TLP:WHITE
Szabadon terjeszthető!

Riasztás
Qbot malware kampányról
(2022. április 01.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **Qbot (más néven Quakbot/Pinkslipbot) terjedésével kapcsolatban**. Az NBSZ NKI tapasztalatai alapján a malware terjesztésére irányuló e-mail tevékenység az elmúlt időszakban ugrásszerűen megemelkedett. A **Qbot** egy moduláris felépítésű trójai, amely 2008 óta van jelen. Elsősorban különböző szenzitív adatok megszerzésére tesz kísérletet, mint pl.: banki adatok, böngészőben mentett adatok, különböző azonosítók, azonban billentyűzetfigyelési funkcióval is rendelkezik. Új változatai **zsarolóvírus telepítésre is alkalmasak**, elsősorban az *Egregor* ransomware-vel hozható összefüggésbe.

A **Qbot** terjesztése jellemzője fertőzött **Office dokumentumokkal** történik, a jelenleg futó kampányban Excel állományokon keresztül kísérlik meg telepíteni a káros tartalmat. A **Qbot** jellemzője, hogy terjesztése során **korábban megszerzett e-mail üzenetek** kerülnek felhasználásra, amelyre „válasz”-ként küldik a káros tartalom eléréshez szükséges URL-t. A levelekben az URL dinamikusan változik, illetve egy négykarakteres jelszót tartalmaz, amely az állomány futtatásához szükséges. Jelen esetben a felhasznált levelek megszerzése vélhetően a 2021. 11-12. hónapban történt, a Microsoft Exchange szerverek egyes változatait érintő sérülékenység kihasználásával.

Fontos tudni, hogy a feladó – Intézetünk tapasztalatai alapján – **minden esetben hamisított**, az eredeti levelezéshez hozzáfűzött kiegészítés pedig jellemzően nyelvtanilag hibás, magyartalan megfogalmazással készült.

Az NBSZ NKI az eset kapcsán javasolja a kapcsolódó indikátorok tiltást a határvédelmi rendszeren.

TLP:WHITE
Szabadon terjeszthető!

IoC-k:

- SHA256: 5954bf97fdde4d060c829258fe5f19b91161b8df5b85933cdc3def2cf6c150b1
- SHA256: 7c0f2e52846584547bb42fa9460dce37097334a4370f389c62281880a47fe63d
- SHA256: 9fcefa8fe0b52b1b46d166ebcd4ccaa00583ec4d67b6bd961925b022824d5cd8
- SHA256: 7a7b21534d62cd6f3660d998c97149e865875d2e650aac28385e86449a25b280
- SHA256: e3296366bc2fa1fb8d737f674c77196cbd978cf975bba2ff7eb03dd193ec1fbe
- SHA256: 9e064a4c60f5738cd020dc615b422af461d2d188dafd2cea9f2118a9b5ca4e0d
- SHA256: d2d994becc9c471eefd5ab7e0ea4e8d6d8b36bdfb5dab15d2a522442aef649b9
- SHA256: 69998b47d29db39339b7c6cbe0489fff87245f33009921c36992ce4b757474fe
- SHA256: 4c998351051ee903a3f00dd24feb5608548ace31d252bc93bbd83a47c433f728
- SHA256: f3356281469930106916192e0ff653b784a6f9a548b0bc1ccee4f3d0dfa854f5
- SHA256: d180eff6bc063c732d26d6408eab3c0b244cbd421aca6c5fdd152b2b2b996725
- SHA256: f475466d67bdc6ea9f816cf1efe5bdafbb3fce131702d76480f212e397362979
- SHA256: 240b4c43ba1f2ecc9a1fa328b30bb088369efc53c96883a7e5b5e22b715f66fd
- SHA256: 6a6410c4d722720e56f4af781bec3ce667b2a8600f7aa4a582ec0f83e86ebbca
- SHA256: 989026428c073b83ad49b9b22e33c610ef8e865c7ef943eee97704eda3ce0b75
- renwinautovaluers[.]com
- buy-100mgviagra[.]com
- timeinindianow[.]com
- 207[.]174[.]212[.]128
- 162[.]241[.]123[.]45

TLP:WHITE
Szabadon terjeszthető!

További, kockázatcsökkentő / megelőző intézkedések:

- Makrók futtatásának tiltása.
- Felhasználók tudatosítása, különös tekintettel, ha a beérkezett levél jóval korábbi (tavalyi) levelezésre érkezik válaszként.
- **Határvédelmi rendszerek szoftvereinek naprakészen tartása.**
- **Alkalmazások és operációs rendszerek naprakészen tartása.**
- **Határvédelmi eszközök feketelistájának frissítése** (több gyártó rendelkezik nyilvánosan elérhető listákkal pl.: Cisco), ezáltal csökkentve a támadás kockázatát.
- Rendszeres online és **offline** (szalagos egység, külső merevlemez) **biztonsági mentés**, archiválás.

Biztonsági incidens bekövetkezése esetén az NBSZ NKI javasolja:

- Az érintett eszköz **hálózatról** történő **leválasztás**át.
- Az érintett adathordozók helyreállítása előtt **bitazonos másolat készítését**.
- **Incidens bejelentését** az NBSZ NKI részére a CSIRT@nki.gov.hu e-mail címen.

További hivatkozások:

- https://nki.gov.hu/figyelmeztetesek/karos-kod/egregor-ransomware-leiras/
- https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/
- Közigazgatási Kibervédelmi Eszköztár
- Biztonsági mentés

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