2026 január 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 januárjában a globális kiberfenyegetettségi környezet a decemberi csúcsponthoz viszonyítva stabilizálódott. Ez megfelel a szokásos kiberbiztonsági éves trendeknek, az év végi kampányidőszakot jellemzően januárban visszaesés követi. Mindezek mellett megmaradt a kínai és észak-koreai államilag támogatott APT-csoportok rendkívüli aktivitása. A támadások célkeresztjében januárban jellemzően a távközlési szektor és kritikus infrastruktúra állt, valamint a legitim felhőszolgáltatások. Megfigyelhető az adathalászati módszerek finomodása, például a mesterséges intelligencia integrációjának erősödése, illetve az automatizált technikák fejlődése.

A világ különböző régióiban tapasztalt támadások egyre inkább stratégiai célpontokra fókuszáltak, beleértve a SCADA/ICS rendszereket és a pénzügyi infrastruktúrákat is. Ezzel párhuzamosan megnőtt a nem állami szereplők által használt Malware-as-a-Service megoldások és az ellátási láncokon keresztüli kompromittálások száma is. A célpontok köre folyamatosan bővül, a lakossági IoT-eszközöktől egészen a magas szintű politikai, kormányzati rendszerekig.

A részletes jelentésben olvasható konkrét esetek technikák és csoportok bemutatása alapján azok a trendek, amelyek a 2025-ös év végét uralták, valószínűleg meghatározóak lesznek kiberbiztonsági szempontból 2026-ban is. A támadók eszköztára folyamatosan fejlődik, a mesterséges intelligencia alapú integrációk, automatizációk, a támadások komplexitásának és rétegeinek fejlődése (nemcsak adat, hanem rendszerelemek lopása) megköveteli, hogy a védekezés oldalán is hatékony felhasználásra kerüljenek ezek a technikai eszközök.

Káros kódok és zsarolóvírusok

APT csoportok

2026 januárjában a globális kiberfenyegetettségi kép relatív stabilitást mutatott a decemberi csúcspontokhoz képest, bár a kínai és észak-koreai állami hátterű csoportok továbbra is rendkívül aktívak maradtak. A múlt hónap kampányai elsősorban a távközlési szektor és a kritikus szolgáltatók elleni kémkedésre összpontosítottak. Megfigyelhető volt a legitim felhőszolgáltatások (GitHub, Discord) és hirdetési hálózatok (Google Ads) általi fokozott visszaélések, valamint az adathalászati módszerek finomodása, például a mesterséges intelligencia segítségével fejlesztett kártevők és a biztonsági szoftverek kijátszására alkalmas automatizált technikák megjelenése.

Oroszország

Az ESET szakértői szerint a 2025 végén a lengyel energia hálózat ellen elkövetett összehangolt támadássorozat mögött az orosz katonai hírszerzéshez köthető[1] Sandworm (más néven APT44) csoport állhat, amely a DynoWiper nevű adatmegsemmisítő kártevővel próbált meg kiterjedt áramkimaradásokat okozni. A támadás technikai érdekessége, hogy a korábbi, nagy erőműveket célzó akciókkal ellentétben ezúttal a megújuló energiaforrások (nap- és szélerőművek) és az elosztóhálózat közötti kommunikációs csatornákat vették célba, ami új típusú fenyegetést jelent az infrastruktúra stabilitására nézve. Bár a lengyel hatóságoknak sikerült elhárítaniuk a kritikus üzemzavart, a szakértők hangsúlyozzák, hogy a támadás sikere esetén akár félmillió ember maradhatott volna áram nélkül, ami rávilágít a lakossági szolgáltatások sérülékenységére és az államilag támogatott kiber-szabotázsakciók növekvő intenzitására.

[1] https://therecord.media/russia-eset-sandworm-poland-hack

Kína

A Kínához köthető UAT-7290 (más néven APT10 vagy RedFoxtrot) elnevezésű kiberkémcsoport 2022 óta szisztematikusan támadja[2] Dél-Ázsia és Délkelet-Európa távközlési infrastruktúráját. A támadássorozat technikai sajátossága egy többlépcsős, Linux-alapú fertőzési lánc, amely a hálózati eszközök ismert sérülékenységeit és az SSH-szolgáltatások elleni jelszópróbálgatásos (brute-force) módszereket használja ki a bejutáshoz. A csoport olyan specializált kártevőket vet be, mint a RushDrop, a DriveSwitch és a SilentRaid, amelyek lehetővé teszik a fertőzött rendszerek feletti teljes kontroll átvételét, az adatszivárogtatást, valamint a hálózat távoli megfigyelését. A jelentések szerint a támadók nemcsak kémkednek, hanem a kompromittált eszközökből egyfajta „átjátszó állomásokat" (úgynevezett ORB-node-okat) is létrehoznak, amelyeket később más kínai állami hacker-csoportok is felhasználhatnak további műveleteik elrejtésére, jelentős kockázatot jelentve ezzel a nemzetközi adatforgalom biztonságára.

A Kínához köthető UAT-8837 néven azonosított hacker-csoport 2026 elején célzott támadásokat indított[3] észak-amerikai kritikus szolgáltatók ellen, kihasználva a Sitecore rendszerek egy súlyos, CVE-2025-53690 azonosítójú zero-day sérülékenységét. A támadók a bejutást követően olyan nyílt forráskódú és egyedi eszközöket vetettek be – mint az Earthworm, a SharpHound és a GoExec –, amelyekkel feltérképezték a belső hálózatokat, gyengítették a biztonsági beállításokat (például kikapcsolták az admin hozzáférésű RDP korlátozását), majd kiterjedt jogosultságokat szereztek az Active Directory rendszerekben. Különösen aggasztó technikai részlet, hogy a csoport nemcsak adatokat lopott, hanem szoftveres könyvtárakat (DLL fájlokat) is eltulajdonított a célpontok saját termékeiből, ami a szakértők szerint egy jövőbeni, jóval veszélyesebb ellátási lánc elleni támadás (supply chain attack) előkészítése lehet, ahol a legális szoftverekbe építhetnek be rejtett kártevőket.

Az eSentire jelentett folyamatban lévő kibertámadási kampányt[4] indiai célpontok ellen, amely az adóhatóság nevében küldött e-mailekkel terjeszti a Blackmoon kártevőt. Az elemzés szerint a feltételezhetően kínai hátterű támadók egy kifinomult fertőzési láncot

[2] https://blog.talosintelligence.com/uat-7290/
[3] https://blog.talosintelligence.com/uat-8837/
[4] https://www.esentire.com/blog/weaponized-in-china-deployed-in-india-the-syncfuture-espionage-targeted-campaign

használnak, amely során a használt káros kód képes kijátszani a biztonsági szoftvereket (például az Avast-ot) azáltal, hogy automatizált egérmozgásokkal hozzáadja magát a kivételek listájához. A folyamat végén egy legális kínai távfelügyeleti eszközt (SyncFuture TSM) telepítenek, amely teljes körű hozzáférést biztosít az áldozatok eszközeihez, lehetővé téve a képernyőfigyelést, az e-mailek naplózását és a hosszú távú kémkedést.

Ázsiai kormányzati szervek ellen jelentett támadásokat a Kaspersky[5], amely során a HoneyMyte (más néven RedDelta) hacker-csoport a CoolClient hátsó kapu (backdoor) egy frissített változatát vetette be. Az elemzés feltárta, hogy a fertőzési lánc legitim, aláírt programok (például Sangfor alkalmazások) elleni DLL-sideloading technikával indul, majd a kártevő különféle módszerekkel - például token-imitációval és a felhasználói fiókok felügyeletének (UAC) megkerülésével - szerez emelt szintű jogosultságokat. A támadók a CoolClient segítségével teljes körű megfigyelést végeznek, amely magában foglalja a billentyűleütések naplózását, a vágólap tartalmának figyelését és a böngészőkből kinyert jelszavak ellopását, a megszerzett bizalmas dokumentumokat pedig nyilvános fájlmegosztókon keresztül szivárogtatják ki.

Észak-Korea

2026 januárjában a Genians jelentett célzott adathalász támadásokat[6] ("Operation Poseidon"), amely során az észak-koreai Konni APT csoport dél-koreai pénzintézetek és emberi jogi szervezetek nevében elküldött adathalász e-mailekkel terjesztette az EndRAT kártevőt. Az elemzés szerint a támadók a Google Ads és a Naver hirdetési infrastruktúrájával éltek vissza, mely során olyan átirányítási linkeket (redirection URL) használtak, amelyek a legitim marketing-hálózatok hírnevét kihasználva kikerülik a különböző reputáció-alapú biztonsági szűrőket. A fertőzési lánc során a gyanútlan felhasználók kompromittált WordPress oldalakról töltenek le kártékony archívumokat, amelyek egy „AutoIt-szkript" segítségével, közvetlenül a memóriába töltve indítják el az EndRAT-ot, távoli hozzáférést és tartós ellenőrzést biztosítva a hackereknek az áldozatok rendszerei felett.

[5] https://securelist.com/honeymyte-updates-coolclient-uses-browser-stealers-and-scripts/118664/
[6] https://www.genians.co.kr/en/blog/threat_intelligence/spear-phishing

Szintén a KONNI csoporthoz köthető támadást jelentett a CheckPoint[7] japán, ausztrál és indiai szoftverfejlesztők ellen, amely során a csoport egy valószínűsíthetően mesterséges intelligencia segítségével fejlesztett backdoor kártevőt vetett be. Az elemzés szerint a támadók blokklánc- és kriptovaluta-témájú, hitelesnek tűnő projekt-dokumentációnak álcázott adathalász anyagokkal tévesztik meg a szakembereket, majd a fertőzési lánc során Discordon tárolt archívumokon keresztül juttatják be a kártevőt. A technikai érdekesség, hogy az AI-támogatott backdoor fejlett elemzésgátló funkciókkal bír (például hardveres küszöbértékek és elemzőeszközök jelenlétének ellenőrzése), képes megkerülni a felhasználói fiókok felügyeletét (UAC bypass), végül pedig a legális SimpleHelp távfelügyeleti eszköz telepítésével biztosít hosszú távú, interaktív hozzáférést a támadóknak a fejlesztői környezetekhez.

Dél-Ázsia

A Zscaler ThreatLabz jelentése szerint[8] 2025 szeptembere óta egy Pakisztánhoz köthető – az APT36 csoporttal hasonlóságokat mutató – hacker-csoport hajt végre célzott támadásokat indiai kormányzati szervek ellen a „Gopher Strike" és a „Sheet Attack" kampányok keretében. Az elemzés feltárta, hogy a támadók adathalász PDF-fájlokkal tévesztik meg az áldozatokat, amelyek egy hamis Adobe szoftverfrissítés telepítésére buzdítanak, majd egy földrajzi alapú szűréssel ellátott ISO-fájlon keresztül juttatják be a kártevőket. A technikai folyamat során a Go nyelven írt GOGITTER letöltő szoftver építi ki a tartós jelenlétet, majd privát GitHub-tárolókból hívja le a GITSHELLPAD hátsó kaput és a GOSHELL betöltőt, amelyek végül egy memóriában futó Cobalt Strike Beacont aktiválnak. Ez a többlépcsős, felhőalapú infrastruktúrára épülő módszer lehetővé teszi a támadók számára a teljes körű távoli hozzáférést, a fájlok ellopását és a rendszeren belüli észrevétlen mozgást.

[7] https://research.checkpoint.com/2026/konni-targets-developers-with-ai-malware/?_gl=1*1tbhkgr*_gcl_au*MTQwMjUwNDIxMC4xNzYxMzI0MzY2
[8] https://www.zscaler.com/blogs/security-research/apt-attacks-target-indian-government-using-gogitter-gitshellpad-and-goshell

Általános káros kód trendek

Az NKI által közétett közzétett rendszeres IT-biztonsági hírek alapján a közelmúltban azonosított fenyegetések rávilágítanak a kiberbűnözés egyre professzionálisabbá válására, ahol a Malware-as-a-Service (MaaS) modellek és a mesterséges intelligencia integrációja dominál. Kiemelkedő kockázatot jelentenek a rosszindulatú böngészőbővítmények, mint például a Stanley platform[9] vagy a GhostPoster[10] kampány, amelyek képesek kijátszani a Google és a Microsoft ellenőrzési folyamatait. Ezek a bővítmények gyakran vizuális megtévesztést (pl. láthatatlan iFrame-ek) alkalmaznak adathalászatra, csalásokra vagy vállalati ERP-rendszerek[11] (Workday, SAP) hitelesítő adatainak ellopására.

Ezzel párhuzamosan a mobil fenyegetések szintet léptek, megjelentek az olyan androidos trójaik, amelyek a TensorFlow.js gépi tanulási könyvtár segítségével[12], vizuális elemzés útján hajtanak végre láthatatlan kattintásos csalásokat, miközben a Kimwolf botnet[13] már több mint 2 millió eszközt (főként olcsó Android TV boxokat) fertőzött meg, hogy azokat DDoS-támadásokhoz vagy proxyhálózatok sávszélesség-értékesítéséhez használja fel. A vállalati szektorban pedig az APT-stílusú támadások, mint a PDFSider malware[14], a legitim szoftverek (pl. PDF24) aláírásait és a DLL side-loading technikát kihasználva építenek ki hosszú távú hátsó kapukat, gyakran social engineering módszerekkel kombinálva.

