NEMZETI KIBERVÉDELMI INTÉZET

# HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 35. hét

## HÍREK

- Kritikus Chrome sebezhetőségek veszélyeztetik a felhasználókat és vállalatokat
- PromptLock: az első zsarolóvírus, amely mesterséges intelligenciát használ a támadó kód generálására
- Súlyos Citrix sebezhetőség fenyeget több mint 28 000 rendszert világszerte
- Google Classroom visszaélések: Több mint százezer adathalász e-mail egy hét alatt
- SpyNote újratöltve: Hamis Google Play weboldalakkal támadják az Android-felhasználókat

## STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

## BESZÁMOLÓ

- SANS DFIR Summit 2025 – Salt Lake City - konferencia

## KONTAKT

**edt@nki.gov.hu**

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

További hírekért, látogasson el **weboldalunkra**!

# NEWS

IT biztonsági
# HÍREK

## Kritikus Chrome sebezhetőségek veszélyeztetik a felhasználókat és vállalatokat

**(ghackers.com 1, 2)**

A Google két súlyos biztonsági rést javított nemrégiben a Chrome böngészőben, amelyek közül az egyik már aktív kihasználás alatt áll. **Bővebben...**

## PromptLock: az első zsarolóvírus, amely mesterséges intelligenciát használ a támadó kód generálására

**(gbhackers.com)**

Az ESET Research kutatócsapata egy új típusú zsarolóvírust, a PromptLock nevű kártevőt azonosította, amely egyedülálló módon helyben futó nagy nyelvi modellt (LLM) alkalmaz a támadó kód valós idejű generálására az áldozat gépén. **Bővebben...**

## Súlyos Citrix sebezhetőség fenyeget több mint 28 000 rendszert világszerte

**(gbhackers.com)**

Egy rendkívül kritikus, nulladik napi távoli kódfuttatási (RCE) sérülékenység veszélyezteti több mint 28 000 Citrix rendszer biztonságát globálisan. A hibát a CVE-2025-7775 azonosító alatt regisztrálták, és jelenleg aktív kihasználás alatt áll, sürgős intézkedéseket követelve minden érintett szervezet részéről. **Bővebben...**

## Google Classroom visszaélések: Több mint százezer adathalász e-mail egy hét alatt

**(gbhackers.com)**

A Check Point biztonsági kutatói egy nagyszabású adathalász kampányt tártak fel, amely során a kiberbűnözők a népszerű oktatási platformot, a Google Classroomot használták ki rosszindulatú célokra. **Bővebben...**

## SpyNote újratöltve: Hamis Google Play weboldalakkal támadják az Android-felhasználókat

**(gbhackers.com)**

2025 augusztusában a kiberbiztonsági kutatók újabb SpyNote malware kampányra lettek figyelmesek, amely az Android-felhasználókat célozza meg. A támadás különösen megtévesztő, mivel a támadók professzionálisan felépített, hamis Google Play Áruház oldalakat használnak, hogy népszerű alkalmazásokat utánzó fertőzött APK-fájlokat terjesszenek. **Bővebben...**

# Statisztikai Adatok

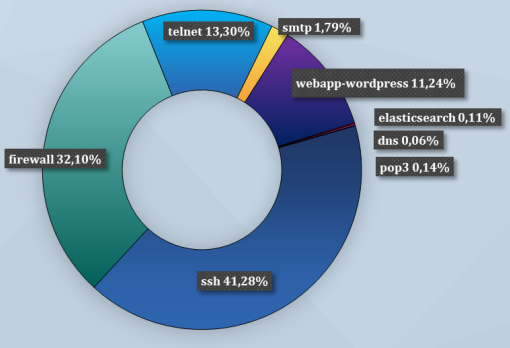
2025.08.22.-2025.08.28.

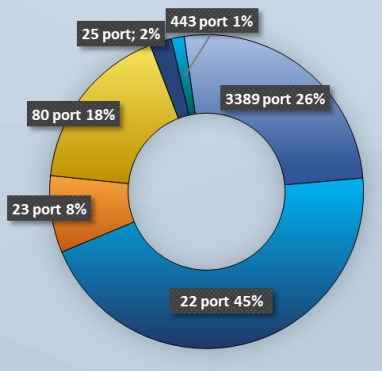
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony


Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:




További érdekességekért, látogasson el **weboldalunkra**!

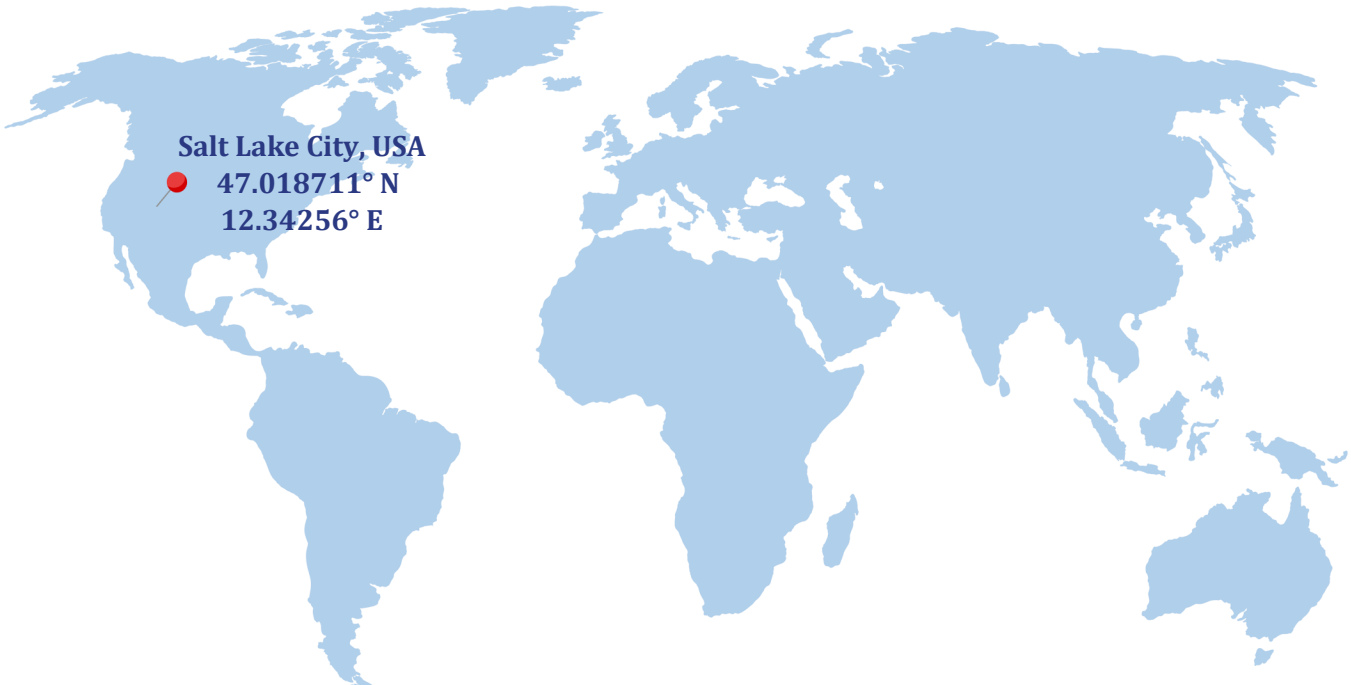
BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

# SANS DFIR Summit 2025 – Salt Lake City - konferencia

**2025. július 24-25.**

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi 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.




Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

A Nemzeti Kibervédelmi Intézet munkatársai részt vettek a **2025. július 24-25.** között Salt Lake City-ben megrendezésre kerülő éves **SANS DFIR Summit 2025 konferencián**. A SANS Institute a világ egyik **legismertebb és legelismertebb kiberbiztonsági oktatási és tanúsítványt nyújtó szervezete.** Célja, hogy releváns és naprakész tudást adjon át hallgatóinak, melyet közvetlenül alkalmazhatnak a való életben a kibertér védelme érdekében – legyen szó szervezetek eszközeinek, adatainak vagy emberek biztonságáról. A SANS oktatásait, azok gyakorlati szemlélete, a szervezet tapasztalt oktatói és az iparági sztenderddé vált GIAC tanúsítványai teszik különösen értékessé a szakemberek számára világszerte.

A SANS DFIR Summit a SANS egyik kiemelt éves eseménye, amely a **digitális elemzés (DF – Digital Forensics) és az incidensreagálás (IR – Incident Response) területére fókuszál.** A rendezvény célja, hogy gyakorlatorientált előadásokon és tréningeken keresztül mutassa be a legújabb technikákat, esettanulmányokat és eszközöket. A DFIR Summit lehetőséget ad a közösségépítésre is, mivel összehozza a világ vezető szakértőit, kutatóit és gyakorlati szakembereit, akik megosztják tapasztalataikat és tudásukat.

## Kiknek ajánlott a beszámoló megismerése?

- Incidenskezelők számára
- Digitális elemzéssel foglalkozó szakemberek számára
- Kiberbiztonsági szakemberek számára

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

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

# Tedd mesterséges intelligenciával hatékonyabbá a DFIR munkafolyamataidat / DFIR AI-ze Your Workflow

*(Mari DeGrazia — Certified Instructor @ SANS Institute)*

Az előadás egy technológiailag és szakmailag is előremutató szemléletváltást mutatott be a **digitális nyomelemzés területén alkalmazható mesterséges intelligencia (MI) eszközökkel** kapcsolatban. Mari saját gyakorlati tapasztalatai alapján ismertette, hogyan képes az MI hatékonyabbá és biztonságosabbá tenni a mindennapi digitális elemzői feladatokat – például eseménynaplók feldolgozását, JSON-fájlok értelmezését vagy nyelvi fordításokat.

Először ChatGPT-t használt, majd költséghatékonysági és adatvédelmi okokból áttért a **helyben futó modellekre** (pl. Ollama és Open Web UI). Ezek lehetővé teszik a **bizalmas adatok külső szolgáltatók felé történő megosztása nélküli** munkavégzést, ami jelentős előrelépés az adatvédelem terén. Emellett lehetőséget nyújtanak **saját MI-eszközök és dedikált elemzői botok fejlesztésére**, például API-lekérdezések, hálózati naplók értelmezése vagy IOC-k automatizált felismerése céljából.

Az MI-t különféle célokra kezdte használni, például:

- ShimCache elemzés gyanús folyamatok azonosítására,
- SMS-ek és egyéb üzenetek fordítása spanyolról angolra,
- Eseménynaplók automatikus elemzése és kiértékelése.

Fontos problémaként említette az **MI „hallucinációs” hajlamát** – például, hogy azonos bemenetekre különböző időbélyegeket adott vissza –, és hangsúlyozta a **"trust but verify" („bízz, de ellenőrizz”) elvet**. Megmutatta, hogyan lehet eszközöket (pl. IP-cím validálása, geolokációs elemzés, abuseDB-ellenőrzés) integrálni az LLM-ek mögé, így a modellek pontosabb, reprodukálható eredményeket adhatnak. Külön hangsúlyt kapott a Modular Capabilities Platform (MCP) koncepciója, amely lehetővé teszi,hogy különböző elemzői eszközök (pl. Velociraptor) mögé LLM-alapú döntési logika kapcsolódjon.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

Demózott egy Pythonban írt ügynökrendszert is, amely képes volt:

- Base64 dekódolást,
- Gzip tömörítés kibontását,
- IP-címek elemzését végezni,
- és ezekből automatikus következtetéseket levonni.

Bemutatta a **Vanna AI nevű rendszert**, amely **SQL lekérdezéseket generál természetes nyelvi kérdésekből** – ez lehetővé teszi, hogy hatékonyan és gyorsan dolgozzunk nagy adatmennyiségeken, például eseménynaplókon.

Az előadás végén Mari bemutatott egy **saját fejlesztés alatt álló, MI-vel vezérelt vizsgálati rendszert**, amely képes üzleti e-mail kompromittálódás esetén önállóan elvégezni egy teljes elemzési folyamatot: bejelentkezések vizsgálatától kezdve a gyanús IP-címek azonosításán, e-mail fiók szabályokon keresztül a végső jelentés elkészítéséig.

Az előadásról készült videó az alábbi linken érhető el.

## Észak-koreai kiberművelet: rejtett C2-csatornák, WebSocket-alapú vezérlés és videókonferencia-eszközökkel való visszaélés / A North Korean Cyber Operation: Exposing ARP-Based Convert C2s, WebSocket Malware, and Video Conference Software Abuse

*(Matthew Mosley, Luis Garcia — ncident Respond @ Sygnia)*

A Sygnia incidensreagáló csapatának előadása egy FBI által lefoglalt laptopfarm kapcsán feltárt, **Észak-Koreához köthető kiberművelet digitális nyomelemzését** mutatta be. Az eset különlegességét az adta, hogy a kompromittált eszközökön nem hagyományos malware-tevékenységet találtak, hanem **Python-alapú, célzott észlelés-elkerülő szkriptekből álló arzenált**. Ezek WebSocket protokollt, ARP-csomagokat és a Zoom videókonferencia-alkalmazást használták a C2-funkciók megvalósítására.

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

**A támadás során:**

- a támadók legitim IT-szolgáltatói pozíciókba jutottak be,
- az általuk vezérelt laptopfarmról rejtett C2-csatornát építettek ki,
- egy szkript WebSocketen keresztül fogadott parancsokat,
- egy másik ezekből ARP-pakkokat generált, amelyeket a lokális hálózaton (pl. Wi-Fi interfészen) továbbított,
- a célgépeken egy másik szkript dekódolta az ARP-pakkokból a parancsokat és szimulált inputokat hajtott végre (pl. egérmozgás),
- egy harmadik modul a Zoomot teljesen automatizálva indította el, létrehozta a hívást, majd elfogadta a távoli vezérlésre irányuló kérést (pl. RGB-szűrőkkel detektálva az „admit” gombot).

A támadók célja a **„működő gép látszatának” fenntartása** volt, hogy valós munkavégzés illúzióját keltsék, miközben **távoli irányítást gyakoroltak a rendszerek felett**. A demókon bemutatott megoldások képesek voltak az utasításokat egymás között broadcastolni, így decentralizált C2-működést valósítva meg.

**Az elemzés főbb tanulságai:**

- a WebSocket-forgalom monitorozása kiemelt prioritás,
- a pyinput, scapy és más szkript-alapú inputszimulátor könyvtárak jelenléte gyanús lehet,
- a Zero Trust alapú onboarding során nem elegendő a HR-ellenőrzés – technikai felügyelet már a munkakezdéstől szükséges.

Az előadásról készült videó az alábbi linken érhető el.

# Forgatókönyvek felturbózva: Moduláris tervezés alkalmazása incidenskezelési forgatókönyvek skálázható fenntartásához / Playbook Power-Up: Applying Modular Design to Maintain IR Playbooks at Scale

*(Jessica Gorman — Security Director of Security Operations and Incident Response @ Experian)*

Jessica Gorman a Georgetown Egyetemen végzett kiberkockázat-menedzsment mesterszakos kutatása alapján mutatta be, hogyan lehet **az incidenskezelési forgatókönyvek moduláris szemlélettel kezelhetőbbé, könnyen frissíthetővé tenni.** Rámutatott, hogy ezek a dokumentumok – amelyek lépésről lépésre szabályozzák a SOC-csapat reakcióját a különféle fenyegetésekre – kritikusak a gyors reagáláshoz és a megfelelőségi előírások teljesítéséhez, mégis sokszor nem naprakészek: egy felmérés szerint ugyan a biztonsági szakemberek 70%-a használ playbookokat, 52%-uk ritkán frissíti őket.

Saját tapasztalatai szerint az **erőforráshiány, a szervezeti és technológiai változások** – például amikor a cégét felvásárolta egy befektetési alap, és minden eszköz, csapatstruktúra átalakult – gyorsan **elavulttá teszik a meglévő forgatókönyveket.** A hagyományosan szöveges vagy folyamatábrás playbook-halmazt (akár több tucatot) ilyenkor külön-külön kellene átírni, ami rengeteg manuális munkát igényel, miközben a fenyegetési környezet folyamatosan változik, az AI-alapú automatizálás pedig ma még csak korlátozottan segít ezen a területen.

Megoldásként Gorman **„modularizált forgatókönyv-tervezési keretrendszert”** javasol. A kiindulópont egy **mester-sablon**, amelyből **újrahasznosítható al-playbookok** (modulok) ágaznak le. Elkülönítik a minden forgatókönyvben közös, a többivel kombinálható és az egyedileg egy-egy fenyegetésre jellemző lépéseket. Így amennyiben változik egy értesítési folyamat vagy egy elemzőeszköz, elég a modult módosítani, az új verzió automatikusan megjelenik minden érintett playbookban.

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

Kutatása szerint ezzel a módszerrel a frissítések alkalmazási ideje átlagosan 56%-kal csökkent, a szervezetek pedig **20–40% teljes időmegtakarításról** számoltak be, miközben a **feldolgozható riasztások száma nőtt** anélkül, hogy több elemzőt kellett volna felvenni. A modularizálás SOAR nélkül, akár egyszerű tudásbázisokban is működhet, és a playbookokon túl bármilyen folyamatmenedzsment-területen nőhet a hatékonyság.

Az előadásról készült videó az alábbi linken érhető el.

## Kiskapuk és nyomok: így maradnak jelen a támadók a Microsoft 365 környezetedben / Backdoors and Breadcrumbs: How Threat Actors Persist in Your Microsoft 365

*(Federico Sidolini — DFIR Senior Consulant @ Stroz Friedberg)*

Federico Sidolini, digitális igazságügyi és IR szakértő, részletesen bemutatta, **hogyan képesek fenntartani jelenlétüket a támadók egy kompromittált Microsoft 365 környezetben** – még azután is, hogy a jelszavakat és a többtényezős hitelesítést (MFA) újra beállították. Előadása során több technikát és azok vizsgálati módszereit ismertette, valamint javaslatokat adott a védekezéshez.

A leggyakoribb technikák közé tartoztak a **beérkező levelekhez rendelt szabályok** (inbox rules), amelyek lehetővé tették az e-mailek automatikus áthelyezését vagy továbbítását külső címekre – gyakran rejtett mappákba. Ezáltal a támadók akkor is olvashatták a leveleket, amikor már nem volt aktív fiókhozzáférésük. Federico hangsúlyozta, hogy ezt a technikát szinte minden üzleti e-mail kompromittálás során alkalmazzák.

Ezután bemutatta az **alkalmazásjelszavak** (application passwords) **veszélyét,** amelyek a régi, MFA-t nem támogató alkalmazásokhoz lettek tervezve. Bár alapértelmezetten ki vannak kapcsolva, ha engedélyezve vannak, a felhasználók akár 40 különféle alkalmazásjelszót is létrehozhatnak. A probléma az, hogy az **adminisztrátorok nem látják, milyen alkalmazásjelszavak léteznek** – csak törölni tudják őket. Egy konkrét eset példáján keresztül mutatta be, hogyan maradt aktív a támadó még a jelszó és MFA újraállítása után is – mivel alkalmazásjelszót használt, amit nem távolítottak el.

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

A következő technika a **jelszó önkiszolgáló visszaállítási lehetőség** (SSPR) kihasználása volt. A támadó egy új MFA-eszközt regisztrált a fiókhoz, és az SSPR segítségével új jelszót állított be magának. Mivel az SSPR alapértelmezés szerint csak egy hitelesítési módszert kér, ez elég volt a visszatéréshez. Federico javasolta, hogy **legalább két MFA-módszer megkövetelése jelentősen csökkenti az ilyen visszaélések kockázatát**.

Haladóbb támadói technika a **bejegyzett alkalmazások** (app registrations) és az azokhoz kapcsolódó **service principal objektumok manipulálása**. Ezek lehetőséget adnak a támadónak arra, hogy háttéralkalmazásként, hitelesített módon férjen hozzá a teljes levelezéshez és más adatokhoz – például a Microsoft Graph API-n keresztül. Federico bemutatta, hogyan lehet titkos kulcsokat (secrets) és tanúsítványokat (certificates) hozzáadni ezekhez a service principal entitásokhoz, amelyek az adminfelületen nem láthatók, csak PowerShell-ből érhetők el. Ez komoly kihívást jelent a **forenzikus vizsgálatok** során, mivel könnyen észrevétlen maradhat.

Ezután a **domainfederációs támadásokat** ismertette, ahol a támadó saját identitásszolgáltatót regisztrál a target tenantba , vagy meglévő domainhez ad hozzá új tanúsítványokat. Így lehetőség nyílik **SAML tokenek generálására bármelyik felhasználó nevében, jelszó vagy MFA megkerülésével**. Bár ez a technika magas jogosultságot igényel (pl. globális admin), Federico hangsúlyozta, hogy **érdemes figyelni a tanúsítványváltozásokat és új federációs kapcsolatok megjelenését**, mert ezek rendkívül ritkák – így jól detektálhatók.

