2026 augusztus 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 2026. augusztusi időszak fenyegetettségi képe alapján a támadók továbbra is elsősorban a külsőleg elérhető vállalati rendszerek, távoli hozzáférési megoldások és központi infrastruktúrák sérülékenységeit, valamint a felhasználói bizalmat igyekeznek kihasználni. Az APT-csoportok új és továbbfejlesztett eszközökkel, infrastruktúrával és több lépcsős támadási láncokkal jelentek meg, miközben a zsarolóvírus-műveletekben egyre hangsúlyosabbá vált az RMM-eszközök, a PowerShell és a kompromittált hálózati peremeszközök használata. A sérülékenységek területén különösen az internet felől elérhető, központi szerepet betöltő rendszerek – többek között a TeamCity, SPIP és PaperCut aktívan kihasznált

hibái jelentettek kiemelt kockázatot. Az ICS/SCADA-környezetek esetében a lengyel energiaipari incidens rávilágított arra, hogy a privát hálózatok és az IT/OT elkülönítés önmagában nem jelent megfelelő védelmet, míg a honeypot-adatok alapján a kriptobányászati kampányok újbóli erősödése, különösen Linux és SSH-környezetekben, szintén figyelmet érdemel.

APT csoportok

A 2026. augusztusi időszakban több APT-csoport is új vagy továbbfejlesztett támadási láncokkal jelent meg. Az Iránhoz köthető Tortoiseshell új eszközökkel és infrastruktúrával bővítette arzenálját: fordított SSH-alagutazást alkalmazó komponenst, DLL search-order hijacking technikára alkalmas, TWOSTROKE-szerű hátsó kaput és új vezérlőszervereket (C2) azonosítottak, miközben a malware HTTPS-en keresztül fájlkezelési, parancsvégrehajtási és rendszerfelderítési műveleteket támogatott. A Jewelbug kompromittált webmail-infrastruktúrát használt watering hole támadásokhoz, WebSocket-kapcsolaton keresztül munkamenet-cookie-kat gyűjtött, majd az Antino hátsó kaput és rosszindulatú böngészőbővítményt telepített; Linux-szervereken és routereken a Rust-alapú ClientKing implantátumot is alkalmazta. Egy feltételezett APT-szereplő a VMware vCenter kritikus CVE-2026-59310 sérülékenységét használta ki tetszőleges kódfuttatásra és a reverse_ssh keretrendszerrel tartós távoli hozzáférés kialakítására. A Head Mare a TrueConf Server két sérülékenységének láncolásával SYSTEM jogosultságot szerzett, web shellt telepített, manipulálta a kliens telepítőjét, PhantomCore és OneDrive-alapú C2-t használó PhantomGraph hátsó kapukat helyezett el, továbbá LSASS-memóriát mentett és fordított SSH-alagutat létesített. A SideWinder eközben kiterjedt spear-phishing és typosquatting infrastruktúrát épített ki: több mint 60 megtévesztő aldomaint alkalmazott dél-ázsiai szervezetek megszemélyesítésére, ugyanakkor a vizsgált időszakban sikeres kompromittálást vagy konkrét kártevőt nem erősítettek meg.