[9] https://nki.gov.hu/it-biztonsag/hirek/bongeszobovitmenyeken-keresztul-terjedo-uj-kartevoszolgaltatas/
[10] https://nki.gov.hu/it-biztonsag/hirek/bongeszobovitmenyekkel-tamad-a-ghostposter-840-ezerszer-kerult-letoltesre/
[11] https://nki.gov.hu/it-biztonsag/hirek/vallalati-adatokat-vettek-celba-rosszindulatu-chrome-bovitmenyekkel/
[12] https://nki.gov.hu/it-biztonsag/hirek/mi-t-hasznal-az-uj-android-malware-hogy-rejtett-reklamokra-kattintson/
[13] https://nki.gov.hu/it-biztonsag/hirek/lakossagi-proxyhalozatokon-keresztul-novekszik-a-kimwolf-android-botnet/
[14] https://nki.gov.hu/it-biztonsag/hirek/pdfsider-malware-penzugyi-szektort-celzo-tamadasokban/

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Januárban 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	↔
Tiny Banker	↑
Ngioweb	↔
Matsnu	↑
SmokeLoader	↑
OSnatch	↑

1. ábra: Káros kód trendek Magyarországon

A beérkezett adatok elemzése alapján megállapítható, hogy az elmúlt hónapban növekvő tendenciát mutattak a .hu TLD-vel rendelkező weboldalakon az adathalász és egyéb malware-terjesztésre használt fertőzések, illetve a vezérlőszerverként működő webszerverek száma is.

Zsarolóvírusok

A 2026 januárjában visszaesést tapasztaltunk a sikeres zsarolóvírus támadások számaiban. A visszaesés egyik kulcsfontosságú eleme lehet, hogy az ünnepi időszak alacsonyabb munkaerő-kapacitásának enyhülésével a humán felügyelet hatékonysága helyreállt, így a IT biztonsággal foglalkozó szakemberek gyorsabban reagálhattak a gyanús tevékenységekre. Ezt támogathatta az egyre szélesebb körben elterjedő, gépi tanulásra épülő AI-alapú védelmi rendszerek térnyerése, amelyek képesek lehetnek még a fájltitkosítás megkezdése előtt detektálni a behatolókat. A technológiai fölény mellett a bűnüldözés is komoly csapást mért az ökoszisztémára: az

Operation Endgame-hez hasonló nemzetközi fellépések[15] során végrehajtott szerverlefoglalások és letartóztatások komoly csapást mértek a legnagyobb Ransomware-as-a-Service (RaaS) csoportok infrastruktúrájára.

Szektoranalízis

A novemberben megismert információk szerint a zsarolóvírus-csoportok elsősorban az egészségügyi-, jogi-, ipari-, valamint gyártószektort vették célba. A legtöbb incidens az Amerikai Egyesült Államokban történt, ugyanakkor Európa, illetve Közép-Európa továbbra is érintett: Magyarországról, Ausztriából, Szlovákiából, Romániából, Lengyelországból, Csehországból, Szlovéniából is jelentettek ilyen eseményeket.

[15] https://www.europol.europa.eu/media-press/newsroom/news/end-of-game-for-cybercrime-infrastructure-1025-servers-taken-down

Zsarolóvírus-csoportok havi aktivitási trendje

2026 januárjában ismételten a Qilin bizonyult a legaktívabb zsarolóvírus-csoportnak, habár összességében az elért sikeres támadási számaikban csökkenés látható. A Qilin egy Ransomware-as-a-Service (RaaS) modellben működő, Windows, Linux és VMware környezetekre szabható zsarolóvírusokat használó kiberbűnözői csoport. A támadásaikat főként adathalászattal és távoli felügyeleti eszközök (RMM) kihasználásával hajtják végre, az összegyűjtött váltságdíjakból pedig magas, 80-85%-os jutalékot kínálnak partnereiknek, miközben szigorúan tiltják a Független Államok Közössége (FÁK) országainak célba vételét. Bár követeléseik általában 50 ezer és 800 ezer dollár közé esnek, a Synnovis egészségügyi szolgáltató elleni támadás során már 50 millió dollárt követeltek, ami jelzi a csoport növekvő ambícióit és a kritikus infrastruktúrákra jelentett veszélyét.

Típus	Trend
Qilin	↓
CLOP	↑
Akira	↓
Sinobi	↑
Lynx	↑
INC	↑
Gentlemen	↑
Play	↑
Tengu	↑
NightSpire	↑

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 év elején a CISA több jelentős kiberbiztonsági figyelmeztetést és sebezhetőségi tanácsot adott ki, amelyek ipari irányító rendszereket és SCADA technológiákat érintettek. Január hónap során számos gyártó, például a Rockwell Automiation, Mitsubishi Electric, Schneider Electric és még több, az alábbiakban felsorolt gyártók termékeiben azonosítottak súlyos, bizonyos esetekben kritikus besorolású sérülékenységeket. Ezek a sebezhetőségek jellemzően távoli kódfuttatást, szolgáltatásmegtagadást (DoS) vagy jogosulatlan hozzáférést, illetve jogosultságkiterjesztést tettek lehetővé. Mind olyan támadási vektorok, amelyek súlyosan veszélyeztetik az OT/ICS rendszerek rendelkezésre állását.

