NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2025. 51. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58 A2D0 E9DD E078 ABD3 E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- IT BIZTONSÁGI TIPP
- CTI JELENTÉS
- BBA+ BESZÁMOLÓ

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Manipulált PayPal „Subscriptions” levelek
(bleepingcomputer.com)

Egy új, e-mail alapú csalási kampány során a kiberbűnözők a PayPal „Subscriptions” (előfizetések) számlázási funkcióját használják ki. A támadók a PayPal nevében, hitelesnek tűnő e–maileken keresztül juttatnak el csalárd vásárlási értesítéseket a felhasználókhoz. A támadók a levélben arról értesítik a címzetteket, hogy az automatikus fizetésük megszűnt. „Your automatic payment is no longer active.” **Bővebben...**

Kártevőt terjeszt a „One Battle After Another” c. film címével visszaélő torrent
(bleepingcomputer.com)

A Bitdefender kiberbiztonsági kutatói azonosítottak egy, a One Battle After Another címével visszaélő torrentcsomagot, amely a feliratfájlba rejtett rosszindulatú PowerShell-loadereken keresztül Agent Tesla RAT-fertőzést terjeszt. **Bővebben...**

Aktívan kihasználják a GeoServer kritikus sérülékenységét
(securityweek.com)

A CISA múlt héten figyelmeztetést adott ki az OSGeo GeoServer szoftvert érintő, aktívan kihasznált sérülékenység kapcsán. A CVE-2025-58360 azonosítón nyomon követett, kritikus súlyosságú (CVSS-pontszáma: 9,8) hiba XML External Entity (XXE)-típusú sebezhetőség, amely lehetővé teheti tetszőleges fájlok elérését, szerveroldali kéréshamisítás (SSRF) végrehajtását, illetve szolgáltatásmegtagadás (DoS) előidézését. **Bővebben...**

Google hirdetésekkel terjed az új macOS infostealer
(bleepingcomputer.com)

A Kaspersky kiberbiztonsági kutatói egy új AMOS infostealer kampányt azonosítottak, amely Google keresési hirdetéseket használ arra, hogy felhasználókat navigáljon olyan, nyilvánosan megosztott ChatGPT- és Grok-beszélgetésekbe, amelyek legitimnek tűnő „hasznos” segédleteket kínálnak, valójában viszont a macOS-t érintő AMOS infostealer telepítéséhez vezetnek. **Bővebben...**

Kritikus sérülékenységekre figyelmeztet a Fortinet
(bleepingcomputer.com)

A Fortinet biztonsági frissítéseket adott ki több termékét érintő két kritikus sérülékenység javítására, melyek kihasználása lehetővé teheti a támadók számára a FortiCloud SSO-hitelesítés megkerülését. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

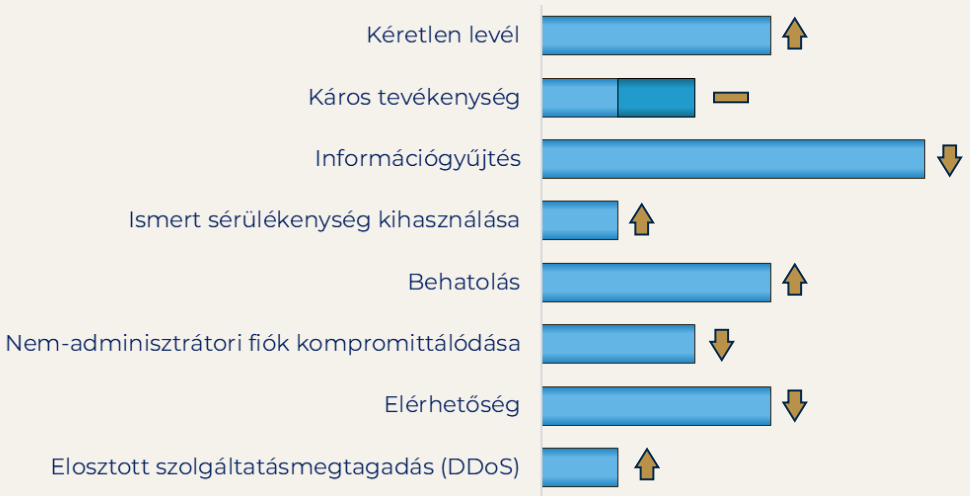
2025. 12. 12. — 2025. 12. 18.

Fenyegetettségi szint:

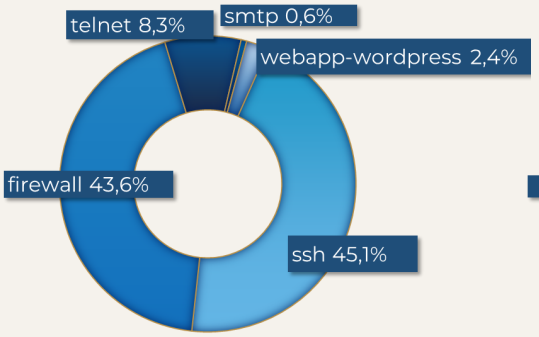
alacsony | közepes | magas | kritikus

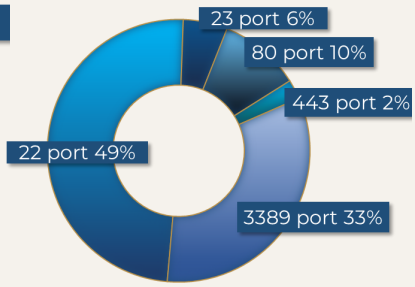
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

TIPP

Átverés az ajtónk előtt

Bár egész évben találkozhatunk a csomagos átverések különböző fajtáival, az ünnepi szezon közeledtével – amikor jelentősen megnő az internetes rendelések és a kibertámadások száma – érdemes különös óvatossággal eljárni, ha egy nem várt futár csenget be hozzánk csomaggal a kezében. Amennyiben váratlan csomagot kapunk, először érdemes körbekérdezni családunk, barátaink körében, hátha valaki meglepett minket valamivel, csak elfelejtette megemlíteni. Azonban, ha senki nem jelentkezik a csomag miatt, elképzelhető, hogy az alábbi átverések egyikével nézünk szembe.

Elolvasom

Készüljünk együtt biztonságosan az ünnepekre!

További hasznos tippekért és szórakoztató játékokért, tekintse meg az ünnepi kiadványunkat!

NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI JELENTÉS

Honeypot

Jelen dokumentum célja, hogy bemutassa a Honeypot-ok működését, ismertesse azok használatának előnyeit és kockázatait, valamint, hogy átfogó képet adjon a csapdarendszerek üzemeltetéséről és az azokból származó adatok felhasználhatóságáról. Az elemzés végén található kérdőív segítséget nyújthat abban, hogy a szervezetek felmérjék mennyire felkészültek a csapdarendszerek használatára, illetve milyen szinten érdemes elindítani azok bevezetését.

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

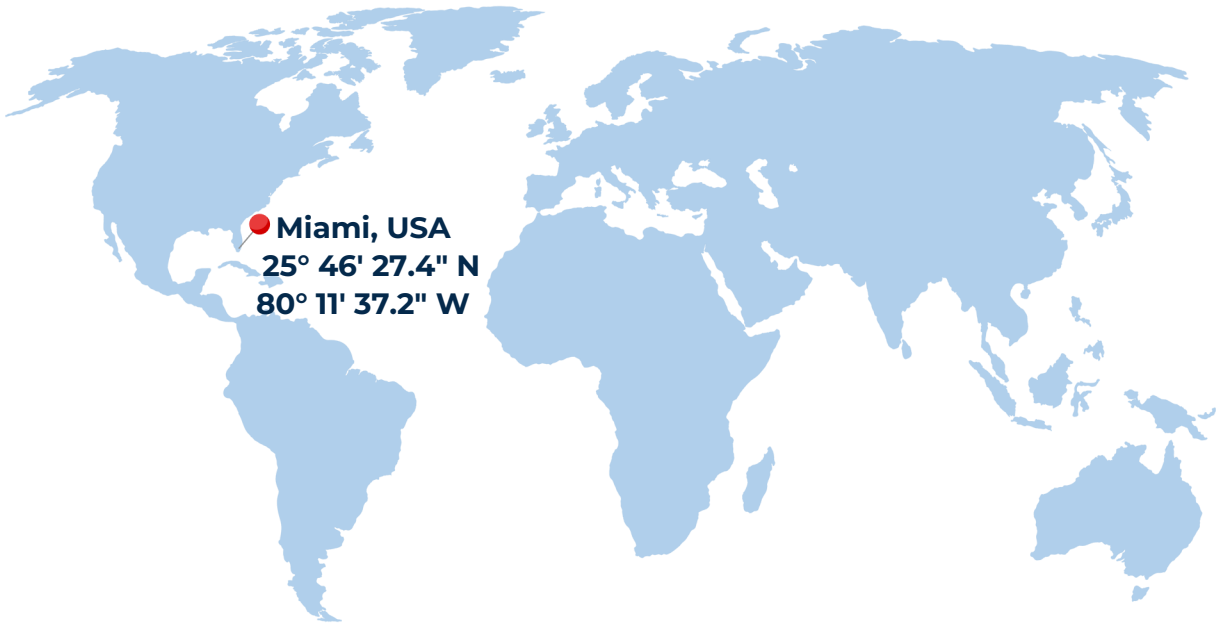
BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

EAI ICDF2C konferencia – Miami

2025. november 17-19.

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.



NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzeti Kiberbiztonsági Intézet munkatársai részt vettek a 2025. november 17-19. között Miamiban megrendezésre kerülő EAI ICDF2C konferencián. Az ICDF2C 2025 (EAI International Conference on Digital Forensics & Cyber Crime) konferenciát 2025-ben 16. alkalommal rendezték meg a Florida International University Kovens Conference Centerben. A rendezvény a digitális kriminalisztika és a kiberbűnözés területén tevékenykedő szakemberek és kutatók számára biztosít szakmai fórumot. A program középpontjában a gyakorlati forenzikus munka, a kiberbiztonság, valamint a bűnüldözés és az információbiztonság metszetében megjelenő aktuális kihívások és megoldások álltak. A konferencia célja a legújabb módszerek, eszközök és esettanulmányok bemutatása, különös tekintettel a digitális bizonyítékok kezelésére, az incidenskezelésre, illetve a hálózati és felhőalapú környezetekben végzett vizsgálatokra. Az ott bemutatott kutatási eredmények jelentős része nemzetközi kiadványokban is megjelenik, ezáltal hosszú távon is hivatkozhatóvá válik a szakmai közösség számára.

BBA-PLUSZ-312-24-2024-00003. sz. pályázat részeként

Kiknek ajánlott a beszámoló megismerése?

- Incidenskezelők számára
- Digitális elemzéssel foglalkozó szakemberek számára
- Minden kiberbiztonsági szakember számára

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

BBA+ BESZÁMOLÓ

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

Analyzing Digital Forensic Data Using Process Mining Techniques: A Case Study

Az előadás a **folyamatbányászat alkalmazását mutatta be digitális forenzikus vizsgálatok értékelésében**, különös tekintettel a hatékonysági hiányosságok és a szűk keresztmetszetek azonosítására. A kutatás célja, hogy a rendezetlen, nem formalizált vizsgálati lépéseket mérhető, elemezhető folyamatmodellekké alakítsa, mégpedig úgy, hogy a jelentésekből előállított, strukturált NCS eseménynaplókat folyamatbányászati módszerekkel elemzi. A vizsgálat olyan technikákat alkalmaz, mint a **„directly follows graph" (DFG) és a Petri-hálók**, amelyek segítségével a teljes forenzikus vizsgálati folyamat rekonstruálható és elemezhető. Ezek az eszközök átláthatóvá teszik a munkafolyamatokat, és támogatják a fejlesztendő pontok beazonosítását. A kutatás valós vizsgálati jelentések adatain alapul; az adatok rendezetlenségéből adódó kihívások kezelésére **természetesnyelv-feldolgozási (NLP) eljárásokat alkalmaz**, többek között adatnormalizálást, entitáskinyerést és témamodellezést az eseménynaplók előállítása érdekében.

A folyamatbányászati módszerek makro- és mikroszintű áttekintést egyaránt biztosítanak. A **DFG-k** az **események gyakoriságát és sorrendiségét** mutatják meg, míg a **Petri-hálók** a **párhuzamos végrehajtást és a függőségi viszonyokat** tárják fel, ezáltal rávilágítva az esetleges hatékonysági hiányokra és erőforrás-átfedésekre. Az esettanulmány elemzése ismétlődő helyszíndokumentációs ciklusokat és beágyazott bizonyítékgyűjtési lépéseket azonosított, amelyek potenciális hatékonysági problémákra és standardizálási hiányosságokra utalnak. Az eredmények két fő következtetést emelnek ki. Egyrészt **csökkenthetők a redundáns dokumentációs lépések** és **javítható a bizonyítékgyűjtés sorrendje és priorizálása**. Másrészt a szervezetek a **folyamatmodelleket a munkafolyamatok standardizálására és folyamatos fejlesztésére** használhatják. A kutatás végkövetkeztetése szerint a folyamatbányászat **hatékony**

eszköz a forenzikus vizsgálatok rejtett hatékonysági problémáinak feltárására, és indokolt a módszer kiterjesztése nagyobb esetszámú adathalmazokra, valamint az adat-előfeldolgozás további automatizálása.

Resilient Satellite Cybersecurity: Integrating NIST and AI Governance

Az előadás egy olyan kutatást mutatott be, amely a **műholdrendszerek kiberbiztonságának és irányítási keretrendszerének megerősítésére törekszik a különböző NIST-modellek összehangolásával.** Kiindulópontja a műholdak számának drasztikus növekedése és a kibertámadások gyors fejlődése, amelyek sürgetővé teszik egy egységes, több szereplőt integráló védelmi megközelítés kialakítását. A Viasat KA-SAT hálózat 2022-es kompromittálása, valamint Ukrajna Starlink-függősége az orosz–ukrán konfliktusban jól érzékeltették, **mennyire sérülékeny a polgári és katonai infrastruktúrák műholdas komponense**. Részletesen ismertette, hogy a régebbi **műholdakban alkalmazott titkosítási megoldások ma már nem nyújtanak megfelelő védelmet** a hamisítási, zavarási és behatolási technikákkal szemben, különösen az egyre fejlettebb AI-alapú támadások fényében. Ehhez társul a földi állomások informatikai sérülékenysége, valamint a felhőalapú szolgáltatások kockázatainak növekedése. A műholdas ökoszisztémát tovább gyengíti, hogy a magán- és állami szolgáltatók saját, egymással nem kompatibilis protokollokat alkalmaznak, ami széttagolt működéshez, átláthatatlan adatáramláshoz és hiányos biztonsági felügyelethez vezet. Az **irányítási és szabályozási struktúrák pedig nehezen tartják a lépést** a technológiai fejlődéssel, és nem biztosítanak kellően összehangolt együttműködési keretet a civil, állami és katonai szereplők számára. A javasolt megközelítés egy **többrétegű védelmi modell**, amely a NIST Cybersecurity Framework és az AI Risk Management Framework elemeit integrálja.

