NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 8. hét

HÍREK

- Új adathalász módszert használnak az észak-koreai hackerek
- A Google Chrome is AI alapú védelmet használ
- A Xerox VersaLink nyomtatók sérülékenységei laterális mozgást tesznek lehetővé
- Drasztikusan nő az adatok nyilvánosságra hozatalával is fenyegető zsarolóvírus támadások száma
- Kritikus hibát javított a Google

STATISZTIKAI ADATOK

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

BESZÁMOLÓ

- Suricon 2024 conference

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

IT biztonsági HÍREK

Új adathalász módszert használnak az észak-koreai hackerek

(bleepingcomputer.com)

Az észak-koreai „Kimsuky” (más néven „Emerald Sleet” vagy „Velvet Chollima”) nevű állami hackercsoport egy új taktikát alkalmaz, amelyet a terjedő ClickFix kampányok ihlettek. **Bővebben...**

A Google Chrome is AI alapú védelmet használ

(bleepingcomputer.com)

A Google Chrome frissítette a meglévő „Speciális védelem” funkciót mesterséges intelligenciával, hogy valós idejű védelmet nyújtson a veszélyes webhelyek, letöltések és bővítmények ellen. **Bővebben...**

A Xerox VersaLink nyomtatók sérülékenységei laterális mozgást tesznek lehetővé

(securityweek.com)

A Xerox VersaLink multifunkciós nyomtatók sérülékenységei lehetővé teszik a támadók számára, hogy hitelesítési adatokat szerezzenek pass -back támadások révén, amelyek az LDAP (Lightweight Directory Access Protocol) és SMB/FTP szolgáltatásokat célozzák. **Bővebben...**

Drasztikusan nő az adatok nyilvánosságra hozatalával is fenyegető zsarolóvírus támadások száma

(knowb4.com)

Egy friss jelentés szerint a 2024. utolsó negyedévében 46%-kal nőtt a nyilvánosságra hozatallal is fenyegető a ransomware támadások száma. A Nuspire kutatása rámutat, hogy a zsarolóvírusok már nemcsak adatok titkosítására, ezáltal elérhetetlenné tételére, hanem azok kiszivárogtatására is összpontosítanak, ezzel további nyomás alá helyezve az áldozatokat. **Bővebben...**

Kritikus hibát javított a Google

(bleepingcomputer.com)

Google két olyan sérülékenységet javított, amelyek együttes kihasználása lehetővé tette a YouTube fiókok e-mail címeinek felfedését, ezáltal súlyos adatvédelmi incidenst okozva azok számára, akik anonim módon használják az oldalt.

Bővebben...

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Végleges adattörlés IT eszközökről

CTI jelentés

Jelen dokumentumunk célja felhívni a figyelmet a már nem használt informatikai eszközök végleges adattörlésének fontosságára, továbbá ajánlásokat nyújtunk a végleges adattörlés hatékony kivitelezéséhez.

Az elemzésünkben megismerhetjük **Solymos Ákos** iparági szakértő véleményét illetve javaslatait a témával kapcsolatban, például hogy hogyan semmisíthetjük meg otthoni környezetben a már nem használt adattárolókon lévő adatainkat - beleértve a már megunt, vagy lecserélt mobil eszközeinket is.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!

LinkedIn

Instagram

Facebook

Statisztikai Adatok

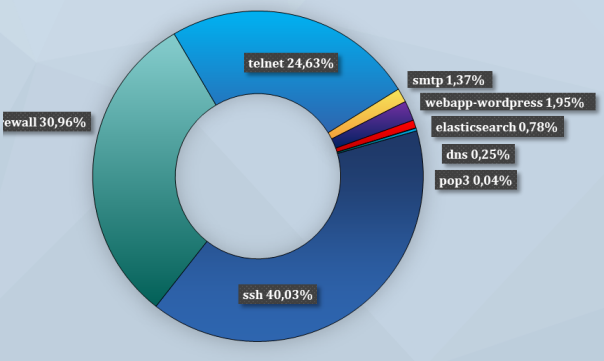
2025.02.14.-2025.02.20.

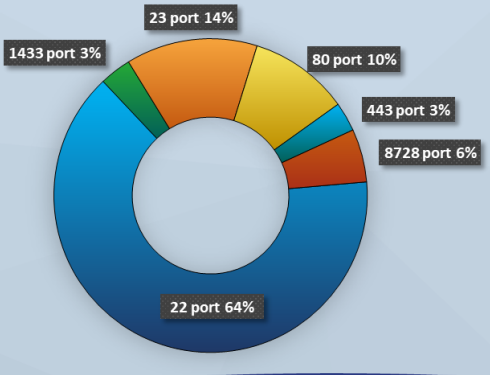
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

Incidensek eloszlása típus és kockázati besorolás szerint

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





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

#halozatbiztonsag #esemenyeszleles #llm

Suricon 2024 conference

2024. november 12-15.

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 részt vettek a 2024.11.12-15. között Madridban megrendezésre kerülő éves Suricon 2024 konferencián. Az esemény egy 2015 óta minden évben megrendezett rendezvény, amely során az **OISF (Open Information Security Foundation)** alapítvány által publikált ***Suricata* nyílt forráskódú hálózatbiztonsági megoldással kapcsolatos iparági fejlesztéseket lehet megismerni**. A világ minden tájáról érkeztek előadók (fejlesztők, alapítványtagok, szponzorok, szervezetek), akik **beszámoltak saját fejlesztéseikről vagy bemutatták kutatási eredményeiket**. A rendezvényen nagyságrendileg 100-120 fő vett részt. A három napos esemény során több mint 30 előadás hangzott el az esettanulmányoktól kezdve teljesítményoptimalizációkon át behatolás detektációs megoldásokig. A szakmailag legfontosabb előadások rövid összefoglalója az alábbiakban olvasható.

Kiknek ajánlott a beszámoló megismerése?

- **Minden kiberbiztonsági szakember** számára
- **CTI specialisták** számára
- **Hálózati rendszerüzemeltetők** számára
- **Hálózatbiztonsági szakemberek** számára

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

State of Suricata

(Victor Julien)

Az konferencia nyitó előadást az OISF egyik alapítványi tagja tartotta, amely alatt betekintést nyerhettünk az **utóbbi egy év eseményeibe és fejlődésbe**. A Suricata nyílt forráskódú bázisa által kiemelésre kerültek a legnagyobb **kontribútorok** (egyének és szervezetek is).

Fejlesztések:

- Protokoll kiegészítések (websocket, ldap, SIP/TCP, Pop3, DNS, ARP
- KKV-kra szabott teljesítményszabályzók, optimalizáló modulok
- Plugin API 2
- Lua revamp
- DNS és SMB detekciós kulcsszavak (Detection)

Ezen felsorolásból próbálták a **8.0.0-ás verzió újdonságai**t előrevetíteni (jelenleg is elérhető legfrissebb verzió – 7.0.7). A tervek szerint **5 hónapon belül kiadásra kerül az új főverzió**, azonban még 370 nyitott ticket van hátra. Ez a nagy mennyiségű kezeletlen hibajegy problémákat vetít előre, amelyre az előadó felhívta a figyelmet kérve a kontribútorokat a támogatásra.

Egy év alatt körülbelül **60-70 ezer sornyi kód változott** (mind kiegészítésben és törlésben), CISA ajánlás alapján megpróbálnak eltávolodni az olyan memória rizikókkal járó programozási nyelvektől, mint a C.

Biztonsági szabályozás fejlesztése érdekében az OISF tagjai létrehoztak egy úgynevezett **Github Security Advisor** profilt, ahol a fejlesztők és **harmadik felek tudnak biztonsági sérülékenységeket bejelenteni**. A Github által mindezek visszakövethetőbbek és támogatja az átláthatóságot a felhasználók felé.

Előadói prezentáció

Előadás videó formátumban

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

Deploying Suricata in a Large Corporate Network, Be Suprised!

(John Graat - Holland rendőrség, Security Operations Center)

A holland rendőrség által használt üzemeltetési és belső biztonsági megfelelésre kialakított hálózatmonitorozó rendszer általános bemutatására került sor. Az előadás egy tapasztalat-megosztó esettanulmány volt. Az előadó előnyként sorolta fel a nyílt forráskódú modulok használatát az erősebb kontroll és a más kormányzati rendszerek könnyebb integrálása érdekében, több alkalommal hangsúlyozva a kezdeti tervezés fontosságát (hálózati ábrák, VLAN kapcsolati gráfok stb.).

A tervezési fázishoz tartozott a szenzorok megfelelő elhelyezése is. A hálózati kijáratok/átjárók biztosítják a megfelelő adatforgalmat. Az előadó **jó tanácsként hozta fel a VLAN becsatornázás megfontolását**. Szerinte a VLAN-ok gyakran feleslegesen nagy forgalmat generálnak „kevés" hasznos információval (kifejezetten csúcsidőben). A bevett hálózatbiztonsági gyakorlat ugyanis azt mondja, hogy a hálózat legyen mindenképpen funkcionálisan szeparált, azonban emiatt megnövekszik a hálózati forgalom, amely nagy performancia terhet ró az IDS rendszerekre. A terhelhetőséget javítja a nem releváns adatok kiszűrése is, mint például:

- duplikátumok
- backup
- vMotion
- remote syslog
- SNMP

Előadói prezentáció

Előadás videó formátumban

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

Community Leader — Sponsor Talk - How to Catch a Phish

Az előadó a Suricata egyik kiemelt támogatójától érkezett az **Emerging Threats** (Proof Point almárka) vállalattól. A prezentáció során felvázolódott az a probléma, amely megannyi **piaci ágazatot** és **nem utolsó sorban a kiberbiztonsági szervezeteket is kiemelten érint**.

A phising elleni küzdelem gyakran nehézségekkel jár. Az állandóan változó technikák és megoldások miatt nem lehet konkrét indikátorok alapján automatizált detektációt használni a védekezésre. Az előadó bemutatta milyen metódusok alapján készítenek Suricata szabályokat, amelyek **nagy hatásfokkal ismerik fel a phising tartalmú forgalmat**.

A vállalat rendelkezik egy **ET Pro** nevű 3 szabálycsomaggal, amelyet **folyamatosan bővítenek a kutatásaikból és a fenyegetettségelemzéseikből származó találatokkal**. Az ET Pro ugyanis tartalmazza a phishing detektációs csomagokat, amely nagymértékben megnövelheti a védekezési képességeket.

Előadói prezentáció

Előadás videó formátumban

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

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

Jumping Over Geo-Fences

(Konstantin Klinger, Matthew Bing)

A két előadó Proofpoint információ- és IT-biztonsággal foglalkozó vállalat képviseletében érkeztek. A bemutatójuk során az előzőekhez hasonló témát elemeztek a **malware-ek** kapcsán.

Állításuk szerint a 2020-as évekig a malware detekció egy könnyebb folyamat volt, azonban manapság a **káros kódok álcázása új szintet lépett**. Valós példák során mutatták be, hogy a malware kézbesítésére szolgáló weboldalak **Captcha és egyéb felhasználói interakció alapú védelmet használnak** a malware szkennerek ellen.

Gyakori, hogy egérmozgatásra oldódik fel a titkosított Javascript kód, amely átirányítja a felhasználót a káros kódot tartalmazó weboldalra. Mindemellett a támadók kódjaikat úgy alakítják ki, hogy azok **képesek legyenek felismerni a népszerűbb malware-elemző sandbox környezeteket**. Az előadók a megoldást az elemző alkalmazásokban látják. Fel kell készülni arra, hogy a támadók használnak valamilyen álcázási technikákat, és ehhez az elemző környezeteinket is fel kell készíteni.

Előadói prezentáció

Előadás videó formátumban

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

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

Suricata Extreme Performance Tuning — SepTun Mark III

(Andreas Herz, Peter Manev)

Kutatási téma keretein belül a két előadó felvázolta saját tapasztalatait a **Suricata adatfolyamatok hardveres gyorsítása kapcsán**. A probléma igen komplex, mivel komoly összehangolást igényel, hogy ez a teljesítményjavulás érezhető legyen, mind a hálózati kártyák, a merevlemezek, az I/O portok, a processzorok és a grafikai gyorsítók kapcsán. A kutatás során megvizsgálták az egyes hardverelemek külön tulajdonságait a különböző – Suricatára jellemző – regexes keresések során.

Végeredményképpen azt tudták elmondani, hogy az **egyes videókártyák kifejezetten hatásosan felhasználhatók** komplex keresések során.

Előadói prezentáció

Előadás videó formátumban

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

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

Supercharging Security with RAG

(Anthony Tellez and Leo Meyerovich)

Ugyancsak saját kutatási munkák során a két előadó esettanulmányukban mutatta meg, hogy miként lehet felhasználni a **nagy nyelvi modell** (LLM – Large Language Model) **alapú mesterséges intelligenciákat** egyes kiberbiztonsági elemzői munkafolyamatok kapcsán.

Az LLM-ek esetében megemlítik, hogy **gyakori az a probléma, amikor a rendszerek nem képesek „visszaemlékezni" az azelőtti chat folyamatokra**, amely által gyakran időigényesebbé válhat a munka. A kutatási projekt **Loui AI**-on alapszik, amely képes adatbázisok felhasználásával komplex adathalmazokat feltárni, azok között összefüggéseket keresni és végül a döntéstámogatás érdekében ábrázolni a találatokat (kapcsolati gráf). Mindemellett a LLM mesterséges intelligenciák képesek nagy hatékonysággal Suricata szabályokat is létrehozni, amely szakértői munkával is, hosszú időbe telne.

A metódusaik között kiemelték **a Python programozási nyelv alapú adatelemzési formákat**. A Pandas könyvtár Dataframe-jei ugyanis képesek rugalmasan és könnyen kezelni az AI és az adatalapú rendszerek igényeit. A kutatási találataik és metódusaik nagy segítségére válhatnak a biztonsági elemzők mindennapjai során. Az egyik kész munkájuk során ábrán bemutatták az IDS-en átjutó fals pozitív eseményeket, amelyeket a honeypot rendszer felfog.

Előadói prezentáció

Előadás videó formátumban

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