TLP: WHITE
Szabadon terjeszthető!

Tájékoztatás kormányzati és pénzügyi szektorokat érintő DDoS támadásokkal kapcsolatban

(2020. szeptember 08.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatást ad ki a **kormányzati és pénzügyi szektorokat érintő DDoS támadásokkal kapcsolatban.** Az NBSZ NKI nemzetközi partnereitől a közelmúltban több jelzés érkezett olyan, nagy volumenű DDoS támadásokkal kapcsolatban, melyek jellemzően a kormányzati és pénzügyi szektorokat, valamint a digitális szolgáltatókat, jellemzően internetszolgáltatókat (ISP) ért. Az elmúlt hetekben több európai ország is jelzett hasonló támadásokat, melyek mértéke egyes esetekben elérte a 500Gbps átviteli sebességet, több, mint 200.000 forrás IP cím felhasználásával.

A DDoS támadásokkal párhuzamosan több jelzés is érkezett olyan zsarolási kísérletekről, melyek jellemzően a Lazarus, vagy a Fancy Bear néven ismert APT csoportok nevével visszaélve követelnek váltságdíjat annak érdekében, hogy a megzsarolt intézményt ne érje DDoS támadás. Egyes esetekben a zsarolást egy kisebb volumenű (40 Gbps) támadás követte.

A két jelenség között egyelőre nem sikerült egyértelmű kapcsolatot azonosítani, mindazonáltal az NBSZ NKI javasolja ügyfeleinek, hogy fokozott óvatossággal járjanak el, amennyiben hasonló zsarolási kísérletet észlelnek.

Indikátorok:

Feladó e-mail címe: fufisobur1981@protonmail.com
Feladó e-mail címe: letxchahandca1973@protonmail.com
Feladó IP címe: 185.70.40.140
BTC tárca: 1CK9aiTNK73FUDw9iJawoAhdJEQVy7Pxir

Az NBSZ NKI felkéri tisztelt ügyfeleit, amennyiben a fentiekhez hasonló támadást vagy zsarolási kísérletet észlelnek, jelezzék azt az NBSZ NKI incidensbejelentéseket fogadó alábbi elérhetőségein!

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu