NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 7. hét

HÍREK

- Ransomware támadás miatt 21 romániai kórház offline üzemmódba kényszerült
- A Roundcube sebezhetőség aktív kihasználását jelentette a CISA
- 200 ezer sornyi Facebook Marketplace felhasználói adat szivárgott ki egy fórumra
- A Microsoft és az OpenAI együtt lép fel az APT-csoportok ellen
- A RustDoor macOS malware Visual Studio frissítésként terjed

SÉRÜLÉKENYSÉGEK

- Riasztás Microsoft termékeket érintő sérülékenységekről
- Tájékoztatás Adobe szoftverek sérülékenységeiről

STATISZTIKAI ADATOK

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

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági

HÍREK

Ransomware támadás miatt 21 romániai kórház offline üzemmódba kényszerült

(bleepingcomputer.com)

Legalább 21 romániai kórház került offline állapotba, miután egy zsarolóvírus támadás leállította az egészségügyi irányítási rendszerüket. A román Nemzeti Kiberbiztonsági Igazgatóság (DNSC) közleménye szerint a támadók a Backmydata zsarolóprogramot használták a kórházak adatainak titkosítására. **Bővebben...**

A Roundcube sebezhetőség aktív kihasználását jelentette a CISA

(bleepingcomputer.com)

A CISA arra figyelmeztet, hogy a Roundcube e-mail szerver szeptemberben már javított sebezhetőségét most aktívan kihasználják cross-site scripting (XSS) támadásokban. A sebezhetőség az 1.4.14-nél újabb, 1.5.4 előtti és 1.6.3 előtti verziókat futtató Roundcube e-mail szervereket érinti. **Bővebben...**

200 ezer sornyi Facebook Marketplace felhasználói adat szivárgott ki egy fórumra

(bleepingcomputer.com)

A kiszivárgott rekordok sokféle személyazonosításra alkalmas adatot tartalmaznak, többek között neveket, telefonszámokat, e-mail címeket, Facebook azonosítókat és profilinformációkat. A kiberbűnözők ezeket a típusú adatokat általában adathalász-támadásokhoz használják fel. **Bővebben...**

A RustDoor macOS malware Visual Studio frissítésként terjed

(bitdefender.com)

A Bitdefender kutatói egy új, MacOS felhasználókat célzó backdoort fedeztek fel. Ez a korábban nem dokumentált malware Rust nyelven íródott, és számos érdekes funkciót tartalmaz. A kutatók RustDoor néven követik nyomon. **Bővebben...**

Microsoft

OpenAI

A Microsoft és az OpenAI együtt lép fel az APT-csoportok ellen

(securityweek.com)

A Microsoft szerdán megjelent kutatásából kiderül, hogy az OpenAI-jal együttműködve tanulmányozták a **nagy nyelvi modellek (LLM)** fenyegetési aktorok általi használatát, és több ismert APT-t találtak, amelyek a népszerű ChatGPT-t próbálták felhasználni annak érdekében, hogy információt szerezzenek a potenciális áldozataikról.

Bővebben...

SÉRÜLÉKENYSÉGEK

Riasztás Microsoft termékeket érintő sérülékenységekről

A Microsoft 2024. február havi biztonsági csomagjában összesen **73** különböző **biztonsági hibát javított**, köztük **5 kritikus** kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kódfuttatást, szolgáltatásmegtagadást, jogosulatlan adathozzáférést és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren. A javított sérülékenységek között **2 db nulladik napi (zero-day)** sebezhetőség található.

CVE-2024-21351
Windows SmartScreen Security Feature Bypass Vulnerability

CVE-2024-21412
Internet Shortcut Files Security Feature Bypass Vulnerability

A sebezhetőségek patchelése MAGAS prioritású, mivel adathalász technikával (e-mail csatolmány segítségével) felhasználható káros kóddal történő fertőzésre. A Trend Micro biztonsági közleménye szerint legalább egy **APT** csoport (**DarkCasino (Water Hydra)** aktívan ki is használta a sebezhetőségeket a **DarkMe** elnevezésű káros kód terjesztésére.

Bővebben...

Tájékoztatás Adobe szoftverek sérülékenységéről

Összesen **30 különálló CVE számmal rendelkező sérülékenység** került javításra, ezek közül **16 kritikus**, **13 db magas** és **1 db közepes** kockázati besorolású.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítésen keresztül, valamint manuálisan is letölthetők a gyártói honlapokról.

Bővebben...

További tájékoztatókért, látogasson el **weboldalunkra**!

Aktuális tartalmak

KiberPajzs
Védelem a pénzügyekben

NEMZETI KIBERVÉDELMI INTÉZET

A romantikus csalás

CTI jelentés

A Nemzeti Kibervédelmi Intézet Valentin-nap alkalmából egy gyakori csalási formára szeretné felhívni a figyelmet.
Jelen dokumentum célja, hogy bemutassa a romantikus csalások legfőbb jellemzőit, jellegzetességeit, fajtáit, megelőzésére tanácsokat adjon és néhány esettanulmányt tárjon az olvasó elé.

Mik az intő jelek?

Hogyan védekezzünk?

Mit tehetünk, amikor rájövünk, hogy átvertek?

Elolvasom

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

Nemzeti Kibervédelmi Intézet

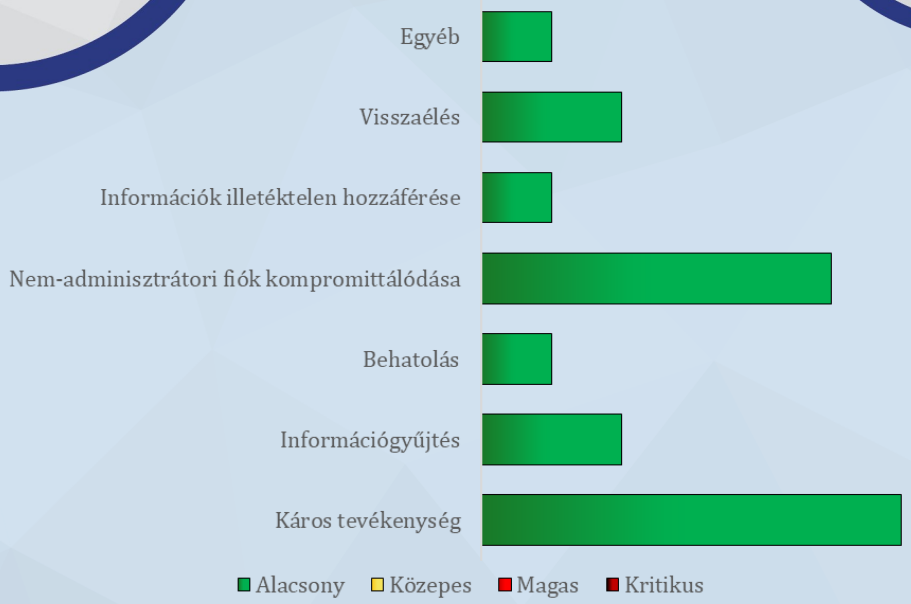
@nki.gov.hu

Statisztikai adatok

2024.02.09-2024.02.15.

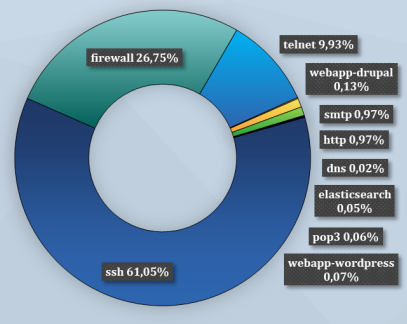
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

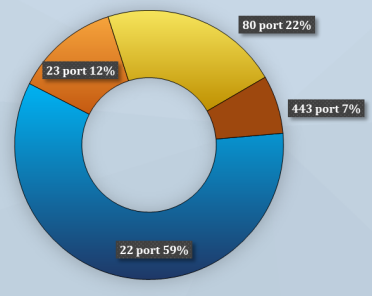
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!