2026 május 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

Az e havi CTI jelentés átfogó képet ad az aktuális kiberfenyegetési környezetről, kiemelt figyelmet fordítva a fejlett állami hátterű támadócsoportok (APT-k), a káros kódok és zsarolóvírusok tevékenységére, valamint a legfontosabb sérülékenységi trendekre. A jelentés bemutatja többek között a kínai és orosz kötődésű fenyegetési csoportok legújabb műveleteit, amelyek kormányzati, kritikus infrastruktúra és oktatási célpontok ellen irányultak, továbbá ismerteti az alkalmazott támadási módszereket, a felhasznált kártevőcsaládokat és az adatszivárogtatási technikákat.A dokumentum külön fejezetben foglalkozik a globális károskód-trendekkel, köztük az ellátásilánc-támadások erősödésével, az IoT-eszközöket célzó botnetkampányokkal, valamint a legaktívabb kártevőcsaládok havi mozgásával. Emellett áttekintést nyújt a hazai fenyegetettségi helyzetről és a Magyarországot érintő releváns fejleményekről.

A jelentés részletesen elemzi a zsarolóvírus-ökoszisztéma alakulását is, bemutatva a legaktívabb csoportok tevékenységét, a havi aktivitási trendeket, valamint a fenyegetési környezetben megfigyelhető változásokat, majd kitér a támadók által leggyakrabban kihasznált sérülékenységekre, továbbá az ipari vezérlőrendszereket (ICS/SCADA) érintő biztonsági kockázatokra és incidensekre, amelyek a kritikus infrastruktúrák védelme szempontjából kiemelt jelentőséggel bírnak.

Káros kódok és zsarolóvírusok

APT csoportok

A Webworm nevű, Kínához köthető fejlett és tartós fenyegetést jelentő (APT) hackercsoport jelentősen kibővítette eszköztárát és módosította célpontjait, amelyek között már belga, olasz, szerb és lengyel kormányzati szervek, valamint egy dél-afrikai oktatási intézmény is szerepel. A támadók a kezdeti hozzáférést vélhetően webes felderítést követően, a SquirrelMail levelezőrendszer egy távoli kódfuttatást (RCE) lehetővé tevő biztonsági résén (CVE-2017-7692) keresztül szerezték meg, miközben legalább 56 egyéb célpontot – köztük magyarországi rendszereket is – pásztáztak. A fertőzött környezetekben a csoport két új kártevőt telepített: az EchoCreep hátsó ajtót (backdoor), amely a rendszerszintű perzisztencia (tartós jelenlét) biztosítására egy álcázott ütemezett feladatot használ, és a Discord csevegőprogram alkalmazásprogramozási felületén (API) keresztül, titkosított HTTP-kérésekkel kommunikál; valamint a GraphWorm hátsó ajtót, amely a Windows rendszerleíró adatbázisán (Registry) keresztül indul el automatikusan, és a Microsoft Graph API-t használja az adatszivárogtatásra. A támadók emellett egy nyilvános GitHub-tárhelyet használtak a kártevők terjesztésére, a hálózati felderítés és a nyomok eltüntetése érdekében pedig négy egyedi proxyeszközt (WormFrp, ChainWorm, SmuxProxy, WormSocket) is bevetettek, amelyek segítségével titkosított csatornákon, több belső és külső hálózati ugróponton (hop) keresztül, rejtve irányították a kompromittált rendszereket a vezérlőszervereikről (C2).

A lengyel Belbiztonsági Ügynökség (ABW) nyilvánosságra hozta, hogy több lengyelországi víztisztító létesítményt ért kibertámadás, amelyek során az elkövetők sikeresen hozzáfértek az ipari vezérlőrendszerekhez (ICS) és módosították azok technikai

paramétereit, közvetlenül veszélyeztetve a vízellátási folyamatokat. Emellett a hatóság beszámolt a Lengyel Doppingellenes Ügynökség (POLADA) elleni korábbi támadásról is, amely adatbázis-kompromittálódáshoz, valamint sportolók érzékeny orvosi és doppingteszt-adatainak kiszivárogtatásához, majd internetes közzétételéhez vezetett. Bár ezeknél az incidenseknél a pontos attribúció – azaz a támadók kiléténekhivatalos megállapítása – még nem megerősített, az ABW folyamatos és intenzív kibertevékenységet azonosított az ország infrastruktúrája ellen olyan ismert, fejlett fenyegetési csoportok (APT) részéről, mint az orosz kötődésű APT28 és APT29, valamint a fehérorosz UNC1151. Ezek a formációk a rendelkezésre álló információk alapján elsősorban célzott kiberkémkedést, stratégiai adatszerzést, valamint dezinformációs műveleteket hajtanak végre a célpontok ellen, ugyanakkor a támadások részletes technikai indikátorait (IoC) és a pontos bejutási vektorokat a hatóságok egyelőre nem hozták nyilvánosságra.

A Cisco Talos kiberbiztonsági kutatócsoportja azonosította az UAT-8302 kódnevű, Kínához köthető fejlett állami fenyegetési (APT) csoportot, amely dél-amerikai és délkelet-európai kormányzati szerveket vesz célba célzott kémkedés és hosszan tartó hálózati jelenlét kiépítése érdekében. A támadók a kezdeti hozzáférést feltehetően korábbi (úgynevezett n-day) vagy még javítatlan (zero-day) biztonsági réseken keresztül szerezték meg, majd legitim Windows-eszközökkel és egyedi PowerShell-szkriptekkel részletes belső felderítést és hálózati pásztázást végeztek. Az Active Directory címtárakból és egyéb alkalmazásokból kinyert hitelesítési adatok birtokában a hálózaton belüli oldalirányú mozgást (lateral movement) hajtottak végre, és több egyedi kártevőcsaládot telepítettek. Köztük a Microsoft Graph API-n és OneDrive-on keresztül kommunikáló NetDraft hátsó ajtót, a legitim platformokról (például GitHub) utasításokat fogadó CloudSorcerer kártevőt, valamint a VSHELL, SNAPPYBEE és ZingDoor nevű fejlett trójai programokat. A kártevőket olyan kifinomult módszerekkel juttatták be, mint a DLL oldaltöltés (side-loading), amelynek során egy teljesen ártalmatlan programot kényszerítenek a rosszindulatú kódok futtatására, a fertőzött rendszerek feletti tartós ellenőrzést és az adatszivárogtatást pedig titkosított proxyhálózatokon és VPN-alagutakon (Stowaway, AnyProxy, SoftEther) keresztül biztosították.

Általános káros kód trendek

Május hónap kiemelt eseménye a Shai-Hulud elnevezésű szoftveres ellátásilánc-támadás szintlépése volt, miután a kártevőt nyílt forráskódúvá tették a GitHubon, így az bárki számára szabadon módosíthatóvá vált. A féreg eddig legkevesebb 169 npm programcsomagot fertőzött meg a szoftverfejlesztői (CI/CD) környezeteket célozva, ahol felhőszolgáltatásokhoz és forráskód-kezelőkhöz kapcsolódó hozzáférési kulcsokat lop el, majd ezekkel visszaélve automatikusan további fertőzött szoftververziókat publikál.

Egy új Mirai-alapú botnet az xlabs_v1 kezdte el támadni a nyitott ADB fejlesztői szolgáltatásokat (5555-ös TCP port) futtató okostévéket, okosdobozokat és lakossági routereket. A fertőzött IoT-eszközök sávszélességét leginkább játékszerverek elleni, túlterheléses (DDoS) támadásokra használják fel. A kártevő különlegessége, hogy nem ágyazza be magát tartósan a rendszerbe (hiányzik a perzisztencia), így újraindításkor törlődik, de a nyitott portokon keresztül a támadók folyamatosan újrafertőzik az eszközöket, miközben a konkurens kártevőket eltávolítják róluk.

A CloudZ RAT (távoli hozzáférést biztosító trójai) és annak Pheno nevű beépülő modulja, a Windows 10 és 11 rendszerek beépített Microsoft Phone Link alkalmazását használja ki. A Pheno modul képes leolvasni a Phone Link által használt helyi SQLite adatbázisokat, és amennyiben a felhasználó telefonja csatlakoztatva van a számítógéphez, a támadók képesek eltéríteni és ellopni a telefonra érkező SMS-értesítéseket, köztük a kétlépcsős azonosításhoz szükséges egyszer használatos kódokat is.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. Májusban erős trendemelkedés látható az IPIDEA – mely egy azonos nevű úgynevezett „Residental Proxy Network" segítségével rejti el a káros hálózati forgalmát – a mirai, illetve Popcorn Time zsarolóvírus fertőzési számaiban. A TOP3 legsikeresebb kártevő viszont ebben a hónapban sem változott.

Káros kód	Trend
Vextrio	↔
BADBOX 2.0	↔
Vo1d(2)	↔
IPIDEA	↑
Randybus	↓
mirai	↑
Nymaim	↓
Ngioweb	↓
Tiny Banker	↓
Popcorn Time	↑

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

A 2026. májusi adatok alapján a zsarolóvírus-aktivitás viszonylagos csökkenése mutatható ki az előző hónaphoz képest.

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. májusi adatok alapján továbbra is a Qilin zsarolóvírus-csoport megőrizte piacvezető szerepét, viszont az elért sikeres támadásainak száma csökkenést mutat. Kiemelt trendnövekedés látható a Safepay, Nova csoportok sikeres támadásai alapján, illetve új belépőként látható a File Manager és a Genesis zsarolócsoport.

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

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

A májusi adatok elemzése során az látható, hogy a zsarolóvírus-akciók során leggyakrabban kihasznált sebezhetőségek technikai szempontból az alábbi négy fő kategóriába sorolhatók:

- Kezdeti hozzáférés és hálózati átjárók kompromittálása: A belső hálózatokba való észrevétlen bejutáshoz a támadók gyakran vesznek célba VPN-eszközöket, tűzfalakat és hálózati átjárókat. Kiemelten kockázatosak a Citrix rendszereit érintő CVE-2023-3519 és CVE-2023-4966 (Citrix Bleed) sebezhetőségek, amelyek a hitelesítés megkerülését és munkamenetek átvételét teszik lehetővé. Hasonlóan kritikus belépési pontot jelentenek a Cisco eszközök hibái (CVE-2020-3259 és CVE-2023-20269), amelyek jogosulatlan hozzáférésre vagy információgyűjtésre adnak módot.
- Alkalmazás-alapú sebezhetőségek és távoli kódvégrehajtás (RCE): A védelmi vonalak áttörésére és a szerverek feletti ellenőrzés megszerzésére a támadók előszeretettel alkalmaznak távoli kódvégrehajtást biztosító réseket. Ide tartoznak

a centralizált menedzsment- és biztonsági szoftverek kritikus hibái, mint a VMware vCenter rendszereket érintő CVE-2021-21972, a Veeam megoldásait támadó CVE-2024-40711, a SonicWall tűzfalakat sújtó CVE-2024-40766, a Fortinet központi kezelőit célzó CVE-2023-48788, valamint a Veritas Backup Exec infrastruktúráját veszélyeztető CVE-2021-27876.

