24/12/2021

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι κυκλοφορεί αλλοιωμένο Notepad++ πακέτο εγκατάστασης (installer της εφαρμογής) σε ιστότοπους πέρα από την επίσημη ιστοσελίδα.

Το πακέτο εγκατάστασης έχει τεθεί σε κυκλοφορία από ομάδα hacking – κρατικό δρώντα, μη φιλικό προς τη χώρα μας.

Εγκαθίσταται χωρίς δείγματα «αφύσικης» συμπεριφοράς και επομένως είναι δύσκολο να παρατηρηθεί.

Στη συνέχεια όμως, εγκαθιστά κακόβουλο λογισμικό, το οποίο εδραιώνει την πρόσβασή του στο σύστημα και έχει ως σκοπό την κυβερνοκατασκοπεία και συλλογή πληροφοριών.

Για την ασφάλειά σας, προτείνεται η χρήση αποκλειστικά της επίσημης ιστοσελίδας (https://notepad-plus-plus.org/) για μεταφόρτωση του Notepad++, καθώς και έλεγχος του πακέτου εγκατάστασης με το GPG(GNU Privacy Guard) κατά τη μεταφόρτωση.

IOC – hashes:

setup.exe, SHA-256:
7d3192cad53f934173187f91d8555065d69e09b4f127275a1d47f9f1f9405c5c

notepad++ installer, SHA-256:
18107fa059cf457b0b351b683e08e01a3b029ba277f5ca4583a4e3322df21622

winpickr.exe, SHA-256:
1380160229604c7d499372dd8192024451291d8bf54e87f19c9e2077b1f165c6

ntuis32.exe, SHA-256:
ed2eae7c0a6cd81d108d71289a49e4a187078a9a6af8400c6a3253d802a7ac95

Domains - C2 Server: hxxps://advancedtoenableplatform[.]com

Παρακαλούμε για τις ενέργειές σας.