2026 június havi CTI riport

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet havi rendszerességgel ad ki fenyegetéselemzést, mely összefoglalja a kibertér globális, valamint magyarországi helyzetét. A riport megismerése megfelelő támpontot adhat az olvasó számára, hogy szervezete milyen IT biztonsági kihívásokkal nézhet szembe a közeli jövőben.

Helyzetkép

A vizsgált időszakban a kiberfenyegetettségi környezetet továbbra is az államilag támogatott fenyegető csoportok aktív működése, a zsarolóvírus-kampányok magas intenzitása, valamint a kritikus sérülékenységek gyors kihasználása jellemezte. A támadók egyre nagyobb mértékben alkalmaznak automatizált eszközöket, kifinomult támadási technikákat és legitim szolgáltatásokat a kompromittálás, a perzisztencia kialakítása és az észlelés elkerülése érdekében.

A jelentés áttekintést nyújt az időszak legfontosabb APT-tevékenységeiről, a hazai és nemzetközi károskód és zsarolóvírus-trendekről, valamint a legaktívabb fenyegető csoportok működéséről. Emellett bemutatja a leggyakrabban kihasznált

sérülékenységeket, különös tekintettel a távoli kódfuttatást, hitelesítés-megkerülést és jogosultságkiterjesztést lehetővé tevő hibákra, valamint kitér az ipari (ICS/SCADA) környezeteket érintő aktuális kockázatokra is.

A dokumentum ismerteti továbbá a honeypot-rendszerek által megfigyelt támadási mintázatokat és a hitelesítési próbálkozások alakulását, valamint összefoglalja azokat a főbb trendeket és megállapításokat, amelyek támogatják a szervezetek kockázatértékelését, a fenyegetések időbeni felismerését és a védekezési intézkedések tervezését.

Káros kódok és zsarolóvírusok

APT csoportok

A 360 Threat Intelligence Center jelentése szerint az észak-koreai kötődésű Lazarus (APT-C-26) fenyegetési csoport a kritikus súlyosságú CVE-2025-55182 (React2Shell) sebezhetőséget használta ki, amely a React Server Components (RSC) komponensben hitelesítés nélküli távoli kódfuttatást (RCE) tesz lehetővé. A támadók a sérülékeny rendszerek tömeges felderítésére és kompromittálására egy Windowsra fordított exploitot alkalmaztak, majd a hozzáférés megszerzése után MultiRelay és Akagi64 eszközökkel oldalirányú mozgást és jogosultságkiterjesztést hajtottak végre. Ezt követően a Copperhedge Loader memóriában visszafejtette és betöltötte a Copperhedge Backdoor kártevőt, amely a korábban ismert Manuscrypt malware egyik változata. A hátsó ajtó titkosított konfigurációt tárol, rendszerinformációkat gyűjt, egyedi áldozatazonosítót hoz létre, majd HTTP-alapú vezérlőszerveres (C2) kommunikációt folytat, amely során Base64, XOR és ChaCha20 titkosítást alkalmaz az adatok védelmére. A kártevő képes parancsok végrehajtására, rendszerfelderítésre, fájl- és folyamatkezelésre, további kártevők memóriából történő betöltésére, valamint konfigurációjának távoli frissítésére. A kampány elsődleges célpontjai feltehetően pénzügyi intézmények és blokklánc-alapú infrastruktúrák voltak, ahol adatlopás, jogosulatlan pénzügyi tranzakciók és hírszerzési célú adatgyűjtés lehetett a támadások célja.

Az ESET szerint a Gamaredon APT-csoport 2025-ben fokozta Ukrajna elleni kiberkémkedési műveleteit, elsősorban kormányzati és katonai intézményeket célozva adathalász

