TLP:WHITE
Szabadon terjeszthető!

Tájékoztatás terjedőben lévő csalási módszerről
(2016.08.05.)

Tisztelt Ügyfelünk!

A Kormányzati Eseménykezelő Központ saját ügyfélkörből valamint nemzetközi partnerektől származó információk alapján tájékoztatást ad ki egy, az utóbbi időben tapasztalt csalási módszerről, amellyel a támadók több esetben sikeresen utaltattak pénzt saját bankszámláikra.

A csalók az általuk különböző módszerekkel feltérképezett vélt vagy valós üzleti kapcsolatok mentén kísérelnek meg pénzhez jutni, melyhez az alábbi módszereket használják:

1. Nyílt adatforrásokból (OSINT), például a szervezet saját weboldaláról kapcsolati információkat szereznek a számlabefogadó cég pénzügyi részlegén dolgozó vezetőkhöz, munkatársakhoz.
2. Létrehoznak egy domain-t, amely a számlakibocsátó céghez tartozó domain névvel kezdődik (pl. acme.hu alapján acme-hu.com), vagy ahhoz nagyon hasonló (pl. amce.hu). A családhoz létrehozott domain-hez álcázási célból weboldalt is készítenek. A honlap általában a megszemélyesített cég oldalára irányít át, azt a látszatot keltve, hogy a létrehozott domain is a számlakibocsátó céghez tartozik.
3. A számlabefogadó cég megfelelő szintű munkatársainak megtévesztő elektronikus levelet küldenek a csaló domain felhasználásával, melyhez mellékelhetnek egy számlát, vagy kérhetik a korábban megadott számlainformációkban bekövetkezett változások átvezetését (a megszemélyesített számlakibocsátó cég számlaszámát átíratják az általuk kívántra).
4. Ha a körülmények a csalóknak kedvezőek, pl. szabadságolási/helyettesítési időszakok idején, illetve ha megfelelő szintű személyt (CEO, CFO) találnak meg a levelükkel, akkor a csalók célt érhetnek.

A módszer észlelése érdekében a Kormányzati Eseménykezelő Központ az alábbiakat javasolja számlakibocsátó illetve számlabefogadó szervezetek számára:

- Javasolt folyamatosan monitorozni a szervezetek weboldalainak hozzáférési naplóját (access log), melyekben „HTTP Referer”-ként a fenti módon létrehozott domaint kell keresni.
- A számlabefogadó szervezetek levelező szervereinek napló állományában is felfedezhetők a csaló domain-ekről érkező levelekkel. Olyan bejegyzésekre javasolt

szűrni, amelyekben a beszállítói körükbe tartozó cégek domain nevéhez hasonló kifejezés szerepel a feladó mezőben.

Amennyiben a fenti vizsgálatok elvégzéséhez szakmai támogatásra van szüksége, kérjük, forduljon a GovCERT-hez az alábbi elérhetőségeken.

Kérjük, hogy ha a fenti vizsgálatok a csalási szándékot alátámasztják, úgy haladéktalanul tegyenek incidensbejelentést a GovCERT felé.

A hasonló visszaélések elkerülése érdekében javasoljuk továbbá az érintett területek munkatársai számára a csalási módszerekkel kapcsolatos időszakos tájékoztatást, folyamatos információbiztonsági tréningek szervezését valamint a tranzakciók jóváhagyása esetén „a négy szem elv” folyamatos alkalmazását.

Nemzeti Kibervédelmi Intézet
Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu