

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

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

Αθήνα, 31.1.2021
Αριθμ. Πρωτ: 7049

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

Προς
Αποκεντρωμένες Διοικήσεις της Χώρας
Περιφέρειες της Χώρας
Δήμους της Χώρας

Διευθύνσεις και Τμήματα Πληροφορικής

ΘΕΜΑ: Ενημέρωση για νέα προσπάθεια εξαπάτησης μέσω εκβιαστικών emails (sextortion scam)

Σας ενημερώνουμε, ότι τις τελευταίες ημέρες αποστέλλονται **εκβιαστικά email**, με σκοπό να εξαπατήσουν τους αποδέκτες αυτών. Η προσπάθεια εκβίασης των θυμάτων με την απειλή δημοσιοποίησης αρχείων ερωτικού περιεχομένου αναφέρεται διεθνώς ως σεξουαλική εκβίαση "sextortion".

Οι άγνωστοι δράστες στέλνουν μαζικά μηνύματα στα υποψήφια θύματά τους, τα οποία ενημερώνουν, ότι διαθέτουν πρόσβαση στη συσκευή τους.

Παράλληλα υποστηρίζουν ότι δήθεν έχει εγκατασταθεί κακόβουλο λογισμικό, μετά από την επίσκεψή τους σε κάποιον ιστότοπο, το οποίο έχει ενεργοποιήσει την κάμερα και τους έχει καταγράψει σε προσωπικές στιγμές.

Στη συνέχεια αναφέρεται ότι το κακόβουλο λογισμικό έχει συλλέξει όλες τις επαφές των χρηστών, από τα μέσα κοινωνικής δικτύωσης και οι δράστες απειλούν με την αποστολή του επίμαχου προσωπικού υλικού στις επαφές τους, **σε περίπτωση που δεν λάβουν bitcoins**.

Παρακαλούμε όπως ενημερώσετε το σύνολο των στελεχών των φορέων σας για την αποστολή των εκβιαστικών email, προκειμένου να:

- Αγνοούν τα μηνύματα και να μην καταθέτουν χρήματα στους λογαριασμούς, που τους παραθέτει ο δράστης.
- Μην ανοίγουν τυχόν συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς.
- Μην επικοινωνούν ποτέ και για κανένα λόγο με τους εκβιαστές.
- Αλλάζουν άμεσα κάθε κωδικό ασφαλείας (password) που νομίζουν ότι διακυβεύεται.

Σημειώνεται ότι τα εκβιαστικά αυτά μηνύματα ηλεκτρονικού ταχυδρομείου έχουν κυρίως τις παρακάτω μορφές και περιεχόμενο, ενώ πολλές φορές γίνεται αναφορά σε πραγματικούς κωδικούς, ώστε οι χρήστες να πεισθούν για το αληθινό της απειλής (τις περισσότερες φορές οι κωδικοί αυτοί είναι αρκετά παλαιοί και δεν χρησιμοποιούνται πλέον, γεγονός που καταδεικνύει ότι προέρχονται από παλαιότερη διαρροή δεδομένων)

ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

From: grb@focusmail.com.hr (mailto:grb@focusmail.com.hr)
Sent: Thursday, January 28, 2021 2:38 PM
To: angelos@focus.gr
Subject: Ειδεικτική ασφαλείας για τον λογαριασμό σας

Χαίρετε! Όσοι μαρτυράς να δες, αυτό το email ήλθε από τον λογαριασμό σου. Αυτό είναι ίσχυον να για σένα, αλλά μην ανησυχείς. Θα σου εξηγήσω.
Έχω πρόσβαση στη συσκευή σου και παρακολούθη ήδη τη δραστηριότητά σου εδώ και μέρες.
Πώς συνέβη αυτό; Επισκεφτήκα; Ήταν κατόπι που έχει παρωμαστέ; και η συσκευή σου μαλάνθηκε από το δικό μου κακόβουλο λογισμικό.

Είμαι ένα εξαιρετικά πολύπλοκο λογισμικό, λειτουργεί σαν Δούρειος Ίππος; και επειδή είναι κωδικό - κανένα πρόγραμμα προστασίας από υούς δεν μπορεί να το εντοπίσει. Βασικά η συσκευή σου; παραβιάστηκε από εκείνη τη στιγμή.
Έχει ένα πρόγραμμα που καταγράφει τα πλήκτρα που πατάς, μπορεί να ελέγξει την κάμερα και μικρόφωνο, να μεταφέρει αρχεία και να παίζει πρόσβαση στο τοπικό σου δίκτυο.
Μου πήρε λίγο χρόνο να αποκτίσω πρόσβαση στις πληροφορίες; από τη συσκευή, αλλά τώρα έχω όλες τις επαφές και τα κείμενά σου.

Για να είμαι ειλικρινής, αρχικά δεν ήθελα να κίνω κάτι κακό... Το έκανα μόνο για αλάκα. Αλλά μετά αφρότητα λόγω COVID και έχουσα τη δουλειά μου.
Είτοι, μου ήθελε μια ιδέα για να εκμεταλλευτώ αυτήν τη συγκορία και να βγάλω χρήματα από σου;

Τράβηξα ένα βίντεο ενώ αυτανόζουσα. Είναι ένα βίντεο διακεκομμένης οθόνης; που φαίνεται να κοιτάς; την οθόνη και να εργάζεσαι.
Έχοντας διακεκομμένη είναι εντάξει μαζί μου, αλλά δεν είναι εντάξει με τη φήμη σου. Δεν είμαι περήφανος; γι' αυτό, αλλά χρειάζομαι χρήματα.

Έτσι, εδώ είναι ό, τι θα κάνουμε. Με αφρότητα; ό, τι σου ζητήσω και δεν θα το στείλω στους αγαπημένους σου, τους φίλους και τους συγγενείς σου. Δεν θα το μάθει ποτέ κανείς και η φήμη σου θα παραμείνει άθικτη.
Προσολή; δεν σου ταιριάζει. Μπορώ να το στείλω μέσω email, κειμένου ή ακόμη και μέσω κοινωνικών μέσων δικτύωσης.

Πρέπει να στείλετε 0,05 Bitcoin (περίπου 1200 EUR) στο πορτοφόλι BTC μου 1EFrbZdeJ35c5MwZGkQqDPXr0n4SWbQwZB.

Εάν δεν θέρετε πώς να χρησιμοποιήσετε το bitcoin, αναζητήστε στο google "αγορά bitcoin".
Θα διαγράψω το βίντεο μόλις λάβω τα χρήματα. Θα διαγράψω επίσης το κακόβουλο λογισμικό από τη συσκευή σου και όλες τις πληροφορίες; που έχω. Ποτέ δεν θα ακούσετε από μένα και πάλι.

Ας θέσουμε λοιπόν μια προθεσμία; γι' αυτήν τη συμφωνία. Έχετε 2 ημέρες. Θα δω πότε θα απυξείτε από το email. Το ποσό δεν είναι διαπραγματεύσιμο.
P.S. Μην προσπαθήσεις να το αναστρέψεις. Χρησιμοποιώ TOR και bitcoin τα οποία δεν μπορούν να εντοπιστούν. Αν κάνεις κάτι ήλιο, θα το διακρίνω.

Παρακάτω μην μου ή τον εαυτό σου; κατηγορήσει γι' αυτό. Δεν θα γυαρίζεις; ότι η κάμερα καταγράφει.

Ο Διευθυντής

Άγγελος Κουλόσ

Εσωτερική διανομή:

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