BBA-PLUSZ-312-24-2024-00003. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

A koncepció célja a műholdas eszközök kockázatainak átfogó feltérképezése, a titkosítási és hozzáférés-kezelési megoldások korszerűsítése, a mesterséges intelligenciával támogatott valós idejű anomáliaészlelés bevezetése, valamint az incidenskezelés és helyreállítás összehangolt folyamatrendjeinek kialakítása. Az előadás hangsúlyozta, hogy **tartósan hatékony védelmet** csak akkor lehet elérni, ha a **kereskedelmi szolgáltatók, az állami szervek és a védelmi szervezetek egységesen meghatározott protokollok és közös eljárásrend alapján működnek együtt.**

A bemutatott esettanulmányok rámutattak a firmware-sérülékenységek, a végpontvédelmi biztonsági hiányosságok és a hiányos irányítási kontroll jelentős kockázataira. A kutatás fő következtetése szerint **a műholdas rendszerek ellenállóképessége csak előrelátó, egységes irányítási struktúrával biztosítható**, amely közös szakpolitikai alapokra, szabványosított protokollokra és összehangolt védelmi eljárásokra épül. Egy ilyen keretrendszer képes mérsékelni a jövőbeli válsághelyzetek kockázatát, és hosszú távon is hozzájárul a modern, műholdfüggő infrastruktúrák biztonságos működéséhez.

iOS Cookie Forensics with Autopsy Tool

Az előadás az Autopsy digitális forenzikus eszköz számára fejlesztett **cookie-elemző modul** tervezését és megvalósítását mutatta be. A projekt kiindulópontja az volt, hogy az Autopsy aktuális verziója nem rendelkezett olyan funkcióval, amely képes lett volna a cookie-fájlok értelmezésére. Ennek áthidalására először egy olyan **script készült, amely a cookie-fájlokat és a belőlük kinyerhető forenzikus adatokat tudta feldolgozni**, ezt követően pedig **NetBeans környezetben egy teljes értékű cookie-parser modul** került kifejlesztésre. A forenzikus vizsgálathoz használt adatkészlet egy, a NIHT által publikált datasetből származott, a cookie-fájlok azonosítása pedig MIME-típus és hexadecimális aláírás alapján történt.

A modul kialakításának kulcslépése volt a **cookie-fájlok struktúrájának visszafejtése**, valamint a vizsgálat szempontjából releváns adatok kinyerése, ideértve többek között az oldalszámokat, oldalméreteket és fejléceket. A fejlesztés célja az volt, hogy a modul zökkenőmentesen integrálható legyen az Autopsy rendszerébe, ennek érdekében .npm fájl készült, amely lehetővé teszi a cookie-fájlok parse-olását, és a kinyert információk részletes megjelenítését a Data Content Viewer felületén. A modul olyan adatokat tesz könnyen elérhetővé a vizsgálók számára, mint a cookie útvonala, neve, értéke, URL-je, lejárati ideje és létrehozási dátuma. A jövőbeni fejlesztési irányok között szerepel a modul **bővítése további IIS-alapú böngészők** támogatásával, különféle adatkészletek bevonása a robusztusság növelése érdekében, valamint **gépi tanulási technikák integrálása** a cookie-adatok hatékonyabb kategorizálására és priorizálására.

Online Learning for Android Malware Detection under Concept-Drift

A prezentáció az **Android-alapú kártevők gépi tanulással támogatott detektálásának egy új megközelítését ismertette**. Az Android operációs rendszer piaci dominanciája, valamint a kártevők egyre kifinomultabb támadási technikái miatt a hagyományos, aláírásalapú felismerési módszerek sok esetben már nem bizonyulnak elegendőnek, mivel nem képesek lépést tartani a gyorsan változó malware-taktikákkal. A kutatás erre válaszul egy **window-based online retraining stratégiát** alkalmazott a **Corridorics adatkészlet felhasználásával**, amely statikus és dinamikus jellemzőket egyaránt tartalmaz. Ez a megközelítés lehetővé teszi a concept drift, vagyis a **viselkedésminták időbeli eltolódásának kezelését**. A concept drift azt a jelenséget írja le, amikor a kártevők viselkedése, szerkezete vagy működési logikája idővel megváltozik, így a korábban megtanult mintázatok fokozatosan érvényüket vesztik. Mivel a támadók folyamatosan új technikákat és elrejtési módszereket vezetnek be, a régebbi modellek egyre kevésbé képesek

