TLP:WHITE

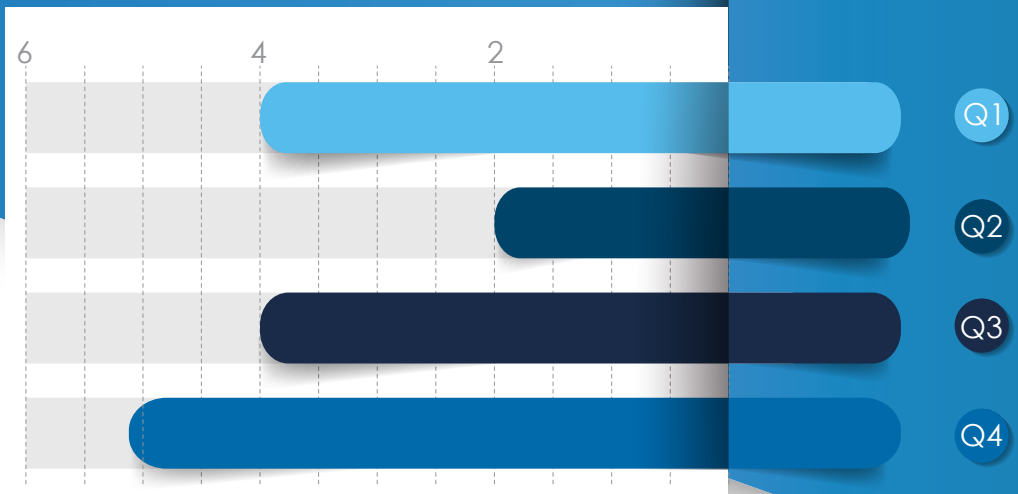
EURÓPAI FENYEGETETTSÉGI HELYZETKÉP 2022 Q1

NEMZETI KIBERVÉDELMI INTÉZET

Európai Uniós intézményeket, testületeket és ügynökségeket (EUINT) érintő közvetlen kiberfenyegetések

INCIDENSEK

2022 Q1 során az EUINT szervezeteket 4 jelentős incidens érintette.
Kettő esetben a támadók érvényes hitelesítőadatokkal fértek hozzá online platformokhoz.
A másik kettő incidens során a támadók Microsoft Web Services (EWS) rendszerek ellen hajtottak végre brute force támadást.



JELENTŐS INCIDENSEK 2021-BEN, AMELYEK EUINT-EKET ÉRINTETTEK

FENYEGETÉSEK

- Több, mint egy tucat EUINT ellen hajtott végre password spraying kampányt egy fenyegetési szereplő, amelyek Microsoft Exchange szolgáltatásokat céloztak.
- Legalább 7, EUINT-ek ellen végrehajtott adathalász kampány köthető állami támogatású fenyegetési szereplőkhöz.

A CERT-EU összesen 42 riasztást adott ki 2022 Q1 során.

- Ennek közel háromnegyede kiberkémkedési aktivitáshoz volt köthető.
- Háromnegyed részük adathalász témájú volt.
- A jelentett kibertámadások 23%-a esetében diplomáciai entitás (nagykövetség, delegáció, vagy harmadik országbeli képviselők) került célpontba, ami egy példátlan számadat.
- Valószínűsíthető, hogy az Európai Uniós kormányzati entitásokat célzó kiberhírszerzési műveletek száma az Ukrajna elleni háború hatására emelkedett.

Forrás: CERT-EU, CERT for the EU Institutions, Bodies, and Agencies https://cert.europa.eu

TLP:WHITE

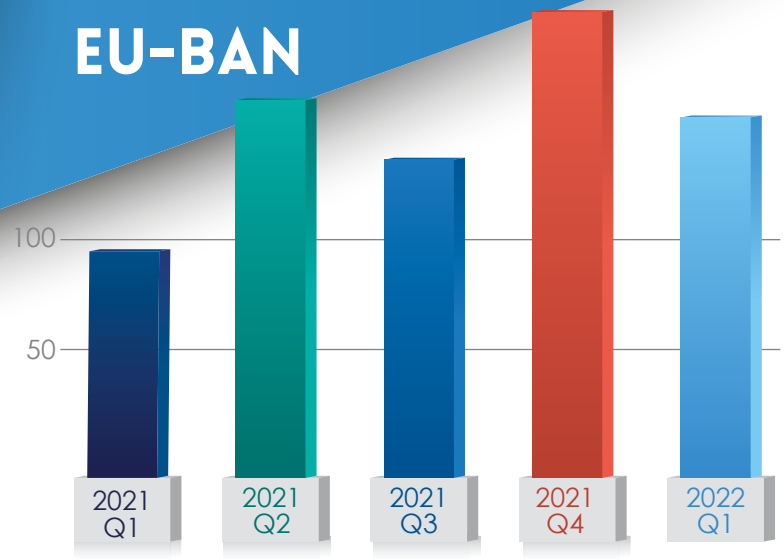
TOP FENYEGETÉSI SZEREPLŐK

- A CERT-EU 11 kiemelt fenyegetési szereplőt (TTA) követ figyelemmel.
- Közülük 7 — valószínűsíthetően kínai vagy orosz hátterű — volt aktív EUINT-ek ellen az első negyedév során.
- A további 4 az EU közelében, vagy teljesen más régióban volt aktív.
- Továbbá EUINT-ek nem kiemelt fenyegetési szereplők műveleteinek is céltáblájául szolgáltak:
- Ezek közül 4 nagy valószínűséggel állami támogatású csoport, 3 kiberbűnözői volt, 2 esetében pedig ismeretlen a motiváció.

TECHNIKÁK

- Brute force / passwords spraying támadások nagy számban fordultak elő Microsoft Exchange szerverek ellen.
- Legalább 7 EUINT ellen történt megszemélyesítéses támadás. Legalább 5 EUINT detektált olyan támadást, amelynek során legitim Microsoft Teams üzenetek voltak a megszemélyesítés eszközei.

ZSAROLÓVÍRUS ÁLDOZATOK AZ EU-BAN



FENYEGETÉSEK EURÓPÁBAN

- **Ukrajnai háború.** Összességében az európai kiberincidensek túlnyomó részét az ukrajnai háborúval összefüggésben álló kiberbiztonsági esetek jelentették. Az egyik leginkább kiemelkedő esemény a KA-SAT műholdas internet szolgáltatás elleni februári kibertámadás volt, ami Európa több részén is zavart keltett. Az Ukrajnában történt kibertámadások internetszolgáltatók és kritikus infrastruktúrák ellen irányultak, szándékos károkozási célú (wiper) vagy szenzitív információk megszerzésére szolgáló káros kódok felhasználásával. A korlátozott hatásfokú elosztott túlterheléses (DDos) támadások leginkább a figyelem elterelésére szolgáltak.
- **Kiberkémkedés.** Több fenyegetési csoport is aktív volt Európa-szerte, többségük Oroszországhoz köthető, azonban egy kínai kiberkémkedési műveletre is fény derült, amely az ukrajnai orosz invázió témáját használta fel csaliként.
- **Kiberbűnözés.** A zsarolóvírus maradt a legjelentősebb kiberbűnözési fenyegetés az EU tekintetében.