- Hitelesítés megkerülése és szenzitív adatok megszerzése: A külső elérésű felületek és adatmozgató rendszerek hiányosságai közvetlen utat nyitnak a belső hálózat felé. A CVE-2024-0204 (Fortra GoAnywhere MFT) hiba a hitelesítési folyamatok teljes megkerülését teszi lehetővé, míg a CVE-2023-27532 (Veeam Backup & Replication) segítségével a támadók titkosított hitelesítő adatokat szerezhetnek meg a mentési környezetből, ami megágyaz a későbbi infrastruktúra-szintű támadásoknak.
- Jogosultságszint-emelés és belső infrastruktúra kompromittálása: A bejutást követően a zsarolóvírusok teljes hálózatra kiterjedő, tömeges élesítéséhez elengedhetetlen a magasabb jogosultságok megszerzése. A virtuális környezetek feletti uralom átvételét és a hálózaton belüli mozgást szolgálja a VMware ESXi rendszereket érintő CVE-2024-37085, valamint a jogosultsági visszaélésekre lehetőséget adó CVE-2024-1853 sebezhetőség, amelyek segítségével a támadók adminisztrátori szintre emelhetik magukat.

ICS/SCADA

A 2026. májusi globális ICS/SCADA fenyegetési környezetet elsősorban a kritikus ipari rendszereket érintő sérülékenységek magas száma, valamint az OT-közeli ransomware- és célzott támadási aktivitás jellemezte. Az időszak fenyegetési képe alapvetően a sérülékenységek nyilvánosságra kerüléséről és az ezekből fakadó potenciális kockázatok növekedéséről szólt, nem pedig széles körben dokumentált, közvetlen OT-romboló incidensekről. A CISA több hullámban adott ki biztonsági figyelmeztetéseket jelentős ipari technológiai gyártók termékeire, köztük az ABB, Siemens, Hitachi Energy, Johnson Controls, Fuji Electric, Universal Robots, ScadaBR és Schneider Electric megoldásaira. Az érintett rendszerek között PLC-k, DCS-platformok, ipari hálózati eszközök, energiaipari vezérlők, robotikai rendszerek és menedzsmentplatformok egyaránt szerepeltek. Kiemelt figyelmet kaptak a Siemens SIMATIC S7 PLC Web Server, SIMATIC és RUGGEDCOM

termékcsaládokat érintő sérülékenységek, valamint az ABB AC500 V3 vezérlőkben, az ABB B&R Automation Studio és Automation Runtime környezetekben, továbbá a ScadaBR platformban feltárt hibák. A sérülékenységek között távoli kódfuttatást (RCE), jogosultság-emelést, parancsbefecskendezést és szolgáltatásmegtagadást (DoS) lehetővé tevő problémák is szerepeltek, amelyek potenciálisan az energetikai, víziközmű, gyártóipari és közlekedési infrastruktúrák működését is érinthetik.

A hónap egyik legjelentősebb ICS-biztonsági eseménye a Universal Robots PolyScope 5 platformot érintő, CVE-2026-8153 azonosítójú kritikus sérülékenység nyilvánosságra kerülése volt. A 9,8-as CVSS pontszámmal rendelkező távoli parancsbefecskendezési hiba sikeres kihasználása lehetővé teheti a támadók számára a robotikai rendszerek feletti jogosulatlan távoli vezérlés megszerzését, ami közvetlen kockázatot jelenthet az ipari termelési folyamatok rendelkezésre állására, integritására és biztonságára. Európa szempontjából továbbra is a Siemens ökoszisztémát érintő sérülékenységek tekinthetők a legjelentősebb fenyegetésnek, figyelembe véve a Siemens technológiáinak széles körű alkalmazását az energetikai, közmű, vasúti és ipari automatizálási környezetekben. Emellett több, villamosenergia-ipari rendszerekben használt Hitachi Energy megoldás, valamint épületautomatizálási és fizikai biztonsági rendszerek is érintettek voltak biztonsági figyelmeztetésekben, ami tovább növelte a kritikus infrastruktúrák kitettségét.

Az időszak legjelentősebb ipari vonatkozású incidense a Nitrogen ransomware-csoport által végrehajtott Foxconn-kompromittálás volt. A rendelkezésre álló nyilvános információk alapján az esemény elsősorban vállalati IT-incidensként értékelhető, és nem áll rendelkezésre bizonyíték közvetlen ICS/SCADA-rendszerleállásra vagy ipari folyamatokat érintő romboló hatásra. Az eset ugyanakkor jól szemlélteti az IT–OT konvergenciából eredő kockázatokat, valamint azt, hogy a vállalati informatikai rendszerek kompromittálása közvetett módon az ipari működést is veszélyeztetheti.