kampányokkal, frissített kártevőkkel és legitim online szolgáltatásokkal elrejtett vezérlőszerveres (C2) infrastruktúrával. A támadásokban archív mellékletek és HTML smuggling technikát alkalmazó XHTML fájlok juttattak el HTA letöltőket, amelyek a PteroSand VBScript downloadert és további payloadokat töltöttek le; 2025 szeptemberétől a csoport a WinRAR CVE-2025-8088 útvonalbejárási sérülékenységét is kihasználta perzisztencia létrehozására a Startup mappán keresztül. A kompromittált hálózatokon belüli terjedést USB-meghajtók, hálózati meghajtók és szoftvertelepítők „felfegyverzésével" támogatták, miközben új PowerShell-alapú eszközök, például a PteroDee, PteroCache, PteroDum, PteroEffigy és PteroPaste memóriabeli futtatást, C2-címlekérést, perzisztenciát és további komponensek betöltését végezték. A Gamaredon az adatlopási folyamatokat egyre inkább felhőalapú tárhelyekre terelte: a PteroPSDoor és PteroVDoor S3-kompatibilis szolgáltatásokra, míg a PteroBox Dropboxra és rclone-alapú feltöltésre támaszkodott. A csoport Cloudflare, Microsoft devtunnels.ms, No-IP, Supabase, Telegram, Telegra.ph, Dropbox, GoFile és paste-szolgáltatások használatával rejtette el C2-feloldását, payload-terjesztését és exfiltrációs útvonalait, ami jelentősen megnehezíti a hálózati detektálást és blokkolást.

Általános káros kód trendek

A friss jelentések alapján több, eltérő célú kiberfenyegetés erősödése látható: a SentinelOne által azonosított macOS.Gaslight kártevő már nemcsak klasszikus backdoor- és adatlopó funkciókat tartalmaz, hanem kifejezetten LLM-alapú malware-elemző rendszerek megtévesztésére szolgáló prompt injection és hamis debug üzeneteket is beágyaz, ami az MI-t célzó elemzésellenes technikák megjelenésére utal. Ezzel párhuzamosan a hatóságok jelentős infrastruktúra-felszámolási műveleteket hajtottak végre: több száz szervert és domaint kapcsoltak le a SocGholish, Amadey és StealC kártevőkhöz kapcsolódó „cybercrime-as-a-service" ökoszisztémában, valamint Hollandiában egy mintegy 17 millió fertőzött eszközből álló proxy/botnet infrastruktúrát is leállítottak. A botnet-fenyegetések továbbra is kiemelt kockázatot jelentenek, amit az AryStinger esete is mutat: a kártevő elavult D-Link routereket és kisebb számban NAS-eszközöket kompromittál, majd azokat proxyként, szkennelésre, alagútforgalom továbbítására, DNS-manipulációra és távoli parancsvégrehajtásra használja. A közös tanulság, hogy az elavult, nem frissített eszközök, a gyenge hitelesítési beállítások és a nyitva hagyott távoli menedzsmentfelületek továbbra is kulcsszerepet játszanak a

tömeges kompromittálásokban, miközben a támadók egyre fejlettebb technikákkal próbálják kijátszani az automatizált és MI-alapú védelmi rendszereket.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Júniusban több változás is tapasztalható, a teljes fertőzött végpontok tekintetében erősödött az Android eszközöket fertőző BADBOX, az IPIDEA, Sailty, csökkent a Ranbyus és Ngioweb jelenléte.

Káros kód	Trend
BADBOX 2.0	↑
IPIDEA	↑
Vo1d(2)	↔
IPIDEA	↑
Socks Escort	↑
Andromeda	↑
Salty	↑
Randybus	↑
Nigoweb	↓
Pykspa	↑

1. táblázat: Káros kód trendek Magyarországon

Zsarolóvírusok

A 2026. júniusi adatok alapján a zsarolóvírus-aktivitás stagnálása mutatható ki az előző hónaphoz képest.

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. júniusi adatok alapján a legtöbb sikeres támadást a Gentlemen zsarolóvírus csoport követte el. A Gentlemen Ransomware Group 2025-ben megjelent, pénzügyileg motivált zsarolóvírus-csoport, amely világszerte támad kritikus szektorokat, különösen Ázsiában. Központosított működéssel, egyedi eszközökkel, adatlopással, titkosítással és kettős zsarolással gyakorol nyomást áldozataira. Az előző hónaphoz képest növekvő aktivitást mutat a LockBit, illetve új szereplőként jelent meg a Settra csoport több országban aktív zsarolóvírus-szereplő, amely kritikus iparágakat támad. Adattitkosítást és kettős zsarolást alkalmaz, lopott adatok kiszivárogtatásával, dark webes nyomásgyakorlással és Tox-alapú kommunikációval kényszerítve fizetésre áldozatait.

