

Χάρη στον @0xAmit

Βρέθηκε το «εμβόλιο» για τον NotPetya: Τι πρέπει να κάνετε βήμα-βήμα

Δημοσίευση: 28 Ιουν 2017, 12:41 | Τελευταία ενημέρωση: 28 Ιουν 2017, 12:41

```
anilc(cpu 2 caller:0xfffffff80002c473a): Kernel trap at 0x
CR2: 0x0000000000001003b, CR3: 0x000000000000d49e, CR4: 0x
RDX: 0x000000000000d256, RBX: 0xfffffff8876a3f400, RCX: 0x
SP: 0xfffffff8874fe3d10, RBP: 0xfffffff8874fe3d10, RSI: 0x
R8: 0xfffffff8876af7800, R9: 0x0000000000000010, R10: 0x
R12: 0x0000000000000000, R13: 0x000000000000d496, R14: 0x
R15: 0x0000000000000000, RIP: 0xfffffff800055a124, CS: 0x
FL: 0x0000000000000000
```



Ο ειδικός σε θέματα ασφάλειας πληροφοριακών συστημάτων Amit Serper βρήκε έναν αποτελεσματικό τρόπο για να αποτρέψουν την μόλυνση υπολογιστών από το λογισμικό με το οποίο απατούνται από αγνώστους λύτρα για την αποκρυπτογράφηση των αρχείων του. Δείτε τι πρέπει να κάνετε βήμα προς βήμα.

Η λύση που προτείνει ο Amit Σέρπερ -και την έχουν ασπαστεί και άλλοι ειδικοί- είναι η δημιουργία ενός αρχείου χωρίς κατάληξη και με δικαίωμα ανάγνωσης μόνο (read-only), στον φάκελο των Windows, με το όνομα perf. Κι αυτό καθώς, αναλύοντας τον κώδικα του λογισμικού που πλήττει από την Τρίτη συστήματα σε πολλές χώρες, διέκρινε ότι αναζητά το αρχείο αυτό και εάν το βρει ήδη, δεν εκτελείται η διαδικασία της κρυπτογράφησης. Εντούτοις, η επέμβαση αυτή δεν εμποδίζει το λογισμικό perf για να αποτρέψει την κρυπτογράφηση των αρχείων του. Γι'αυτό, το perf διεθερεύεται εμβόλιο και όχι φάρμακο για το NotPetya (ονομάστηκε έτσι επειδή αρχικά θεωρήθηκε ότι επρόκειτο για παραλλαγή του ransomware Petya, ενώ σύντομα διαπιστώθηκε ότι δεν συνέβαινε κάτι τέτοιο).

98% sure that the name is is perf.dll Create a file in c:\windows called perf with no extension and #petya #Nopetya won't run! SHARE!! <https://t.co/0l14uwb0p9>

— Amit Serper (@0xAmit) [June 27, 2017](#)

Για να «εμβολιάσετε» το σύστημά σας, πρέπει να ορίσετε στις επιλογές για τους φακέλους σας να εμφανίζονται πάντα οι καταλήξεις των αρχείων. Πηγαίνετε στις Ρυθμίσεις, εντοπίζετε τις Επιλογές Φακέλων και ελέγχετε στην καρτέλα Προβολή ότι δεν είναι επιλεγμένη η Απόκρυψη επεκτάσεων για γνωστούς τύπους αρχείων. Έτσι, θα βλέπετε πάντοτε την κατάληξη των αρχείων (και θα αναγνωρίζετε για τι πρόκειται).

Έπειτα, καλείστε να κάνετε ένα αντίγραφο π.χ. του notepad.exe και να το μετονομάσετε από notepad-Copy.exe σε perf. Μεταβείτε στο C:\Windows (ή όπου έχετε εγκαταστήσει τα Windows) και υπό την προϋπόθεση ότι έχετε δικαιώματα διαχειριστή (κάτι το οποίο δεν συμβαίνει συνήθως σε εταιρικό περιβάλλον τοπικού δικτύου), δημιουργήστε το αρχείο perf, αντιγράφοντας για παράδειγμα το αρχείο του notepad (notepad.exe) με Ctrl+C, Ctrl+V και αλλάζοντας το όνομα αρχείου από notepad-Copy.exe σε perf.

Μετά, με δεξιή κλικ, το αρχείο ορίστε ως Ready-only το αρχείο perf (δεξιή κλικ, Ιδιότητες). Επιλέξτε Εφαρμογή και OK.

Ανθή Παναγιωτάκη, [@anthi](#)

[tech.in.gr](#)