- Festo Firmware
- Hitachi Energy Asset Suite
- Johnson Controls Metasys Products
- Festo Didactic SE MES PC
- iba Systems ibaPDA
- EVMAPA
- Hubitat Elevation Hubs
- AVEVA Process Optimization
- Siemens Industrial Edge Device Kit
- Siemens Industrial Edge Devices
- KiloView Encoder Series

Kiemelkedő eset volt a Johnson Controls több termékét is érintő, CVSS 10.0-s (kritikus) súlyosságú SQL injection sebezhetősége (CVE-2025-26385), amely akár hitelesítés nélküli távoli hozzáférést is lehetővé tehetett, így jelentős kockázatot jelentett a létfontosságú rendszerek integritására, valamint azok adatbiztonságára nézve. A sebezhetőség a Metasys komponenseiben található, mint az Application and Data Server (ADS) SQL Express-sel, az Extended ADS, és a System/Controller Configuration Tool korábbi verziói, amelyek 14.1-es vagy annál régebbi kiadásban futottak. A Metasys rendszerek gyakran

kórházakban, reptereken, adatközpontokban és ipari létesítményekben használatosak, ezért több ipari, és kritikus infrastruktúrák lehetnek érintettek ehhez köthető incidensben. A hiba fizikai környezetek működését is befolyásolhatta, mint például a hűtést működtető, vagy tűzjelző rendszereket.

Sérülékenységek

Sérülékenység publikálások az NKI weboldalán január hónapban (kritikus)	Sérülékenység publikálások a CISA KEV katalógusában[16] január hónapban
CVE-2025-14733	CVE-2009-0556
CVE-2020-12812	CVE-2025-37164
CVE-2026-0625	CVE-2025-8110
CVE-2025-37164	CVE-2026-20805
CVE-2026-21858	CVE-2026-20045
CVE-2025-68613	CVE-2025-68645
CVE-2025-68668	CVE-2025-34026
CVE-2026-21877	CVE-2025-31125
CVE-2025-68428	CVE-2025-54313
CVE-2025-69258	CVE-2024-37079
CVE-2025-54987	CVE-2018-14634
CVE-2026-23550	CVE-2025-52691
CVE-2025-14533	CVE-2026-23760
CVE-2026-22844	CVE-2026-24061
CVE-2026-20045	CVE-2026-21509
CVE-2025-34026	CVE-2026-24858
CVE-2025-52691	CVE-2026-1281
CVE-2026-23760	
CVE-2026-24061	
CVE-2026-23745	
CVE-2026-24858	
CVE-2026-1281	

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

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

2026 januárjában több súlyos és aktívan kihasznált sérülékenység került publikálásra. Ezek közül különös figyelmet érdemel a CVE-2026-20045[17], amely széles körben kihasznált, kritikus besorolású hálózaton keresztül kihasználható sérülékenység. Többek között Cisco Unified Communications terméket is érintett (például: Unifed CM, Unity Connection Webex Calling). A hiba oka, hogy a termékek nem megfelelően validálják a felhasználói http kérésekben érkező bemenetet, így egy hitelesítés nélküli, távoli támadó speciálisan kialakított http kérésekkel tetszőleges parancsokat futtathat az érintett rendszer operációs rendszerén. A sérülékenység sikeres kihasználása esetén a támadó alap felhasználói hozzáférést szerezhet és azt jogosultság-emeléssel root szintre növelheti, ami a teljes rendszer kompromittálásához vezethet. A National Vulnerability Database-ben (NVD) a CVSS 9.8 (kritikus) pontszámmal szerepel, valamint a hiba bekerült az USA CISA Known Exploited Vulnerabilities (KEV) katalógusába, mivel aktívan kihasznált támadásokban is megfigyelhetőek. Ezért azonnali javítási intézkedések szükségesek a sebezhető rendszerekre vonatkozóan:

- a Cisco által kiadott biztonsági frissítések azonnali telepítése
- a hálózati hozzáférés korlátozása (VPN-nel, tűzfallal)
- rendszerforgalom monitorozása, és naplózása különös tekintettel a HTTP kérésekre
- behatolásészlelő rendszerek alkalmazása (IDS/IPS)

Másik szintén kritikus sérülékenység, amit nem hagyhatunk figyelmen kívül, a CVE-2026-24061[18], ami egy kritikus, autentikáció megkerülését lehetővé tevő sérülékenység, amely a már nem támogatott, de OT és beágyazott rendszerekben továbbra is gyakran használt GNU InetUtils telnetd-t érinti, és amelyet a telnet protokollon keresztül küldött, parancssori argumentumként kezelt felhasználói környezeti változók nem megfelelő kezelése okoz. A hiba úgy használható ki, hogy a támadó a USER környezeti változót „-f root" értékre állítja, így amikor a telnetd összeállítja a bejelentkezési parancsot, az /usr/bin/login -h [hostname] „-f root" formát ölt, ahol a -f kapcsoló hatására az authentikáció teljesen kimarad, és azonnal a megadott felhasználó jogosultságával nyílik meg a parancssor. Ennek eredményeként a támadó hitelesítő adatok megadása nélkül azonnali root jogosultságot szerezhet a rendszeren. A hiba 1,9,3-től 2.7-ig terjedő InetUtils-

[17] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-20045/
[18] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-24061/

verziókat érint, 9.8 CVSS pontszámmal rendelkezik, és mivel aktívan kihasznált sérülékenységről van szó, szintén bekerült a CISA KEV katalógusába. Javasolt az elavult Telnet szolgáltatás letiltását az érintett környezetekben.

Honeypot forgalom elemzése

Nem túlzást azt állítani, hogy az IoT botnetek hosszú évek óta uralják az internetet. A Mirai típusú kártékony kódok tömegével jelennek meg a különböző Honeypot csapdákon és számuk nem látszik mérséklődni. A trend érthető mivel olcsó, könnyen fenntartható, skálázható és sajnos sikeres „üzleti modellnek" mondható az IoT botnetek világa. Terjedésével kapcsolatban továbbra is az a helyzet, hogy az interneten nagy számban érhetők el beágyazott, régebbi vagy rosszul menedzselt eszközök. Sokuknál a távoli menedzsment szolgáltatások (köztük a Telnet, SSH, stb.) kitettsége, valamint a gyenge vagy alapértelmezett hitelesítési adatok használata gyakori. Ezt a jelenséget jól illusztrálja, hogy a Shadowserver külön „Accessible Telnet[19]" riportban követi az internet felől elérhető Telnet szolgáltatásokat. A fenyegetési trendek szintjén az ENISA Threat Landscape 2024[20] is kiemeli, hogy a rendelkezésreállás elleni fenyegetések a legjelentősebb kategóriák közé tartoznak, ami összhangban van a tömeges szkennelésből és botnet-alapú infrastruktúrából fakadó kockázatokkal. A Mirai és más, hasonló IoT-botnetek esetében a nyilvánosan dokumentált működésmód része, hogy a botok tömegesen keresnek nyitott menedzsment szolgáltatásokat, majd alapértelmezett/gyenge jelszavakkal próbálnak belépni és eszközöket „toborozni"; a CISA is külön felhívta a figyelmet arra, hogy ezek a botnetek kifejezetten az alapértelmezett jelszavakat használó IoT-eszközöket célozzák.

A hétről-hétre vizsgált Honeypot adatok között Nemzeti Kiberbiztonsági Intézet is felfedezi ezt a tendenciát. A beérkezett esemény nagy hányada botnet aktivitásra utal. Habár a módszerek változnak a rájuk jellemző gyors, tömeges próbálkozási kísérletek állandósultak. A januári riportunkban egy konkrét IoT botnet példát hoztunk, amelyből kicsit jobban megismerhetjük a támadók taktikáit, gondolatmeneteit.

A vizsgált esemény során egy közigazgatási célrendszer mellé helyezett Honeypot szenzor volt érintve. A 23/tcp (Telnet) portján nagy volumenű aktivitás volt megfigyelhető

[19] https://www.shadowserver.org/what-we-do/network-reporting/accessible-telnet-report/
[20] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

egyetlen külső iráni forrás IP-címről (5.235.190.184). A forgalomképen több ezer új kapcsolódási kísérlet volt SYN-only mintázattal, vagyis a próbálkozások túlnyomó többsége a TCP kézfogás első lépésénél megállt. Az ilyen jellegű próbálkozások egy fajta „rejtett" hálózati szkennelésre utalnak, amely során a támadók megpróbálnak információt gyűjteni a célba vett hálózatról és eszközökről.

A szkennelési forgalommal párhuzamosan a naplózás pontosan 32 Telnet bejelentkezési kísérletet rögzített, amelyek között történt sikeres volt: login attempt [admin/] succeeded (azaz admin felhasználó üres jelszóval). Ez a fajta felhasználónév/jelszó mintázat tipikusnak mondható, legyakrabban a legkönnyebb áldozatokat célozzák be.

