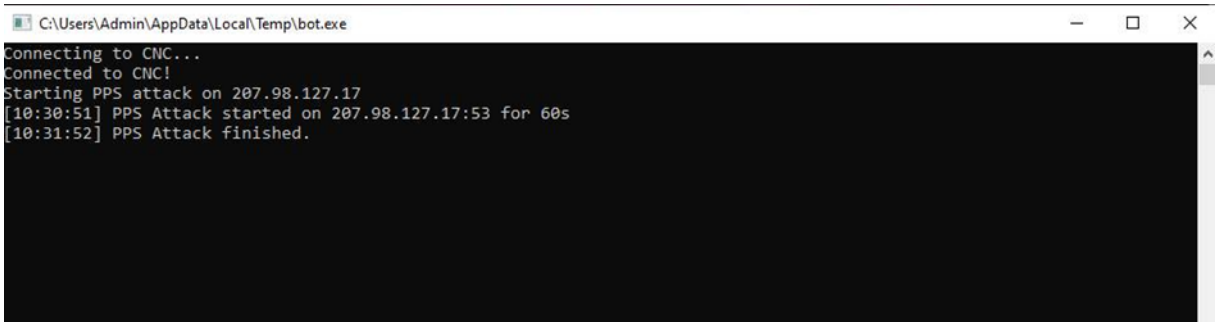
A nyílt internet felől elérhető Honeypot szondánk Telnet szolgáltatásán megjelent egy új gyanús interakció. Az Egyesült Királyságban bejegyzett IP címről több bejelentkezési kísérletet rögzítettünk. A hozzáférés kiépülése után a támadó parancsokat adott ki káros tartalmak letöltésére dropper URL-en keresztül. A kb. 10 MB-os kártékony kód Windows kliensekre specializált Go alapú program. Ennek futtatásakor a megfertőzött kliens egy román IP címen található vezérlő szerverrel (CNC vagy C2) veszi fel a kapcsolatot, majd a tőle kapott parancsokat hajtja végre:

Idő	Forrás	Cél	Üzenet
10:28:37	10.127.0.203	45.128.118.140	*REGISTER windows amd64*
10:30:50	45.128.118.140	10.127.0.203	*pps 207.98.127.17 53 60*

1. A C2 vezérlő szerver rögzíti a megfertőzött klienst a botnet hálózatban (operációs rendszer és architechtúra adatok felhasználásával).
2. A szerver kiadja a parancsot Packet-per-second DoS támadás végrehajtására 60 másodpercig.

A PPS (Packets Per Second) olyan szolgáltatásmegtagadási támadások, amelyek célja a hálózati infrastruktúra túlterhelése rendkívül nagy számú csomag másodpercenkénti küldésével, nem pedig a teljes sávszélesség kimerítésével. A támadók nem nagy mennyiségű adatot küldenek, hanem nagyon kis méretű csomagokat extrém magas sebességgel, ami arra kényszeríti a hálózati eszközöket és szervereket, hogy minden egyes csomagot külön feldolgozzanak. Ez a támadástípus elsősorban a hálózati eszközök – például tűzfalak, routerek, terheléselosztók és szerverek – csomagfeldolgozási kapacitását célozza. Mivel minden csomag feldolgozása CPU-erőforrást igényel (például ellenőrzés, szűrés vagy továbbítás során), egy elég magas csomagküldési sebesség képes kimeríteni a rendelkezésre álló erőforrásokat és szolgáltatáskimaradást okozni.

A forgalom mélyebb elemzése során megállapítható, hogy több mint 3 millió csomag került kiküldésre a 207.98.127.17 IP címen található az Egyesült Államok Oregon Egyetem DNS szerverei irányában túlterhelés reményében. Mindezek tökéletesen beleillenek a PPS típusú DoS támadások karakterisztikájába.



4. ábra Képernyő részlet a kártékony kód futtatása során felugró parancssori eseményekről

Havi vendégszektor elemzés: az európai energetikai kritikus infrastruktúrák

Az európai kritikus infrastruktúrák – különösen az energia - és közműszektor – egyre gyakrabban kerülnek kibertámadások célkeresztjébe. Az energetikai rendszerek digitalizációja, az ipari irányítástechnikai (OT) környezetek hálózatosodása, valamint az informatikai (IT) rendszerekkel való szoros integráció növeli a működési hatékonyságot, ugyanakkor új támadási felületeket is teremt. A kibertámadások ebben a szektorban nemcsak gazdasági károkat okozhatnak, hanem potenciálisan veszélyeztethetik az energiaellátás folyamatosságát és a társadalmi stabilitást is.

2025 decemberében két jelentős incidens is rávilágított az európai energetikai infrastruktúrák sérülékenységére. Lengyelországban egy, elsősorban ipari irányítórendszereket célzó támadás érintette[32] az elosztott energiatermelési létesítményeket, míg Romániában egy zsarolóvírus-támadás bénította meg[33] részben az egyik legnagyobb energetikai vállalat informatikai rendszereit. Bár egyik eset sem vezetett közvetlen ellátáskimaradáshoz, az incidensek jól szemléltetik, hogy a támadók egyre komplexebb módszerekkel próbálják megzavarni a létfontosságú szolgáltatásokat.

Lengyelországban december végén lett kibertámadás áldozata a villamosenergia-hálózatot, amely elsősorban az elosztott energiatermelő rendszerekhez (DER) kapcsolódó létesítményeket célozta. A támadás több kombinált hő- és villamosenergia-termelő egységet (CHP), valamint szél- és napenergia-diszpécser rendszereket érintett. A támadók több ipari vezérlőrendszert kompromittáltak, és egyes berendezésekben maradandó károkat okoztak. Bár az incidens mintegy 1,2 GW kapacitást érintett – ami az ország villamosenergia-termelésének körülbelül 5%-át jelenti –, az ellátásbiztonságot nem veszélyeztette, és nem következett be áramszünet. Nyilvános források legalább 12 érintett telephelyet említenek, azonban a kritikus infrastruktúra-védelemre szakosodott Dragos vállalat becslése szerint a valós szám akár 30 létesítmény is lehetett.

[32] https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-erte-a-lengyel-villamosenergia-halozatot/
[33] https://nki.gov.hu/it-biztonsag/hirek/uriemberek-aldozatava-valt-a-roman-eromu-gentlemen-ransomware/

Romániában 2025. december 26-án zsarolóvírus-támadás érte az Oltenia Energy Complex energetikai vállalatot, amely az ország legnagyobb szénalapú hőerőművi termelője. A támadás következtében a vállalat IT-infrastruktúrája részben működésképtelenné vált, több dokumentum és fájl titkosításra került, valamint átmenetileg elérhetetlenné váltak kritikus üzleti rendszerek, például az ERP-megoldások, a dokumentumkezelő rendszerek, a vállalati levelezés és a vállalati weboldal. A több mint 19 000 alkalmazottat foglalkoztató, négy erőművet üzemeltető vállalat összesen 3900 MW kapacitással rendelkezik, amely Románia villamosenergia-termelésének mintegy 30%-át biztosítja. A vállalat közlése szerint a támadás nem érintette közvetlenül az energiahálózat működését, és a termelés fenntartható maradt. Az incidens kezelése során a vállalat együttműködik a hatóságokkal a rendszerek mielőbbi helyreállítása érdekében.

Az európai energetikai infrastruktúra egyszerre van kitéve OT-rendszereket célzó ipari kibertámadásoknak és IT-rendszereket érintő zsarolóvírus-tevékenységnek, amelyek bár nem minden esetben okoznak közvetlen szolgáltatás-kiesést, jelentős működési és biztonsági kockázatot jelentenek a kritikus infrastruktúrák számára.

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.

A kritikus infrastruktúrák esetében fontos a kockázatalapú kiberbiztonsági irányítás, beleértve a rendszeres sérülékenységvizsgálatokat, incidenskezelési gyakorlatokat és biztonsági auditokat. A digitalizált rendszerek védelmét erősíti a redundáns rendszerek kialakítása, a folyamatos monitoring, valamint a beszállítói lánc biztonságának ellenőrzése, hogy a támadók ne tudjanak indirekt módon hozzáférést szerezni a kritikus rendszerekhez.

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