ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ,
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
Ταχ. Δνση: Χανδρή 1 & Θεσσαλονίκης
Ταχ. Κώδικας: 183 46 Μοσχάτο
Τηλ.: 210-4803255/2266
Fax: 210-4802069
Email: gen_gramm@gsdp.gr

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

Αθήνα, 28/6/2017
Α.Π.: 658/Σχ. 190

Προς:
Δ/νσεις και Τμήματα Πληροφορικής Υπουργείων & Εποπτευόμενων Φορέων τους (βλ. Πίνακα Αποδεκτών)

ΘΕΜΑ: Κυβερνοεπίθεση Ransomware Petya - Μέτρα πρόληψης και αντιμετώπισης

Τις τελευταίες ώρες εκδηλώνονται κυβερνοεπιθέσεις τύπου ransomware σε χώρες εντός και εκτός της Ευρωπαϊκής Ένωσης. Στον τύπο αναφέρθηκαν επιπτώσεις από το Petya ransomware σε μεγάλες επιχειρήσεις σε αυτές τις χώρες. Στην Ελλάδα δεν έχει αναφερθεί ακόμη αντίστοιχο περιστατικό.

1. Τεχνικές επιπτώσεις της κυβερνοεπίθεσης

Μια καινούργια έκδοση του Petya ransomware, πιθανόν το Petya/Misha γνωστό ως Golden Eye, διαδόθηκε αστραπιαία, προκαλώντας παγκόσμια δυσλειτουργίες.

Το συγκεκριμένο ransomware **δεν κρυπτογραφεί τα αρχεία** του στόχου ένα προς ένα. **Προκαλεί επανεκκίνηση των υπολογιστών** - θύματα και κρυπτογραφεί το master file table του σκληρού δίσκου (MTF), σταματά τη λειτουργία του master boot record (MBR), περιορίζει την πρόσβαση σε ολόκληρο το σύστημα παίρνοντας πληροφορίες για τα ονόματα αρχείων, μεγέθη και τοποθεσίες στο φυσικό δίσκο. Το Petya ransomware αντικαθιστά το MBR του υπολογιστή με το δικό του κακόβουλο κώδικα που εμφανίζει με το μήνυμα του ransomware και δεν επιτρέπει στον υπολογιστή να επανεκκινήσει.

Το Petya ransomware χρησιμοποιεί το EternalBlue exploit (MS17-010), διαδίδεται σε εσωτερικά δίκτυα με WMIC PSEXEC και μπορεί να μολύνει πλήρως αναβαθμισμένα συστήματα. Παρατηρούνται συνδέσεις στις θύρες 445, 139 και 135. Μολύνει σταθμούς εργασίας και εξυπηρετητές και έχει μεγάλες επιπτώσεις στα Windows 7.

2. Μέτρα πρόληψης και αντιμετώπισης

Για την πρόληψη και αντιμετώπισης του "Petya Ransomware", προτείνονται τα παρακάτω μέτρα:

- Απενεργοποίηση του WMIC (Windows Management Instrumentation Command-line).

- Δημιουργία αρχείου "perfc" στο «c:\windows\» για αποφυγή μόλυνσης ransomware.
- Η διαδικασία κρυπτογράφησης ξεκινάει στην επανεκκίνηση. Εάν το μηχάνημα επανεκκινήσει και δείτε μήνυμα κρυπτογράφησης , κλείστε το αμέσως.
- Χρησιμοποιείστε Livecd ή εξωτερικό μηχάνημα για την ανάκτηση των αρχείων.
- Πάρτε backup τακτικά και κρατείστε αντίγραφα ασφαλείας offline.
- Προσθέστε κανόνα στο δρομολογητή ή στο firewall να μπλοκάρει την εισερχόμενη κίνηση στη θύρα 445 από μη έμπιστες πηγές.
- Βάλτε φίλτρο στη θύρα 139 του NETBIOS για να εμποδίσει την μόλυνση από άλλες συσκευές στο ίδιο τμήμα του δικτύου. Διαμοιράστε κατάλληλα τα δίκτυα , εφαρμόστε τυπικές τεχνικές anti-ransomeware.
- Αναβαθμίστε το αντι-ικό σας πρόγραμμα στην τελευταία του έκδοση.

Παρακαλούμε όπως γνωστοποιούνται άμεσα τυχόν περιστατικά μολύνσεων στη Γενική Γραμματεία Ψηφιακής Πολιτικής (email Kostas.IOANNOU@gsdp.gr).

Ακριβές αντίγραφο
από το πρωτότυπο

Μαριάννα Καλέντη,
ΠΕ Ανθρωπιστικών & Κοινωνικών Επιστημών
Μοσχάτο, 28/6/2017

Ο Γενικός Γραμματέας Ψηφιακής Πολιτικής

Ιωάννης Ταφύλλης

ΠΙΝΑΚΑΣ ΑΠΟΔΕΚΤΩΝ

1. ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
2. ΜΑΚΕΔΟΝΙΑΣ-ΘΡΑΚΗΣ
3. ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ
4. ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ
5. ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
6. ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
7. ΥΠΟΥΡΓΕΙΟ ΕΡΓΑΣΙΑΣ, ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ ΚΑΙ ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΛΕΓΓΥΗΣ
8. ΥΠΟΥΡΓΕΙΟ ΕΞΩΤΕΡΙΚΩΝ
9. ΥΠΟΥΡΓΕΙΟ ΔΙΚΑΙΟΣΥΝΗΣ, ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΑΝΘΡΩΠΙΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ
10. ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΚΩΝ
11. ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
12. ΥΠΟΥΡΓΕΙΟ ΔΙΟΙΚΗΤΙΚΗΣ ΑΝΑΣΥΓΚΡΟΤΗΣΗΣ
13. ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ ΚΑΙ ΑΘΛΗΤΙΣΜΟΥ
14. ΥΠΟΥΡΓΕΙΟ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΚΑΙ ΕΝΕΡΓΕΙΑΣ
15. ΥΠΟΥΡΓΕΙΟ ΥΠΟΔΟΜΩΝ ΚΑΙ ΜΕΤΑΦΟΡΩΝ
16. ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΝΑΣΤΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
17. ΥΠΟΥΡΓΕΙΟ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΝΗΣΙΩΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
18. ΥΠΟΥΡΓΕΙΟ ΑΓΡΟΤΙΚΗΣ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΤΡΟΦΙΜΩΝ
19. ΥΠΟΥΡΓΕΙΟ ΤΟΥΡΙΣΜΟΥ
20. ΥΠΟΥΡΓΟ ΕΠΙΚΡΑΤΕΙΑΣ