Általános káros kód trendek

A vizsgált időszak fenyegetési képe alapján továbbra is a zsarolóvírus-műveletek, a social engineering és a vállalati távoli elérési megoldások kompromittálása jelentik a legfontosabb kockázatokat. A Chaos kampány Microsoft Teams-alapú vishinggel, Quick Assist és RMM-eszközök alkalmazásával, PowerShell-futtatással, registry- és Startup-alapú perzisztenciával, valamint Python- és Go-alapú implantokkal jutott el akár 17 órán belül a hálózati szintű titkosításig. Hasonlóan súlyos kockázatot jelent a Storm-1175, amely az N-able N-central CVE-2026-18577 sérülékenységének kihasználásával MSP-környezeteken keresztül terjesztheti a StormEncryptor zsarolóvírust, miközben AnyDesk, SimpleHelp, Mimikatz és Cloudflared eszközöket használ felderítésre, hitelesítőadat-lopásra és tartós hozzáférésre. A Gunra csoport Fortinet-sérülékenységeket, köztük a CVE-2024-55591 és CVE-2025-24472 hibákat használja kezdeti hozzáféréshez, míg a Clop a PTC Windchill és FlexPLM CVE-2026-12569 sérülékenységén keresztül JSP webshell-ek telepítésével és adatlopással támad vállalati környezeteket. A Teams-alapú SynkLoader kampány szintén a felhasználói bizalom kihasználására épít, fájlmentes PowerShell-kódot, hitelesítőadat-lopó ál-zárolási képernyőt, tunnelinget és VNC-hozzáférést alkalmazva. A trendek alapján prioritást kell kapnia a külső Teams-kommunikáció korlátozásának, az RMM- és PowerShell-használat monitorozásának, az alkalmazásengedélyezésnek, a kritikus sérülékenységek gyors javításának, valamint az identitás- és végpontvédelmi események központi korrelációjának.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. A jelenlegi trendek alapján az első három kártevő stagnálást mutat, emelkedő tendenciát látunk a NetNut, AdLoad és Tinba káros kódok elterjedtségében.

Káros kód	Trend
BADBOX 2.0	↔
IPIDEA	↔
Vo1d(2)	↔
NetNut	↑
Popcorn Time	↓
Socks Escort	↔
AdLoad	↑
Tinba	↑
Ranbyus	↓
Andromeda	↓

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. augusztusi adatok alapján a Quilin csoport újra a legnagyobb aktivitást mutatta, miközben több új csoport, mint a Orova, Dark Project, is bekerült a legtöbb fertőzést végrehajtó csoportok közé.

Típus	Trend
Quilin	↑
Gentlemen	↓
CL0P	↑
INC	↔
Storm	↑
Krybit	↑
Akira	↑
Dire Wolf	↑
Dark Project	↑
Orova	↑

2. ábra: Top 10 zsarolóvírus trendadatai

Kihasznált sérülékenységek

Megállapítható, hogy a vizsgált időszakban, a felderített zsarolóvírus-támadások néhány sebezhetőség kihasználásával valósultak meg, melyek technikai szempontból az alábbi fő kategóriákba sorolhatók:

- Kezdeti hozzáférés és hálózati átjárók kompromittálása: A támadók továbbra is kiemelten célozzák az internet felől elérhető VPN-, hálózatbiztonsági és távoli hozzáférési megoldásokat. Jelentős kockázatot jelentenek a Fortinet FortiOS (CVE-2024-21762), az F5 BIG-IP/BIG-IQ (CVE-2021-22986), valamint a Pulse Secure VPN (CVE-2019-11510) sérülékenységei. Ezek kihasználása lehetőséget teremthet a szervezeti hálózatba történő kezdeti behatolásra, illetve további támadási műveletek előkészítésére.

- Szerver- és infrastruktúra-rendszerek távoli kompromittálása: A támadók előszeretettel használják ki a központi infrastruktúra- és szerveralkalmazások távoli kódfuttatást lehetővé tevő hibáit. Ebbe a körbe sorolható a VMware vCenter Server (CVE-2021-21972), az Apache Log4j2 (CVE-2021-44228), a SolarWinds Serv-U (CVE-2021-35211), a Fortra GoAnywhere MFT (CVE-2023-0669), valamint a PaperCut MF/NG (CVE-2023-27350) sérülékenysége. E rendszerek sikeres kompromittálása magas jogosultságú hozzáférést, távoli kódfuttatást, illetve a támadás további hálózati kiterjesztését teheti lehetővé.

- Jogosultságkiterjesztés, oldalirányú mozgás és érzékeny adatok megszerzése: A kezdeti hozzáférést követően különösen veszélyesek a központi hitelesítési és adatkezelési rendszereket érintő sérülékenységek. A Microsoft Netlogon (CVE-2020-1472 – Zerologon) kihasználása a tartományvezérlő kompromittálását és ezáltal a teljes Active Directory környezet feletti ellenőrzés megszerzését segítheti elő. A Veeam Backup & Replication (CVE-2023-27532) hitelesítő adatok megszerzésére használható, míg a Progress MOVEit Transfer (CVE-2023-34362) sérülékenysége jogosulatlan adatbázis-hozzáférést és jelentős mennyiségű érzékeny adat megszerzését teheti lehetővé.

ICS/SCADA

2026 augusztusában az ICS/SCADA fenyegetettségi kép fő üzenete, hogy a támadók továbbra sem elsősorban kifinomult, célzott ipari malware-re támaszkodnak, hanem az OT-környezetekhez kapcsolódó gyenge pontokat használják ki: internet felől elérhető peremeszközöket, gyenge vagy alapértelmezett hitelesítő adatokat, nem megfelelő IT/OT-szegmentációt, valamint téves biztonsági feltételezéseket a „privát” kommunikációs csatornákról.

A hónap legfontosabb európai fejleménye a lengyel energiainfrastruktúrát érintő incidens volt, ahol a támadók egy privát APN-en keresztül jutottak be az OT/ICS környezetbe. Ez azért kiemelten fontos, mert azt mutatja, hogy az elkülönítettnek hitt mobil adatkapcsolatok sem tekinthetők önmagukban biztonságosnak. Emellett

augusztusban hangsúlyos volt a Siemens S7 PLC-k elleni fokozódó fenyegetés, ahol AI-generált exploitkódok csökkentették a támadók belépési küszöbét.

Magyarország esetében a rendelkezésre álló adatok alapján nem azonosítható nagy bizonyossággal nyilvánosan megerősített, közvetlen SCADA- vagy PLC-manipulációval járó incidens. Ugyanakkor egy esetben tapasztalható volt célzott kibertámadás egy agrárfejlesztési hálózat ellen. Mindemellett megjelentek magyar forrású rosszindulatú hálózati aktivitások is, ami azt jelzi, hogy a hazai operatív környezetek kitettsége valós.

Kiber-fizikai peremeszközök és IIoT rendszerek

A lengyel energiatermelő létesítményt érintő incidens rámutatott, hogy a peremeszközök (például ipari routerek, távoli hozzáférési eszközök, mobilkapcsolatot kezelő berendezések) kiemelt támadási felületet jelentenek. A támadók egy privát APN-en, valamint távolról elérhető hálózati és vezérlőeszközökön keresztül jutottak el az OT-rendszerekhez.

Ez volt a legkritikusabb kockázati kategória a vizsgált időszakban, a továbbiakban bővebben kifejtjük.

Ipari kommunikációs csatornák és hálózatfelügyelet

A hónap egyik legfontosabb tanulsága az volt, hogy a kommunikációs csatornákba vetett bizalom önmagában nem védelmi mechanizmus.

A privát APN-nel kapcsolatos lengyel eset különösen fontos, mert azt mutatja, hogy egy dedikált mobil adatkapcsolat is támadási útvonallá válhat. Emellett az augusztusi fenyegetési képben több esetben jelent meg olyan rosszindulatú hálózati aktivitás, amely európai infrastruktúrához és különféle RAT/C2 ökoszisztémákhoz kapcsolódott.

Folyamatvezérlési és gyártásirányítási környezetek

A folyamatvezérlési rendszerek ellen irányuló támadások fő veszélye az, hogy közvetlenül érinthetik az üzemmenetet, a termelést vagy a szolgáltatásfolytonosságot.

A lengyel esetben a támadók PLC-ket STOP állapotba tettek, és egyes folyamatokat leállítottak. Ez egyértelmű példa arra, hogy az IT-ből induló kompromittálódás hogyan vezethet fizikai hatású OT-eseményhez. Augusztusban a Siemens S7 PLC-k elleni aktív fenyegetések is kiemelt figyelmet kaptak, különösen azért, mert AI-generált kódokkal egyszerűbbé vált a támadások végrehajtása.

Mérnöki Munkaállomások (EWS) és Fizikai Biztonsági Zónák

Bár a vizsgált források kevesebb konkrét példát adtak az EWS-rendszerek közvetlen kompromittálására, a fenyegetési mintázat alapján ezek továbbra is kulcsfontosságú kockázati pontok.

Az EWS-k jellemzően azok a rendszerek, amelyeken keresztül a PLC-k programozása, konfigurálása és felügyelete történik. Ha egy támadó eljut ezekhez a gépekhez, azzal aránytalanul nagy hatást érhet el. A fizikai biztonsági zónák jelentősége szintén nő, mivel sok szervezet logikailag elkülönítettnek tekinti az OT-t, de valójában a távoli elérés, karbantartási csatornák vagy mezőszinti összeköttetések áttörik ezt az elkülönítést.

Kiemelt fenyegetési esemény

A lengyel energiaipari támadássorozat újabb részleteinek nyilvánosságra kerülése volt. A CERT Polska augusztus 8-án közzétett utólagos vizsgálati jelentése egy korábban nem publikált, 2025. december 29-én bekövetkezett támadást mutatott be egy olyan lengyel kapcsolt hő és villamosenergia-termelő létesítmény ellen, amely mintegy 50 ezer lakos hőellátásában vett részt. Az incidens az ugyanazon a napon végrehajtott, mintegy 30 szélerőművi és naperőművi létesítményt, valamint egy nagyobb CHP-létesítményt érintő összehangolt támadási kampány része volt. A CERT Polska vizsgálata szerint a második CHP-létesítményben a támadók leállították a gőzturbinát és a technológiai víz előállítására használt vízkezelő rendszert, ezzel megszakítva a kogenerációs folyamatot. Az üzemeltetők gyors beavatkozásának köszönhetően az incidens rövid ideig tartott, és nem okozott fennakadást a fogyasztók hőellátásában.

A vizsgálat egy olyan támadási útvonalat tárt fel, amelyben a magánhálózati APN önmagában nem jelentett megfelelő biztonsági határt. A CERT Polska szerint a támadók egy korábban kompromittált környezeten keresztül jutottak el a privát APN-hez, amelyen belül egy konfigurációs hiányosság lehetővé tette, hogy a hálózat különböző eszközei szabadon kommunikáljanak egymással. Innen elérhetővé vált egy WAGO PFC200 vezérlő, amelyen az alapértelmezett adminisztrátori hitelesítési adatok használata további lehetőséget biztosított a támadóknak. A kompromittált vezérlőből az OT-környezet további komponensei, köztük Siemens S7 PLC-k váltak elérhetővé. A támadási útvonal jelentősége túlmutat az érintett termékeken: azt a képet vetíti előre, hogy egy üzemi kommunikációs hálózat vagy privát mobilhálózat biztonsági kontrolljai csak akkor tekinthetők tényleges védelmi rétegnek, ha az azon található végpontok közötti kommunikációt és a végpontok saját biztonsági állapotát is megfelelően korlátozzák.

A lengyel incidensben különösen figyelemre méltó az IT- és OT-környezet közötti határ fokozatos eltűnése. A támadási láncban nem egyetlen, klasszikus értelemben vett „ICS-sérülékenység” biztosította a hozzáférést, hanem több, egymást erősítő konfigurációs és hitelesítési hiányosság: a hálózati hozzáférés védelmének hiányosságai, a privát APN nem megfelelő izolációja, egy ipari vezérlő gyenge hitelesítése, majd az OT-hálózaton belüli további elérhetőség. Az incidens ezért jól szemlélteti az úgynevezett „defense in depth” megközelítés jelentőségét: még abban az esetben is, ha az egyik védelmi réteg – például a privát APN – kompromittálódik, további független kontrolloknak kell megakadályozniuk az OT-rendszerek és a fizikai folyamatok elérését. A CERT Polska azt is kiemelte, hogy hasonló, egymás közötti kommunikációt lehetővé tevő APN-konfigurációkat több vizsgált szervezetnél is azonosítottak, és ezek a megoldások nem kizárólag Lengyelországban használatosak.