Felhasználónév	Előfordulás	Jelszó	Előfordulás
admin	26	(üres)	25
root	6	1111	1
		admin	1
		alpine	1
		hi3518	1
		klv1234	1
		qazxsw	1
		realtek	1

4. ábra: Az esemény során használt felhasználónevek és jelszavak

A sikeres hitelesítést követően rövid, szkriptelt parancssorozat látható, amely tipikusan automatizált „loader" (betöltő/telepítő) viselkedésre utal: a bot több ismert parancsot próbál ki, hogy eljusson egy használható shellhez, majd egyszerű környezetfelmérést végez és megkísérli a további komponensek letöltését/lefuttatását. Az alábbi részlet a munkamenet naplózott „beszélgetése" időrendi sorrendben.

```
login attempt [admin/] succeeded
(empty)
CMD: enable
CMD: system
Command not found: system
CMD: shell
Command not found: shell
CMD: sh
CMD: cat /proc/mounts; /bin/busybox PEWUF
CMD: cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox PEWUF
CMD: tftp; wget; /bin/busybox PEWUF
CMD: dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done <.s
Command not found: while read i
CMD: /bin/busybox PEWUF
CMD: rm .s; exit
Connection lost after 4 seconds
```

5. ábra: Az esemény során lefuttatott Telnet parancsok

A parancsok értelmezése alapján a munkamenet elején az enable, majd a system és shell próbálkozások azt sugallják, hogy a célrendszeren kezdetben egy korlátozottabb, eszköz-/appliance-jellegű CLI fogadhatta a kapcsolatot, amelyből a bot ismert „kilépési" mintákkal igyekezett valódi parancsértelmezőhöz jutni; végül a sh végrehajtása jelzi, hogy shell elérésére tett kísérlet történt. A cat /proc/mounts tipikus minimális felderítő lépés: a fájlrendszerek és csatolások alapján a bot keresi az írható helyeket és a környezet jellegét. Ezt követi a /dev/shm használata, amely egy RAM-alapú ideiglenes fájlrendszer; a .s nevű „marker" fájl létrehozása/olvasása (cat .s || cp /bin/echo .s, majd többféle fallback-olvasási módszer dd … || cat … || while read …) arra utal, hogy a bot a rendelkezésre álló parancsokat és shell-konstrukciókat teszteli, különösen minimális erőforrású BusyBox-környezetekben. A tftp; wget; … sorok a megszokott IoT-loader módszerekre utalnak (ha van elérhető letöltő/átviteli eszköz, megkísérlik payload lehúzását), a végén pedig a rm .s; exit és a gyors kapcsolatbontás a rövid életű, nyomminimalizáló automatizmusokra jellemző.

Összességében az esemény a megfigyelt mintázatok alapján leginkább egy automatizált IoT-botnettel összefüggő, Telnetre épülő „szkennelés → belépési kísérletek → rövid loader szekvencia" folyamatnak felel meg. Habár konkrét botnet család nem ismerhető fel a rendelkezésünkre álló naplókból a módszerek jól illeszkednek a széles körben dokumentált IoT-botnet működési mintákhoz.

Havi vendégszektor elemzés: fókuszban az online kártya csalások

Folytatva múlt havi, a pénzügyi szektort vizsgáló elemzésünket, ezúttal az online bankkártya-adatlopásokra, valamint az ehhez kapcsolódó kiberbűnözési ökoszisztémára fókuszálunk. Ezek a támadási és adatlopási technikák a hagyományos, nyers erőn alapuló módszereknél jóval szofisztikáltabb megközelítést alkalmaznak, ugyanakkor könnyen és nagy tömegben replikálhatók, így széles rétegeket érintenek.

Mivel az online bankkártyás fizetési lehetőségek mára széles körben elterjedtek, mind a pénzügyi szektor, mind a lakosság kitettsége jelentős. Az ilyen támadások közvetlenül kártyaadatokkal dolgoznak, ezért a tényleges pénzügyi kár azonnal és direkt módon jelentkezik.

A szektor kitettségének és aktivitásának egyik fontos indikátora nem feltétlenül a közvetlen támadások számában vagy az ezekről szóló hírekben jelenik meg, hanem az eladási oldalon figyelhető meg: a sötét weben rendszeresen kínálnak[21] részleges vagy akár teljes bankkártyaadatokat értékesítésre. Ezeket esetenként nagy csomagokban – akár százezres vagy milliós nagyságrendben – próbálják meg eladni. Mindezek alapján elmondható, hogy 2025-ben, illetve az idei év januárjában ezek a piacok rendkívül aktívak voltak. A korábbi kvázi monopolhelyzetben működő Hydra összeomlását követően a piac fragmentálttá és specializálttá vált: egyes platformok kifejezetten meghatározott „termékekre", például lopott bankkártyaadatokra fókuszálnak. Előfordul az is, hogy bizonyos piacterek „reklámkampányokat"[22] indítanak, amelyek során ingyenesen tesznek hozzáférhetővé lopott bankkártyaadatokat.

