

Πώς μπορούμε να προστατευτούμε ενάντια σε μια επίθεση ransomware;

/ [Επιστήμες, Τέχνες & Πολιτισμός](#)



Η τεράστια επίθεση με ransomware που πραγματοποιήθηκε την περασμένη Παρασκευή προκάλεσε πανικό σε ολόκληρο τον κόσμο, με τις υπηρεσίες και εταιρείες ασφάλειας να προσπαθούν απεγνωσμένα να ανακαλύψουν την προέλευση του ιού, ο οποίος μέχρι στιγμής έχει προσβάλει τουλάχιστον 200.000 συστήματα

ηλεκτρονικών υπολογιστών.

Στόχος της επίθεσης ήταν τα Windows της Microsoft και ιδιαίτερα οι παλαιότερες εκδόσεις του λειτουργικού συστήματος της εταιρείας.

Το ransomware WannaCry, που χρησιμοποιήθηκε κατά την πρόσφατη επίθεση, εκμεταλλεύτηκε μια ευπάθεια σε ένα στοιχείο του Windows Server με αποτέλεσμα ο ιός να εξαπλωθεί εντός των εταιρικών δικτύων, αναφέρει σε δημοσίευσμά της η βρετανική εφημερίδα The Guardian.

Η ευπάθεια είχε αρχικά αποκαλυφθεί στο πλαίσιο μιας μαζικής απόθεσης ευπαθειών λογισμικού που είχε ανακαλύψει η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA) και οι οποίες στη συνέχεια κλάπηκαν από μια ομάδα χάκερς με την ονομασία Shadow Brokers.

Η Microsoft είχε καταφέρει να διορθώσει την ευπάθεια λίγο πριν δημοσιευτούν τα κλεμμένα δεδομένα, κάτι που οδήγησε πολλούς στο συμπέρασμα ότι η NSA ενημέρωσε κρυφά την τεχνολογική εταιρεία σχετικά με την ύπαρξη του ελαττώματος.

Επιπλέον, παρά το γεγονός ότι η Microsoft έχει σταματήσει να παρέχει υποστήριξη για παλαιότερες εκδόσεις του λειτουργικού, όπως τα Windows XP και Server 2003, εντούτοις διέθεσε δωρεάν ενημερώσεις ασφαλείας, οι οποίες μπορούν να ληφθούν μέσω της ιστοσελίδας της.

Αλλά πώς μπορούν οι χρήστες να προστατευτούν από μία επίθεση με ransomware; Καταρχήν, η ευπάθεια δεν υφίσταται στα Windows 10, την πιο πρόσφατη έκδοση του λειτουργικού, αλλά, όπως αναφέρει η Guardian, υπάρχει σε όλες τις εκδόσεις πριν από αυτό (από τα XP και έπειτα).

Έτσι μέσω των ενημερώσεων ασφαλείας που είχε ήδη διαθέσει η Microsoft, οι χρήστες των Windows Vista, 7 και 8.1 μπορούν εύκολα να προστατεύσουν τα συστήματά τους εκτελώντας το Windows Update. Στην πραγματικότητα, τα πλήρως ενημερωμένα συστήματα ήταν προστατευμένα σε μεγάλο βαθμό, ακόμα και πριν την επίθεση της Παρασκευής.

Πολλοί από τους ηλεκτρονικούς υπολογιστές που επηρεάστηκαν, οι χρήστες τους είχαν επιλέξει να καθυστερήσουν την εγκατάσταση των ενημερώσεων ασφαλείας.

Στη συνέχεια, οι χρήστες των Windows XP, Server και 8 μπορούν να προστατεύσουν τα συστήματά τους ενάντια σε μια επίθεση ransomware, εγκαθιστώντας τις νέες ενημερώσεις ασφαλείας που διέθεσε πρόσφατα η Microsoft.

Σημαντικό είναι να γνωρίζουμε ότι όλοι οι χρήστες μπορούν να προστατευτούν από κακόβουλο λογισμικό όντας επιφυλακτικοί με τα συνημμένα που ανοίγουν στα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνουν, καθώς και τους συνδέσμους που πατούν σε διάφορες ιστοσελίδες.

Όλο και περισσότερες πλατφόρμες προστασίας από ιούς, συμπεριλαμβανομένου του Windows Defender, έχουν πλέον τη δυνατότητα να αναγνωρίσουν και να εμποδίσουν την εγκατάσταση κακόβουλου λογισμικού, ωστόσο οι χρήστες θα πρέπει να είναι επιφυλακτικοί αφού μια νέα έκδοση του ιού θα μπορούσε να παρακάμψει το τείχος ασφαλείας.

Παραλλαγές του WannaCry έχουν ήδη εντοπιστεί, ωστόσο δεν έχουν την ικανότητα εξάπλωσης, γεγονός που περιορίζει σημαντικά τη διάδοσή τους.

Για όσους χρήστες έχουν επηρεαστεί από την επίθεση, η πληρωμή των λύτρων πιθανόν φαντάζει ως η πιο δελεαστική και εύκολη διέξοδος.

Ωστόσο, ειδικοί σε θέματα ασφάλειας προειδοποιούν τους χρήστες να μην προβαίνουν σε μια τέτοια κίνηση, υποστηρίζοντας ότι όχι μόνο δεν εγγυάται η αποκατάσταση του συστήματος αλλά περαιτέρω δίνει αφορμή για τη συνέχιση τέτοιου είδους εγκλημάτων.

ΠΗΓΗ: ΑΠΕ-ΜΠΕ