NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2025. 43. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- ESEMÉNYEK
- BBA+ BESZÁMOLÓ

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

GlassWorm kártevővel célozzák ellátási lánc támadások során a VS Code bővítményeket

(securityweek.com)

A Koi Security jelentése szerint a Visual Studio Code fejlesztőit egy önszaporító féreggel (worm) célozták meg egy kifinomult ellátási lánc (supply chain) támadásban az OpenVSX platformon keresztül. **Bővebben...**

Cirtix sebezhetőségen keresztül támadhatott meg egy Kínához köthető hackercsoport egy európai távközlési céget

(thehackernews.com)

A Darktrace szerint 2025. július első hetében egy európai távközlési szervezet célpontja lett a Kínához köthető Salt Typhoon nevű kiberkémkedési csoportnak. A támadók a Citrix NetScaler Gateway egyik sebezhetőségét kihasználva szereztek kezdeti hozzáférést a rendszerhez, majd tovább terjesztkedtek a Citrix Virtual Delivery Agent (VDA) hosztokra az ügyfél Machine Creation Services (MCS) alhálózatán belül. **Bővebben...**

A Dolby Unified Decoder-ben talált sérülékenység zero-click támadásokat tesz lehetővé

(securityweek.com)

A Dolby Unified Decoder-ben felfedezett, magas súlyosságú sérülékenység távoli kódfuttatást tehet lehetővé, bizonyos esetekben felhasználói interakció nélkül. A Unified Decoder egy Dolby Digital Plus (DD+) szabványra épülő szoftver/hardver komponens, amely DD+, Dolby AC-4 és egyéb hangformátumokat dolgoz fel, és alakít át lejátszható formátumokká. **Bővebben...**

TikTok-videókban terjesztenek információlopó programokat

(bleepingcomputer.com)

A kiberbűnözők továbbra is TikTok-videókat használnak információlopó programok terjesztésére ClickFix típusú támadások kihasználásával. **Bővebben...**

Feltörték a Xubuntu weboldalát

(omgubuntu.co.uk)

Október közepén a Xubuntu (az Ubuntu egyik hivatalos, könnyűsúlyú változata) weboldalán egy furcsa és aggasztó jelenséget észleltek. Aki a hivatalos letöltési oldalról akarta letölteni az operációs rendszert, az nem a megszokott telepítőfájlt vagy torrentet kapta, hanem egy „xubuntu-safe-download.zip” nevű csomagot. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2025. 10. 17. — 2025. 10. 21.

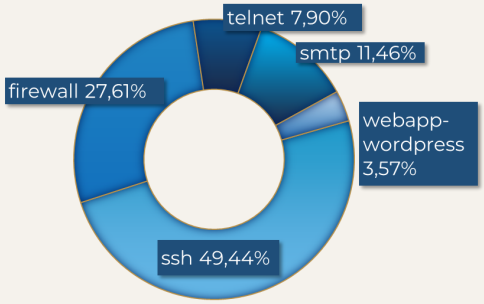
Fenyegetettségi szint:

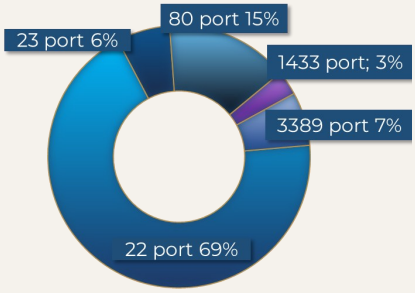
alacsony | közepes | magas | kritikus

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

Future IT 2025 konferencia

2025. november 17. - 19.

Siófok, Azúr Hotel

A Future IT 2025 egy olyan egyedülálló rendezvény, amely egyfajta **ernyőkonferenciaként számos kulcsfontosságú IT területet egyesít**, mint például a mesterséges intelligencia, a kiberbiztonság, az adatmenedzsment vagy a kvantumtechnológia.

A konferencián az ICT Global társszervezőjeként találkozhatnak az **NBSZ NKI** által szervezett előadásokkal is, ahol a **CTI-kérdéskörön** át a **hatósági és auditori témakörökön** keresztül egészen az **incidenskezelési folyamatokig** számos érdekes előadást hallgathatnak meg a résztvevők.

Az **NKIFUTUREIT2025** kuponkóddal most **25% kedvezményhez** juthatnak a konferencia jegyeinek árából. A kedvezmény a szállásdíjra nem vonatkozik.

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

ESEMÉNY

HTE EIVOK-64 konferencia

2025. október 30.

Gödöllő, Szent István Campus

A **HTE EIVOK** és a **Magyar Agrár- és Élettudományi Egyetem** közös szervezésében, 2025. október 30-án kerül megszervezésre az EIVOK-64 konferencia.

