NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 34. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- ESEMÉNY
- CTI RIPORT
- BBA+ BESZÁMOLÓ

KIBERTÁMADÁS! PODCAST

Ukrajnában 94 csaló call centert számoltak fel, és több millió dollárnyi készpénzt foglaltak le

(bleepingcomputer.com)

Az ukrán hatóságok országszerte 94 csaló call centert számoltak fel egy nemzetközi nyomozás keretében. A művelet során 411 házkutatást tartottak, és jelentős mennyiségű informatikai eszközt, bankkártyát, SIM-kártyát, valamint több millió dollár értékű készpénzt és egyéb vagyont foglaltak le. **Bővebben...**

Hitelesítés nélküli, root jogosultságú kódfuttatás a Citrix NetScalerben

(watchtowr.com)

A watchTowr Labs biztonsági kutatói egy friss Citrix NetScaler ADC és NetScaler Gateway, csendben kijavított “heap overflow” hibából egy teljesen működő, hitelesítés nélküli, root jogosultsággal futó, távoli kódfuttatásig (RCE) eszkalálódó exploitot építettek. A Citrix NetScaler egy vállalati forgalomkezelő és terheléselosztó platform, amely szinte minden nagyvállalati hálózatban megtalálható a világon. **Bővebben...**

A Threema üzenetküldő szolgáltatását két napon át DDoS-támadások zavarták

(cyberinsider.com)

A svájci székhelyű, titkosított üzenetküldő szolgáltató, a Threema nagyszabású DDoS támadássorozat miatt jelentős szolgáltatáskimaradást tapasztalt. A támadások múlt héten kedd este kezdődtek, és a vállalat szolgáltatásai 19:30 és 23:30 között teljesen elérhetetlenek voltak. **Bővebben...**

Aktívan kihasznált macOS hibára figyelmeztet az NCSC

(bleepingcomputer.com)

A holland Nemzeti Kiberbiztonsági Központ (NCSC) a macOS egy hitelesítést megkerülő sebezhetőség aktív kihasználására hívja fel a figyelmet, miután nyilvánosságra kerültek a kihasználáshoz szükséges exploitok. **Bővebben...**

Új biztonsági funkciót vezet be a WhatsApp

(securityweek.com)

A WhatsApp megkezdte a Scam Alert, vagyis a csalásokra figyelmeztető funkció béta verziójának bevezetését, amely egy eszközön futó gépi tanulási modell segítségével képes felismerni és megjelölni a gyanús, potenciálisan csaló üzeneteket.

Bővbben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 08. 14. - 2026. 08. 18.

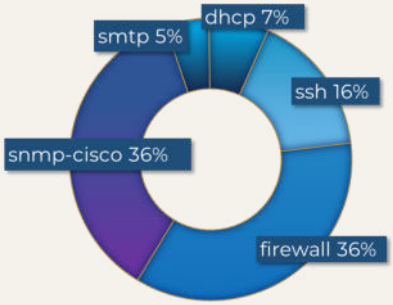
Fenyegetettségi szint:

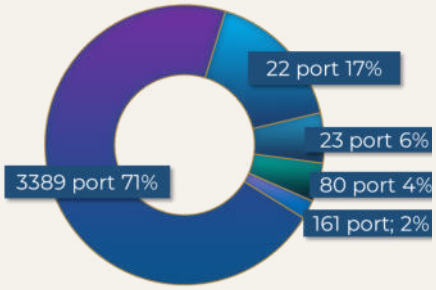
alacsony | közepes | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.

Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

ESEMÉNY

ITBN 2026

2026. szeptember 24.
1093 Budapest, Fővám tér 11-12.
— Bálna Honvédelmi Központ

Idén az ITBN történetének legszélesebb és legmélyebb szakmai programjára lehet számítani: a központi téma a **Seregszemle** lesz. Ezen a napon 5300 négyzetméteren felsorakozik a **szakma teljes spektruma** a fiatal tehetségektől a veterán szakemberekig, a törzsközönségtől a hacker közösségig.

Megindulnak az ezredek, hogy közösen alakítsák ki a jövő védelmi vonalait. Az **AI integrációja** mellett idén a védelem **megszilárdítása**, a **kockázatok radikális csökkentése**, valamint a **szigorodó szabályozási környezetnek való megfelelés** lesz a fókuszban.

Exkluzív ajánlat az NKI szakmai közösség részére

Az NBSZ NKI ügyfelei most **30% kedvezménnyel** vehetnek részt a teljes rendezvényen.

Kuponkód:
KEDV-5LL7S4

További információ

Jegyvásárlás

NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI RIPORT

2026. július havi CTI riport

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.

Elolvasom

Érdekli, hogyan formálhatják a jövőt a különböző kiberbiztonsági kihívások?

Fedezze fel velünk a legizgalmasabb témákat, a szakértői tippektől egészen a legújabb trendekig!

Kövesse podcastünket a legnépszerűbb felületeken!

NEMZETI KIBERBIZTONSÁGI INTÉZET

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

AREA41 Konferencia

2026. június 18-19.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** munkatársai **Széchenyi Terv Plusz pályázat** részeként szakmai ismeretbővítésen vesznek részt a súlyos és szervezett, határon átnyúló bűncselekmények elleni küzdelem, illetve ilyen jellegű bűncselekmények megelőzésének fejlesztése céljából.

A projekt célja a kiberfenyegetések elleni fellépéshez szükséges friss ismeretek gyűjtése és megosztása a hazai kiberbiztonsági szakemberekkel.

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. június 18-19.** között részt vettek a **Zürich-ben kétévente megrendezésre kerülő AREA41 konferencián**.

Az **informatikai biztonsággal**, illetve **etikus hacker témakörökkel** foglalkozó Area41 konferencia kétévente kerül megrendezésre. A konferencia középpontjában olyan IT biztonsággal kapcsolatos témák állnak, amelyek meghatározzák a **szektor trendjeinek alakulását, konkrét esettanulmányokat** hoznak az előadások során **IoT, Microsoft Enterprise hacking és egyéb** témakörökben. A konferencia maga kisebb látogatói közönséggel rendelkezik, mint a szervező trendvezető DefCon rendezvényei, de tartalmát tekintve megegyező színvonalat képvisel, elsősorban szakemberektől szól szakembereknek.

Az „AREA41" konferencia főbb témakörei:

- mesterséges intelligencia fejlődése;
- kriptovaluták és blockchain technológia;
- blue team és red team specifikus workshopok;
- IoT eszközök védelme;
- OT infrastruktúrák védelme;
- biztonságos adattárolásra használt eszközök tárhelyvédelmének kijátszása;
- hálózati forgalom vizsgálata;
- jelszókezelés, jelszótárolás;
- social engineering újdonságok;
- cloud szolgáltatások megvédése;
- gépjármű-hacking;
- RF-hacking;
- social media kockázatai;
- személyes adatok védelme;
- adatbázisok védelme.

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Hacking Every Entra ID Tenant With Actor Tokens

(Dirk-Jan Mollema — Outsider Security)

Az előadás bemutatta a **CVE-2025-55241**-et, ami egy CVSS-10.0-ás sérülékenység a Microsoft **Entra ID környezetben**. A felhőalapú CVE-k viszonylag ritkák, a Microsoft világában csak a kritikus felhőalapú sérülékenységek kapnak ilyen azonosítót. Az előadáson bemutatásra került, hogy a sérülékenységet **ki lehetett használni bármely felhasználó tenantjának megfertőzésére**, a felhasználó megszemélyesítésére.

Egy rosszul kezelt backend token-szolgáltatás kihasználásával és a felhasználókezelő API-val kombinálva lehetséges volt olyan szerepkör tokeneket kérni, amelyek segítségével jogosultság **kiterjesztés, felhasználói megszemélyesítés vált elérhetővé** tetszőleges felhasználók, beleértve a globális **rendszergazdák esetében is**. A gyakorlatban ez lehetővé tette **bármely Entra ID teljes átvételét**, minimális naplózással és korlátozott felderítési lehetőségekkel. Az előadás nem csak a kihasználásra koncentrált, hanem a kutatás hátterét is bemutatta, és azt, hogy az évek során hány apró részlet vezetett el a sérülékenység felfedezéséhez.

DFIR Report at Cons - Deconstructing Real-World Intrusions

(Angelo Violetti — Swisscom & The DFIR Report,
Alessandro Di Carlo — ThreatDown & The DFIR Report)

A DFIR Report a **kiberfenyegetési hírszerzés és az incidenskezelés** közösségében jól ismert vállalat és projekt, köszönhetően azoknak a kiváló minőségű, részletes jelentéseinek, amelyek technikai betekintést nyújtanak a valós támadási esetekbe. Az előadásban bemutatásra kerültek a DFIR Report jelentései a legutóbbi, nagy hatással bíró esetekről. Az előadás **mélyreható elemzések** jellegzetes idővonal-ábrákon és a technikai elemzéseken keresztül vezette végig a közönséget az **incidensek teljes életciklusán**.

A jelentés a következő két incidenst mutatta be**: „Contagious Interview”:** ez az észak-koreai állam által támogatott szereplők folyamatos erőfeszítése az **Észak Koreai-rezsim működését támogató bevételi források biztosítására.** A támadás során több npm-csomagot használtak a parancs- és vezérlőinfrastruktúra működtetéséhez. A moduláris, többfázisú eszközkészlet tartalmazta az OtterCookie-t, az InvisibleFerret-et és a Tsunami telepítőt, amelyek lehetővé tették a kezdeti hozzáférést, az interaktív parancsok végrehajtását, a perzisztenciát és a payload továbbítását több operációs rendszeren keresztül.

A **„GootLoader visszatér”:** egy olyan támadás, amelyet egy olyan szereplő hajtott végre, aki a **GootLoader SEO-poisoning kampányon keresztül** szerzett kezdeti hozzáférést. Ezt követően a támadás során Kerberoasting-et, Supper-proxyk futtatását, valamint egy „MEOWBACKCONN” néven azonosított proxy DLL-t alkalmaztak. A végső szakaszban a naplóbejegyzések törlésével, az RDP-nyomok elrejtésével és a rendszerleíró kulcsok manipulálásával próbálták eltüntetni a nyomokat.

MIB2: Still Running, Still Vulnerable

(Raphael Lipp — Cyber Security Consultant, Popp Schweiz AG.,
Pascal Gujer — Security Researcher, Teamleader Digital Forensics).

Az előadás rámutatott a **gépjármű iparban használt kommunikációs protokollokra és azok gyengeségeire**. A prezentációban bemutatásra került a VW, Audi, Skoda, Porsche, Bentley modellekben alkalmazott **MIB2 protokoll**, amely az autók fedélzeti computere és érzékelők, szenzorok közötti kommunikációért felel. Live Demo során az előadók egy Audi Q5 gépjármű fedélzeti rendszerében lévő hard-code-olt adatokkal, gyenge hozzáférés vezérlést kihasználva, és plain text-ben tárolt hitelesítő adatok alkalmazásával szereztek teljes hozzáférést a gépjármű rendszere felett. Az előadás kitért az **autóipari biztonság jövőbeli irányainak áttekintésére**, valamint a **MIB3** bemutatására is.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

DragonForce: the cartel makes a TURN in Ransomware Capabilities

(Thibaut Passilly — Threat Researcher, Broadcom)

Az előadás bemutatta egy amerikai céget érintő **zsarolóvírus támadás esettanulmányán** keresztül, hogy a **DragonForce művelet a RaaS** (Ransomware as a Service)-modellről egy rendkívül kifinomult kartellré alakult át. A kezdeti behatolás és a pozíció megszilárdítása után a csoport fejlett védelmi kijátszási módszerei között szerepelt az alkalmazás-eltérítésen keresztüli kódvégrehajtás, valamint egy többvektoros **„Bring Your Own Vulnerable Driver" (BYOVD) stratégia.** Ez a BYOVD-megközelítés a Tower of Fantasy és a Topaz Antifraud legitim gyártói illesztőprogramjaiban található ismert sérülékenységeket használta ki, és bevezetett egy újszerű **„Havoc Process Terminator" nevű eszközt**, amely egy Huawei-alkatrészt használt a biztonsági folyamatok kernel-szintű leállításához. A jellegzetes eszköz egy új, **Go-alapú távoli hozzáférést biztosító backdoor-t tartalmazott**, amely a Command and Control (C2) szerver elérését segített kialakítani. A rejtőzködést úgy érte el, hogy egy népszerű kommunikációs szolgáltatás névtelen tokenjét használta a legitim Microsoft-relé-kiszolgálóval való interakcióhoz, mielőtt közvetlen, rosszindulatú QUIC C2-csatornát hozott volna létre. A backdoor átfogó ellenőrzést biztosított, beleértve a parancsok végrehajtását, a felderítést és a hitelesítő adatok ellopását.

The Linux Evasion Stack: Breaking All Three EDR Pillars with io_uring and ELF Packing

(Massimo Bertocchi — Cybersecurity Professional, SIX Group).

Az előadás bemutatta, hogy melyek a **modern Linux endpoint-detection és response (EDR) megoldások három alapvető pillére**. Ezek a rendszerhívások kernel-tracepontokon keresztüli figyelése, a felhasználói térben lévő függvények könyvtár-beiktatáson keresztüli átkapcsolása, valamint a lemezen található futtatható fájlok statikus bináris elemzése.

Ebben az előadásban mindhárom lehetőség bemutatásra került, így teljes EDR-recon-t érve el. Bemutatásra került egy **layered evasion módszertan**, amely három független technikát kapcsolt össze egyetlen támadási lánccá. Először automatizált EDR-felderítést végzett az előadó, amely során egy hook-felismerő eszköz végigjárta a betöltött könyvtárak GOT/PLT-jét, és összehasonlítja a memóriában lévő függvényprológusokat a lemezen található másolatokkal, pontosan azonosítva, hogy az egyes EDR-termékek mely függvényeket figyelik. Ezzel a térképpel felvértezve egy egyedi ELF-packert alkalmazott, amely a memfd_create és a fexecve segítségével fájlmentes, memóriában történő végrehajtást valósított meg, közvetlen rendszerhívás-stubokkal, amelyek teljes mértékben megkerülték az összes felhasználói szintű hookot. Végül az összes végrehajtás utáni műveletet kizárólag az io_uring benyújtási/befejezési ring interfészen keresztül irányította, így a ptrace, a seccomp-bpf audit vagy a kernel tracepoint-alapú monitorok számára látható rendszerhívás-nyomok száma nulla lett. Így a ransomware láthatatlanná vált.

Breaking Every Guardrail Everywhere All At Once

(Donato Capitella — Software Engineer, Reversec)

Az előadás a **GenAI-rendszerek biztonsági tesztelésével és azok gyakorlati kihívásaival foglalkozott.** Rávilágított az előadás, hogy napjainkban gyakran csupán **„LLM red teaming”**-re korlátozódik: a modell elszigetelt vizsgálatára, hogy kiderüljön, milyen veszélyes vagy sértő tartalmakat generál. Azonban ez a megközelítés nem elégséges. Egy vizsgálat során az LLM-alkalmazások **teljes használati eseteit kell értékelni**, különös figyelmet fordítva arra, hogy a bemeneti és kimeneti adatok hogyan terjednek az alkalmazás logikáján keresztül, és hogyan teszik lehetővé konkrét biztonsági kockázatok, mint például az adatlopás, a cross-site scripting és a jogosultsági ellenőrzés megkerülését.

Az előadásban a különböző vizsgálatok során szerzett gyakorlati tapasztalatok, valamint a munkához kifejlesztett nyílt forráskódú keretrendszer, a **Spikee** is bemutatásra került.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

A Spikee-t olyan LLM-alkalmazások vizsgálatára lehet használni, ahol **a modell az alkalmazás logikájába van beágyazva**, ahelyett, hogy egyszerű következtetési végpontként lenne elérhető. Az előadás kitért a nem beszélgetésalapú GenAI munkafolyamatok, a WebSockets és az egyedi API-k tesztelésére szolgáló megközelítésekre, az alkalmazáslogikához és a megbízási korlátokhoz igazodó, hatókörrel rendelkező prompt-injektálási adatkészletek létrehozására, a brute-force alapú jailbreak-technikák (pl. anti-spotlighting, best-of-n, crescendo) alkalmazására a védelmi korlátok vizsgálatára és a gyakorlati megkerülési módszerek bemutatására, valamint az izolált vagy air-gapped környezetekben végzett tesztelésekre.

Copy, Paste Persist: Inside the .NET Malware Gene Pool

(Jonathan Peters — Threat Researcher, Detection Engineer, Nextron Systems)

Az előadás azt mutatta meg, hogy **milyen mértékű a kód újrafelhasználás a .NET-alapú kártevőprogramok ökoszisztémájában**, és hogyan tudják ezt a jelenséget a védekezéssel foglalkozó szakemberek a saját javukra fordítani.

Az előadás főbb pontjai: **Elemzés és adatok**, amelyek több mint 150 millió feldolgozott kártevőprogram-minta alapján készültek. Kiemelten figyelve a .NET-alapú rosszindulatú programok ökoszisztémájában tapasztalható hatalmas mértékű **kódújrafelhasználásra**. Bemutatásra került a **közvetlen másolás-beillesztéses újrafelhasználása** olyan jól ismert rosszindulatú programcsaládok között, mint a Quasar, az AsyncRAT, a Pulsar és az XWorm.

Az előadó rávilágított arra, hogy mennyi olyan állítólag **„új" rosszindulatú programcsalád van, ami valójában csak meglévő projektek módosított változata**. Valódi kódpéldák bemutatásra kerültek, amelyek feltárták a közös implementációkat, például a kriptográfiai rutinokat és a kommunikációs logikát. Elmagyarázta, hogyan használhatják fel a védekezéssel foglalkozó szakemberek ezeket az ismereteket olyan **általános észlelési módszerek kidolgozásához**,

amelyek az egyes családok helyett az újrahasznosított kódokat célozzák meg. Valós észlelési eredmények és adatok bemutatására is sor került, amelyek megmutatták, hogy ez a stratégia hogyan teszi lehetővé a **számos rosszindulatú programváltozat széles körű felismerését**.

Rust & Ransomware: Defending Legacy OT Environments against Modern Threats

(Ueli — Etikus hacker, Bug-Bounty vadász, IoT/OT szakember)

Az előadás keretében bemutatásra került az **IT és OT területek közötti különbségek**, valamint az ezekből fakadó kihívások a **vulnerability management** tükrében. Amíg az IT környezetben egy kiforrott folyamatról beszélhetünk, addig az OT területéről ez nem mondható el, és folyamatosan egyedi kihívások elé állítja az OT-ban dolgozó szakembereket. A két terület különbségének megértése kulcsfontosságú az OT környezetek biztonságossá tételéhez, amelyek egyre szorosabb kapcsolatban állnak és egyre inkább függenek egymástól az informatikai rendszerekkel. Az előadásban egy **valós elektromos közműveknél feltárt sérülékenység kezelése került prezentálásra**, valamint bemutatásra került, hogyan haladnak végig a támadók az **ICS Cyber Kill Chain**-en, hogy az IT-hálózatokról átjussanak a fizikai üzembe. Végül gyakorlati, zavarmentes védelmi stratégiák kerültek felvázolásra.

Toward Verifiable Microcode: Reverse Engineering AMD Zen5 Update

(Kaya Ercihan — Security Engineer, SWITCH,
Antonio Vazquez Blanco — Industrial Engineer, Security Researcher, Tarlogic)

Az előadás betekintést nyújtott a **mikrokód-frissítések világába**, amelyek lehetőséget nyújtanak a processzorgyártóknak arra, hogy a **gyártás után módosítsák a belső vezérlési viselkedést,** például a hibás vagy sérülékeny végrehajtási útvonalak kockázatának csökkentése érdekében, anélkül, hogy a chipet újra kellene tervezni.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Ennek eredményeként a mikrokód a modern CPU-k biztonsági szempontból **kritikus**, de nagyrészt **átláthatatlan** rétegét képezi.

Ennek az előadásnak az alapja az a tanulmány volt, amely az **AMD Zen 5 mikrokód-frissítéseinek strukturált visszafejtési elemzését** mutatta be. Az előadók nyilvános kernel-forráskódok és a korpuszszintű validáció alapján rekonstruálták a javításformátumot, azonosították az AMD mikrokód-javítások főbb szerkezeti területeit, és elkülönítették a metaadatokat, a kriptográfiai anyagokat, az átirányítási állapotot és a végrehajtható payload-kat. A szisztematikus elemzés támogatására kidolgoztak egy munkafolyamatot az AMD mikrokód-javítások gyűjtésére, elemzésére, kivonására és normalizálására, és az így nyert formátumismeretet egy Binary Ninja bővítményben valósították meg, amely a javítás szerkezetét, valamint a revíziós és betöltő azonosítókat közvetlenül az elemzési környezetben jeleníti meg. Továbbá elemezték a titkosított és titkosítatlan payload-kat, és statisztikai profilalkotást alkalmaztak a kezdeti opkód-címkék és a heurisztikus control-flow megszerzésére. Az így **kialakított módszertan** és eszközök reprodukálható alapot teremtettek a titkosítás feloldásához, az utasítások osztályozásához és a biztonsági szempontból releváns mikrokód-revíziók differenciálelemzéséhez.

Mask off: analyzing a secure SD card

(Nicolas Oberli — Security Engineer)

Az előadó egy olyan **SD-kártya-modellt** mutatott be, amelyet biztonságos adathordozóként forgalmaznak, mivel **jelszóval védi a rajta titkosított módon tárolt tartalmat**. A gyártó szerint az adatokhoz való hozzáférés egyetlen módja a jelszó ismerete. Az előadás bemutatta az eszközön elvégzett vizsgálatokat, amelyek következtében a kliensalkalmazás visszafejtését, a protokoll Python nyelven történő újra implementálását, valamint a további elemzéseket, melyek eredményeként végül **két olyan sérülékenység felfedezésével zárultak, amelyek lehetővé tették a védelem teljes megkerülését**.