BBA-PLUSZ-312-24-2024-00003. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

felismerni az új fenyegetéseket. Ez indokolja, hogy a **gépi tanulási rendszerek ne statikus, egyszer betanított modellekre, hanem folyamatosan frissülő, adaptív megoldásokra épüljenek**. A vizsgálati módszertan része volt az adatok előfeldolgozása, az alapszintű modellek kiválasztása, valamint egy olyan online tanulási keretrendszer kialakítása, amely a beérkező új adatok alapján fokozatosan újratanulja a kártevők jellemzőit. Az így kialakított, ablakalapú újratanulási megközelítés érdemben növeli az Android-platformot célzó kártevők felismerésének hatékonyságát, különösen olyan környezetekben, ahol a fenyegetések gyorsan és kiszámíthatatlanul változnak.

Validation of IP Reputations Through Redirection of Unsolicited Network Traffic to an Interactive Honeynet

Az előadás egy olyan kutatási projektet mutatott be, amely az **IP-címek reputációjának hitelesítésére fókuszált,** úgy, hogy a **nem várt, kéretlen hálózati forgalmat egy interaktív honeynet-rendszerbe irányította át.** A kiindulópont az volt, hogy a különböző kereskedelmi és nyílt forrású kiberfenyegetettségi hírszerzési (CTI) szolgáltatók által megadott IP-reputációk gyakran csak részben tükrözik a tényleges viselkedést. A kutatás célja ennek megfelelően az volt, hogy a kéretlen forgalom valós aktivitásának megfigyelésével pontosabban meghatározható legyen, mely IP-címek feleltethetők meg rosszindulatú mintázatoknak, és mely esetekben indokolt a reputáció módosítása. A vizsgálat során a kutatók egy T-Pot honeynetet állítottak fel az Amazon Web Services környezetében. A hálózati architektúra központi eleme egy olyan tűzfal -konfiguráció volt, amely alapértelmezett „deny-all” szabállyal minden nem várt bejövő forgalmat blokkolt, ugyanakkor ezt a forgalmat párhuzamosan át is irányította a honeynetbe további megfigyelésre. Két adathalmaz készült: egy 13 napos, Zeek-alapú kiinduló adatgyűjtés összehasonlítási alapként, valamint egy 31 napos dataset, amely kizárólag az átirányított

forgalomból származott. A két adatforrás együttes elemzése tette lehetővé a **kéretlen forgalom részletes, viselkedésalapú vizsgálatát.** Az eredmények azt mutatták, hogy az IP-címek viselkedése alapján jól körülhatárolható mintázatok rajzolódnak ki, amelyek alkalmasak a reputációk finomítására. Négy, erős indikátornak tekinthető viselkedési jellegzetességet azonosítottak:

1. nulla bájt hosszúságú szállítási payloadok,
2. TCP reset flag gyakori jelenléte,
3. túlzott mértékű portscan-tevékenység,
4. a kapcsolatok számának feltűnő, szokatlan ingadozása.

