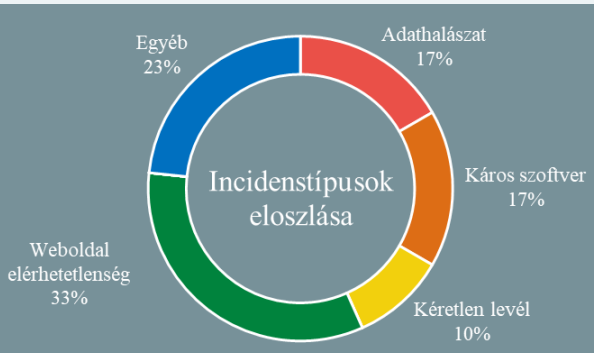
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 15. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.04.08. - 2022.04.13.



Kövessen minket weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Már nem csak Office fájlokkal fertőz a Qbot botnet

(bleepingcomputer.com)

Az NBSZ NKI nemrég riasztásta dott ki a Qbot botnet terjedésével kapcsolatban, amely egy moduláris felépítésű trójai, ami különböző szenzitív adatok megszerzésére tesz kísérletet, mint például a banki adatok. Kiemelt fenyegetést jelent többek között azért, mert a malware kifejezetten agresszívan igyekszik továbbterjedni a hálózaton, brute force támadás alá vonva az Active Directory admin fiókokat, új változatai pedig már **zsarolóvírusok** telepítésére is alkalmasak. **Bővebben...**

A bank ügyfélszolgálata helyett a kiberbűnözőket kapcsolja a hívás során egy új androidos trójai

(bleepingcomputer.com)

Fakecalls-nak nevezik azt az új androidos banki trójai programot, amely képes a felhasználó által indított banki ügyfélszolgálati hívást átirányítani a rosszindulatú program készítőihez. A Fakecalls egy népszerű banki mobilalkalmazásnak álcázza magát, működése során pedig képes az általa megszemélyesített bank telefonszámát, sőt még a hivatalos logót és egyéb arculati elemeit is megjeleníteni. Mikor az áldozat hívást kezdeményez a bank irányában, a káros program megszakítja a kapcsolatot, megjeleníti a bank telefonszámát a fertőzött eszköz képernyőjén, és átirányítja a felhasználót a kiberbűnözőkhöz. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az admin fiókokkal kapcsolatos kockázatokról olvashat bővebben...

A Sandworm APT csoport sikertelen kibertámadást hajtott végre egy ukrán energiaszolgáltató ellen

(bleepingcomputer.com)

Az ESET és az ukrán nemzeti CERT-tel (CERT-UA) jelzése szerint a Sandworm orosz állami kötődésű hacker kollektíva április 8-án kibertámadást indított egy ukrán energiaszolgáltató ellen az ipari vezérlőrendszerekre (ICS) specializált Industroyer malware, és a CaddyWiper adattörlő új verzióival. A kifejezetten ICS rendszerek ellen készített hírhedt Industroyer káros kód 2016-ban már okozott áramszünetet, akkor körülbelül Kijev egyötöde maradt áram nélkül egy órán keresztül. **Bővebben...**

DDoS támadás ért több finn kormányzati weboldalt

(securityaffairs.co)

Április 8-án elosztott szolgáltatásmegtagadással járó (DDoS) támadás sújtotta a finn Védelmi- és Külügyminisztérium weboldalait, miközben Volodimir Olekszandrovics Zelenszkij ukrán elnök beszédet tartott a finn parlamenti képviselőknek. A támadás dél körül kezdődött, és nagyjából egy órán át tartott ─ olvasható a finn kormányzat közleményéből. Bár a kormány hivatalosan nem kötötte Oroszországhoz az akciót, szakértők szerint a támadás mégis összefüggésben állhat azzal, hogy Finnország támogatás ajánlott fel Ukrajnának és elítéli az orosz inváziót.

Újabb aktívan támadott sérülékenységek a CISA listájában, a Watchguardot is kötelező javítani

(securityweek.com)

Újabb nyolc sérülékenységgel bővült az Egyesült Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynöksége (CISA) által gondozott, **aktívan kihasznált** sérülékenységekről vezetett lista. Többek között a Watchguard tűzfal termékek (WatchGuard Firebox és XTM) Fireware OS sebezhetősége (CVE-2022-23176) is felkerült a katalógusba, amelyet orosz állami szponzorálású fenyegetési szereplők a nemrég lekapcsolt **Cyclops Blink** botnettel támadtak. **Bővebben...**