A korábbi években visszaesés volt tapasztalható ezen a területen, mivel az egyszerűbb technikák elleni hatékonyabb védekezés és a szigorodó szabályozások – például az egyszerű kétfaktoros autentikáció bevezetése – jelentősen megnehezítették a csalók tevékenységét. 2025-ben azonban ismét felfutóban[23] van ez a kiberbűnözési trend,

[21] https://www.breachsense.com/blog/dark-web-markets/
[22] https://socradar.io/blog/b1acks-stash-releases-4-million-credit-cards-for-free/
[23] https://outpost24.com/blog/carding-ecosystem-fall-financial-cybercrime/

amelyhez a technológiai fejlődés, többek között a mesterséges intelligencia integrációja is hozzájárul.

A kártyaadatok megszerzésének egyik jellemző módszere a magecart technika, amely a korábbi kártékony oldalakhoz képest kifinomultabb megoldás. A Magento e-kereskedelmi platform nevéből származó Magecart egy 2015 óta aktív hackercsoporthoz köthető kibertámadási forma, amely online vállalkozásokat céloz érzékeny adatok, különösen fizetési kártyaadatok ellopására. A támadások a webes skimming egyik típusát jelentik: a támadók harmadik felek sebezhetőségeit kihasználva rosszindulatú kódot juttatnak az online kiskereskedők fizetési oldalaira, amely a böngészőn belül futva rögzíti a vásárlók által megadott kártyaadatokat, majd azokat egy támadók által ellenőrzött domainre továbbítja. A Magecart-támadások nehezen felismerhetők[24], mivel kliensoldalon történnek, a kártékony kód gyakran a legitim weboldali kódba ágyazva jelenik meg, és a hagyományos védelmi megoldások, például a webalkalmazás-tűzfalak nem képesek észlelni őket. Emiatt a támadások hosszú ideig rejtve maradhatnak, miközben az ügyfelek tudtukon kívül kompromittált oldalon adják meg adataikat.

Magasabb szintű támadások esetén a sötét weben már pénzügyi rendszerek sebezhetőségeit és hozzáféréseit is árulják. Példaként említhető, hogy egy „bigbandz" nevű felhasználó január 11-én a WEX vállalati fizetési rendszer[25] egyik kereskedelmi fiókjához kínált hozzáférést. A csomag állítólag SOAP API-kulcsokat is tartalmazott, amelyekkel megtekinthetők a napi tranzakciók, valamint fizetések indíthatók és kártyák bocsáthatók ki. Az ilyen ajánlatok valódisága azonban érdemben nem ellenőrizhető.

A szervezeteknek többszintű biztonsági megközelítést kell alkalmazniuk a nagyméretű adatszivárgások által jelentett kockázatok csökkentése érdekében. Ennek részeként rendszeresen figyelemmel kell kísérniük a pénzügyi tranzakciókat a szokatlan vagy jogosulatlan tevékenységek időbeni észlelése érdekében, valamint be kell vezetniük a többfaktoros hitelesítést (MFA) a jogosulatlan hozzáférés megakadályozására. Fontos továbbá a munkavállalók és az ügyfelek oktatása az adathalász csalások felismerésére és a biztonságos online gyakorlatok alkalmazására, illetve a pénzintézetekkel való szoros együttműködés a kompromittált kártyákra történő gyors reagálás és a csalárd

[24] https://threatpost.com/magecart-credit-card-skimmer-avoids-vms-to-fly-under-the-radar/175993/
[25] https://darkwebinformer.com/alleged-sale-of-unauthorized-access-to-wex-corporate-payment-system-soap-api-keys/

tranzakciók megelőzése érdekében. Ügyféloldali láthatóság biztosításaként sok szervezet a webhelyén a tartalombiztonsági politika (CSP) segítségével létrehoz egy listát a megbízható domainekről, amelyekről tartalom tölthető be. Bár a CSP-k hatékonyan blokkolják a jogosulatlan szkripteket, folyamatos karbantartást igényelnek, és nem nyújtanak védelmet a megbízhatónak minősített forrásokból érkező támadások ellen, illetve a böngészőben végrehajtott forrás szkriptjeinek tekintetében korlátozott védelmet biztosítanak.

Összességében az online kártyacsalások és adatlopások továbbra is komoly kihívást jelentenek a pénzügyi szektor számára. Még csökkenő esetszám mellett is számottevő pénzügyi és reputációs veszteségeket okozhatnak, ezért a hatékony megelőzés és védekezés kiemelt jelentőséggel bír.

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.

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 elérhetőségét, és azok telepítését haladéktalanul végezzék el. Ezzel jelentősen csökkenthető a külső fenyegetésekkel szembeni sérülékenység.

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