A kiberbiztonság alapvető feladatai mára mindenhol jelen vannak. Többek között érintik a felsőoktatást és agráriumot is a NIS2 és egyéb jelenleg hatályos kiberbiztonsági jogszabályokon keresztül. Az EIVOK-64 konferencia a **kiberbiztonság**, a **felsőoktatás** és az **agrárium** szakmai kérdéseit dolgozza fel.

A rendezvény **ingyenes**, de **regisztrációhoz kötött**. További információk és a regisztráció elérhető az alábbi QR kód beolvasásával.

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogass el LinkedIn oldalunkra!

NEMZETI KIBERBIZTONSÁGI INTÉZET

BBA+ BESZÁMOLÓ

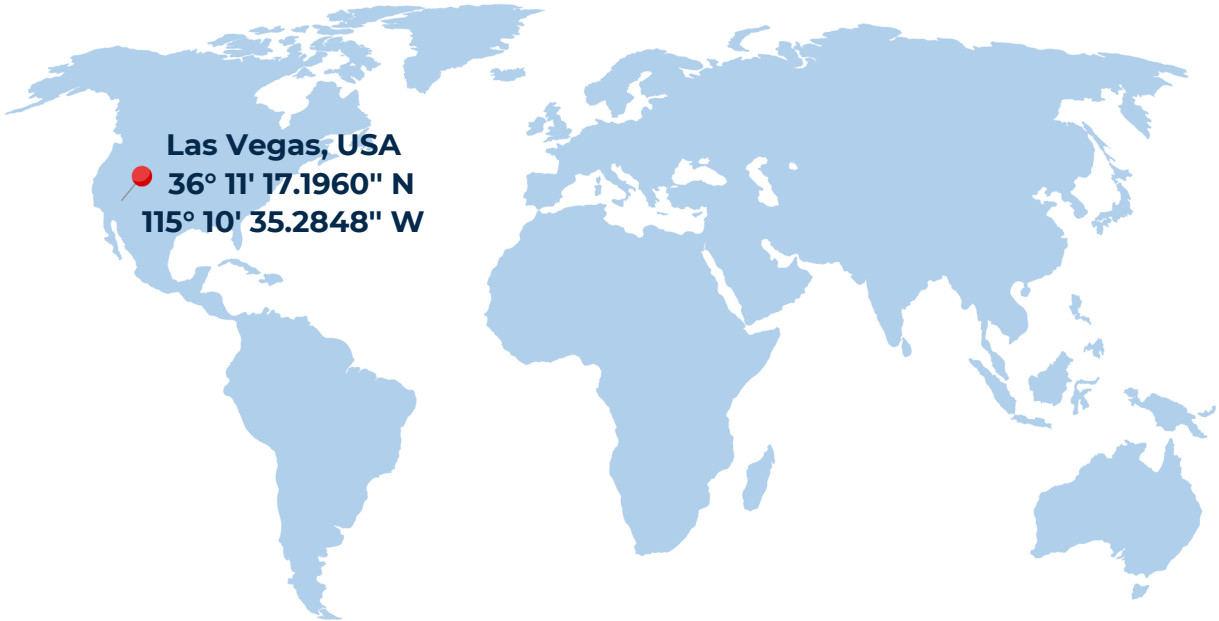
BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

BlackHat USA 2025 és DefCon 33 - konferencia

2025. augusztus 06-10.

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.



NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzeti Kiberbiztonsági Intézet munkatársai részt vettek a **2025. augusztus 6-10.** Las Vegas-ban megrendezésre kerülő éves **BlackHat USA 2025 és DefCon 33** konferenciákon. Évente megrendezésre kerülnek az informatikai biztonsággal kapcsolatos, illetve etikus hacker témájú BlackHat USA és DefCon konferenciák. Ezek bemutatóit, valamint előadásait **informatikai szakértők** tartják. A „BlackHat USA 2025" és a „DefCon 33" konferenciák főbb **témakörei:**

- Választási rendszerek befolyásolása informatikai szempontból
- Mesterséges intelligencia fejlődése
- Kriptovaluták és blockchain technológia
- Blue Team és Red Team specifikus workshopok
- IoT eszközök védelme
- Biometrikus hitelesítés kockázata
- Deep fake technológiák
- SSO bejelentkezés kockázata és védelme
- Hálózati forgalom vizsgálata
- Jelszókezelés, jelszótárolás
- Social Engineering újdonságok
- Cloud szolgáltatások megvédése
- Gépjármű-hacking
- Social media kockázatai
- Személyes adatok védelme
- Adatbázisok védelme

Kiknek ajánlott a beszámoló megismerése?

- Sérülékenységvizsgálattal foglalkozó IT biztonsági szakembereknek
- Minden kiberbiztonsági szakember számára

A szakmailag legfontosabb előadások és bemutatók rövid összefoglalója az alábbiakban olvasható.

BBA-PLUSZ-31.2-24-2024-00003. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

From Prompts to Pwns: Exploiting and Securing AI Agents [BlackHat USA 2025]

(Rebecca Lynch, Rich Harang)

Ez az előadás a **mesterséges intelligencia-ügynökök (AI agents) biztonsági kockázatait és a védekezési lehetőségeket** járta körül, különös hangsúllyal a nagy nyelvi modellek (LLM-ek) kihasználására. A kutatók részletesen bemutatták, hogyan lehet különféle prompt-injection technikákkal – akár felhasználói interakció nélkül, úgynevezett **„0-click" módszerrel** – elérni, hogy egy AI-ügynök nem kívánt műveleteket hajtson végre. Ezek között szerepelhet **távoli parancsvégrehajtás (RCE), érzékeny adatok kinyerése** vagy a **rendszer működésének manipulálása**.

Az előadók kitértek arra, hogy az AI rendszerek egyre gyakrabban kapnak hozzáférést külső API-khoz, vállalati adatbázisokhoz vagy felhőszolgáltatásokhoz, így egy sikeres támadás hatása sokkal szélesebb körben érezhető. A bemutató során példákat hoztak arra, hogyan lehet a rosszindulatú utasításokat ártalmatlannak tűnő forrásokban – például dokumentumokban, naptári bejegyzésekben vagy webes űrlapokban – elrejteni, amelyek később, az AI által feldolgozva, automatikusan végrehajtódnak. Részletesen elemezték a különféle támadási vektorokat: a **közvetlen prompt injection** esetében a támadó közvetlenül kommunikál a modellel, míg az indirekt változatnál a támadó tartalmat helyez el a környezetben, amelyet a modell később olvas be. Ezen felül bemutatták a válaszmanipulációs támadásokat is, ahol a modell kimenete tartalmaz további, rejtett utasításokat, amelyeket egy másik AI-ügynök vagy rendszer hajt végre. A védekezési stratégiák között szerepelt a **bemeneti adatok szigorú szűrése**, a magas kockázatú műveletekhez szükséges **többlépcsős jóváhagyás**, valamint a modell és a külső rendszerek közötti kommunikáció sandboxolása. Az előadás egyértelmű üzenete az volt, hogy a mesterséges intelligencia használata során a hagyományos biztonsági

modelleket újra kell gondolni, mivel az AI-ügynökök képesek a korábbi automatizációs rendszereknél sokkal összetettebb és veszélyesebb interakciókra.

Az előadás prezentációja az alábbi linken érhető el.

HTTP/1.1 Must Die! The Desync Endgame [BlackHat USA 2025]

(James Kettle)

Ez az előadás a **HTTP/1.1 protokoll alapvető tervezési hibáit** és az **ezekből fakadó támadási lehetőségeket** mutatta be, különös tekintettel a „desynchronization" típusú támadásokra. James Kettle részletesen elmagyarázta, hogy a HTTP/1.1-ben lévő kérés-határkezelési problémák miatt a kliens és a szerver eltérően értelmezheti ugyanazt a kérést. Ez a különbség lehetővé teszi, hogy egy támadó **manipulált kéréseket juttasson be** a kommunikációs folyamatba, amelyek egy másik felhasználó kéréséhez **csatolódva kerülnek feldolgozásra**. A bemutatott technikák között szerepelt a „request smuggling" és a fejlécek ütköztetésén alapuló manipuláció, amellyel adatlopást, session-átvételt vagy cache-mérgezést lehet végrehajtani. Különösen aggasztó, hogy ezek a támadások nemcsak kisebb weboldalak, hanem **nagy tartalomszolgáltató hálózatok (CDN-ek) ellen is sikerrel alkalmazhatók**, így akár több millió felhasználó is érintett lehet. Az előadás kitért arra is, hogy a védekezés rendkívül nehéz, mivel a HTTP/1.1 szabványos viselkedése maga is hozzájárul a probléma fennmaradásához. A jelenlegi javítások többnyire **szolgáltató-specifikusak**, és sok esetben **csak részlegesen nyújtanak védelmet**. James Kettle kiemelte, hogy hosszú távon a megoldás csak a HTTP/2 vagy újabb protokollverziókra való átállás lehet, amelyek jobban kezelik a kérés-határ problémákat.

A prezentáció technikai része lépésről lépésre bemutatta a **sebezhetőség felderítését**, a **támadás kivitelezését**, valamint az **eszközöket**, amelyekkel a fejlesztők **saját rendszereik sebezhetőségét ellenőrizhetik**.

Az előadás prezentációja az alábbi linken érhető el.

Invitation Is All You Need! Invoking Gemini for Workspace Agents with a Simple Google Calendar Invite [BlackHat USA 2025]

(Ben Nassi, Or Yair, Stav Cohen)

Ez az előadás az úgynevezett „promptware" támadások egyik leginnovatívabb formáját mutatta be, amely egyszerű **Google Calendar meghívón keresztül** célozza meg a **Google Gemini for Workspace AI-ügynököt**. A támadás lényege, hogy a meghívó szövegébe rejtett, speciálisan kialakított utasítások akkor hajtódnak végre, amikor a felhasználó a Geminitől kéri a napi eseményeinek összefoglalását. A bemutatott példák között szerepelt, hogy a támadó képes volt **okosotthoni eszközöket vezérelni**, például kinyitni ablakokat, bekapcsolni a fűtést, vagy Zoom-hívást indítani – mindezt anélkül, hogy a felhasználó közvetlen parancsot adott volna erre. A támadás teljesen indirekt módon működik, mivel a felhasználó csak egy naptári eseményt lát, miközben a Gemini a háttérben a **rejtett utasításokat is végrehajtja**. A kutatók bemutatták, hogy a módszer nemcsak fizikai eszközök irányítására használható, hanem érzékeny adatok kiszivárogtatására, e-mailek továbbítására vagy rosszindulatú linkek megnyitására is. Az előadás hangsúlyozta, hogy az AI-ügynökök biztonságának tervezésekor **nemcsak a közvetlen felhasználói interakciókat** kell védeni, hanem **minden olyan adatforrást is, amelyből az AI információt szerezhet**. A bemutató rávilágított arra is, hogy a támadások elleni védelem

komplex feladat: szükség van tartalomszűrésre, kontextus-ellenőrzésre és felhasználói jóváhagyásra minden olyan esetben, amikor az AI külső rendszereket vezérelhet.

Turning Camera Surveillance on its Axis [BlackHat USA 2025]

(Noam Moshe)

Ez az előadás a fizikai biztonsági rendszerek és a kiberbiztonság közötti határterület egyik legsúlyosabb sérülékenységét tárta fel. Noam Moshe és a Claroty Team82 kutatói az Axis Communications egyik legelterjedtebb videómegfigyelő megoldását vizsgálták, és négy **kritikus sebezhetőséget fedeztek fel** az Axis.Remoting nevű protokollban. Ez a protokoll a gyártó két fő alkalmazása – az Axis Device Manager (szerveroldali eszközkezelő) és az Axis Camera Station (kliensoldali felügyeleti szoftver) – közötti kommunikációt biztosítja. A felfedezett hibák láncolatban kihasználva lehetővé tették a **pre-autentikációs távoli kódfuttatást** mind a szerver, mind a kliens oldalán. A kutatók bemutatták, hogyan lehet a sérülékeny szolgáltatásokat **az interneten keresztül felderíteni**, majd célzott támadásokkal kompromittálni. Egy ilyen támadás következtében a támadó nemcsak hozzáférhet az élő kameraképekhez és felvételekhez, hanem **módosíthatja is a beállításokat**, leállíthatja **a rögzítést** vagy **új kártékony firmware-t tölthet fel** a kamerákra. A veszélyt tovább fokozza, hogy ezek a kamerarendszerek gyakran vállalati hálózatokba integráltak, így egy kompromittált kamera potenciális belépési pontot jelenthet a teljes IT-infrastruktúrába. A prezentációban részletesen elemezték a hibák technikai okait, például a **hitelesítési folyamatok hiányosságait** és a protokoll adatátviteli struktúrájának sebezhetőségeit. A védekezési javaslatok között szerepelt a firmware frissítése, a hálózati hozzáférés korlátozása, a szolgáltatások leválasztása az internetről, valamint a forgalom TLS-sel történő titkosítása. Moshe hangsúlyozta, hogy a fizikai

biztonsági rendszerek kiberbiztonsági védelme **gyakran alulértékelt**, pedig a modern fenyegetések fényében ezek is elsődleges célponttá váltak.

Az előadás prezentációja az alábbi linken érhető el.

Lost & Found: The Hidden Risks of Account Recovery in a Passwordless Future [BlackHat USA 2025]

(*Sid Rao, Gabriela Sonkeri, Amel Bourdoucen, Janne)*

Ez az előadás a **jelszómentes hitelesítési rendszerek** egyik kritikus, sokszor alábecsült aspektusára, a fiók-helyreállítási mechanizmusokra fókuszált. A jelszómentes világ ígérete szerint a felhasználók **biometrikus azonosítással, biztonsági kulcsokkal vagy egyszer használatos kódokkal** léphetnek be, így megszűnik a jelszólopás kockázata. Azonban az előadók rámutattak, hogy ezek a rendszerek is **tartalmaznak „hátsó ajtót”** a fiók-helyreállítás formájában – és ez gyakran sokkal kevésbé védett, mint maga a fő hitelesítési csatorna. A kutatás bemutatta, hogy a legtöbb rendszer a fiók-helyreállítást e-mailre, SMS-re vagy biztonsági kérdésekre alapozza, amelyek könnyen támadhatók social engineering, SIM-swap vagy adatszivárgás révén. Egy támadó, aki nem tudja megkerülni a fő hitelesítést, gyakran **sikerrel járhat a helyreállítási folyamat manipulálásával**. Az előadók konkrét példákat hoztak olyan támadási láncokra, ahol a helyreállítási folyamatot kihasználva sikerült hozzáférést szerezni felhasználói fiókokhoz, majd onnan további rendszerekhez. Kiemelték, hogy a jelszómentes rendszerek terjedésével ezek a támadások **egyre vonzóbb célponttá válnak**, hiszen a támadók tudják, hogy a helyreállítási mechanizmus maradt az utolsó gyenge láncszem. A védekezés érdekében javasolták a **többtényezős helyreállítás bevezetését**, a **helyreállítási kérések erőteljes naplózását** és **felhasználói értesítését**, valamint a **helyreállítási útvonalak minimalizálását**. Az előadás tanulsága egyértelmű: a jelszómentes

biztonság **nem teljes**, ha a helyreállítási folyamat nincs ugyanazzal a gondossággal **megtervezve és védve**.

Browser Extension Clickjacking: One Click and Your Credit Card Is Stolen [BlackHat USA 2025]

(Marek Tóth)

A böngészőbővítmények (extensions) **hatalmas hozzáféréssel rendelkeznek** a felhasználói böngészési adatokhoz, weboldalak tartalmához és a böngésző különböző API-jaihoz. Ez az előadás bemutatta, hogyan lehet ezeket a jogosultságokat egy teljesen új támadási vektor — a „**browser extension clickjacking**” — segítségével kihasználni. A módszer lényege, hogy a támadó **láthatatlan, átlátszó rétegeket helyez** a felhasználó által használt weboldalak fölé, amelyek valójában a kártékony bővítmény funkcióit aktiválják. A felhasználó úgy hiszi, hogy egy ártalmatlan gombot vagy linket kattint meg, de valójában **engedélyt ad például fizetési adatok, jelszavak vagy e-mail fiókokhoz való hozzáférés átadására**. A prezentációban bemutatták, hogy az engedélykérések és felugró ablakok hogyan integrálhatók megtévesztő módon, elkerülve a felhasználó gyanúját. Mivel sok bővítmény „content script”-je a weboldal kontextusában fut, ezek **képesek szinte láthatatlanul manipulálni a felhasználói felületet**, és adatokat továbbítani külső szerverekre. A legveszélyesebb esetekben a támadó egyetlen kattintással képes teljes hitelkártyaadat-készleteket megszerezni, miközben a felhasználó nem észlel semmilyen rendellenességet. A védekezési javaslatok között szerepelt **a bővítmények engedélyezési modelljének szigorítása**, az **UI-integritás** valós idejű ellenőrzése, valamint az **engedélyek dinamikus, felhasználói interakcióhoz kötött megadása**. A bemutató rámutatott, hogy a böngészőbővítmények piacán a felhasználók gyakran vakon megbíznak a telepített kódokban, miközben ezek akár a teljes digitális életük felett átvehetik az irányítást.

One Modem to Brick Them All: Exploiting Vulnerabilities in the EV Charging Communication [BlackHat USA 2025]

(Sebastian Köhler, Marcell Szakály, Jan "SP3ZN45" Berens)

Az elektromos járművek (EV) töltőinfrastruktúrája **egyre összetettebb**, és az energiaellátás mellett hálózati kommunikációt is folytat a jármű és a töltőoszlop között. Ez az előadás a **töltési kommunikációs protokollok sebezhetőségeit** tárta fel, és bemutatta, hogyan lehet ezeket a hibákat kihasználva a töltőket **működésképtelenné** (brick) tenni, vagy akár **távolról átvenni az irányítást** a töltési folyamat felett. A kutatók kifejtették, hogy a legtöbb EV-töltő az Open Charge Point Protocol (OCPP) verzióit használja, amely TCP/IP vagy WebSocket alapú kommunikációt folytat. A hibás implementációk gyakran **nem ellenőrzik megfelelően** az üzenetek forrását és tartalmát, így a támadó képes lehet **hamis töltéskezdési vagy -leállítási parancsokat küldeni**. Egyes esetekben firmware-frissítési funkciókat is ki lehetett használni, amelyek hitelesítés nélkül engedtek új kódot telepíteni a készülékekre. A bemutatóban szerepelt egy demonstráció, amely során egyetlen sebezhető modemről kiindulva **több száz töltő működését sikerült megzavarni**. A veszély különösen nagy, mivel az EV-töltők gyakran nyilvános hálózatokon keresztül érhetők el, és egy ilyen támadás egyszerre okozhat logisztikai problémákat, pénzügyi károkat és biztonsági kockázatot a járműtulajdonosok számára. A védekezéshez a szakértők **javasolták az erős hitelesítési protokollok** alkalmazását, a **firmware integritásának kriptográfiai ellenőrzését**, valamint a **hálózati szegregáció** és **behatolásészlelés** bevezetését a töltőinfrastruktúrában.

Securing America: Readiness, Response, and Resilience for Critical Infrastructure Defense [BlackHat USA 2025]

(Chris Butera, Bob Costello, Frank Cilluffo)

Ez az előadás a **kritikus infrastruktúrák** – például energiaellátás, vízművek, közlekedési rendszerek és kommunikációs hálózatok – **védelmének átfogó stratégiáját** mutatta be, különös tekintettel az Egyesült Államokban érvényes kiberbiztonsági követelményekre. Az előadók, akik mindannyian komoly tapasztalattal rendelkeznek a nemzeti kiberbiztonsági irányítás területén, részletesen elemezték, hogyan változott meg az infrastruktúrák fenyegetési képe az elmúlt években. Kiemelték, hogy a korábbi, főként opportunista támadások helyét egyre inkább **célzott, államilag támogatott, kifinomult akciók vették át**, amelyek célja nem csupán a károkozás, hanem a stratégiai előny megszerzése. A prezentáció három fő pillérre építette a védelmi stratégiát: **felkészültség, reagálás és ellenállóképesség**. A felkészültség részeként hangsúlyozták a **rendszeres kockázatelemzést**, a **sebezhetőség-menedzsmentet** és a **folyamatos biztonságtudatossági képzést**. A reagálás kapcsán bemutatták a nemzeti szintű incidenskezelési protokollokat, a szövetségi és magánszektor közötti együttműködés fontosságát, valamint a gyors helyreállítási képességeket. Az ellenállóképesség alatt azokat az intézkedéseket értették, amelyek biztosítják, hogy a kritikus rendszerek **akkor is működőképesek maradjanak, ha részben kompromittálódnak**. Az előadásban szó esett az új technológiák – például a mesterséges intelligencia és a gépi tanulás – szerepéről a fenyegetések felismerésében és a támadások előrejelzésében, valamint a szimulációs gyakorlatok jelentőségéről a **valós reagálási képességek fejlesztésében**. Az üzenet egyértelmű volt: a kritikus infrastruktúrák védelme **nem egy egyszeri feladat**, hanem **folyamatos**, **dinamikus** folyamat, amely csak széles körű együttműködéssel és proaktív intézkedésekkel lehet sikeres.

BBA-PLUSZ-31.2-24-2024-00003. sz. pályázat részeként

Virtualization-Based (In)security – Weaponizing VBS Enclaves [DefCon33]

(*Ori David*)

A **Virtualization-Based Security (VBS)** egyik legizgalmasabb, ám kevéssé ismert aspektusa az enclave-technológia, amely lehetővé teszi, hogy egy folyamat elkülönítsen egy memóriaterületet, amelyhez még maga a folyamat vagy akár a kernel sem fér hozzá. Ez a technológia olyan biztonsági funkciókat támogat, mint a **Credential Guard** vagy a **Hypervisor-Code Integrity (HVCI)**. Az előadás azonban rávilágított arra az ellenérdekes felvetésre, hogy ez a biztonsági elszigetelés maga is kiváló terep lehet támadóknak, ha sikerül a támadó kódot egy enclave-ben végrehajtani – hiszen az onnan láthatatlan marad a rendszer számára. A „enclave malware" fogalmát bemutatva a kutatás feltárta a **VBS enclave**-ek korábban dokumentálatlan viselkedéseit, különös tekintettel azokra a technikákra, amelyek lehetővé teszik a **rosszindulatú kód futtatását anélkül**, hogy az **EDR-ek vagy elemzők észrevennék**. Bemutatták a „Bring Your Own Vulnerable Enclave" módszert is, amely során egy sérülékeny, de aláírt enclave-modul betöltésével megkerülhető az aláírás-ellenőrzés – így a támadó kód futtatása teljesen elfogadhatónak tűnik a rendszer szemében. A „Mirage" technika során pedig a **kód futtatás idejére kerül a felhasználói memóriába**, majd ott rögtön el is tűnik, minimalizálva a nyomokat és jelentősen csökkentve a detektálás esélyét. Az előadás rendkívül részletesen ismertette ezeknek a technikáknak a működési mechanizmusát, beleértve a **kernel-enclave közötti hozzáférés korlátozását**, az **enclave létrehozásának és kiürítésének folyamatait**, valamint az **ebből következő biztonsági kockázatokat**. A biztonsági védekezés szempontjából javasolt stratégiai gyakorlatok közé tartozik a **gyanús enclave-használat monitorozása**, az **enclave-folyamatok környezetének és viselkedésének felügyelete**, továbbá a **konfigurációs és biztonsági baseline-ok szigorítása** annak érdekében, hogy csak megbízható és megfelelően ellenőrzött enclave-modulok kerülhessenek be a rendszerbe. Az előadás így nemcsak a

támadási lehetőségeket mutatta be, hanem **konkrét, gyakorlatban alkalmazható védelmi javaslatokat** is nyújtott.

Az előadás az alábbi linken megtekinthető.

Ghosts in the Machine Check – Conjuring Hardware Failures for Cross-ring Privilege Escalation [DefCon33]

(Christopher "xoreaxeaxeax" Domas)

A modern számítógépes rendszerek célja a **hardverhibák észlelése és kivédése** – ennek része a **Machine Check Exception (MCE)**, amely súlyos hardveres problémák esetén – például memóriacella-hiba, CPU-hiba vagy váratlan bit-flip következtében – a rendszer biztonságos leállását idézi elő. Ez az előadás azonban azt villantotta meg, **hogyan lehet szoftveres eszközökkel elérni olyan állapotot**, amely hardverhibára emlékeztet, de nem állítja le a rendszert, viszont lehetőséget ad egy **privilegizált kódra való átállásra**. A módszer lényege a CPU belső működésének és ritka utasításainak **tudatos manipulálása**, melynek hatására a rendszer **MCE-hez hasonló állapotba kerül**, mégsem omlik össze. Ezzel a támadó **kiléphet az alkalmazói (ring 3) szintről**, és közvetlenül **kereskedhet kernel szintű (ring 0) végrehajtással**. A támadás különösen stealth, mert nem hagy a rendszer által szokásosan rögzített logokat – így a **biztonsági elemző eszközök észlelése hiányos** marad. Az előadás mély technikai magyarázatokat adott a MCE generálásának körülményeiről, a CPU viselkedésének finomságairól, valamint arról, hogyan lehet egy sérült rendszerből is privilegizált kódszekvenciába átmenni. A védekezés szempontjából a bemutató felhívta a figyelmet arra, hogy **nemcsak a szoftveres sérülékenységekre**, hanem **a hardveres állapotok és viselkedés változásaira is szükséges figyelni**. A jövőben a biztonsági monitoringnak képesnek kell lennie az ilyen **rendkívül rejtett támadási vektorok észlelésére** is – többek között a CPU anomáliák aktív felügyeletével.

From Spoofing to Tunneling: New Red Team's Networking Techniques for Initial Access and Evasion [DefCon33]

(Shu-Hao, Tung 123ojp)

A hálózati hozzáférés megszerzése és fenntartása a Red Team műveletek egyik legkritikusabb része, hiszen a védelmi mechanizmusok **elsődleges célja ezeknek a próbálkozásoknak a megakadályozása**. Ez az előadás a legújabb hálózati manipulációs módszereket mutatta be, amelyekkel a támadók **képesek kezdeti hozzáférést nyerni**, majd elkerülni a hálózati forgalom elemzésére és blokkolására hivatott rendszerek figyelmét. A bemutatott technikák között szerepelt az **IP- és DNS-spoofing**, amellyel a támadó legitim forrásnak álcázza magát, valamint olyan fejlett **tunneling** megoldások, amelyek képesek teljes kommunikációs csatornákat elrejteni látszólag ártalmatlan protokollokba csomagolva. Kiemelt figyelmet kaptak a "living off the land" jellegű módszerek, amelyek során a támadó a célkörnyezet meglévő infrastruktúráját és szolgáltatásait használja ki — például **meglévő webszolgáltatásokon keresztül továbbít adatokat vagy indít parancsokat**. A prezentáció részletesen bemutatta, miként lehet a hálózati rétegek közötti aszimmetriákat kihasználni, például hogyan használható a TCP-kezdőcsomagok időzítése és sorrendje a tűzfalak viselkedésének feltérképezésére. A védelem szempontjából különösen érdekes volt, hogy a legtöbb módszer nem az ismert aláírásokon bukik el, hanem a **forgalmi minták finom eltérésein**, amelyek csak mélyreható, valós idejű forgalomelemzéssel ismerhetők fel. Az előadás így nem csupán új támadási lehetőségeket, hanem a modern hálózati észlelés fejlesztésének irányait is megvilágította.

Mastering Apple's Endpoint Security for Advanced macOS Malware Detection [DefCon33]

(Patrick Wardle)

Az **Apple Endpoint Security (ES)** keretrendszere az egyik legerősebb, valós idejű eseményfigyelő API, amely lehetővé teszi a macOS rendszeren zajló folyamatok, fájlműveletek, hálózati kapcsolatok és más kritikus műveletek figyelését. Ez az előadás azt mutatta be, hogyan használható ki az ES API a legmodernebb macOS **malware-ek felismerésére és blokkolására** — beleértve azokat is, amelyek már **képesek megkerülni** a hagyományos antivírus megoldásokat. A részletes technikai elemzés kitért a kártékony kódok viselkedésmintáira, például az önmódosító binárisokra, a beágyazott és titkosított payloadokra, valamint a rendszerhívások szokatlan sorrendjére. Külön hangsúlyt kapott a **kernel szintű hozzáférés korlátozása**, és annak fontossága, hogy a biztonsági szoftverek a felhasználói térben is képesek legyenek **mélyen elemezni a folyamatok viselkedését**. Az előadás során bemutattak egy fejlesztői példát, amely valós időben képes a gyanús fájlmódosításokat, script-futtatásokat és hálózati kéréseket detektálni, majd automatikusan blokkolni a folyamatot. Érdekes tapasztalat volt, hogy sok macOS kártevő a telepítési folyamat során olyan **apró, de jellegzetes** eseménysorozatot generál, amely következetesen azonosítható ES-en keresztül. Ez azt sugallja, hogy a jövő macOS biztonsági megoldásai egyre inkább a **viselkedésalapú, valós idejű figyelés** felé fognak elmozdulni.

Az előadás az alábbi linken érhető el.

The Ultimate Hack: Applying Lessons Learned from the loss of TITAN to Maritime Cybersecurity [DefCon33]

(Rear Admiral John Mauger)

A TITAN tengeralattjáró tragikus elvesztése nemcsak a mélytengeri kutatás biztonságának kérdéseit vetette fel, hanem rávilágított arra is, hogy a **kritikus tengeri rendszerek** kiberbiztonsági felkészültsége sok esetben nem áll arányban a rájuk nehezedő kockázatokkal. Az előadás részletesen bemutatta, hogyan lehet a **baleset tanulságait átültetni a tengeri iparág kiberbiztonsági gyakorlatába**. A TITAN esetében a kommunikációs rendszerek megbízhatatlansága, a redundancia hiánya és a biztonsági protokollok elégtelensége hozzájárult a katasztrófához. Ezek a problémák analógiaként szolgálnak a tengeri kiberfenyegetések kezeléséhez, ahol hasonló hibák végzetes következményekkel járhatnak. A bemutató rávilágított, hogy a modern hajók és tengeralattjárók **egyre inkább szoftvervezérelt rendszerekre** és hálózatokra támaszkodnak, amelyek gyakran összeköttetésben állnak a szárazföldi irányítóközpontokkal. Ez a kapcsolódás óriási előnyöket jelent az operatív irányításban, ugyanakkor megnöveli a támadási felületet, különösen, ha a kommunikációs csatornák titkosítása vagy hitelesítése gyenge. Egy célzott kiberincidens képes lehet **megbénítani** a navigációs rendszereket, a hajtóművezérlést vagy a fedélzeti biztonsági rendszereket, hasonlóan ahhoz, ahogy a TITAN esetében a kritikus rendszerek meghibásodása vezetett a teljes működésképtelenséghez. Az előadó kiemelte, hogy a kiberbiztonságot a tengeri műveletek **minden szakaszába integrálni kell** — a tervezéstől kezdve a napi üzemeltetésen át a vészhelyzeti protokollokig. Fontos a rendszeres behatolástesztelés, a szimulált kiberincidensek gyakorlása és a redundáns biztonsági rendszerek kiépítése. A baleset tanulsága, hogy nem elég csak a műszaki meghibásodásokra felkészülni, hanem a **digitális támadások és zavarások lehetőségét is aktívan kezelni kell**. Az előadás végkövetkeztetése szerint a TITAN tragédiája egy figyelmeztető példa: a fizikai és a kiberbiztonság szoros

összefonódása miatt a jövő tengeri műveleteiben a **kiberbiztonsági védelem ugyanolyan kritikus lesz**, mint a hajótest szerkezeti integritása vagy a navigációs képességek.

Az előadás az alábbi linken érhető el.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként