TLP:WHITE
Szabadon terjeszthető!

Riasztás

Emotet malware kampánnyal összefüggésben

(2022. június 15.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **Emotet malware terjedésével kapcsolatban**. Az NBSZ NKI tapasztalatai alapján a malware terjesztésére irányuló e-mail tevékenység az elmúlt időszakban ugrásszerűen megemelkedett. Az **Emotet** egy moduláris felépítésű trójai, amely 2014 óta van jelen. Elsősorban szenzitív adatok megszerzésére tesz kísérletet, mint például banki adatok, böngészőben mentett adatok, különböző azonosítók, emellett billentyűzetfigyelési funkcióval is rendelkezik, és **zsarolóvírus telepítésre** is alkalmas. Egyes változatai az áldozat postafiókjának felhasználásával terjesztik tovább a malware-t.

Az **Emotet** terjesztése jellemzően fertőzött MS Office dokumentumokkal történik, a jelenlegi kampányban a támadók elsősorban **Excel állományokon** keresztül kísérlik meg telepíteni a káros tartalmat. Az **Emotet** ezen variánsának egyik jellemzője, hogy terjesztése során korábban megszerzett e-mail üzenetek kerülnek felhasználásra, amelyre „válasz”-ként küldik a káros tartalmú e-mailt. A levelekben jelszóvédett ZIP állomány található, illetve a kibontáshoz szükséges jelszót is tartalmazza, amely az állomány futtatásához szükséges.

Fontos tudni, hogy a feladó – Intézetünk tapasztalatai alapján – minden esetben hamisított.

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

TLP:WHITE
Szabadon terjeszthető!

IoC-k:

- SHA256: 26b2882818d7770891f8575fa07867db07e124178d0e09398a4f0b89c9373af9
- SHA256: 4d5962ace9c2bd95791ea49700d42b81cc72b59185e37c92fee2b7c588415674
- SHA256: b0442f61bd6e0abf13f7ed06e278e1cdf5340c17a9a0979c679fe30cb93830de
- SHA256: 597d54d0f8fe09ca1e412e86f1ed9788ab9c67cca08411f2043e9ca2f941e584
- SHA256: 1a6c1fef8c949dcf2c2e8f50529e3ef887dd864e6368a59947edcbcf50919f37
- SHA256: ebc11c680c8960dfbebcaa20740172db6194133c0cf498f13405a9b365d4f140
- SHA256: a1708a6558d4694df6c1895c7654cbddb4506dab74c86ef78fe940274acb2f4b
- SHA256: d20e172af33add124675da7980d8b89277048356ec3aa617f9b5cf8d509c46f1
- SHA256: fbcba24f92756db5f1bce80dbc40b9f8c5629d871f72f5bc5336ad5e644c10ef
- SHA256: c76c145a73029f6b4e2c65038e662328308119b16c5e805aaa3bcddd863e19d4
- SHA256: 12d9abba0bf4d1a072a518a6ff32294d56767b9ff7c1eb1f2071825cbd0c2d19
- SHA256: 3ed857c10d33a53a252c09fa818eedecaeb598d0f644ac3d6ec2cff8b1f6f523
- SHA256: ca800f4812c2558e8dfc323a1c88d012949c4603479fc6830cd41f7ef7d62924
- SHA256: 0803c2c31d0a6832bce8ded87b15cda95b8c6ce4dc703f36958dfb9575c9f4af
- SHA256: 3f95a725e08025663845bca57409dab94264d437998839bb4ad6fcdce8c56ed5
- SHA256: 2e57fb4cc6836cc78ce9c3e0574f08e80e70c5f61b5db85db769d09dba8a0738
- SHA256: a7f261c74ba04e91f8215d3c1857935a7e4898564169cab7cb64d77b6f43b627
- SHA256: d2073c834d42b1debed020585d8376e326a4ab0dbb7ab121cf108197c90c1746
- SHA256: ae0f819c7fd9de6f41b9663a2d45495ef9714914ea2915836173e5db102de7e5
- SHA256: b2df036395587685c4f16ed516aaf5e55f54de0de7e443adac45bbf186830824
- SHA256: 859af4fbf7fde72f4a6c2dbe23ba65aff9762b36383436615a6c2f85c2693268
- SHA256: f9e265a7660e3d54b12c9ec9b7f9aff04e1217e705ae7c69809caf44170261b1
- SHA256: efac2bbbedb0ce1d4170d184ca471897f57eb8fc3d92ec253c9dafb4aeddb2ae
- SHA256: 2b8d3693b5919bc17bda4da2a38afecd326e353e6d88ea1d3d99c1746d163ad9
- SHA256: 529d70448ed5cdc0e6bb89432214e880bd53f3fc2ea9117f5a9f9262d5bdd852
- SHA256: 3222e79f5792e7f95782d3c41371c78f455ed200bb48e08cc0ccdc5feb370781
- SHA256: 620ca25390834d7f3ab3606e586f9c6ee76faea9261c27341c2c1ddc709949ed
- SHA256: 824c316a8de6dcd94c54f65e0191dc1a4655ddb31b45e2d4e1971ff0ea40aa82

- SHA256: e8385e853408eb414c1744770b1f1584c7a34ffaaf08f857761b50f1ed806660
- SHA256: 14bcb00e3dccfd1a9bfbc70c257d427d4d1ff722f22f6b8d7ebdbcd317d3e746
- SHA256: 8cf3b70bf816bdbb7cad61aad71ab0d52298779da5d2a09237039e19d712e090
- SHA256: f78ac98c6c2d5af1542c2516f26e6af6c0e186bca4a17592e8fb732a6dcf3af5
- SHA256: 8cd6b8f459d147c5d99cba422527224071b72980b04881c51b9a0978b9c4c3c3
- aacl[.]co[.]in
- agir-santeinternationale[.]com
- agretto[.]com
- ahan[.]org[.]pk
- alpsawnings[.]co[.]za
- alrotec[.]co[.]uk
- alzheimerzamora[.]com
- andecam[.]com[.]ar
- ftp.yourbankruptcypartner[.]com
- ftp[.]yuecmr[.]org
- iluminaguarapuava[.]com[.]br
- kbmpti[.]filkom[.]ub[.]ac[.]id
- macssolutions[.]co[.]uk
- mass-gardinen-shop[.]de
- nazreghadir[.]ir
- nicolassportafolio[.]atwebpages[.]com
- nrc-soluciones[.]com[.]ar
- tvstv.yunethosting[.]rs
- upscalifornia[.]us
- usa-ltd[.]ie
- vanlaereict[.]nl
- wahkiulogistics.com [.]hk
- webbandi[.]hu
- webnet[.]ltd[.]uk/

- wolffram[.]dk
- wordpress[.]agrupem[.]com
- www[.]hangaryapi[.]com[.]tr
- www[.]zvdesign[.]info
- 120.72.119[.]5
- 129[.]232[.]138[.]161
- 14.225.238[.]176
- 144.91.78[.]55
- 145.239.206[.]130
- 157.245.196[.]132
- 159.89.202[.]34
- 162.214.119[.]46
- 168.195.204[.]82
- 172.105.226[.]75
- 175.45.184[.]161
- 178.18.197[.]4
- 178.238.236[.]240
- 179.43.124[.]129
- 180[.]149[.]241[.]246
- 185.176.43[.]112
- 185.98.131[.]156
- 194.247.196[.]66
- 194.38.104[.]132
- 204.11.59[.]91
- 37.17.210[.]93
- 41.73.252[.]195
- 45.186.16[.]18
- 46.23.71[.]2
- 51.161.73[.]194
- 54[.]36[.]167[.]79
- 59.188.217[.]182
- 75.103.114[.]38
- 85.214.64[.]234
- 86.109.166[.]218
- 88.198.100[.]31
- 94.182.227[.]250
- 95.216.42[.]246

TLP:WHITE
Szabadon terjeszthető!

További kockázatcsökkentő / megelőző intézkedések:

- Makrók futtatásának tiltása.
- A felhasználók figyelmének felhívása arra, hogy tekintsék gyanúsnak, amennyiben egy beérkezett üzenet egy jóval korábbi (például 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 **leválasztását**.
- Az érintett adathordozók helyreállítása előtt **bitazonos másolat készítését**.
- **Incidens bejelentését** az NBSZ NKI részére a CSIRT@nki.gov.hu e-mail címen.

További hivatkozások:

- 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