Végül szó esett egy egyre gyakoribb jelenségről, amikor a támadók **külső szolgáltatásokhoz** (pl. Dropbox, FileShare) **regisztrálnak fiókokat a megszerzett céges e-mail címekkel**, és ezeket később **adathalászatra használják** – még akkor is, amikor a belső hozzáférés már megszűnt. Ezt rendkívül nehéz megelőzni, de a vizsgálatok során figyelni kell a bejövő e-mailek között az automatikus regisztrációs visszaigazolásokra.

Federico előadását azzal zárta, hogy a hatékony védekezéshez szükséges a **beállítások rendszeres felülvizsgálata**, a **magas jogosultságú fiókok korlátozása**, valamint az **átfogó audit- és naplóelemzés** bevezetése. *Az előadásról készült videó az alábbi linken érhető el.*

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

# macOS Endpoint Security Framework: Nem csak egy újabb naplóforrás / macOS Endpoint Security Framework: Not Another macOS Log Source

*(Jacob Latonis — Staff Software Engineer @ Proofpoint, Julia Paluch — Engineer @ GreyNoise Intelligence)*

Ez az előadás a **macOS Endpoint Security (ES) Framework nyomkövetési képességeit mutatta be digitális nyomelemzési szemszögből.** Az ESF lehetővé teszi, hogy kernel szintű beavatkozás nélkül figyeljük a rendszerfolyamatokat, fájlműveleteket, hálózati kapcsolódásokat és egyéb végponti aktivitásokat.

A bemutatott vizsgálatok kiemelték, hogy:

- a macOS ES Framework – különösen az eslogger – részletgazdag eseményadatokat biztosít, amelyek jól kombinálhatók például a Unified Log vagy az FSEvents adataival,
- új elemzési lehetőségek nyíltak meg a mac apt, a KAPE macOS-moduljai, valamint a mac4n6 eszköztár segítségével,
- a kutatók saját MITRE ATT&CK mappinget készítettek a macOS-specifikus TTP-kre az ES Framework által gyűjtött események alapján,
- bemutatásra került egy esettanulmány is, amelyben egy adathalász Word-dokumentum PowerShell payloadját az ESF segítségével sikerült nyomon követni – beleértve a gyermekfolyamat -fát (child process tree) és a hálózati kapcsolódásokat is.

A legfontosabb tanulság: a **korábban „fehér foltként" kezelt macOS mára teljes értékű**, megbízható nyomkövetési képességekkel rendelkezik. Az ES Framework lehetővé teszi olyan szofisztikált támadások észrevétlen nyomon követését is, amelyek korábban a hagyományos macOS-naplók alapján nem voltak rekonstruálhatók.

Az előadásról készült videó az alábbi linken érhető el.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

## Workshop | Nem is olyan privát böngészés! / Not So Private Browsing!

*( Mattia Epifani — Certified Instructor @ SANS Institute)*

Az előadó egy gyakorlatorientált workshopban azt mutatta be, hogy a **„privát"/inkognitó böngészés mennyire hagy mégis vizsgálható nyomokat különböző platformokon**. A cél az volt, hogy a résztvevők megértsék: **milyen adatnyomok maradtak vissza** Windows-on és mobilokon (Android, iOS), milyen eszközökkel és mely szcenáriókban érdemes keresni őket, és hogyan lehet akkor is eredményt elérni, ha a gép már nincs bekapcsolva.

Először röviden **rendszerezte a böngészőcsaládokat**: a Chromium-alapúakat (Chrome, új Edge, Opera, Brave) és a Gecko-alapúakat (Firefox, Tor). Áttekintette a **„klasszikus" böngésző-adatnyomok** (előzmények, cache, sütik, letöltések, könyvjelzők, preferenciák), majd rátért a **modern tárolási megoldásokra**: normál módban ezek döntően fájlokban/SQLite-ban találhatóak meg, jól parszolhatók; privát módban azonban a böngészők egyre inkább memóriában tartják az állapotokat, lemezre alig írnak, ezért a bizonyítékgyűjtés hangsúlya a RAM-on és a lapozófájlon volt.