Típus	Trend
Qilin	↔
Gentlemen	↔
Dragon Force	↑
Akira	↔
INC	↑
Safepay	↑
Nova	↑
LockBit	↓
File Manager	↑
Genesis	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

A vizsgált időszak adatai alapján megállapítható, hogy a zsarolóvírus-támadások során leggyakrabban kihasznált sebezhetőségek technikai szempontból az alábbi négy fő kategóriába sorolhatók:

- Kezdeti hozzáférés és hálózati átjárók kompromittálása: A támadók továbbra is elsősorban az internet felől elérhető hálózati eszközöket és távoli hozzáférési szolgáltatásokat veszik célba. Kiemelkedő kockázatot jelentenek a Citrix NetScaler sérülékenységei (CVE-2019-19781, CVE-2023-3519, CVE-2023-4966 – Citrix Bleed), a Pulse Secure VPN hibája (CVE-2019-11510), a Fortinet SSL VPN sebezhetősége (CVE-2018-13379), valamint a Cisco ASA (CVE-2020-3259, CVE-2020-2021, CVE-2023-20269), a ConnectWise ScreenConnect (CVE-2024-1708,

CVE-2024-1709) és a F5 BIG-IP (CVE-2021-22986) sérülékenységei, amelyek hitelesítés megkerülését, jogosulatlan hozzáférést vagy távoli kódfuttatást tesznek lehetővé.

- Alkalmazás-alapú sebezhetőségek és távoli kódvégrehajtás (RCE): A támadók továbbra is előszeretettel használják ki a kritikus szerveralkalmazások távoli kódfuttatást lehetővé tevő hibáit. Gyakran visszaélnek a VMware vCenter (CVE-2021-21972, CVE-2021-22005), Spring Framework (Spring4Shell, CVE-2022-22965), Apache Log4j (Log4Shell, CVE-2021-44228), Microsoft Exchange (CVE-2021-34473, CVE-2022-41040, CVE-2022-41082), Veeam Backup & Replication (CVE-2024-40711), SonicWall (CVE-2021-20028, CVE-2024-40766), Fortinet FortiManager (CVE-2023-48788), MOVEit Transfer (CVE-2023-34362), PaperCut MF/NG (CVE-2023-27350, CVE-2023-27351), Confluence (CVE-2023-22515), valamint Veritas Backup Exec (CVE-2021-27876) sérülékenységeivel a szerverek feletti teljes ellenőrzés megszerzése érdekében.
- Hitelesítés megkerülése és érzékeny adatok megszerzése: A külső elérésű rendszerek és adatkezelő megoldások sebezhetőségei továbbra is fontos belépési pontot jelentenek. A Fortra GoAnywhere MFT (CVE-2024-0204) és MOVEit Transfer (CVE-2023-34362) hibái hitelesítés megkerülésére vagy adatlopásra adnak lehetőséget, míg a Veeam Backup & Replication (CVE-2023-27532) révén a támadók titkosított hitelesítő adatokat szerezhetnek meg. A Cl0p által is széles körben kihasznált GoAnywhere és MOVEit sérülékenységek jól mutatják, hogy a menedzselt fájlátviteli rendszerek továbbra is kiemelt célpontok.
- Jogosultságszint-emelés és belső infrastruktúra kompromittálása: A kezdeti hozzáférést követően a támadók rendszerint magasabb jogosultság megszerzésére és a hálózaton belüli laterális mozgásra törekednek. Ennek során továbbra is jelentős szerepet játszanak a Zerologon (CVE-2020-1472), a Windows RDP (BlueKeep, CVE-2019-0708), a Windows Win32k (CVE-2018-8453), a Windows CLFS (CVE-2022-24521, CVE-2022-37969), a VMware ESXi (CVE-2024-37085), valamint a Windows rendszereket érintő további jogosultságkiterjesztési sérülékenységek (például CVE-2021-36942 és CVE-2021-34523). Ezek lehetővé teszik a tartományi jogosultságok megszerzését, a laterális mozgást és végső soron a zsarolóvírus tömeges telepítését a teljes infrastruktúrán.

