



# HÍRLEVÉL

Nemzetközi  
IT-biztonsági sajtószemle  
2024. 38. hét



## HÍREK

- Braille szóköz Windows sebezhetőséget használtak ki zero-day támadásokban
- A SolarWinds kritikus sebezhetőséget javított az Access Rights Manager-ben
- Malware blokkolja a böngészőt kioszk módban, így szerzik meg a támadók a Google hitelesítő adatokat
- Ransomware bandák most a Microsoft Azure termékeivel élnek vissza
- Microsoft: A Vanilla Tempest az INC ransomware-rel sújtja az egészségügyet



## STATISZTIKAI ADATOK

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



## KONTAKT

[edt@nki.gov.hu](mailto:edt@nki.gov.hu)

PGP kulcs

FBC3 88A2 E465 BF51  
AD58 A2D0 E9DD E078  
ABD3 E75D



# NEWS

## IT biztonsági HÍREK

Braille szóköz Windows sebezhetőséget használtak ki zero-day támadásokban  
(bleepingcomputer.com)

A Void Banshee nevű APT csoport aktívan kihasználta támadásokhoz a CVE-2024-43461 kódon nyomon követhető Windows MSHTML spoofing sebezhetőséget. **Bővebben...**

Malware blokkolja a böngészőt kioszk módban, így szerzik meg a támadók a Google hitelesítő adatokat  
(bleepingcomputer.com)

Egy malware-rel kapcsolatos kampány szokatlan módszere, hogy zárolja a böngészőt kioszk módban, ezzel a Google hitelesítő adataik megadására kényszeríti a felhasználókat. **Bővebben...**

Ransomware bandák most a Microsoft Azure termékeivel élnek vissza  
(bleepingcomputer.com)

A BianLian-hez és Rhysida-hoz hasonló zsarolóvírus bandák egyre gyakrabban használják a Microsoft Azure Storage Explorer és AzCopy eszközt arra, hogy adatokat lopjanak el a feltört hálózatokból és azokat az Azure Blob-ban tárolják. **Bővebben...**

Microsoft: A Vanilla Tempest az INC ransomware-rel sújtja az egészségügyet  
(bleepingcomputer.com)

A Microsoft állítása szerint a Vanilla Tempest zsarolóvírus csoport amerikai egészségügyi szervezeteket céloz meg INC Ransom RaaS (Ransomware-as-a-Service) támadásokban. **Bővebben...**



A SolarWinds kritikus sebezhetőséget javított az Access Rights Manager-ben  
(securityweek.com)

A SolarWinds bejelentette, hogy két sérülékenység is javításra került az Active Directory (AD) és Azure AD felhasználói jogosultságkezelő eszközében, az Access Rights Manager-ben, beleértve egy kritikus súlyosságút is.  
**Bővebben...**

További hírekért, látogasson el **weboldalunkra!**



Aktuális  
tartalmak



## Budapesten kerül megrendezésre a 9. eHealth Security Conference!

Számos külföldi szakértő mellett előad  
**Szabó Lajos**, az **NBSZ NKI igazgatója**,  
továbbá **Orosz Péter**, a **NBSZ Mesterséges  
Intelligencia Nemzeti Labortól**.

A konferencia központi témái:

- a **NIS2 irányelv** egészségügyi szektorba való implementációja,
- **EHDS, AI** és egyéb **e-egészségügyi** szakpolitikai fejlesztések,
- és a folyamatosan változó **fenyegetések**, illetve az **egészségügyi adatok megosztásával kapcsolatos aggályok** állnak.

Az eseménnyel  
kapcsolatos további  
információkért  
látogasson el  
az alábbi weboldalra!



**Regisztráció**



További hírekért, látogasson el **weboldalunkra!**

# Statisztikai Adatok

2024.09.13.-2024.09.19.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:



Fenyegetettségi szint: alacsony

Nem-adminisztrátori fiók kompromittálódása



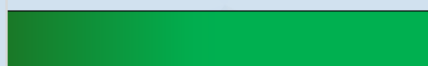
Adminisztrátor fiók kompromittálódása



Behatolási kísérlet



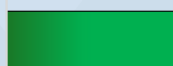
Információgyűjtés



Káros tevékenység



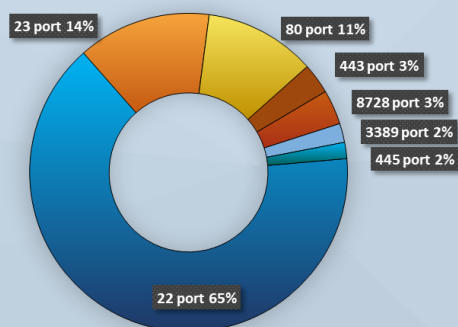
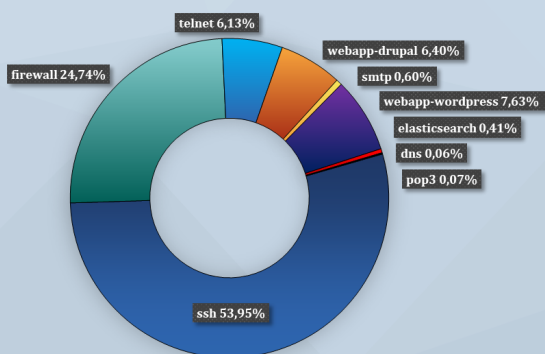
Kéretlen levél



■ Alacsony ■ Közepes ■ Magas ■ Kritikus

Incidensek eloszlása típus és kockázati besorolás szerint

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



További érdekességekért, látogasson el [weboldalunkra!](#)