**A módszertan két fő helyzetre épült**. Élő rendszeren memóriadumpot készítettek (DumpIt, WinPMEM), majd két megközelítést használtak: egyrészt **„nyers" adatkinyerést** (bulk carving) Bulk Extractor-ral, amellyel URL-eket, IP-ket, e-maileket és egyéb mintákat listáztak; másrészt **strukturáltabb elemzést MemProcFS-szel,** amellyel a dumpolható processz-memóriát (például a futó böngésző PID-jének „minidumpját") külön meghajtóként böngészték, célzottan csak a böngésző memóriaterületén keresve. Megjegyezte, hogy egyszerű szövegkereséssel gyakran előkerült a lapon megjelenő URL-cím, oldal-cím vagy akár a tartalomrészlet is.

Külön blokk foglalkozott a memóriából történő IndexedDB/LevelDB visszanyeréssel: a DFRWS-ben publikált kutatásokat és egy proof-of-concept eszközt említett, amellyel Chromium-alapú böngészőkből memóriadumpból lehetett kulcs-érték párokat kinyerni (például keresőkifejezéseket és időbélyegeket). Firefox esetén friss kutatás mutatta, hogy a privát mód adatkezelése más, de a memória- adatnyomok itt is visszanyerhetők; POC kód helyett itt elsősorban a módszer volt a hangsúly.

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

Képfájlokra és kisebb SQLite-darabokra fotó-alapú carve-olást (PhotoRec) is végzett: sikerült Wikipédia -képeket és oldalrészleteket részlegesen visszahozni.

Arra is rátért, **mi történik a böngésző bezárása után.** Tizenöt perccel a zárás után is talált visszamaradt URL nyomokat a RAM-ban; újraindítás után pedig a lapozófájl bizonyult kincsesbányának, ahol még napokkal később is előkerülhettek látogatott domainek – igaz, gyengébb időbeli és felhasználói hozzárendeléssel. Hangsúlyozta: a lapozófájl megléte/állapota rendszertől és beállításoktól (pl. titkosítás) függ.

A „privát" mód nem gátolta a felhasználót abban, hogy **könyvjelzőt adjon hozzá vagy fájlt töltsön le** – ezek viszont már tartós, **fájlrendszerbeli nyomokat hagytak**. Könyvjelzőknél például a Chrome/ Edge JSON állományokban a date_added összevethető más futtatási adatnyomokkal.

A workshophoz előkészített adatcsomagok és az eszközkészlet (Bulk Extractor, MemProcFS, HxD, PhotoRec, Registry Explorer, SQLite Browser) segítette a gyakorlatot; két szcenárióban (futó és bezárt böngészőállapottal) a résztvevőknek kellett URL-eket, böngészőhöz köthető nyomokat, képek/kis adatbázisok carve-olható maradványait és könyvjelző-hozzáadások időpontjait azonosítaniuk, illetve privát mód futtatási jeleit megtalálniuk. Zárásként az előadó összefoglalta a tanulságot: élő rendszeren a memóriadump szinte kötelező; offline esetben a pagefile és a letöltött fájlok/könyvjelzők adják a legjobb kapaszkodót; és soha nem szabad egyetlen toolra vagy technikára hagyatkozni – a kombinált megközelítés hozza a legtöbb használható eredményt.

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

## Workshop | Gyors válaszok megtalálása: Tudás kinyerése az információs zajból / Finding Answers Fast: Extracting Knowledge From the Noise

*(Kevin Ripa — Senior Instructor @ SANS Institute)*

Az előadó a digitális elemzés egyik legnagyobb kihívásáról beszélt: **hogyan lehet az óriási adatrengetegből** – amelyben a ténylegesen értékes információk mindössze 1-2%-ot tesznek ki – **rövid idő alatt kinyerni a releváns bizonyítékokat.** Már az elején hangsúlyozta, hogy a siker kulcsa a jól megfogalmazott kérdések és a célzott adatkinyerés. Felhívta a figyelmet arra, hogy a szakmában sokan hajlamosak bonyolult szakkifejezésekkel "villogni", ami elriaszthatja a kezdőket, pedig a forenzikus vizsgálat lényege mindig az, hogy **konkrét kérdésekre keressük a választ:** például, hogy valaki hozzáfért-e egy fájlhoz, futtatott-e egy adott programot, vagy mit csinált az adott szoftver. Röviden áttekintette a legfontosabb elsődleges forrásokat – ilyenek a Windows registry hive-ok, a prefetch fájlok, a shell bag adatok, a link fájlok és a jump list –, majd jelezte, hogy ezek közül több is részletesen bemutatásra kerül.

Ezután részletesen bemutatta a **legfontosabb gyors nyomkövetési artefaktumokat:**

- **Registry hive-ok:** rendszer- és felhasználói szintű konfigurációs adatbázisok, amelyek számos tevékenység nyomát megőrzik.
- **Prefetch fájlok:** a Windows által készített, programfuttatásokat rögzítő állományok. Ezekből látható a program első és utolsó futási ideje, az utolsó hét futtatás időpontja, a futtatás helye, az összes hívott függőség, valamint az utolsó futáskor érintett fájlok listája. Példaként hozta fel, hogy egy fájl-wipert (pl. SDelete) így lehet lebuktatni, mert a prefetch mutatja, mely fájlokat törölt.

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

- **Shell bag-ek:** mappanézetek és könyvtármegnyitások nyomai, amelyekből egyértelműen bizonyítható, hogy a felhasználó belépett egy adott mappába – például egy USB-meghajtón található „secret stuff" könyvtárba.
- **Link fájlok:** a fájlok megnyitásakor automatikusan létrejövő gyorshivatkozások, amelyek tárolják a megnyitás idejét, a forrás helyét és akár a csatlakoztatott külső meghajtó betűjelét.
- **Jump list-ek:** a link fájlokhoz hasonlóan a felhasználói aktivitás nyomai, de bővebb időbélyegekkel és a megnyitó program azonosításával.

A következő részben bemutatta a **Volume Shadow Copy technológiát,** amely a teljes meghajtó adott időpontban készült pillanatfelvételeit tárolja. Ezekből a törölt, majd felül nem írt adatok – például egy asztalra helyezett és később USB-re másolt, majd törölt mappa – visszaállíthatók. Ezt korábban a ransomware helyreállítására is használták, mivel a régi változatokat a kártevők nem érték el, bár mára a kártevők első lépései között szerepel a VSS (Volume Shadow Service) leállítása. Példaként megemlítette, hogy **célszerű figyelőszabályokat létrehozni** az ilyen kísérletek detektálására, mivel ez sokszor a zsarolóvírus támadások előjele.

Ezután rátért az **Arsenal Image Mounter** használatára. Elmagyarázta, hogyan kell egy képfájlt úgy felcsatolni, hogy az írásvédett legyen, és az esetleges változtatások külön „differencing file"-ba kerüljenek. Így **a meghajtó teljes értékűen működik, de az eredeti bizonyíték változatlan marad.** Megmutatta, hogyan lehet a csatolt meghajtót egyszerű meghajtóként böngészni, majd a fizetős verzióval akár

közvetlenül egy virtuális gépként is elindítani. Ezzel a módszerrel a felhasználó eredeti környezetét lehet vizsgálni, beleértve az asztali elrendezést, jegyzeteket, beállításokat. Ráadásul a bejelentkezési jelszót is ki lehet kerülni, így teljes hozzáférést kapunk a rendszerhez a felhasználó nézetéből.

Továbbá az Eric Zimmerman által fejlesztett **CAPE (Collection and Analysis of Program Execution) eszközt** is bemutatta, amely adatnyomok tömeges kinyerésére és feldolgozására alkalmas. A CAPE képes egy **meghatározott célterületről gyorsan kinyerni előre definiált típusú adatokat** (pl. prefetch, registry, event log), majd ezekre automatikusan elemző modulokat futtatni. Az eredmények konténerekbe (pl. VHDX) kerülnek, kategorizált mappaszerkezetben. A parancssoros mód mellett a grafikus felületen összeállított feladatok parancssorba exportálhatók, így távoli, nem technikai felhasználó is képes lehet egy pendrive-ról a szükséges gyűjtést lefuttatni és visszaküldeni.

Gyakorlati példaként bemutatta, hogyan lehet két és fél perc alatt prefetch, AppCompatCache és MFT adatokból CSV-ket készíteni, majd ezeket a Timeline Explorerben rendezve, szűrve gyorsan kiszúrni gyanús folyamatokat. Felhívta a figyelmet, hogy bár a CAPE képes hatalmas adattömegek kinyerésére, a **cél mindig a szükséges adatok célzott gyűjtése legyen, mert a túl sok adat elemzése lassíthatja a folyamatot.**



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