13/1/2022

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι έχει παρατηρηθεί η υιοθέτηση ενός νέου τρόπου phishing και διακίνησης malware, η μέθοδος RTF (rich text format) template injection.

Πρόκειται για ένα “weaponized” αρχείο RTF (τύπου .rtf και .doc.rtf), το οποίο ανοίγει με την εφαρμογή Microsoft Word και επιτρέπει στο αρχείο να ανοίξει έναν πόρο URL, αντί για ένα αρχείο προτύπου, επιτυγχάνοντας την ανάκτηση απομακρυσμένων εξωτερικών κακόβουλων payloads, τα οποία στη συνέχεια εγκαθίστανται στα συστήματα των θυμάτων.

Σημειώνεται πως:

1) Τα αρχεία που έχουν παραχθεί με αυτήν τη μέθοδο έχουν χαμηλότερο ποσοστό εντοπισμού από τα γνωστά antivirus engines, συγκριτικά με άλλες σχετικές μεθόδους.

2) Η συγκεκριμένη μέθοδος χρησιμοποιεί αρχεία τύπου .rtf και .doc.rtf, η διακίνηση των οποίων είναι δύσκολο να περιοριστεί. Συνεπώς, για την αντιμετώπισή της ισχύουν οι γενικοί κανόνες προστασίας από phishing: Πρέπει οι χρήστες να είναι ενήμεροι για τους κινδύνους, να έχουν πάντα ενημερωμένο το λογισμικό τους και να μην ανοίγουν αρχεία και emails από αποστολείς που δε γνωρίζουν ή φαίνονται ύποπτοι.

4. Περισσότερες πληροφορίες στους παρακάτω συνδέσμους:

https://www.proofpoint.com/us/blog/threat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread

https://www.zdnet.com/article/hackers-are-turning-to-this-simple-technique-to-install-their-malware-on-pcs/

https://securityaffairs.co/wordpress/125189/hacking/rtf-template-injection-technique.html