Lengyel hírszerzési jelentések alapján 2025-ben ismeretlen kiberfenyegetési szereplők több lengyelországi vízkezelő létesítmény ellen hajtottak végre támadásokat, amelyek öt települést érintettek. A támadók ipari vezérlőrendszerekhez is hozzáférhettek, ami potenciálisan a vízellátási folyamatok megzavarásának kockázatát vetette fel. A tevékenységet hivatalosan nem tulajdonították konkrét csoportnak, ugyanakkor az incidensek illeszkednek a Lengyelországot és más NATO, illetve EU-tagállamokat célzó, orosz érdekekhez köthető kiber és szabotázsműveletek szélesebb trendjébe.

Sérülékenységek

A hónap során továbbra is jelentős figyelem irányult a Linux kernel „Copy Fail" néven ismert CVE-2026-31431 sérülékenységére, amelyet az NKI már áprilisban is kiemelten kezelt. A hiba lehetővé teszi, hogy egy alacsony jogosultságú helyi felhasználó vagy folyamat root jogosultságot szerezzen az érintett rendszeren. A Linux kernelhez kapcsolódó további a hónapban ismertté vált sérülékenységek – köztük az xfrm/ESP és az rxrpc komponenseket érintő hibák – arra utalnak, hogy a támadói és kutatói figyelem továbbra is a rendszermag alacsony szintű hálózati feldolgozási mechanizmusaira összpontosul.

A hónap elején az NKI figyelmeztetést tett közzé az „NGINX Rift" néven ismert CVE-2026-42945 azonosítójú sérülékenységről. A hiba az ngx_http_rewrite_module komponensben található hibából ered, és speciális körülmények között távoli kódfuttatásra adhat lehetőséget. A sérülékenység különösen nagy kockázatot jelent internet felől elérhető NGINX-alapú szolgáltatások esetében.

Május második felében az NKI a Microsoft havi biztonsági frissítéseihez kapcsolódóan adott ki riasztást. A javítások több mint száz sérülékenységet kezeltek, amelyek közül kiemelt figyelmet kaptak a Windows Remote Desktop Gateway (CVE-2026-41089) és a Windows LDAP szolgáltatás (CVE-2026-41096) kritikus hibái. A sérülékenységek sikeres kihasználása távoli kódfuttatást vagy jogosultságkiterjesztést tehet lehetővé, ezért az érintett rendszerek mielőbbi frissítése kiemelten indokolt.

A CISA Known Exploited Vulnerabilities (KEV) katalógusa májusban 21 új bejegyzéssel bővült. Az NKI által is publikált, kiemelt jelentőségű sérülékenységek közé tartozott a Cisco Catalyst SD-WAN Manager (CVE-2026-20182), a Microsoft Defender komponenseit érintő CVE-2026-41091 és CVE-2026-45498, a Drupal Core CVE-2026-9082, valamint a LiteSpeed cPanel/WHM Plugin CVE-2026-48172 azonosítójú hibája. A Cisco Catalyst SD-WAN Manager sérülékenysége különösen kritikusnak tekinthető, mivel maximális, CVSS 10.0 súlyossági értékelést kapott, és a sérülékenységhez kapcsolódóan sürgősségi intézkedéseket is elrendeltek.

Kiemelt fenyegetést jelentettek az internet felől elérhető peremvédelmi rendszereket érintő sérülékenységek. A Palo Alto Networks PAN-OS, a Cisco Catalyst SD-WAN

platformok, valamint a WebPros cPanel & WHM környezeteket érintő hibák több esetben hitelesítés-megkerülést vagy távoli kódfuttatást tettek lehetővé.