ICS/SCADA

Az érintett gyártók és fejlesztők között szerepel a Schneider Electric, a Mitsubishi Electric, a Rockwell Automation, a Siemens, a Delta Electronics, az AVer, az EVoke Systems, a StoneFly, az AzeoTech, továbbá több ipari környezetben alkalmazott nyílt forráskódú szoftverkomponens fejlesztője. A közzétett sérülékenységek jellemzően jogosultságkiterjesztésre, távoli kódfuttatásra, szolgáltatásmegtagadás (DoS) előidézésére, hitelesítési mechanizmusok megkerülésére, valamint bizalmas információkhoz történő jogosulatlan hozzáférésre adhatnak lehetőséget. Az érintett rendszerek között ipari vezérlők (PLC), Ethernet/IP kommunikációs adapterek, felügyeleti és adatgyűjtő megoldások, hálózati kamerák, energiatöltő infrastruktúrák menedzsmentrendszerei, adattároló rendszerek, valamint felhőalapú és mobilalkalmazások egyaránt megtalálhatók.

Kiemelt figyelmet érdemelnek a Siemens OpenSSL alapú termékeit érintő sérülékenységek, amelyek a széles körű termékérintettség miatt jelentős kockázatot hordozhatnak. Szintén fontosak a Rockwell Automation FLEX I/O EtherNet/IP adaptereit és a Delta Electronics DVP12SE PLC-it érintő biztonsági hibák, amelyek sikeres kihasználása kedvezőtlen esetben hatással lehet az ipari folyamatok rendelkezésre állására és integritására. Az AVer PTC kamerák, az EVoke Systems töltőállomás-kezelő rendszere, valamint a StoneFly Storage Concentrator sérülékenységei szintén növelhetik az érintett rendszerek kitettségét, amennyiben azok megfelelő védelem nélkül érhetők el.

A jelentési időszakban nyilvánosságra került sérülékenységek között IoT- és felhőalapú szolgáltatásokat érintő hibák is szerepelnek, többek között a Yarbo Android/iOS mobilalkalmazásához és felhőinfrastruktúrájához, valamint a Naxclow IoT Platformhoz kapcsolódóan. További érintett komponensek közé tartoznak a pydicom/pynetdicom és az OFFIS DCMTK nyílt forráskódú könyvtárak, amelyek számos ipari és egészségügyi rendszer kommunikációs funkcióinak alapját képezik. Az ilyen komponenseket felhasználó rendszerek esetében indokolt az érintettség felmérése, tekintettel arra, hogy a sérülékenységek közvetetten több gyártó termékeiben is megjelenhetnek.

Az érintett szervezetek számára javasolt a gyártók által kiadott biztonsági közlemények és javítások mielőbbi áttekintése, az elérhető biztonsági frissítések telepítése, valamint az érintett eszközök kitettségének felülvizsgálata. Emellett indokolt az ipari hálózatok szegmentálásának, a távoli hozzáférések szabályozásának, a naplózási és monitorozási képességeknek, valamint az incidensészlelési mechanizmusoknak a rendszeres felülvizsgálata és megerősítése a sérülékenységek kihasználásából eredő kockázatok csökkentése érdekében.

Sérülékenységek

A vizsgált időszakban nyilvánosságra hozott kritikus sérülékenységek alapján továbbra is meghatározó trend, hogy a támadók elsődleges célpontjai a széles körben alkalmazott vállalati infrastruktúra-elemek, hálózati biztonsági megoldások, webes alkalmazáskeretrendszerek és menedzsmentplatformok. A listában szereplő CVE-azonosítók olyan elterjedt technológiákat érintenek, mint a QNAP, Ubiquiti UniFi OS, valamint Oracle PeopleSoft. Az érintett termékek köre jól mutatja, hogy a sérülékenységek nem egyetlen gyártóhoz vagy technológiai területhez kapcsolódnak, hanem a vállalati IT-infrastruktúra teljes spektrumát lefedik.