Sérülékenységek

A vizsgált időszakban kiemelt jelentőségű sérülékenységek érintették többek között a JetBrains TeamCity, a SPIP tartalomkezelő rendszer, valamint a PaperCut NG/MF nyomtatásmenedzsment-platformokat. Az érintett termékek köre jól mutatja, hogy a támadók továbbra is elsősorban olyan, központi szerepet betöltő és jellemzően

hálózaton keresztül elérhető rendszereket céloznak, amelyek kompromittálása további vállalati erőforrásokhoz biztosíthat hozzáférést.

Az exploitációs aktivitást vizsgálva a Log4Shell néven ismert CVE-2021-44228 továbbra is kiemelkedik, 75 alkalommal szerepelt a megfigyelt kihasználási jelentésekben, ezzel immár újabb hónapban is ez volt a legtöbbször jelentett sérülékenység. Ezt követte a React Server Components előhitelesítés nélküli távoli kódfuttatást lehetővé tevő CVE-2025-55182, 41 jelentéssel, majd a Cisco IOS XE webes felületének jogosultság-emelési hibája, a CVE-2023-20198, 35 esettel. A négy leggyakrabban kihasznált sérülékenység közé került a cPanel/WHM bejelentkezési folyamatának hitelesítés-megkerülési hibája, a CVE-2026-41940 is, amely 34 jelentéssel az egyetlen 2026-ban publikált sérülékenység ebben a csoportban.

A proof-of-concept, vagyis a sérülékenységek gyakorlati kihasználását demonstráló kódok aktivitása ugyanakkor elsősorban két újabb hibára összpontosult. A Linux kernel rtmutex komponensének CVE-2026-43499 azonosítójú sérülékenységéhez 91 PoC-észlelés kapcsolódott, míg a WordPress bejelentkezési oldalán található, előhitelesítés nélkül kihasználható, reflektált XSS-hiba, a CVE-2026-64638 70 alkalommal szerepelt. Utóbbit augusztus 7-én hozták nyilvánosságra, és felhasználói közreműködés mellett akár kódfuttatásig is tovább eszkalálható. A számok alapján jól elkülönül egymástól a már régóta ismert sérülékenységek tényleges kihasználása és az újonnan megjelent hibákhoz kapcsolódó proof-of-concept aktivitás.

A hónap egyik jelentős sérülékenységi eseménye a JetBrains TeamCity CVE-2026-63077 azonosítójú hibája volt. A sérülékenység a TeamCity On-Premises környezeteket érinti, és a nem megbízható adatok deszerializálásával kapcsolatos problémából ered. A hiba kihasználása hitelesítés nélküli távoli támadó számára lehetővé teheti tetszőleges operációsrendszer-parancsok végrehajtását a TeamCity szerverfolyamat jogosultságaival. A sérülékenység CVSS 3.1 alapján 9,8-as, kritikus besorolást kapott, és 2026. augusztus 5-én bekerült a CISA Known Exploited Vulnerabilities (KEV) katalógusába. A Vulnerability-Lookup ugyanezen a napon megerősített kihasználást jelez, míg a JetBrains augusztus 7-i tájékoztatása szerint a gyártó aktív és sikertelen kihasználási kísérletekről is kapott jelentéseket a javítatlan TeamCity szerverek ellen.

A webes alkalmazási rétegben kiemelt kockázatot jelentett a SPIP CVE-2026-77806 azonosítójú sérülékenysége. A 2026. augusztus 21-én publikált hiba a SPIP 4.4.21 előtti verzióit érinti, és egy HTTP-kérésben továbbított, nem megfelelően kezelt X-Spip-Filtre fejléc feldolgozásához kapcsolódó kódbefecskendezési problémából ered. A sérülékenység CVSS 3.1 alapján 9,8-as, kritikus besorolású, és hitelesítés nélküli távoli támadó számára tetszőleges kód végrehajtását teheti lehetővé. A Vulnerability-Lookup augusztus 21-én megerősített, az éles környezetben történő kihasználást jelző rekordot tart nyilván, amely szerint a sérülékenységet már a nyilvánosságra kerülés időszakában aktívan kihasználták.

A SPIP sérülékenysége jól példázza az internet felől elérhető tartalomkezelő rendszerek kitettségének problémáját. Az olyan webalkalmazások, amelyek közvetlenül fogadnak külső HTTP-kéréseket, megfelelő védelem és naprakész verzió használatának hiányában automatizált támadási kampányok célpontjává válhatnak. A CVE-2026-77806 esetében különösen jelentős tényező, hogy a támadáshoz nem szükséges hitelesítés, a támadó pedig távoli kódfuttatást érhet el.

Az augusztusi időszak egyik legjelentősebb eseménye a PaperCut NG és PaperCut MF rendszereket érintő, egymással összefüggő CVE-2026-81578 és CVE-2026-82078 sérülékenységpár volt. A PaperCut 2026. augusztus 27-én sürgős biztonsági riasztást adott ki, amelyben jelezte, hogy a termékeket érintő sérülékenységeket aktívan kihasználják. A két CVE-t ezt követően, augusztus 28-án rendelték hozzá a hibákhoz.

A hálózati és infrastruktúra-rétegben továbbra is jelentős figyelmet igényelnek a Linux kernel sérülékenységei. A CVE-2026-53362 egy IPv6-csomagkezeléssel kapcsolatos memória-korrupciós hibát érint. A sérülékenység esetében egy nem privilegizált helyi felhasználó meghatározott UDPv6-műveletek segítségével memóriakorrupciót válthat ki. A hiba technikai jellegéből adódóan elsősorban az olyan rendszerek esetében jelent kockázatot, ahol a támadó már rendelkezik helyi hozzáféréssel, ugyanakkor a Linux kernel széles körű alkalmazása miatt a sérülékenység infrastruktúraszinten is releváns.

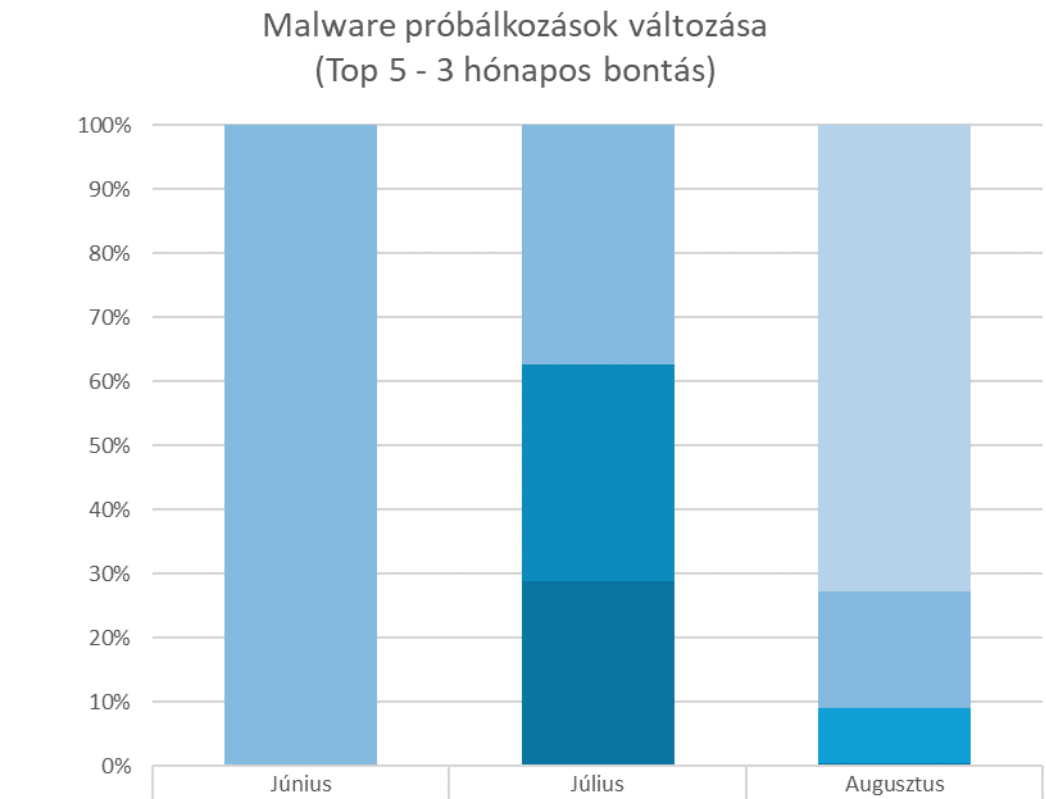
Az augusztusi időszak egyik legfontosabb tanulsága, hogy a vállalati sérülékenységkezelés során nem elegendő kizárólag a magas vagy kritikus CVSS-értékű hibák alapján priorizálni. Kiemelt figyelmet kell fordítani azokra a sérülékenységekre, amelyek esetében hitelesítés nélküli távoli kihasználás, aktív

kihasználás, publikus PoC, automatizálható támadási lehetőség vagy több sérülékenység láncolhatósága is fennáll. A TeamCity, SPIP és PaperCut eseményei egyaránt azt mutatják, hogy az ilyen sérülékenységek esetében a nyilvánosságra hozatal és a tényleges támadási aktivitás között akár csak néhány nap állhat rendelkezésre a szükséges védekezési intézkedések végrehajtására.

Honeypot forgalom elemzése

A GovProbe Honeypot SSH és Telnet csapdáin képesek lehetünk különböző forrásból származó úgynevezett dropper URL elfogására. Az ilyen jellegű „linkek" különböző kártékony tartalmakat hivatottak letölteni és futtatni a célponttá vált rendszereken. A beérkező URL biztonságos vizsgálata során képesek lehetünk kategorizálni kódokat, amelyből pontosabb képet kaphatunk a kibertérben történő változásokról. Az augusztus hónap egy nagyon érdekes malware statisztikája, hogy újból színre lépett a RedTail elnevezésű kriptobányász program. A RedTail egy Linux-központú, többarchitektúrás cryptomining kampányhoz kapcsolódó malware, amely jellemzően gyengén védett vagy alapértelmezett hitelesítő adatokkal elérhető rendszereket céloz, különösen SSH-n keresztül. A fertőzési lánc rendszerint shell-alapú loadereket és dropper szkripteket használ a payload letöltésére, a konkurens malware eltávolítására, valamint a perzisztencia kialakítására, például cron bejegyzésekkel vagy jogosulatlan SSH-kulcsok telepítésével. A RedTail működésének célja elsődlegesen a kriptobányász monetizáció, miközben a folyamatok álcázása, a védelmi eszközök zavarása és a több platformot támogató binárisok használata arra utal, hogy az operátorok a hosszabb távú és rejtett erőforrás-kihasználásra törekednek.

Azonban, ha a malware statisztikákat megtekintjük a nyári időszak egészére egy sokkal fontosabb összefüggést fedezhetünk fel. Ahogyan a júliusi havi CTI jelentésünkben is írtuk a Honeypot szenzorai érkező dropper URL-ek között kifejezetten magas számban tapasztaltunk Prometei káros kódokat. A Prometei hasonlóan a RedTail-hez, egy kriptobányászatra specializált malware típus. Az összképet erősíti az a tény is, hogy míg júniusban egyáltalán nem azonosítottunk kriptobányász kódokat, július és augusztus között mintegy 93%-os növekedést láthatunk.



3. ábra: Leggyakoribb malware-típusok havi megoszlása

A saját környezetben megfigyelt jelenség azonban összhangban van a globális tendenciákkal is. Több forrás is megerősíti, hogy az utóbbi időben a különböző támadói kampányok erősen monetáris fókuszáltságúak amelyek kifejezetten Linux SSH és felhőkörnyezeteket érintenek.

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