Május egyik meghatározó trendjét a szoftverellátási láncot érintő incidensek erősödése jelentette. A TanStack (CVE-2026-45321), az Nx Console (CVE-2026-48027) és a DAEMON Tools Lite (CVE-2026-8398) eseteiben nem klasszikus sérülékenységekről, hanem kompromittált fejlesztői csomagokról, illetve beágyazott rosszindulatú kódról volt szó.

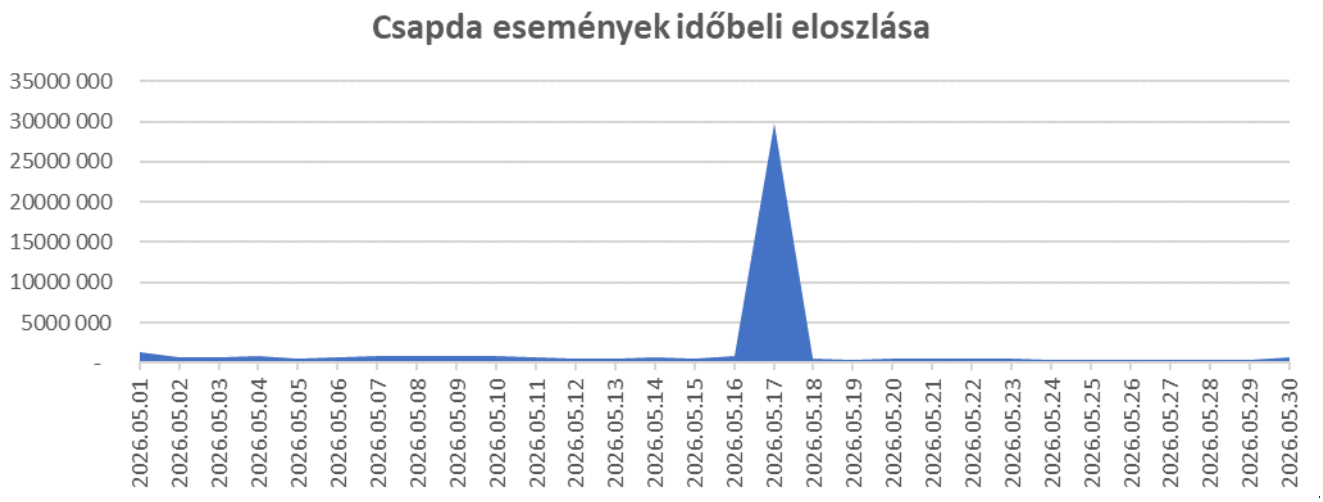
Az AI-ökoszisztéma sérülékenységei szintén egyre hangsúlyosabban jelentek meg. A hónap során több AI-keretrendszert és modellkiszolgáló komponenst érintő sérülékenység került a figyelem középpontjába. Kiemelendő a BerriAI LiteLLM SQL injection sérülékenysége, a Langflow korábban azonosított hibái, valamint az Ollama „Bleeding Llama" néven ismert memóriaszivárgási problémája, amelyek azt mutatják, hogy az AI-alapú infrastruktúrák egyre gyakrabban jelennek meg aktív támadási felületként.

A CISA és más nemzetközi sérülékenység-kezelési kezdeményezések továbbra is felhívták a figyelmet arra, hogy számos, akár több mint egy évtizede ismert sérülékenység változatlanul szerepet kap a támadásokban. A CVE-2008-4250, CVE-2009-1537, CVE-2009-3459, CVE-2010-0249 és CVE-2010-0806 jelenléte arra utal, hogy az elavult rendszerek és a hiányos javításkezelés továbbra is jelentős kockázati tényezőt jelentenek.

Honeypot forgalom elemzése

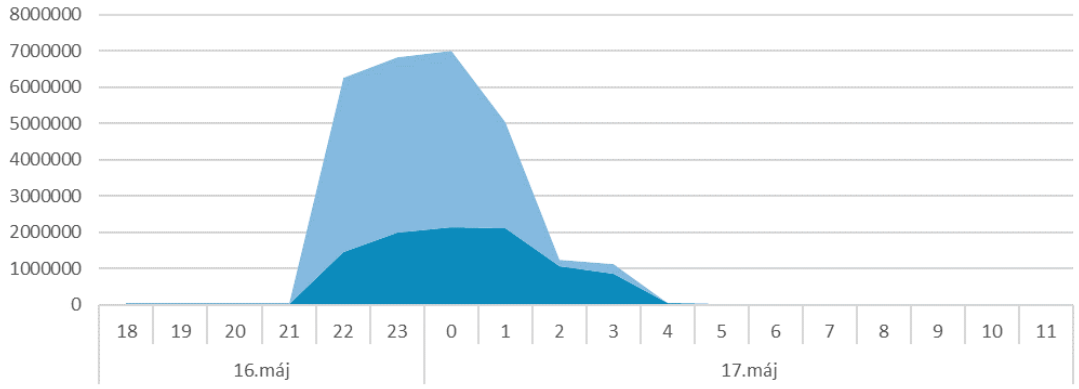
Az évek tapasztalata azt bizonyítja, hogy a kibertér háttérzaja avagy az automatizált, nagy volumenű feltérképezési és sebezhetőségek kihasználási kísérletek mennyisége igencsak erősödött. A kitelepített GovProbe Honeypot szondák adatai között is hónapról hónapra megtalálhatóak a nagy erőforrású botnet próbálkozások. Ezek mind volumenben, mind incidens számban is fokozott élénkülést mutatnak.

Mindezekre a májusi adatok tökéletes példát állítanak. Ha megtekintjük a hónap során beérkezett események változását egy nagyon érdekes forma rajzolódik ki. Amikor megnézzük a lenti ábrát, elsőre arra is gondolhatunk, hogy valamiféle hiba van az adatok megjelenítésében.



3. ábra: Május hónap során beérkezett csapda események időbeli eloszlása.

Az események mélyebb megismerése azonban több érdekességet is feltár. Május közepén körülbelül 4 óra leforgása alatt több mint 24 millió bejegyzés keletkezett egy holland hoszting szolgáltató irányából. Az esemény két azonosítható célja tűzfal irányú felderítés és Wordpress webapp kiszolgáló sérülékenységeinek kihasználása. A támadás intenzitása majdnem 1700 bejegyzést takar másodpercenként. A kifejezetten agresszív próbálkozási kísérlet azonban nem egyedül járt. Az adatlavina mögött tökéletes egybeeséssel megbújik több különböző forrásból származó támadási folyamat is amely más szolgáltatásokat céloztak.



4. ábra: Összefüggő eseménysorozatok összehasonlítása az érintett időszakban.

A két támadási hullám, habár nagy valószínűséggel összetartozik nem feltétlen célzott kampányt rejt. Ha az incidenst más aspektusból közelítjük meg több viselkedési és taktikai részletet figyelhetünk meg, amely árulkodhat az automatizmusok változásáról:

1. Az erőforrás már nem akadály. A támadók már rugalmasabban és gazdaságosabban hozzáférnek komolyabb teljesítményre képes infrastruktúrákhoz, amelyek, rövid idő alatt nagy mennyiségű forgalmat képesek lebonyolítani. Gyakori, hogy az egyes incidensek több különböző forrásból kerülnek lebonyolításra.

2. A rejtőzködés már nem kifizetődő. Az kártékony automatizmusok taktikai felfogása változott az évek során. Zajosabb, de gyorsabb kampányok nagyobb lefedettséget képesek biztosítani, több áldozatot begyűjtve.

3. A hangzavar előnnyel jár. Habár a rendszerüzemeltetők megszokhatták, hogy kibertér egy fajta állandó „zajjal" rendelkezik az intenzív jellegű szkennelések hatalmas üzemeltetési feladatokkal járhatnak. A naplóesemények folyamatos szűrése és ellenőrzése mellett az adatáramlás/adatfeldolgozás megterhelheti a célrendszereket is.

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