ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΜΗΜΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Αθήνα, 4.11.2020
Αριθμ. Πρωτ: 74378

Πληροφορίες: Δρ. Κων/νος Ιωάννου
Ταχ. Δ/νση: Ευαγγελιστρίας 2
Ταχ. Κωδ.: 10183
Τηλέφωνο: 213 136 1022
Email: cybersecurity@ypes.gr

Προς

Διευθύνσεις και Τμήματα Πληροφορικής
Αποκεντρωμένων Διοικήσεων της Χώρας
Περιφερειών της Χώρας
και Δήμων της Χώρας

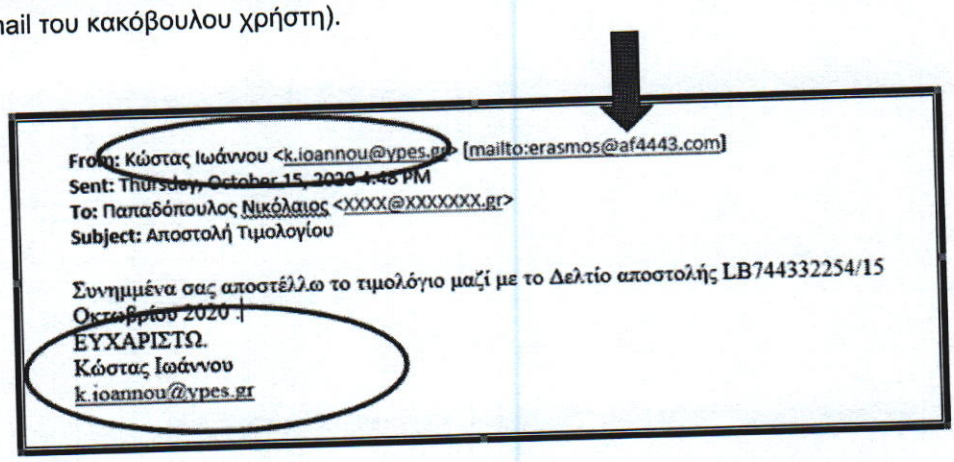
ΘΕΜΑ: Ενημέρωση για Περιστατικά Ασφάλειας σε Κυβερνητικούς Οργανισμούς

Σας γνωρίζουμε ότι το τελευταίο χρονικό διάστημα παρατηρείται **έξαρση περιστατικών ασφάλειας** σε κυβερνητικούς οργανισμούς. Ειδικότερα

1. **Παρατηρείται μεγάλη αύξηση της δραστηριότητας του κακόβουλου λογισμικού EMOTET**

Οι οργανισμοί παρατηρούν έξαρση spam αλληλογραφίας, που φαίνεται προερχόμενη από νόμιμο αποστολέα όμως περιλαμβάνει κακόβουλο λογισμικό. Πρόκειται για κακόβουλο λογισμικό τίπου trojan που εξαπλώνεται κυρίως μέσω ηλεκτρονικών μηνυμάτων τα οποία φαίνονται αυθεντικά με σκοπό την εξαπάτηση των χρηστών (spam). Το spam email περιέχει κακόβουλο σύνδεσμο ή συνημμένο μολυσμένο έγγραφο word που μοιάζει να είναι γνήσιο (π.χ τιμολόγιο, οικονομικό έγγραφο, βιογραφικό, ενημέρωση για τον Covid κ.λ.π). Εάν γίνει λήψη και άνοιγμα του εγγράφου το κακόβουλο λογισμικό εγκαθίσταται στον υπολογιστή του θύματος.

Στην φωτογραφία παρακάτω, φαίνεται ένα email τέτοιου τύπου, το οποίο μπορεί πολύ εύκολα να παραπλανήσει έναν χρήστη, διότι το όνομα και το περιεχόμενο φαίνεται ότι προέρχονται από κάποιον γνωστό σας (π.χ Κώστας Ιωάννου <k.ioannou@ypes.gr> που μπορεί να είναι συνάδελφος στο φορέα σας). Με μια πιο προσεκτική ματιά όμως βλέποντας το email από το οποίο έχει αποσταλλεί, διαπιστώνεται ότι είναι ένα άγνωστο προς εσάς email (π.χ erasmos@11443.com που είναι το email του κακόβουλου χρήστη).


From: Κώστας Ιωάννου <k.ioannou@ypes.gr> [mailto:erasmos@af4443.com]
Sent: Thursday, October 15, 2020 4:48 PM
To: Παπαδόπουλος Νικόλαιος <XXXX@XXXXXXX.gr>
Subject: Αποστολή Τιμολογίου

Συνημμένα σας αποστέλλ.ω το τιμολόγιο μαζί με το Δελτίο αποστολής LB744332254/15 Οκτωβρίου 2020 .
ΕΥΧΑΡΙΣΤΩ.
Κώστας Ιωάννου
k.ioannou@ypes.gr

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

Το Emotet μόλις μολύνει τον υπολογιστή, έχει παρατηρηθεί πως κάνει λήψη και άλλων κακόβουλων προγραμμάτων και υποκλέπτει τα στοιχεία σύνδεσης σε διάφορους λογαριασμούς του χρήστη. Αποκτά πρόσβαση στο ηλεκτρονικό του ταχυδρομείο, διαβάζει τα μηνύματα και δημιουργεί αληθοφανές παραπλανητικό περιεχόμενο που στη συνέχεια αποστέλλει στις επαφές του χρήστη για να συνεχίσει να διαδίδεται. Επιπλέον, προσπαθεί να μολύνει και άλλους υπολογιστές στο ίδιο δίκτυο.

Εξαιτίας του γεγονότος ότι ο καθένας μπορεί να προσβληθεί από το συγκεκριμένο κακόβουλο λογισμικό (ιδιώτες, επιχειρήσεις, δημόσιοι φορείς) είναι σημαντικό να ληφθούν τα παρακάτω μέτρα προστασίας

- Οι χρήστες να είναι ιδιαίτερα προσεκτικοί στο χειρισμό των ηλεκτρονικών μηνυμάτων που λαμβάνουν και στο άνοιγμα των συνημμένων
- Το λειτουργικό σύστημα σταθμών εργασίας και εξυπηρετητών να είναι ενημερωμένο με τις τελευταίες ενημερώσεις ασφαλείας
- Το λογισμικό προστασίας από ιούς να είναι ενημερωμένο
- Να απενεργοποιηθούν οι μακροεντολές στο MS Office (προτείνουμε ενδεικτικά τις οδηγίες στους ακόλουθους συνδέσμους: (https://www.encomputers.com/2018/05/disable-macros-in-microsoft-office-using-group-policy/, https://www.cisecurity.org/white-papers/intel-insight-how-to-disable-macros/)
- Να απενεργοποιηθεί το powershell ή να επιτρέπει την εκτέλεση μόνο υπογεγραμμένων scripts (σχετικά με απενεργοποίηση του Powershell σας προτείνουμε ενδεικτικά τις οδηγίες τον κάτωθι σύνδεσμο: https://activedirectorypro.com/disable-powershell-with-group-policy/)
- Να απενεργοποιηθεί το CMD (σχετικά με την απενεργοποίηση του windows command prompt προτείνουμε ενδεικτικά τον ακόλουθο σύνδεσμο: https://helpdeskgeek.com/how-to/disable-command-prompt-in-windows/)
- Να ενεργοποιηθεί/ενημερωθεί το φίλτρο προστασίας spam του εξυπηρετητή ηλεκτρονικής αλληλογραφίας και επιπλέον απαγόρευση διακίνησης κρυπτογραφημένων συνημμένων και γενικά συνημμένων που δεν μπορούν να ελεγχθούν από το antivirus. Εφόσον ο εξυπηρετητής ηλεκτρονικής αλληλογραφίας είναι του ΣΥΖΕΥΞΙΣ, στις ρυθμίσεις SPAM επιλέξτε βαθμίδα προστασίας «Επιθετική» και επιλέξτε την επιλογή «Αλλαγή από χρήστες: ΟΧΙ»
- Να ενεργοποιηθεί/ενημερωθεί το φίλτρο προστασίας κατά την περιήγηση του χρήση στο διαδίκτυο
- Να περιοριστεί κατά το δυνατόν η επικοινωνία των συσκευών στο ίδιο δίκτυο
- Να απενεργοποιηθεί όπου είναι εφικτό τα file και printing services. Εναλλακτικά να χρησιμοποιούνται ισχυροί κωδικοί (θα πρέπει να είναι μήκους τουλάχιστον οκτώ (8) χαρακτήρων και να περιλαμβάνει τουλάχιστον ένα κεφαλαίο γράμμα (A - Z), τουλάχιστον ένα πεζό γράμμα (a - z), τουλάχιστον έναν αριθμό (0 – 9), τουλάχιστον έναν ειδικό χαρακτήρα από τους ~ ! @ # $ % ^ ή active directory authentication.

Σε περίπτωση που διαπιστωθεί μόλυνση ενός συστήματος θα πρέπει να προβείτε άμεσα στις παρακάτω ενέργειες:

- Άμεση απομόνωση του μολυσμένου μηχανήματος από το υπόλοιπο δίκτυο και απομάκρυνση της μόλυνσης
- Έλεγχος των υπολοίπων μηχανών για μολύνσεις
- Άμεση αλλαγή των κωδικών πρόσβασης του χρήση, των τοπικών λογαριασμών διαχειριστή (local admin) και διαχειριστή τομέα (domain admin)

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:36

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

- Ενημέρωση όσων βρίσκονται στη λίστα επαφών του χρήση να μην ανοίξουν μηνύματα προερχόμενα από αυτόν που περιέχουν συνημμένα αρχεία.

2. Παρατηρείται έξαρση μολύνσεων με κακόβουλο λογισμικό τύπου ransomware

Εφόσον ο οργανισμός μολυνθεί με κακόβουλο λογισμικό τέτοιου τύπου, η αποκατάσταση της κανονικής λειτουργίας του γίνεται ιδιαίτερα δύσκολη αν δεν λαμβάνονται τακτικά αντίγραφα ασφαλείας τα οποία τηρούνται εκτός δικτύου (offline backup). Σας επισυνάπτουμε τεχνικά μέτρα προστασίας από κακόβουλο λογισμικό τύπου ransomware (Συνημμένο 1).

3. Συνεχίζουν να παρουσιάζονται περιστατικά αλλοίωσης ιστοσελίδων (defacement)

Τα περισσότερα περιστατικά που έχουν αναφερθεί αφορούν σε πετυχημένες επιθέσεις σε ιστοσελίδες με μη ενημερωμένες εκδόσεις CMS (wordpress, joomla, drupal) και plugins. Επισυνάπτεται οδηγός που περιλαμβάνει τεχνικά μέτρα για την προστασία της διαδικτυακής υποδομής σας (Συνημμένο 2).

Τέλος, για την προστασία των υποδομών μας, επισυνάπτεται γενικός οδηγός προστασίας πληροφοριακών συστημάτων από ηλεκτρονικές επιθέσεις (Συνημμένο 3).

Σας υπενθυμίζουμε τα στοιχεία επικοινωνίας του Τμήματος Κυβερνοασφάλειας.

Τηλεφωνικό Κέντρο: 213 136 1999

Τηλέφωνο 24ωρης Λειτουργίας: 213 136 1022

Email: cybersecurity@ypes.gr

Ο Διευθυντής

Άγγελος Κουλός

Συννημένα:

1. Μέτρα Προστασίας από κακόβουλο λογισμικό Ransoware
2. Μέτρα προστασίας πληροφοριακών συστημάτων από ηλεκτρονικές επιθέσεις
3. Γενικές Οδηγίες Προστασίας Δικτυακής Υποδομής

Εσωτερική διανομή:

1. Γραφείο Υπουργού Εσωτερικών
2. Γραφείο Υφυπουργού Εσωτερικών
3. Γραφείο Γενικού Γραμματέα Εσωτερικών και Οργάνωσης
4. Γραφείο Γενικής Γραμματέως Ανθρωπίνου Δυναμικού Δ.Τ.
5. Γραφείο Υπηρεσιακής Γραμματέως
6. Γραφείο Γενικού Διευθυντή Εσωτερικών και Ηλεκτρονικής Διακυβέρνησης

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:36

Εθνικό Cert

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων

Μέτρα προστασίας από κακόβουλο λογισμικό Ransomware

Έκδοση 1.0

Μάιος 2016

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:37

Περιεχόμενα

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:37

1. Εισαγωγή

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT σας ενημερώνει για την εμφάνιση ιού τύπου Ransomware :

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που μολύνει έναν υπολογιστή και περιορίζει την πρόσβαση σε αυτόν έως ότου πληρωθούν λύτρα για αυτό.

Το συγκεκριμένο κακόβουλο λογισμικό αποπειράται να αποσπάσει λύτρα από τους χρήστες εμφανίζοντας ένα μήνυμα στην οθόνη. Αυτά τα μηνύματα αναφέρουν ότι ο υπολογιστής είναι κλειδωμένος ή ότι όλοι οι φάκελοι είναι κρυπτογραφημένοι και απαιτούν λύτρα για να αποκατασταθεί η πρόσβαση.

Το Ransomware διαδίδεται συνήθως μέσω ηλεκτρονικών μηνυμάτων phishing που περιλαμβάνουν κακόβουλα συνημμένα αρχεία ή όταν ένας χρήστης επισκέπτεται μια κακόβουλη ιστοσελίδα.

2. Μέτρα πρόληψης Ransomware

Ransomware Prevention measures

Για τις περιπτώσεις αντιμετώπισης περιστατικών από επιθέσεις **Ransomware** είναι πολύ σημαντικό να υλοποιούνται **προληπτικά μέτρα αντιμετώπισης** τα οποία συνοψίζονται παρακάτω:

1) Συνιστάται η χρήση γνήσιων και τακτικά ενημερωμένων λειτουργικών συστημάτων και εφαρμογών.

2) Είναι απαραίτητη η χρήση πάντα ενημερωμένου προγράμματος αντιικής προστασίας σε κάθε ηλεκτρονικό υπολογιστή αλλά και στο mail server.

3) Είναι αναγκαία η χορήγηση περιορισμένων δικαιωμάτων πρόσβασης χρηστών/ διαχειριστών σε αρχεία, φακέλους και στο δίκτυο, καθώς και η ορθή χρήση τους.

4) Αποφεύγετε τη σύνδεση με κωδικό διαχειριστή (administrator), εκτός αν είναι απολύτως απαραίτητο.

5) Τακτική εκπαίδευση χρηστών για θέματα ασφαλούς χρήσης περιήγησης στο Διαδίκτυο και ασφαλούς χρήσης ηλεκτρονικού ταχυδρομείου.

6) Συνιστάται η απόκτηση τακτικών αντιγράφων ασφαλείας (backup) και η φύλαξη αντιγράφου ασφαλείας εκτός δικτύου (off line), και αν είναι δυνατόν η αποθήκευση τους να είναι κρυπτογραφημένη.

7) Συνίσταται η ύπαρξη πολιτική λήψης και τήρησης αντιγράφων (backup), που να περιλαμβάνει τα λειτουργικά συστήματα, τις εφαρμογές και τα δεδομένα.

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:37

8) Συνιστάται η λήψη τακτικών Shadow Copies (για λειτουργικά Windows).

9) Συνιστάται προσοχή στο άνοιγμα ηλεκτρονικών μηνυμάτων που σας φαίνονται άγνωστα ή ύποπτα. Σε περιπτώσεις αμφιβολίας περιεχομένου του ηλεκτρονικού μηνύματος, ζητήστε επιβεβαίωση από τον αποστολέα.

10) Ρυθμίσεις στο ηλεκτρονικό ταχυδρομείο για έλεγχο ή αποφυγή λήψης/αποστολής των εκτελέσιμων αρχείων.

11) Συνίσταται προσοχή σε ποιες ιστοσελίδες κάνουμε αναζήτηση πληροφοριών και δεν ανοίγουμε ύποπτους συνδέσμους.

12) Συχνή αναθεώρηση της πολιτικής ασφαλείας του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου και διασφάλιση ότι είναι ενεργή η καταγραφή ενεργειών (log files).

13) Εφαρμογή των πολιτικών περιορισμού εκτέλεσης εφαρμογών (whitelisting) για αποφυγή μη εξουσιοδοτημένης εκτέλεσης εφαρμογών.

14) Να αποφεύγετε να ακολουθείτε συνδέσμους (Web links), μέσα από ηλεκτρονικά μηνύματα.

15) Κλείδωμα οθόνης μετά από ορισμένο χρονικό διάστημα αδράνειας.

16) Μετά την εγκατάσταση των ανανεώσεων πρέπει να ελέγχονται οι ρυθμίσεις ασφαλείας.

3. Μέτρα αντιμετώπισης επιθέσεων Ransomware

Ransomware Attack Response

Για την **αντιμετώπιση του περιστατικού** σε περίπτωση ανίχνευσης του, συστήνουμε τα παρακάτω γενικά μέτρα:

1) Κλείνετε άμεσα το μολυσμένο σύστημα.

2) Να καταγράψετε την έκταση της μόλυνσης. Έλεγχος του δικτύου (share folders) για επέκταση της μόλυνσης.

3) Λαμβάνετε αντίγραφο δίσκου (raw image format .dd) με σκοπό την επαναφορά δεδομένων (και την περαιτέρω ανάλυση ψηφιακών πειστηρίων).

a. Στο αντίγραφο αυτό μπορεί να γίνει προσπάθεια επαναφοράς των δεδομένων με το shadow copy backup, εάν είχε ενεργοποιηθεί.

b. Επίσης μπορεί να γίνει ανάκτηση των διαγραμμένων αρχείων.

4) Οι διαδικασίες για απεγκατάσταση του συγκεκριμένου τύπου ιού που προτείνονται στο Internet, δεν εγγυώνται την πλήρη εξαφάνιση του

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:37

ιού από το σύστημα σας. Για διασφάλιση απομάκρυνσης του κακόβουλου λογισμικού προτείνεται:

a. Η πλήρη διαγραφή του δίσκου (Format) του συστήματος Η/Υ.

b. Η επαναφορά του συστήματος και των δεδομένων από το πιο πρόσφατο backup, ή επανεγκατάσταση λειτουργικού συστήματος και εφαρμογών.

c. Ενημέρωση (update) λειτουργικού συστήματος και εφαρμογών.

5) Αλλαγή όλων των κωδικών online λογαριασμών και κωδικών διαδικτυακών λογαριασμών κατόπιν αποσύνδεσης του συστήματος από το δίκτυο.

6) Να γνωστοποιήσετε το περιστατικό στην Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων –Εθνικό CERT, για λήψη περαιτέρω οδηγιών ανάλογα με την περίπτωση.

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων-Εθνικό CERT
Π. Κανελλοπούλου 4, Τ.Κ. 10177
Αθήνα, ΕΛΛΑΔΑ
τηλ. +30 210 6973541
fax +30 210 7799122
www.cert.gov.gr
cert@nis.gr

Διανομή μέσω 'ΙΡΙΔΑ' με UID: 5fa24f3c5a2bb5aa272ce762 στις 04/11/20 22:37