Ezek a mintázatok megbízhatóan elkülönítették a rosszindulatú szereplőket a háttérforgalomtól, és számos esetben ellentmondtak a CTI-szolgáltatók eredeti címkézésének. A vizsgálat kimutatta, hogy több olyan IP-cím, amelyet a szolgáltatók „benign” vagy „gray” kategóriába soroltak, valójában felderítő, portscan vagy egyéb gyanús tevékenységet folytatott. Ez rámutat arra, hogy a **CTI-adatbázisok sok esetben statikusak vagy késleltetve frissülnek**, míg a **honeynet-alapú, viselkedéscentrikus megközelítés jóval dinamikusabb és közelebb áll a valós idejű helyzetképhez.** A kutatás hangsúlyozta, hogy a honeynet-rendszer nemcsak a rosszindulatú tevékenységek felismerését támogatja, hanem az IP-reputációk érdemi pontosítását is, ami növeli a védelmi rendszerek megbízhatóságát, és csökkenti a téves pozitív és téves negatív találatok arányát különösen magas biztonsági követelményű környezetekben. A bemutatott eredmények egy jövőbeli, együttműködésen alapuló, több hálózatot lefedő honeynet-hálózat lehetőségét vetítik előre. Egy ilyen, megosztott infrastruktúra nagy mennyiségű, aggregált viselkedési adatot gyűjthetne, amely **alkalmas lenne a feltörekvő támadási trendek, új technikák és akár zero-day típusú fenyegetések korai azonosítására.**

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

A kutatás ugyanakkor rámutatott a széles körű forgalom-átirányítás erőforrás-igényére és teljesítménybeli hatásaira is, miközben kiemelte, hogy egy ilyen rendszer **érdemben hozzájárulhat a szervezetek kiberellenálló képességének növeléséhez és a viselkedésalapú IP-reputációk kialakításához.**

Toward Structured Memory Forensics: A MITRE ATT&CK-Aligned Workflow for Malware Investigation

Az előadás a **memóriaforenzika területének fejlesztésére összpontosított**, ezen belül a **kártevővizsgálatokhoz kapcsolódó módszertani kérdésekre**. A kutatás fő célja egy **formalizált, sztenderdizált, öt fázisból álló vizsgálati módszertan** kidolgozása volt, amely szorosan igazodik a **MITRE ATT&CK keretrendszerhez**, és ezáltal megbízhatóbbá, valamint reprodukálhatóbbá teszi a memóriaforenzikai elemzéseket. Az előadás részletesen ismertette a jelenlegi gyakorlat hiányosságait. A memóriaelemzésben ma használt eljárások sok esetben ad hoc jellegűek, nem támaszkodnak egységes módszertanra, és korlátozottan ismételhetők. Technikai kihívást jelent többek között a lapozás és visszalapozás összetettsége, a RAM és a háttértár között megoszló bizonyítéktöredékek kezelése, valamint a memória- és lemezképek közötti eltérések, amelyek különféle bináris transzformációk eredményeként jönnek létre. A javasolt ötfázisú munkafolyamat olyan lépéseket tartalmaz, mint a bizonyíték integritásának biztosítása, a nyers adatok elemzése, fájlok kinyerése, az illékony adatok vizsgálata, valamint a bináris elemzés. Az előadás bemutatta az alkalmazott eszközöket és technikákat is, többek között az entrópiaelemzést, a YaraScan és MalFind használatát, valamint különböző Volatility plugineket, amelyek az indikátorok azonosítását és az ellenfél jelenlétének feltárását szolgálják. A prezentáció kitért arra, hogy a terület érdemi előrelépéséhez szükség van **benchmarkokra, valós és szintetikus adatkészletek gyűjtésére**, valamint olyan eszközök kialakítására, amelyek

alkalmasak az **új módszertan tesztelésére és alkalmazására**. A kutatócsoport már együttműködést kezdett spanyol bűnüldöző szervezetekkel, hogy a módszert valós incidenstöredékeken is értékeljék. Összegzésként az előadó hangsúlyozta, hogy a **memóriaforenzika fejlődése nem képzelhető el sztenderdizált, átlátható és igazolható módszertanok nélkül.** A további kutatási irányok között szerepel benchmarkok kidolgozása, valamint modern kártevőket tartalmazó memóriadumpokat magukban foglaló, nyilvános adatkészletek létrehozása, amelyek lehetővé teszik a javasolt módszertan további finomítását és validálását.

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként