04/10/2021

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι παρατηρείται μεγάλη αύξηση στις επιθέσεις μέσω διακίνησης μολυσμένων εγγράφων της πλατφόρμας του Microsoft Office. Το ποσοστό των μολύνσεων που διακινούνται μέσω διαδικτύου και αντιστοιχούν σε μολυσμένα έγγραφα MS Office υπερδιπλασιάστηκε φέτος σε σχέση με πέρυσι, αγγίζοντας το 43% του συνόλου των μολύνσεων.

Οι συγκεκριμένες επιθέσεις υλοποιούνται μέσω αποστολής Spam και Phishing μηνυμάτων, εκμεταλλευόμενες τις δυνατότητες που προσφέρουν οι μακροεντολές του MS Office. Για να ξεκινήσει η μόλυνση υπάρχουν δύο προϋποθέσεις: ο χρήστης να ανοίξει το κακόβουλο συνημμένο έγγραφο και οι μακροεντολές του MS Office να είναι ενεργοποιημένες. Στη συνέχεια, η μόλυνση πραγματοποιείται αυτόματα μέσω μακροεντολών.

Το Εθνικό CERT συστήνει:

- Να ενημερωθούν όλοι οι χρήστες να αποφεύγουν να κατεβάζουν και να ανοίγουν συνδέσμους και συνημμένα έγγραφα από μη πιστοποιημένους αποστολείς.
- Στις ρυθμίσεις του MS Office να προεπιλεγεί η απαγόρευση εκτέλεσης μακροεντολών.
- Να ενημερωθούν όλα τα εργαλεία προστασίας που χρησιμοποιούνται και να ελεγχθεί ότι καλύπτουν τις εν λόγω επιθέσεις.

Στους παρακάτω συνδέσμους υπάρχουν αναλυτικότερες πληροφορίες και τεχνικές που χρησιμοποιούνται καθώς και ενδείξεις μόλυνσης (IOCs):

Πληροφορίες:

https://www.hackread.com/malicious-office-documents-malware-downloads/

Τεχνικές και IOCs:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/