



HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 51. hét



HÍREK

- Adathalász kampány célkeresztjében YouTube-os tartalomkészítők
- A rendőrség felszámolta a Rydax online piacteret
- A ConnectOnCall adatszivárgása több mint 900.000 embert érintett
- A Clop ransomware banda magára vállalta a felelősséget a Cleot ért adatlopási támadásokért
- Kifinomult adathalász támadás során próbálják megkerülni az e-mail védelmi szoftvereket a csalók



STATISZTIKAI ADATOK

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



KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D



NEWS

IT biztonsági HÍREK

A rendőrség felszámolta a Rydox online piacteret (bleepingcomputer.com)

Az albán bűnüldöző szervek nemzetközi partnereikkel együttműködve leállították a Rydox illegálisan működő piacteret és letartóztattak három adminisztrátort. **Bővebben...**

A ConnectOnCall adatszivárgása több mint 900.000 embert érintett (securityaffairs.com)

A ConnectOnCall egy olyan teleegészségügyi vállalat, amely munkaidőn kívül biztosít telefonos kapcsolattartást betegek és egészségügyi szolgáltatók között azzal a céllal, hogy javítsa a köztük zajló kommunikációt. **Bővebben...**

A Clop ransomware banda magára vállalta a felelősséget a Cleot ért adatlopási támadásokért (bleepingcomputer.com)

A Clop ransomware banda megerősítette, hogy ők állnak a legutóbbi Cleo adatlopási támadások háttérében, akik a támadások során a [CVE-2024-50623](#) és [CVE-2024-55956](#) elnevezésű nulladik napi sebezhetőségeket használják ki. **Bővebben...**

Kifinomult adathalász támadás során próbálják megkerülni az e-mail védelmi szoftvereket a csalók (blog.knowbe4.com)

Egy átfogó adathalász támadássorozat során próbálják ellopni különböző szervezetek alkalmazottainak hitelesítési adatait. **Bővebben...**



Adathalász kampány célkeresztjében YouTube-os tartalomkészítők (blog.knowbe4.com)

A CloudSEK kiberbiztonsági vállalat kutatói szerint e-mailes adathalász kampány során YouTube-os tartalomgyártókat támadnak hamis együttműködési ajánlatokkal. **Bővebben...**



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

Aktuális tartalmak



A SIEM rendszerek működése

CTI jelentés

Jelen dokumentum célja, hogy bemutassa a **SIEM** (Security information and event management) rendszereket, szerepüket és jelentőségüket vállalati környezetben, valamint ezen rendszerek felépítését, felhasználhatóságát és különböző részelemeit is.

[Eolvasom](#)

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



LinkedIn



Instagram



Facebook



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

Statisztikai adatok

2024.12.13.-2024.12.19.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Elosztott szolgáltatásmegtagadás (DDoS)

Nem-adminisztrátori fiók kompromittálódása

Behatolási kísérlet

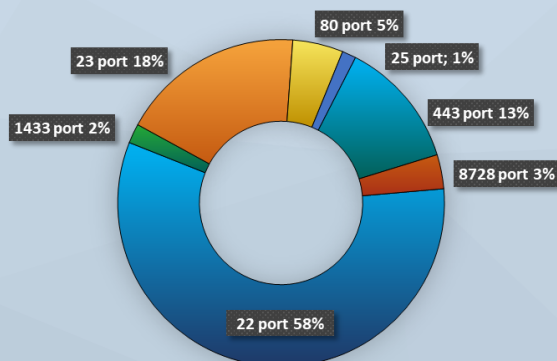
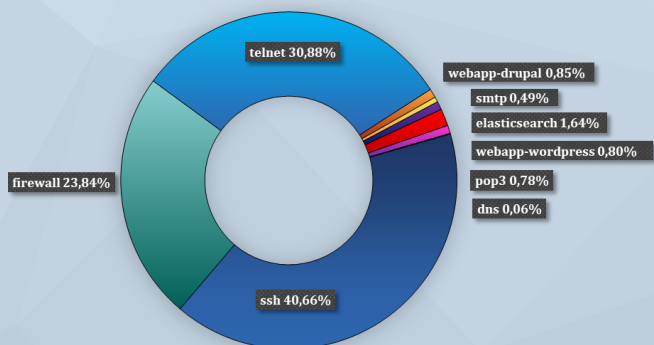
Információgyűjtés

Káros tevékenység

■ Alacsony ■ Közepes ■ Magas ■ Kritikus

Incidensek eloszlása típus és kockázati besorolás szerint

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



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