

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι το τελευταίο χρονικό διάστημα παρατηρείται επανεμφάνιση phishing μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν συνημμένο αρχείο μολυσμένο με Emotet.

Σχετικοί σύνδεσμοι:

**α.** [https://threatpost\[.\]com/emotet-resurfaces-trickbot/176362/](https://threatpost[.]com/emotet-resurfaces-trickbot/176362/)

**β.** [https://www.digitaljournal\[.\]com/tech-science/cyber-warning-signs-are-that-emotet-will-return/article](https://www.digitaljournal[.]com/tech-science/cyber-warning-signs-are-that-emotet-will-return/article)

**γ.** [https://www.bleepingcomputer\[.\]com/news/security/here-are-the-new-emotet-spam-campaigns-hitting-mailboxes-worldwide/](https://www.bleepingcomputer[.]com/news/security/here-are-the-new-emotet-spam-campaigns-hitting-mailboxes-worldwide/)

**δ.** [https://www.bleepingcomputer\[.\]com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/](https://www.bleepingcomputer[.]com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/)

Μέθοδοι προστασίας από το Emotet:

- α.** Εγκατάσταση τελευταίων αναβαθμίσεων για τα Microsoft Windows / Office.
- β.** Προσοχή στα ύποπτα emails και στα συνημμένα που μπορεί να περιέχουν.
- γ.** Χρήση ισχυρού password από όλους τους χρήστες και κατά προτίμηση multi-factor authentication.
- δ.** Απενεργοποίηση χρήσης μακροεντολών από αρχεία του Microsoft Office.
- ε.** Δημιουργία τακτικών backups των δεδομένων τα οποία θα αποθηκεύονται σε διαφορετική τοποθεσία από τα κυρίως αρχεία.
- στ.** Χρήση anti-virus λογισμικού.