NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996

NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 12. hét

HÍREK

- BRUTED: a Black Basta automatizált brute force támadási keretrendszere
- Kötelező tárcamigrációval csapják be az áldozatokat
- Malware a PyPI csomagokban
- A hackerek TP-Link routereket támadnak – Kritikus sebezhetőség veszélyezteti a felhasználókat
- Fájlkonverterek trójai falóval

TÁJÉKOZTATÁSOK, RIASZTÁSOK

- Tájékoztatás káros programot tartalmazó csaló e-mailekről

STATISZTIKAI ADATOK

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

BESZÁMOLÓ

- DEF CON 32 és Black Hat USA

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

További hírekért, látogasson el **weboldalunkra**!

IT biztonsági HÍREK

BRUTED: a Black Basta automatizált brute force támadási keretrendszere

(eclecticiq.com)

Az Az EclecticIQ elemzői egy eddig ismeretlen brute force támadási keretrendszert azonosítottak, amelyet a Black Basta RaaS csoport alkalmaz. A forráskód elemzése alapján a BRUTED alapvető feladata az automatizált internetes szkennelés és hitelesítő adatokkal végzett támadások végrehajtása. **Bővebben...**

Kötelező tárcamigrációval csapják be az áldozatokat

(bleepingcomputer.com)

Egy új, kifinomult adathalász kampány a Coinbase felhasználóit célozza, amelyben a támadók egy hamis, „kötelező" tárcamigrációt színlelve próbálják rávenni az áldozatokat egy új tárca létrehozására egy előre generált helyreállítási kóddal. **Bővebben...**

Malware a PyPI csomagokban

(thehackernews.com)

A kiberbiztonsági szakértők egy újabb kampányra hívták fel a figyelmet, amely a Python Package Index (PyPI) felhasználóit célozza meg. A támadók hamis csomagokat tettek közzé az ismert szoftverkönyvtárban. **Bővebben...**

Fájlkonverterek trójai falóval

(malwarebytes.com)

Az FBI Denver Field Office figyelmeztetést adott ki olyan csaló weboldalak terjedéséről, amelyek ingyenes online fájlkonvertáló szolgáltatásokat kínálnak. Ezek a weboldalak első ránézésre ártalmatlannak tűnnek, azonban valójában kártékony programokat telepítenek a gyanútlan felhasználók eszközeire. **Bővebben...**

A hackerek TP-Link routereket támadnak – Kritikus sebezhetőség veszélyezteti a felhasználókat

(gbhackers.com)

TP-Link TL-WR845N típusú routereknél használnak ki sebezhetőséget a hackerek, amely lehetővé teszi számukra a teljes, rendszerszintű hozzáférést. A támadók így megszerezhetik a rendszergazdai bejelentkezési adatokat a firmware fájlok elemzésével és egy egyszerű MD5 hash-jelszó visszafejtésével. **Bővebben...**

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Tájékoztatás káros programot tartalmazó csaló e-mailekről

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** a **Nemzeti Adó- és Vámhivatal** nevével visszaélő, káros csatolmányt tartalmazó e-mailek terjedésére hívja fel a figyelmet.

Intézetünkhöz több állampolgári, valamint vállalati megkeresés érkezett, amely szerint gyanús, látszólag a Nemzeti Adó- és Vámhivataltól, hivatalos címről érkező és hivatalos formátumú levelet kaptak.

Bővebben...

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

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

KIBERTÁMADÁS! PODCAST

Miként csillog a CSIRT az új törvény fényében? [házunk tája]

Ebben az epizódban azt vizsgáljuk, miként változott meg a **CSIRT szerepe** az új törvény fényében. Szó esik magáról az incidensről, a típusairól, sőt, az incidens bejelentésének mikéntje is kiderül.

Na de egyáltalán **ki jelenthet be incidenst**? És **kiknek**? Azaz **milyen hatóságok felé lehet és kell kiberbiztonsági incidenst jelenteni**? A rövid válasz az, ami az élet sok másik területén is általánosan megállja a helyét: "Hát, az attól függ." Mitől? Kiderül a Kibertámadás! 96. epizódjából.

Meghallgatom

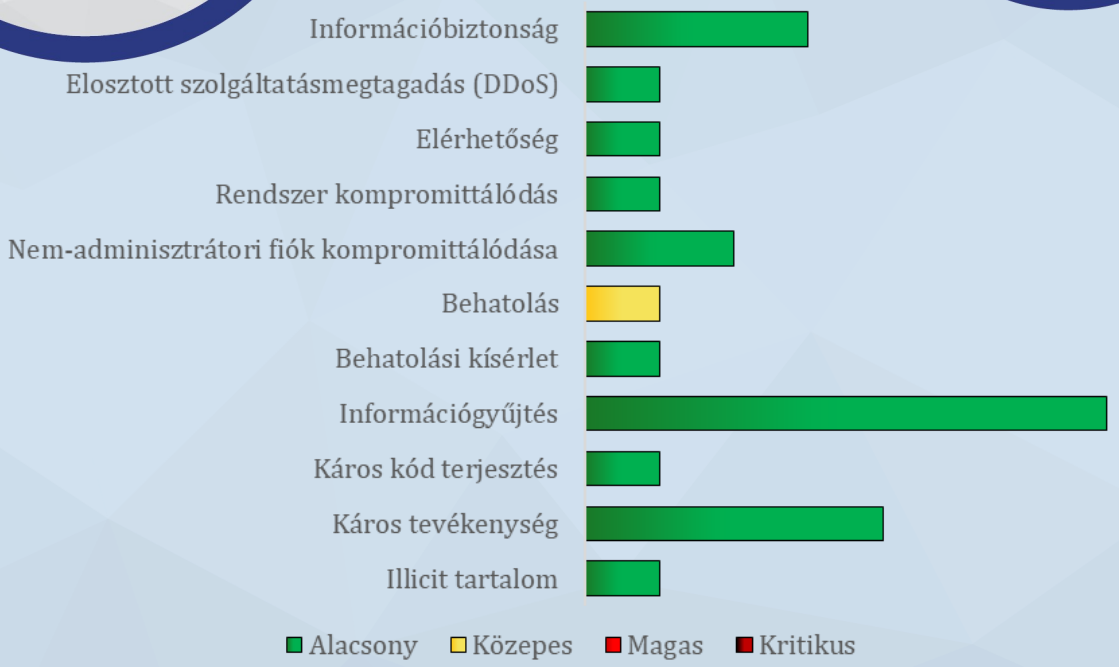
További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Statisztikai Adatok

2025.03.14.-2025.03.20.

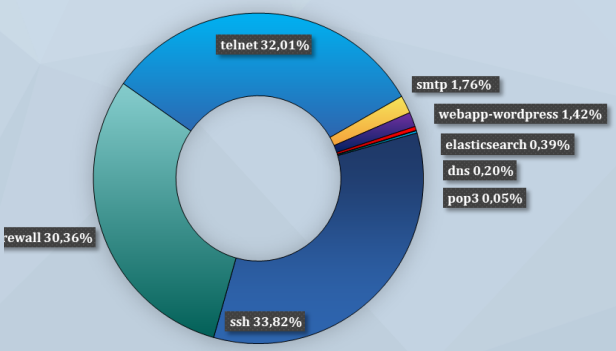
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

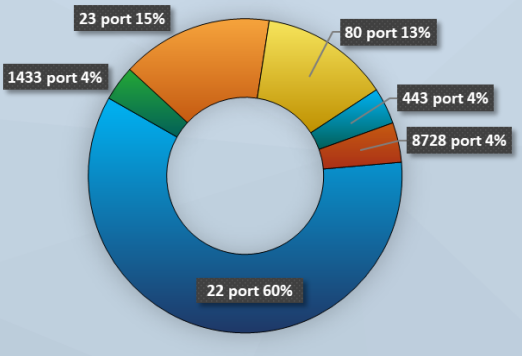
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!

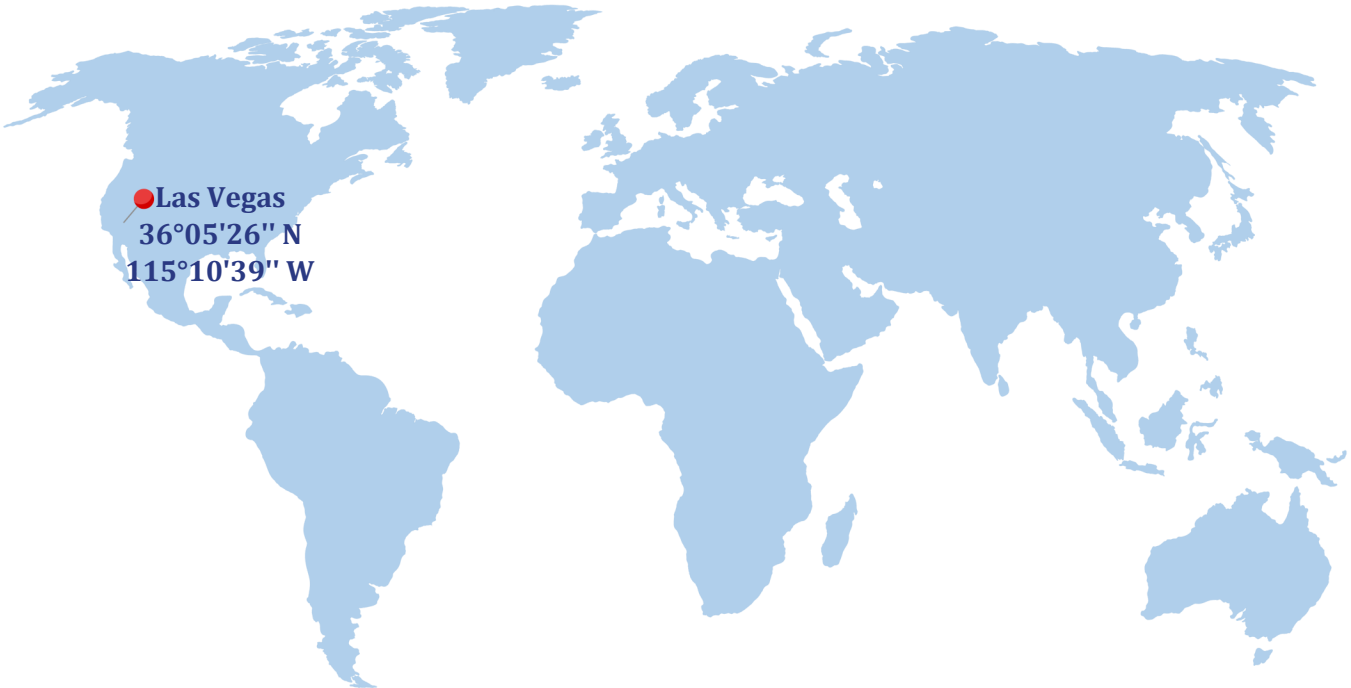
BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

DEF CON 32 és Black Hat USA konferenciák

2024. augusztus 7-11.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** munkatársai **Széchenyi Terv Plus 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-3.1.2-24-2024-00004. sz. pályázat részeként

A **Nemzeti Kibervédelmi Intézet** munkatársai 2024. augusztus 07-11. között részt vettek az Amerikai Egyesült Államokban, Las Vegasban megtartott Black Hat USA 2024, valamint az azt követő DEFCON 32 informatikai biztonsággal kapcsolatos, illetve etikus hacker témájú konferenciákon és szakmai bemutatókon.

A **Black Hat** és a **DefCon** konferenciák az információbiztonsági közösség számára a legizgalmasabb, élvonalbeli kutatásokat, fejlesztéseket és sérülékenységvizsgálati trendeket nyújtó szakmai rendezvényeknek számítanak. A **Black Hat** konferencia szakmailag jól felépített, lényegre törő és mély szakmai információk megszerzésére, aktuális trendek megismerésére ad lehetőséget, míg a **DefCon** a hacker gondolkodás szemléletmód és taktikák megismerése miatt fontos az IT-biztonsági szakemberek számára.

A konferenciák egyik fő vezértémája a **mesterséges intelligenciában rejlő lehetőségek és veszélyek** bemutatása volt, emellett számos szakmailag fontos, újonnan felfedezett **szoftver sebezhetőségről** szerezhettünk információt, amelyeket a kiberbűnözők aktívan kihasználnak. Továbbá az előadások jelentős része **digitális forenzikus és sérülékenységvizsgálati eszközökről, új megoldási lehetőségekről** adott át rendkívül hasznos ismereteket.

Kiknek ajánlott a beszámoló megismerése?

- **Minden kiberbiztonsági szakember** számára
- **Pentesterek** számára
- **CTI specialisták** számára
- **Hálózatbiztonsági szakemberek** számára

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

Blackhat 2024
Corellium bemutató

A **Corellium** cég egy **virtuális hardver platformot biztosít** szoftverfejlesztők és IT biztonsággal foglalkozó szakemberek számára. Részletesen bemutatták a platformjukat és betekintést nyertük, hogyan integrálják a **Frida** elnevezésű eszközt a valós idejű kód-manipulációhoz. A platform segítségével mélyebb **alkalmazás-elemzés** hajható végre, ami magába foglalja a **fizikai szenzorok emulálását**, illetve a hatékony **hibakeresést**. Támogatja mind az Android, mind az iOS operációs rendszer emulálását. Továbbá egyszerűen kiválasztható, hogy melyik operációs rendszer verziót szeretnénk használni a vizsgálathoz. Ez a **fejlett szimulációs képesség** lehetővé teszi a biztonsági kutatók és fejlesztők számára, hogy valós idejű biztonsági elemzéseket végezzenek, sebezhetőségeket fedezzenek fel, és javítsák az alkalmazások biztonságát anélkül, hogy fizikai eszközökre lenne szükség. **Jól integrálható** meglévő fejlesztői eszközökkel és a távoli elérés funkció is támogatott. **On-premise** megoldásuk segítségével pedig nem szükséges a felhőalapú szolgáltatásukat igénybe venni.

Blackhat 2024
Artemis: modular vulnerability scanner with automatic report generation

Az **Artemis** egy **moduláris sebezhetőség-vizsgáló** eszköz, amelyet a lengyel **CERT PL** fejlesztett ki, hogy nagyszabású szkennelési tevékenységeket végezzen. A Black Hat konferencián bemutatták, hogyan működik az eszköz, amely 2023 óta **közel 500 ezer domain és aldomain biztonságát vizsgálta meg**. Az Artemis **több, mint 200 ezer sebezhetőséget és konfigurációs hibát talált,** kezdve a kisebb problémáktól, mint például a nem megfelelő SSL beállítások, egészen az olyan kritikus hibákig, mint az SQL Injection és a távoli kódfuttatás (RCE). Az előadás során részletesen ismertetésre került az Artemis működése, az általa keresett sebezhetőségek, valamint a nagyméretű szkennelési projektekből levont tanulságok. Emellett **az előadó bemutatta, hogyan lehet saját szkennelési rendszert kialakítani és új modulokat bevezetni az eszközbe,** mivel az Artemis egy nyílt forráskódú projekt.

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

DefCon 32—Docker Exploitation Framework

A **Docker Exploitation Framework** (DEF) egy átfogó keretrendszer, amely **a konténer alapú környezetek**, (mint például a Docker és a Kubernetes) **biztonsági rétegeinek tesztelésére és támadására** készült. Lényegében ez egy **post-exploitation keretrendszer**, amely segít a már kompromittált konténerek után végrehajtandó lépésekben. A rendszer **moduláris kliens-szerver** architektúrával rendelkezik, lehetővé téve a különböző modulok rugalmas együttműködését, és automatikusan kezeli a szükséges függőségeket a zökkenőmentes működés érdekében. Bemutásra került egy **Secret Scavenger** elnevezésű kiegészítő is, amely a **törölt fájlokból képes érzékeny információkat kinyerni**. Privilégium növelésre is van lehetőség a **docker socket** segítségével, mivel privilegizált módban tudunk létrehozni egy új konténert. A keretrendszer **Kubernetes pluginokkal** is rendelkezik, amelyek azonosítják a nem biztonságosan felcsatolt fájlrendszereket és a privilegizált podokat. A nem biztonságosan felcsatolt elérések olyan helyek, ahol a konténer hozzáférhet a host fájlrendszeréhez, ami biztonsági kockázatot jelenthet.

DefCon 32—AI Goat

Az **AIGoat** egy nyílt forráskódú projekt, amelyet az Orca Security kutatási csapata fejlesztett ki. **A projekt célja, hogy egy gyakorlati és interaktív környezetet biztosítson a mesterséges intelligencia (AI) alapú biztonsági kihívások és sebezhetőségek tanulmányozásához**, különösen a felhő- és konténeralapú infrastruktúrákban. Az AIGoat lehetővé teszi a kutatók, fejlesztők és biztonsági szakemberek számára, hogy valós környezetben teszteljék és fejlesszék AI-alapú támadási és védelmi stratégiáikat. Az AIGoat különösen értékes eszköz lehet azok számára, akik mélyebb betekintést szeretnének nyerni abba, hogyan befolyásolhatják az egyre több helyen előforduló AI megoldásokat és a felhőalapú és konténerizált környezetek biztonságát. A prezentáció alatt három szoftversérülékenység kihasználása is bemutatásra került, ezek **Data poisoning**, **AI supply chain** és **Output integrity típusú támadások** voltak. A projekt célkitűzése, hogy a jövőben az OWASP gépi tanulással kapcsolatos TOP 10-es listájában szereplő összes sérülékenységet képes legyen lefedni.

DefCon 32—Cyber Security Transformation Chef

A **CSTC** egy Burp Suite bővítmény, amely különféle bemeneti transzformációkat tesz lehetővé, és célja, hogy egy általános megoldást kínáljon számos, eddig különálló bővítmény helyett. A CSTC megoldja azt a problémát, hogy a **Burp Suite**-hoz túl specifikus bővítményeket kelljen használni, illetve, hogy a transzformációkhoz a **CyberChef** weboldalra kelljen látogatni. Széleskörű, egyszerű műveleteket tartalmaz, amelyeket kombinálva összetett transzformációkat lehet létrehozni. **Ez lehetővé teszi a sérülékenységvizsgálók és bug hunterek számára, hogy a szükséges transzformációkat létrehozzák anélkül, hogy kódot kellene írniuk,** ami időigényes feladat. A CSTC segítségével összetett bemeneti transzformációkat lehet konfigurálni mind a kérések, mind a válaszok esetében egyszerűen, **drag-and-drop módszerrel**. Például a tesztelők frissíthetik, illetve titkosíthatják a HTTP kérésekben szereplő adatok bizonyos részeit. Különböző **műveleteket lehet láncba fűzni,** ezáltal komplexebb kéréseket lehet előállítani a transzformációknak köszönhetően. Mivel már számos alapvető művelet implementálva van, a felhasználók könnyedén a tesztelendő alkalmazásra koncentrálhatnak, ahelyett, hogy különböző bővítményeket keresnének az ilyen transzformációk végrehajtásához.

DefCon 32—Moriarty

A **Moriarty** egy .NET alapú eszköz, amelyet a Windows környezetekben történő jogosultsági szint emelésére szolgáló sebezhetőségek azonosítására terveztek. Az eszköz a **Watson és Sherlock** nevű előző eszközökre épít, de tovább bővíti azok képességeit plusz ellenőrzések integrálásával. A Moriarty széles körű támogatást nyújt a különböző Windows verziókhoz, beleértve a Windows 10, Windows 11, valamint a Windows Server 2016, 2019 és 2022 verziókat. Az eszköz különlegessége, hogy **képes felsorolni a hiányzó frissítéseket**, valamint **detektálni** számos jogosultsági szint emeléséhez kapcsolódó **sebezhetőséget**, és **javaslatokat kínál** az esetleges **kihasználási módszerekre.** A Moriarty kiterjedt adatbázisa jól ismert sebezhetőségeket is tartalmaz, mint például **PrintNightmare** (CVE-2021-1675), **Log4Shell** (CVE-2021-44228) és **SBGMhost** (CVE-2020-0796), amelyek révén átfogó megoldást nyújt a Windows rendszerek biztonsági ellenőrzésére.

DefCon 32
Winning the game of active directory

A **Game Of Active Directory** (GOAD) egy nyílt forráskódú projekt, amelyet az Orange Cyberdefense fejlesztett ki. A GOAD **egy előre felépített, sebezhető Active Directory** (AD) **környezet**, amelyet kifejezetten penetrációs tesztelők és biztonsági szakemberek számára hoztak létre, hogy valósághű támadási szimulációkat és biztonsági teszteket végezzenek.

A GOAD **különböző támadási módszerek gyakorlásában segít**, amelyek lehetővé teszik az AD környezet teljes átvételét. Azonban a projekt nem csak a támadások végrehajtására fókuszál, hanem arra is, hogy bemutassa, **hogyan lehet megakadályozni ezeket a támadásokat**, **és biztonságosabbá tenni az AD infrastruktúrát.** A GOAD részletesen bemutatja a különféle támadási stratégiákat, a konfigurációs hibák kihasználását, és azt, hogy hogyan lehet ezeket a hibákat kijavítani.

A projekt célja, hogy a felhasználók mélyebb megértést szerezzenek az Active Directory biztonsági kihívásaival kapcsolatban, és megtanulják, hogyan lehet hatékonyan megvédeni a rendszereiket a gyakori támadások ellen.

A GOAD egy hasznos eszköz, amely **segíti a biztonsági szakembereket képességeik fejlesztésében és naprakészen tartásában.** Ennek köszönhetően könnyebben hozhatnak létre biztonságosabb Active Directory környezeteket.

DefCon 32
How to find a 0day in iOS apps

Ez az előadás bemutatta az **iOS alkalmazásokban található zero-day sebezhetőségek** felfedezésének egyes módszereit és stratégiáit. A prezentáció során az előadó ismertette az iOS operációs rendszer architektúráját, valamint biztonságának alapelveit.

Sajnos életszerű, specifikus példán keresztül nem került bemutatásra, hogyan történik egy iOS applikációban lévő zero-day sérülékenység kihasználása. Ennek ellenére az előadásban **szó esett a kódelemzésről és dinamikus elemzési technikákról.** Támadási technikák szempontjából nagy figyelmet kapott a **buffer overflow**, **stack overflow, heap overflow**, amelyek **súlyos biztonsági kockázatot jelentő memóriakorrupciós sérülékenységek.**

Tárgyalásra került az **AltStore** és a **különböző jailbreak-elési típusok/technikák**, amelyek az iOS rendszer korlátozásainak megkerülésében és a belső mechanizmusok hozzáférésében nyújtanak segítséget. A résztvevők ismereteket szereztek a **„use-after-free”** (UAF) sérülékenységről, valamint a modern védelmi mechanizmusokról is, mint például az **ALSR** és a **stack canary**.

Az előadás továbbá bemutatta a **ROP** (Return-Oriented Programming) **láncok** alkalmazását, amelyek segítségével bizonyos védelmi mechanizmusok megkerülhetők. Az előadó végül ajánlást tett a **Ropper** eszköz használatára, ami megkönnyíti a **gadget-ek** azonosítását.

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

Blackhat 2024
AegiScan: Static Dataflow Analysis Framework for iOS Applications

Az **iOS** az egyik legnépszerűbb operációs rendszer világszerte, így alkalmazásainak biztonsága lényeges, azonban még mindig hiányoznak az erőteljes és hatékony statikus adatfolyam-elemző eszközök, pedig ezek elengedhetetlenek a sebezhetőségek felderítéséhez.

A statikus adatfolyam-elemzés végrehajtása a következő kihívásokkal jár:

- *Objective-C dinamikusan meghívott függvények akadályt jelentenek a statikus metódusfeloldásban,*
- *Az osztályok, struktúrák és modulok közötti műveletek bonyolultak a kontextusérzékeny adatfolyam-elemzés során,*
- *Az optimalizációs technikák, mint például a szimbólumok eltávolítása növelik az elemzés összetettségét.*

Ezen kihívások könnyebb leküzdésében segít az **AegiScan**, statikus **adatfolyam-elemző keretrendszer**. Statikus elemzés és gráf-adatbázis kombinációval rendelkezik, amely hatékonyabbá teszi az olyan feladatokat, mint a sebezhetőségek feltárása, mivel az elemzés után az adatok adatbázisban tárolódnak. A tesztben egy 130 MB méretű iOS alkalmazás bináris fájljának elemzése kevesebb, mint 20 perc alatt befejeződött. E keretrendszer segítségével rengeteg 0-day sérülékenységet találtak eddig.

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

DefCon 32 SHAREM
Advanced Shellcode Analysis Framework

A **SHAREM** egy NSA által finanszírozott **shellcode elemző keretrendszer,** amely elmondásuk szerint forradalmasítja a kódelemzést.

Több mint 25 000 WinAPI függvényt és a Windows rendszerszolgáltatások 99 %-át azonosítja. A SHAREM által elállított **disassembly kód** minősége nagyon magas, felülmúlja a vezető disassembler-ek, például **IDA Pro** vagy a **Ghidra** által produkált eredményeket. Például ezek a szoftverek egy homályos **call edx hívást** generálnának, a SHAREM pontosan meghatározza, hogy melyik függvényt és paramétereket hívják meg, ami különösen nehéz feladat.

Felmerülő probléma általában az **obfuszkáció**. A bemutató során **több fajta technikával obfuszkált adatot sikeresen deobfuszkált**. Új funkciója a **mesterséges intelligencia**, amely pontosabb meghatározásokkal segíti a kódelemzést.

DefCon 32 AntiDebugSeeker
Automatically Detect Anti-Debug to Simplify Debugging

A rosszindulatú szoftverek készítői **gyakran alkalmaznak anti-debugging technikákat**, hogy megnehezítsék az elemzést, ami miatt a malware vagy leállítja futását, vagy szokatlanul kezd el viselkedni, ha egy debugger észleli. Gyakran használnak olyan módszereket a kártékony kódok, mint a virtuális gép észlelés, breakpoint észlelés és időbeli különbség észlelés.

Az **AntiDebugSeeker** **nyílt forráskódú plugin** az **IDA és Ghidra elemző szoftverekhez**. Ezen kívül a plugin olyan funkciókat is biztosít, amelyek megmagyarázzák ezeket az anti-debugging technikákat és a hozzájuk kapcsolódó funkciókat. Ez növeli a kódelemzők lehetőségeit, hogy hatékonyabban megértsék a malware-ek működését.

DefCon 32
Windows Downdate: Downgrade Attacks using Windows Updates

Alon Leviev célja annak felmérése volt, hogy **a Windows rendszer mely egyéb komponensei érintettek az ún. downgrade támadásokban**, és hogy ezek mennyire jelentenek jelentős biztonsági kockázatot.

A Downgrade támadás jellemzői:

- **Láthatatlan**: a korábbi verzióra csökkentett komponensek frissítettnek mutatkoznak,
- **Perzisztens**: a későbbi update-ek nem írják felül a downgrade-elt komponenseket,
- **Nem visszafejthető**: javító programok nem tudják detektálni és javítani ezeket a módosított komponenseket.

Az előadó bemutatta, hogy a **Windows Update architektúra** – a **Trusted Installer**, amely az update folyamatot felügyeli – nem mindig akadályozza meg a támadókat abban, hogy saját maguk hajtsanak végre downgrade támadásokat.

Virtualizáció alapú biztonsági sérülékenységek: a VBS egy biztonságos, izolált virtualizációs környezetet biztosít, amelyet a **Hyper-V hypervisor** működtet. Az előadó ezen kívül **Credential Guard** és **Secure Kernel** sebezhetőséget mutatott be.

DefCon 32
Mobile Mesh RF Network Exploitation – Getting the tea from goTenna

Az előadás Erwin Karincic tolmácsolásában a **goTenna** nevű **mobil mesh hálózati eszköz biztonsági aspektusaira fokuszált.**

A goTenna eszközök lehetővé teszik a felhasználók számára, hogy mobilhálózatok nélkül is kommunikáljanak, így ideálisak olyan helyzetekben is, amikor a hagyományos kommunikációs eszközök nem elérhetők.

Az előadás **részletezett néhány sebezhetőséget**, ahogyan ez az eszköz a felhasználói adatokat és a titkosítást kezeli: **a goTenna** minden küldés során **titkosítatlan egyedi azonosítókat továbbít**, amely **lehetővé teszi a felhasználók nyomon követését különböző helyszíneken**. A goTenna megpróbálta ezt orvosolni, de a probléma még mindig fennáll. Azon részeken, ahol a titkosítás implementálva van, bizonyos metaadatok, mint például az üzenet hossza és egyes címkék továbbra is láthatóak maradnak. Ezek lehetőséget adnak a támadóknak, hogy információkat következtessenek ki a kommunikációról, még akkor is, ha nem tudják dekódolni az üzenet tartalmát.
Kitért az eszköz használhatóságaira, mint például katasztrófahelyzetek, amikor a hagyományos kommunikációs infrastruktúra megszűnik, mivel a goTenna eszközök rádiójelek révén nem függnek a mobiltelefon-tornyoktól vagy internetkapcsolattól.

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

DefCon 32
Dragon Slaying Guide: Bug Hunting in VMware Device Virtualization

Az előadás a **VMware eszköz** virtualizációs környezetében rejlő biztonsági rések felfedezését mutatja be, különös tekintettel a VMware-re, és egy új, eddig nem vizsgált támadási felületre.
A VMware **Workstation/ESXi** a legnépszerűbb **virtualizációs szoftverek** közé tartoznak, és bonyolult rendszereik miatt régóta célpontjai a hackereknek.
A most bemutatott **új támadási felület a VMKernelben található eszközvirtualizáció**. Az előadók nyolc sebezhetőséget tártak fel, amelyből ötnek már van CVE azonosítója, és a további három is megerősítést nyert a VMware részéről.

USB virtualizációs problémák:

- CVE-2024-22255, amely a nem inicializált memória használatból adódik,
- CVE-2024-22252, amely egy Use-After-Free sebezhetőség, valamint
- CVE-2024-22251, ez a hiba a VUsb backend eszközök emulációjában fordul elő, különösen a Smartcard Reader eszköznél.

SCSI virtualizációs problémák:

CVE-2024-22273, amely ARB írási hiba, amely abból adódik, hogy a diszk ellenőrző kód nem megfelelően korlátozza az elérhető szektorok határait, ami tetszőleges írási sebezhetőséget eredményez, és az out-of-bound olvasási/írási hiba, amely lehetőséget ad a támadóknak arra, hogy az UNMAP parancsokat kihasználva hozzáférjenek a diszk szektorok határain túli adatokhoz.

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

DefCon 32
NTLM: The last ride

Az előadás bemutatta az **NTLM protokoll** történelmét, sebezhetőségeit és elkerülhetetlen megszűnését tárgyalja.

Sérülékenységek:

- A **CVE-2024-21413**, amely kihasználja az NTLM protokollt, hogy távoli kódvégrehajtást érjen el, miközben a felhasználó egy rosszindulatú MonikerLink fájlt nyit meg.
- A **CVE-2023-23397** és **CVE-2023-29324**, amelyek Outlook alkalmazást érintő sérülékenységek.
- A **Net-NTLMv1,** automatikusan visszatér az NTLM hitelesítésre, ha a Kerberos nem elérhető, ami lehetőséget ad a támadóknak a hash-ek megszerzésére.
- A **VLC Media Player** lehetővé teszi, hogy lejátszási listákat töltsünk be távoli UNC útvonalakról. Ha a felhasználó ilyen útvonalat nyit meg, a rendszer automatikusan megpróbál hitelesíteni, és ezzel megszerezhető a hash.
- Az **ImageMagick** és **GraphicsMagick**: ezek a képfeldolgozó könyvtárak lehetőséget adnak arra, hogy a támadók NTLM hash-eket szerezzenek meg, miközben egy SVG fájlt dolgoznak fel, amely egy rosszindulatú UNC útvonalra mutat.
- A **Nuget** csomagkezelő eszköz a .NET ökoszisztémában szintén visszaeshet NTLM hitelesítésre, különösen akkor, ha nincs más hitelesítési mód. Ez újabb lehetőség hash szerzésre.
- **Git és Visual Studio**: A git kliens és a Visual Studio integrációja lehetővé teszi, hogy a támadók NTLM hash-eket szerezzenek meg rosszindulatú repository klónozásával vagy git submodule-ok használatával.

Annak ellenére, hogy a Microsoft folyamatosan igyekszik megszüntetni az NTLM protokoll használatát, sok rendszer még mindig erre a protokollra támaszkodik.

Az előadók hangsúlyozták az NTLM teljes letiltásának szükségességét, ahol csak lehetséges, és a modern, biztonságosabb protokollokra való átállás fontosságát.

Blackhat 2024
Tunnel Vision: Exploring VPN Post-Exploitation Techniques

Egy kritikus sérülékenységet fedeztek fel a VPN szervereken, amelyet világszerte kihasználtak. A támadók régóta hozzá szerettek volna férni a VPN szervereken lévő adatfolyamhoz. Mivel a VPN csatorna nem kompromittálható, ezért magát a VPN szervert vették célba. A VPN szerverek elérhetőek az internetről, gazdag támadási felületet tesznek lehetővé, ugyanis a VPN implementációkban nagyon gyakran hiányzik a biztonság és a felügyelet. A cél mindig is az volt, hogy belépést nyerjenek az áldozat belső hálózatába.

A piac két legelterjedtebb VPN-kiszolgálóját vizsgálták meg, az **Invanti Connect Secure**-t és a **Fortigate-et.** Bemutatták, hogy a támadó hogyan tud felhasználói hozzáféréseket összegyűjteni és fenntartani a hozzáférését a hálózaton.

Az előadás befejezéseképp részletezik azokat a bevált gyakorlatokat és elveket, amelyeket követve a biztonsági csapatok csökkenthetik az „utólagos sérülékenység-kihasználás” (post-exploitation) technológiájából eredő kockázatokat.

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

DefCon 32 Behind Enemy Lines
Going undercover to breach the lockbit ransomware operation

Az előadás a „**Lockbit**” nevű kiberbűnözői csapat **által létrehozott ransomware szoftverről, és fejlesztőinek szofisztikált hacker és social engineering módszerekkel történő felkutatásáról, lebuktatásáról szólt.**

2024 februárjában a bűnüldöző szervek **lefoglalták a Lockbit dark webes oldalak „vezérlését”,** amelyekkel a kiberbűnözői szervezet végrehajtotta a támadásokat. A lefoglalás után is jelentettek további LockBit ransomware fertőzéseket, amleyek többnyire Linux és VMware ESXi szervereket vettek célba.

Mint kiderült a szervezet a célzott vállalatokhoz dolgozókat juttatott be, hogy ezáltal közvetlen hozzáférést szerezhessenek a szerverekhez. Emellett kompromittált hozzáféréseket (hitelesítő adatokat) is vásároltak a szerverekhez, ezzel a módszerrel is meg tudták fertőzni a vállalati rendszereket a ransomware szoftvereikkel. A legnagyobb áldozataik többnyire **egészségügyi és oktatási** szektorbeli cégek voltak.

A támadások alapvető célja – mint a legtöbb ransomware esetében – **a váltságdíj kifizettetése, a rendszerzavar visszafordítása, és a titkosított fájlokhoz való hozzáférés visszaállítása volt.** A vállalatok feléjhez kb. összesen 100 millió dollár értékű pénzkövetelés ment ki, és összességében több tízmillió dollárt ki is fizettek az áldozatok. (A megtámadott cégek között óriáscégek is szerepeltek, mint például a chipgyártó TSCM, Fulton County, Industrial and Commercial Bank of China, Boeing, Port of Nagoya, United States Department of Justice (az Amerikai Egyesült Államok Igazságügyi Minisztériuma), BRL Group, China Daily, Royal Mail’s, stb.)

Az előadás bemutatta, hogy a rendvédelmi szervek milyen lépésekkel voltak képesek e bűnszervezet tagjait leleplezni: „bábszínházat rendeztek”. Azokon a helyeken, weboldalakon, darkweb oldalon, fórumokon, programozó site-okon nézelődtek, ahol feltételezhetően megjelennek valamilyen formában a célzott bűnözők.

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

Kapcsolati hálót építettek a Lockbit „üzleti partnereivel”, „leányvállalataival”, majd kémkedni kezdtek utánuk: a LockBitSuppon üzeneteket váltottak az elkövetőkkel. Az egyik leányvállalatukhoz jelentkeztek, mint pentester „munkavállaló”. Barátkozni kezdtek velük, chateltek a LockBituppon keresztül. A feltérképezett leányvállalatok egy adott e-mail címre lettek regisztrálva, amely után nyomozva közösségi médián és egyéb forrásokból további információk derültek ki (további mail címek, botnetek, malwere-ek). A saját e-mail címe már a fejlesztőhöz kapcsolható, neve (Dmitrii Khoroshev) és telefonszáma is elérhetővé vált. Sokat segített a nyomozásban a létrehozott „**Lockbit’s Leak Site**”, ahova bárki, aki információval rendelkezett a bűnszervezettel kapcsolatban, feltölthette információit.

2024 febuár 19-én a **National Crime Agency** (NCA) az Europollal együttműködve lefoglalta a már említett darkweb oldalakat, később a tartalék szervereket is. Egy embert letartóztattak Ukrajnában, egyet Lengyelországban, kettőt az USA-ban, emellett két orosz fejlesztő is megnevezésre került.

Ezt követően 2024 február 24-én az oldal újra megjelent, azzal fenyegetőzve, hogy kórházakat fognak támadni, érzékeny információkat szivárogtatnak ki a **Fulton County**-tól, hacsak nem fizetik ki a váltságdíjat 2024. március 2-ig. Donald Trumppal kapcsolatos információk kiszivárogtatásával is fenyegetőztek, amennyiben nem fizetnek váltságdíjat.

2024 május 7-én vádakat és szankciókat jelentettek be Dmitry Khoroshev, a LockBit feltételezett rendszergazdája és fejlesztője, vezetője ellen.

2024. május 21-én a LockBit vállalta a felelősséget a kanadai London Drugs kiskereskedelmi lánc vállalati irodái elleni támadásért, és 25 millió dollár kifizetését követelte. A támadás miatt 2024. április 28. és május 7. között az összes London Drugs üzlet bezárt országszerte. A London Drugs nem volt hajlandó kifizetni a váltságdíjat, és kijelentette, hogy az ügyfelek és az „elsődleges alkalmazottak” adatai nem kerültek veszélybe.

Dmitry Khoroshev olyannyira biztos volt anonimitásával kapcsolatban, hogy 10 millió dollárt ajánlott annak, aki felfedi identitását (mint a LockBit vezetőjét). Az Egyesült Királyság biztonsági minisztere kijelentette, hogy hiába hiszik azt a kiberbűnözők, hogy elérhetetlenek, biztonságos fiókok mögé rejtőznek, mialatt megpróbálnak pénzt kicsalni az áldozataiktól, a kiberbűnözés elleni szakemberek hamarosan el fogják őket csípni.

A bűnüldöző szervek végül nemcsak magát Dmitry Khoroshevet fedték fel, hanem egy másik szálon a LockBit másik vezetőjét, aki szintén kiadta Dmitry-t. Jól látható tehát, hogy számos oldalról megközelítve lehetséges eredményt elérni a ransomware-ek üzemeltetőinek leleplezésére.

A siker kulcsa az összefogás: célszerű bevonni minden érintett felet, és megosztani a feladatokat (például az adatszivárogtató „Leak" oldalak létrehozásával, üzemeltetésével), mert a ransomware-ek üzemeltetői is hibáznak, ezeket a hibákat pedig meg kell találni, és ezek mentén eljutni az elkövetőkig. A LockBit bár tevékenysége során megtámadott egy kórházat, ahol beteg gyerekeket ápoltak – le is állt több IT rendszerük – de ahogy a hackerek észlelték az általuk okozott problémát, helyreállítottak mindent és a rendszert újra működésbe hozták.

DefCon 32
Where is the money? Defeating ATM Disk Encryption

Az ATM-ek többnyire WinCE vagy Windows 7/10 operációs rendszereket használnak, a jellemzőbb márkák: **Hyosung, Triton, Genmega, NCR, Diebold Nixdorf.**

Az ATM-ek támadási lehetőségeik:

Blackbox, Skimming, fizikai rablás, biztonságos vágás, robbanóanyagok használata. Sok esetben vonzó célpontot jelentenek, mert nagy mennyiségű pénzt tartalmaznak, fizikai hozzáférést biztosítanak a támadóknak. Az Amerikai Egyesült Államokban körülbelül 451 000 ATM van, amelyekkel évi 10 milliárd tranzakciót bonyolítanak le.

Az ATM-es bűnözések aránya 2019-tól 2022-ig **600%-os** növekedést mutatott – csak 2022-ben 165%-kal nőtt. A kártyás lefölözések (card skimming) 109%-ot nőtt 2022-2023 között, a fizikai rablás 10%-ot 2022 és 2023 között. Egy **fizikai rablás** mindössze 5-6 percet vesz igénybe. Mivel az USA-ban nincs különösebben nagy szankció az ATM rablásokra, emiatt gyakori, hogy egyes esetekben az érintett rendőrségi szerv a bejelentésre ki sem ment.

Az előadás a Diebold Nixdorf Vynamic Security Suite sérülékenységeit vizsgálja, mivel az össz ATM piacnak ez a típus jelentős (35%-át) teszi ki. A Vynamic Security Suite USB filterezést, tűzfal beállításokat, TLS titkosítást, „szabotázs észlelést", és lemeztitkosítást alkalmaz. A lemeztitkosítással kapcsolatban merültek fel kérdések a vizsgálatok során.

A rendszer vizsgálatánál **egy sérülékenységet fedeztek fel**, amelyet a rendszer bootolása előtt lehet kihasználni (pre-boot authentication). A bootolást megelőzően érzékeny adatokat (hitelesítő adatokat) képes megszerezni támadó. A sérülékenységet **CVE-2023-24064**-nek nevezték el. Egy sérülékeny modul használata miatt a rendszer a bootolását megelőzően a sérülékenységet kihasználva a támadók hozzáférést szerezhetnek a hitelesítő adatokhoz.

A 2021 decemberében észlelt sérülékenységet 2022. január 1-én bejelentették a gyártónak, amelyet két héten belül jóváhagyott, 1 évvel később adott ki javítást.

Az előadáson részletesen bemutatták:

- CVE-2023-28865
- CVE-2023-24062
- CVE-2023-33206
- CVE-2023-40261

sérülékenységeket, amelyek szintén jól példázzák a rendszer sebezhetőségeit az alkalmazott titkosítás dacára.

A gyártó bár folyamatosan ad ki verziófrissítéseket, ezeket minden alkalommal hamar feltörik. 2024 áprilisában is érkeztek javítások, a készített patchekben a VSS-t lecserélték teljes lemeztitkosításra, a belépéseket aktív felügyelet alá vették, az USB portokat letiltották, fizikailag is ellenállóbbá tették. A problémák, sérülékenységet ugyanakkor továbbra is fennálnak.

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

DefCon 32 Xiaomi the money –
Our Toronto PWN2OWN 2023 Exploit and behind the scenes story

Két biztonsági szakember a **Torontói Pwn2Own 2023**-as versenyen a **Xiaomi 13 Pro hackelésével** nevezett, bemutatták az **exploit chaint** (kiaknázható hibák láncolatát) amit használtak, részletezték az időközben felmerülő problémákat a kutatásuk alatt, és hogy mi történt ezalatt a Pwn2Own versenyben.

*A **Pwn2Own** egy minden évben megrendezésre kerülő verseny, ahol **biztonsági szakemberek versenyeznek**, hogy feltörjenek egy teljeskörűen frissített böngészőt, mobiltelefont vagy más rendszert, és hogy létrehozzanak egy időben folyamatos jellegű támadást olyan rendszerek ellen, amelyeket még nem javított az adott cég/kereskedő.*

Több mint 1 millió dollár össz nyereményért cserébe **a feladat a következő telefonok feltörése volt**:

- Xiaomi 13 Pro (40 ezer dollár),
- Samsung Galaxy S23 (50 ezer dollár),
- Google Pixel 7 (200 ezer dollár),
- Apple iPhone 14 (250 ezer dollár).

A Xiaomi 13-ból két modell áll rendelkezésre: egy „globális” modell (2210132G), és egy kínai modell (2210132C). A firmware-ek eltérőek, a kínai verzióban például nincsenek Google appok, kérdéses, hogy vannak-e regionális appok, illetve a beállításokon keresztül lehet-e imitálni más régiókat. Az utóbbi két pontot vizsgálták.

A firmware régióját megváltoztatva különböző applikációk voltak elérhetőek/tiltva. Például a „GetApps” (App Mall) applikáció elérhető egy olyan telefonon, ahol a régió „Egyesült Királyságra” lett beállítva. Abban az esetben, ha a kezdeti beállításnál az Egyesült Államokat választották, a „GetApps” alkalmazás nem volt elérhető.

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

Kérdéses volt, hogy a kezdeti beállítást követően a régióváltás esetében elérhetőek-e egyes alkalmazások, vagy sem. Oroszország kiválasztása esetében a Yandex böngésző volt elérhető, Spanyolország esetében az Opera, Indonézia esetében pedig a WhatsApp Messenger.

A kutatók a „GetApps" – Xiaomi appstore-t (com.xiaomi.mipicks csomag) törték fel. Három különböző módszert találtak az alkalmazások telepítésére: az egyik, hogy a felhasználó rosszindulatú hiperlinkre kattint, a másik két módszert a gyártó kijavította mielőtt a verseny véget ért.

Időközben a Xiaomi mérnökei javítottak sérülékenységeket a „GetApps" alkalmazáson belül, de a verseny végéig a háromból egy megoldás még mindig elérhető maradt, a két biztonsági szakember végül megnyerte a versenyt a Xiaomi 13 Pro feltörésére irányulóan.

A Xiaomi hivatalosan sokáig nem ismerte el a biztonsági hibákat – a folyamatos patchelés ellenére sem, azonban a Zero Day Initiative adott ki sérülékenységi azonosítót a sebezhetőségekre: ZDI-CAN-22332, ZDI-CAN-22379 (Xiaomi Pro 13 mimarket manual-upgrade Cross-Site Scripting, Remote Code Execution Vulnerability). A sérülékenységet 2023.11.09-én bejelentették a gyártónak, amelyet utóbbi hivatalosan 2024.07.01.-én ismert el.

Később a CVE-2023-26324 sérülékenységet publikálták gyártó szerint „magas" (8.8), az NVD szerint „kritikus" (9.8) besorolással.

DefCon 32 The curious case of Alice and Bob
What you can (and cannot!) do as digital investigators

Az előadó az ismertebb gyártók számítástechnikai eszközök és mobiltelefonok szakértésére szolgáló **szoftvercsomagokat mutatott be**, mint például az **FTK**, az **Encase**, az **XRY**, a **Cellebrite**, a **MAGNET Forensics**, a **Griffeyet**. A következő ingyenes szoftvereket is bemutatta: **Nirsoft** termékei, **Autopsy**, **Paladin Linux** és egyéb **Sumuri** termékek.

Még szakértői körökben sem szokott felmerülni ez a név, de ezen az előadáson bemutatták a **Log2Timeline/Plaso** szoftvert, amely egy Python alapú eszköz, amelyet számos szoftver használ (például az Autopsy is) idővonalak automatikus létrehozására. A szoftver önállóan is használható, egy 1 TB kapacitású Windows rendszert tartalmazó adathordozó feldolgozása erős hardveren napokig is eltarthat, az eredmény egy nagyon részletes idővonal, amelyben olyan műveletek rekonstruálhatók (idővonal – fájlműveletek, alkalmazások telepítése, futása, azok által megnyitott fájlok), amik más módon nem érhetők el.

Az előadó kitért az **SQL Injection** felhasználására szakértői elemzések során: bonyolultabb módszer, azonban hasznos lehet, amikor bűnjelként egy aktív hálózati eszközt, például routert kap a szakértő, nem ismeri a hitelesítő adatait, de elképzelhető, hogy egy SQL Injectiont felhasználva be tud lépni az admin felületre, vagy titkosított részekhez fér hozzá a „hamis” belépést követően.

A **Cellebrite Premium** szakértői szoftverre is kitért az előadó, ami drága 0-day exploitokat használ ki a telefonok védelmi rendszerének megkerülésére, a feloldó kódok megismerésére, feltörésére.