A publikált sérülékenységek többsége kritikus besorolású, ami jellemzően távoli kódfuttatást (Remote Code Execution – RCE), jogosultságkiterjesztést, hitelesítés megkerülését vagy tetszőleges parancsvégrehajtást tesz lehetővé. Ezek a sérülékenységtípusok különösen veszélyesek, mivel sikeres kihasználásuk esetén a támadók teljes rendszerkompromittációt érhetnek el, érzékeny adatokat szerezhetnek meg, oldalirányú mozgást (lateral movement) hajthatnak végre a hálózaton belül, illetve zsarolóvírusok vagy egyéb kártékony komponensek telepítésére használhatják fel a megszerzett hozzáférést.

Kiemelt kockázatot jelentenek az internet felől közvetlenül elérhető rendszereket érintő sérülékenységek. A webes tartalomkezelő rendszereket (Joomla!, Drupal), alkalmazásszervereket (Apache Tomcat, IBM WebSphere), valamint biztonsági és hálózatvédelmi eszközöket FortiSandbox, Cisco ISE, Palo Alto PAN-OS érintő hibák várhatóan rövid időn belül megjelennek a nyilvánosan elérhető exploit-gyűjteményekben, illetve automatizált támadási kampányokban. Az elmúlt évek

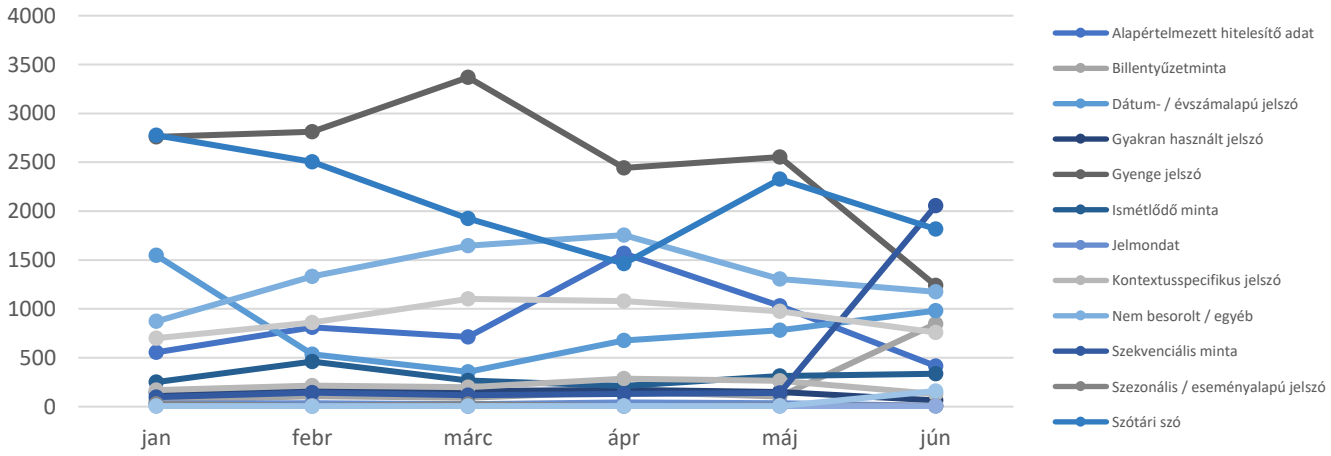
tapasztalatai alapján ezek a termékek rendszeresen szerepelnek tömeges internetes felderítések célpontjai között, ezért a javítások késedelmes telepítése jelentősen növeli a kompromittálódás valószínűségét.

A listában több olyan sérülékenység is szerepel, amely biztonsági termékeket érint, Check Point Quantum Security Gateway, Splunk. Ezek kompromittálása különösen súlyos következményekkel járhat, mivel a támadó hozzáférést szerezhet a hálózat védelmi infrastruktúrájához, módosíthatja a naplózási adatokat, megkerülheti a biztonsági ellenőrzéseket vagy további támadásokat készíthet elő.

Honeypot forgalom elemzése

A 2026. január és június közötti jelszópróbálkozások alapján a megfigyelt támadási aktivitás túlnyomórészt automatizált credential attack jellegű volt. A fenyegető szereplők elsősorban gyenge jelszavakat, szótári szavakat, alapértelmezett hitelesítő adatokat, dátum- és évszámalapú mintákat, valamint egyszerű szekvenciális és billentyűzetmintákat használtak.

