NEMZETI KIBERVÉDELMI INTÉZET

# HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 2. hét

## HÍREK

- Aktuális csaló kampány: a kiberbűnözők most a Microsoft nevében telefonálnak
- Hackerek a Microsoft SQL szervereket veszik célba a Mimic zsarolóvírus támadásokban
- Szíriai hackerek malware-t terjesztenek a kiberbűnözőknek
- A Sea Turtle a holland internet és telekommunikációs szolgáltatókat támadja
- Megjelent a Babuk zsarolóvírus dekódolója, miután letartóztatták a hackereket

## SÉRÜLÉKENYSÉGEK

- Riasztás Ivanti termékeket érintő 0. napi kritikus sérülékenységekről
- Riasztás Microsoft termékeket érintő sérülékenységekről

## 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

## Hackerek a Microsoft SQL szervereket veszik célba a Mimic zsarolóvírus támadásokban

**(bleepingcomputer.com)**

Pénzügyi motivációjú török hackerek egy csoportja világszerte Microsoft SQL (MSSQL) szervereket vesz célba, hogy az áldozatok fájljait Mimic (N3ww4v3) zsarolóprogrammal titkosíthassák. **Bővebben...**

## Szíriai hackerek malware-t terjesztenek a kiberbűnözőknek

**(thehackernews.com)**

Az Anonymous Arabic néven működő kiberbűnözői csoport kifejlesztett egy új távoli hozzáférést biztosító szoftvert (Remote Access Trojan – RAT), amely biztonsági szoftverek megkerülésére és különböző rejtett alkalmazások elindítására is alkalmas. **Bővebben...**

## A Sea Turtle a holland internet és telekommunikációs szolgáltatókat támadja

**(bleepingcomputer.com)**

A török állam által támogatott, Sea Turtle nevű csoport több kémkedési akciót is végrehajtott Hollandiában, amelyek a távközlési vállalatokra, a médiára, az internetszolgáltatókra (ISP-kre) és kurd weboldalakra összpontosítottak. **Bővebben...**

## Megjelent a Babuk zsarolóvírus dekódolója, miután letartóztatták a hackereket

**(bleepingcomputer.com)**

Sikeresen elfogták a Babuk zsarolóvírus mögött álló kiberbűnözőt Hollandiában. A Cisco Talos kutatói a holland rendőrséggel közreműködve megszerezték a Babuk Tortilla nevű zsarolóvírus visszafejtő szoftverét. **Bővebben...**

## Aktuális csaló kampány: a kiberbűnözők most a Microsoft nevében telefonálnak

Az elmúlt napokban az NBSZ NKI-hoz érkezett bejelentés a Microsoft nevével visszaélő angol nyelvű telefonhívásokkal kapcsolatban.
**Bővebben...**


# TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

## Riasztás Microsoft termékeket érintő sérülékenységekről

A Microsoft 2024. január havi biztonsági csomagjában összesen 49 különböző biztonsági hibát javított, köztük 2 kritikus kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kódfuttatást, szolgáltatásmegtagadást és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren. A javított sérülékenységek között nem szerepelt támadásokban már aktívan kihasznált nulladik napi (zero-day) sebezhetőség.

**Bővebben...**

## Riasztás Ivanti termékeket érintő 0. napi kritikus sérülékenységekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) riasztást ad ki az Ivanti Connect Secure és az Ivanti Policy Secure szoftvereket érintő 0. napi, kritikus kockázati besorolású sérülékenységek kapcsán, azok súlyossága és aktív kihasználása miatt.

**CVE-2023-46805**

**CVE-2024-21887**

**Bővebben...**

# Statisztikai adatok

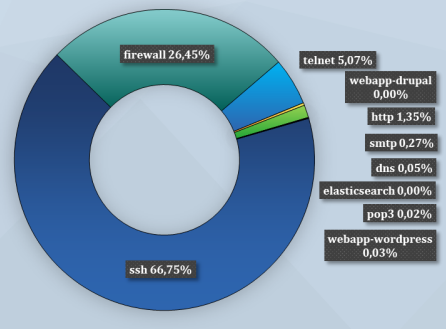
2024.01.05.-2024.01.11.

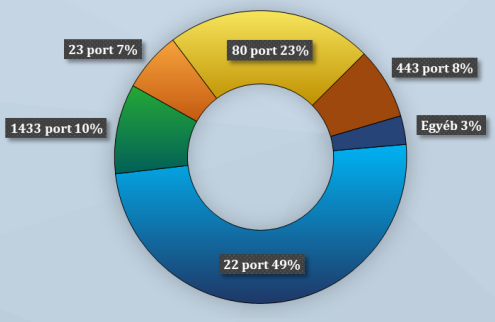
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony


## Incidensek eloszlása típus és kockázati besorolás szerint

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




További információkért, látogasson el **weboldalunkra**!