A frissített kategorizálás pontosabb képet adott a támadók által alkalmazott jelszógenerálási logikáról. Láthatóvá vált, hogy a próbálkozások jelentős része nemcsak általánosan gyenge vagy szótári jelszavakra épült, hanem számsorozatokra, billentyűzetmintás („keyboard walk") és ismétlődő karakterstruktúrákra is. A „Gyenge jelszó" és a „Szótári szó" kategóriák együttesen a teljes adathalmaz közel 47%-át tették ki, ami tömeges, opportunista brute-force vagy password spraying tevékenységre utal.



3. ábra: Jelszótípusok gyakoriságának időbeli változása

A vizsgált időszakban két hónap mutatott kiemelkedő eltérést. Áprilisban az alapértelmezett hitelesítő adatok aránya emelkedett meg, amely az internet felől elérhető adminisztrációs felületek, hálózati eszközök, IoT-rendszerek vagy rosszul konfigurált szolgáltatások elleni próbálkozásokra utalhat. Júniusban ezzel szemben a szekvenciális és billentyűzetminták aránya nőtt jelentősen, ami eltérő jelszólista, új generálási szabályrendszer vagy más automatizált támadóeszköz használatát jelezheti.

Márciusban és áprilisban erősebben jelentek meg a véletlenszerűnek vagy generáltnak tűnő jelszavak is, ami importált hitelesítőadat-listák vagy credential stuffing jellegű próbálkozások lehetőségét veti fel. Ez azonban önmagában nem bizonyítja, hogy az adott jelszavak kompromittált forrásból származtak. A kontextusspecifikus jelszavak mennyisége alacsonyabb volt, azonban fontos jelzésnek tekinthető, mivel részleges célkörnyezet ismeretre, OSINT-alapú jelszógenerálásra vagy célzottabb jelszólisták használatára utalhat.

A vizsgált időszak támadási mintázata automatizált és opportunista jellegű, ugyanakkor az áprilisi és júniusi eltérések külön kampányra, frissített jelszólistára vagy eltérő támadóeszköz használatára utalhatnak. A legfontosabb kockázatot továbbra is a gyenge, szótári, alapértelmezett és mintázatalapú jelszavak jelentik, különösen olyan környezetekben, ahol nincs többfaktoros hitelesítés, hatékony rate limiting vagy jelszótiltólista.

Vendégszektor - A közüzemi vízellátási ágazat kibertámadási kitettségének növekedése és az OT/ICS fenyegetési trendjei

A 2024 és 2026 közötti időszakban a víziközmű-szektor elleni kibertámadások intenzitása és kifinomultsága tovább növekedett. Az elmúlt időszak eseményei alapján egyértelműen megfigyelhető, hogy az ivóvíz és szennyvízkezelő infrastruktúrák egyre fontosabb célpontjaivá váltak mind a pénzügyi motivációjú kiberbűnözői csoportoknak, mind az államilag támogatott vagy hacktivista szereplőknek.

2024-ben az Egyesült Államok kormánya, a CISA és az EPA több alkalommal is figyelmeztette a víziközmű-üzemeltetőket a kritikus sebezhetőségekre és az ipari

vezérlőrendszereket (ICS/OT) érintő növekvő fenyegetésekre. Ennek eredményeként számos új iránymutatás jelent meg a víz és szennyvízrendszerek kiberbiztonságának megerősítésére, valamint a tagállamokat is felszólították a szektor védelmének fejlesztésére. Az EPA vizsgálatai több esetben olyan kritikus hiányosságokat tártak fel az ivóvízrendszerekben, amelyek lehetővé tehették volna a szolgáltatás megzavarását vagy akár fizikai károkozást. Ugyanezen időszakban több jelentős incidens is rámutatott a szektor sérülékenységére. Az Egyesült Államokban és az Egyesült Királyságban működő vízszolgáltatókat zsarolóvírus-támadások érték, míg Texas több vidéki településén kibertámadás következtében egy vízrendszer túlfolyása is bekövetkezett. Kansas egyik vízkezelő létesítménye egy incidens után kénytelen volt manuális üzemmódra átállni, ami jól szemlélteti, hogy a támadások már nem csupán informatikai, hanem közvetlen operatív következményekkel is járhatnak. A fenyegetések jelentős részét továbbra is az internet felé nyitott ICS-komponensek jelentik. A CISA külön figyelmeztetést adott ki az interneten elérhető HMI (Human Machine Interface) rendszerek miatt, később pedig kutatások kimutatták, hogy több száz amerikai ivóvízrendszer volt kitéve olyan támadásoknak, amelyek szolgáltatás-kiesést vagy fizikai károkozást is eredményezhettek. Az izraeli–libanoni konfliktushoz kapcsolódó hacktivista aktivitás szintén rámutatott arra, hogy az egyszerűen kompromittálható ICS rendszerek geopolitikai konfliktusok során is célponttá válhatnak. Kiemelt esemény volt az American Water elleni kibertámadás, amelynek következtében a vállalat ügyfélportálját és számlázási szolgáltatásait ideiglenesen le kellett állítani. Bár a támadás nem eredményezett közvetlen vízellátási kiesést, ismét ráirányította a figyelmet arra, hogy a kritikus infrastruktúrák üzleti és informatikai rendszerei elleni támadások közvetett módon is jelentős társadalmi és gazdasági hatást fejthetnek ki.

2025-ben a szabályozási és megelőzési intézkedések kerültek előtérbe. Az Egyesült Államokban újra benyújtották a vidéki víziközművek kiberbiztonságának támogatását célzó törvényjavaslatot, míg New York állam megkezdte a vízrendszerekre vonatkozó új kiberbiztonsági szabályozás társadalmi egyeztetését. Ugyanebben az évben kutatók ismét felhívták a figyelmet arra, hogy számos HMI-rendszer továbbra is hibás konfiguráció miatt nyilvánosan elérhető, ami minimális technikai tudással rendelkező támadók számára is lehetőséget biztosít a rendszerek felderítésére.

2026-ban a fenyegetési környezet tovább fejlődött. Megjelent a ZionSiphon nevű, kifejezetten víziközművek ipari vezérlőrendszereit célzó malware, amely az OT-környezetek elleni célzott támadások új szintjét jelzi. Egy másik incidens beszámolói szerint a támadók generatív mesterséges intelligenciát (Claude AI) használtak az OT-eszközök azonosítására és a hálózati felderítés támogatására, ami azt mutatja, hogy az MI-alapú eszközök egyre inkább megjelennek a támadási lánc különböző fázisaiban.

A nemzetközi fenyegetések is fokozódtak. A lengyel nemzetbiztonsági hatóság öt vízkezelő létesítmény ICS-rendszereinek kompromittálását jelentette, míg az iráni kötődésű Handala csoport egy kaliforniai vízszolgáltató elleni támadás felelősségét vállalta magára. Bár a Cal Water vizsgálata nem erősítette meg azonnal a támadók állításait, az incidens jól szemlélteti, hogy a kritikus infrastruktúrák elleni információs és pszichológiai műveletek egyre gyakrabban egészítik ki a tényleges kibertámadásokat.

A víziközmű-szektor továbbra is magas prioritású célpontnak tekinthető. A fenyegetési környezetet a zsarolóvírus csoportok, államilag támogatott szereplők, hacktivisták és egyre kifinomultabb OT-specifikus malware-ek egyaránt alakítják. A legnagyobb kockázatot továbbra is az internet felé nyitott vagy hibásan konfigurált ICS/HMI rendszerek, a nem megfelelő hozzáférés-kezelés, valamint a régi ipari eszközök jelentik. A trendek alapján várható, hogy a jövőben növekedni fog az MI-támogatott felderítés, az OT rendszereket célzó specifikus kártevők alkalmazása, valamint a kritikus infrastruktúrák elleni geopolitikai motivációjú kiberműveletek száma, ezért a víziközművek számára kiemelt fontosságú a hálózati szegmentáció, a nyílt internet felől elérhető ICS-eszközök megszüntetése, a folyamatos sérülékenység-kezelés és az incidenskezelési képességek fejlesztése.

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