ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΣΤΡΑΤΟΥ
ΚΕΝΤΡΟ ΠΛΗΡΟΦΟΡΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ
ΕΛΛΗΝΙΚΟΥ ΣΤΡΑΤΟΥ (ΚΕ.Π.Υ.Ε.Σ.)

ΠΡΟΣΤΑΣΙΑ ΑΠΟ Phishing Email ΕΠΙΘΕΣΕΙΣ

ΕΚΔΟΣΗ 1Η
23/10/2020

ΙΣΤΟΡΙΚΟ ΑΛΛΑΓΩΝ

Έκδοση	Ημερομηνία	Περιγραφή αλλαγών	Σύνταξη/ τροποποίηση	Έγκριση
1	23/10/2020	Αρχική έκδοση		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ

Η Phishing Email επίθεση, είναι μια μέθοδος εξαπάτησης των διαδικτυακών χρηστών και συνίσταται κυρίως στην απατηλή υφαρπαγή των εμπιστευτικών πληροφοριών τους, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κλπ, με σκοπό την παράνομη χρήση τους από τον επιτιθέμενο.

Με τη βοήθεια κυρίως της απρόσκλητης εμπορικής επικοινωνίας (το γνωστό Spam) για την αυτοματοποιημένη στόχευση των υποψήφιων θυμάτων τους, οι επιτιθέμενοι, εμφανιζόμενοι κυρίως στο διαδίκτυο ως εκπρόσωποι ενός οργανισμού τα χαρακτηριστικά του οποίου έχουν αντιγράψει παράνομα, προβαίνουν σε δόλιες πράξεις ή παραλείψεις με τις οποίες πείθουν τα στοχευμένα θύματά τους, ν' αποκαλύψουν ή εισάγουν σε σύστημα ηλεκτρονικών υπολογιστών στοιχεία της ταυτότητάς τους και εμπιστευτικές πληροφορίες.

Η επικοινωνία σε αυτές τις Social Engineering Επιθέσεις επιθέσεις μπορεί να διεξαχθεί με ηλεκτρονικό ταχυδρομείο, με χρήση πλαστών διαδικτυακών τόπων, με εργαλεία στιγμιαίας επικοινωνίας, με τηλεφωνική επικοινωνία, και με χρήση παραβιασμένων ως προς την ασφάλειά τους διακομιστές/servers.

Οι περισσότερες επιθέσεις Phishing συνήθως γίνονται με χρήση ηλεκτρονικού ταχυδρομείου. **Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με ηλεκτρονικό ταχυδρομείο περιλαμβάνουν:**

1. Χρήση ηλεκτρονικής αλληλογραφίας που μοιάζει να έχει σταλεί από έμπιστη πηγή.
2. Χρήση αντίγραφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks.
3. Χρήση HTML ηλεκτρονικής αλληλογραφίας στην οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks.
4. Χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε ηλεκτρονική αλληλογραφία.
5. Χρήση εξατομικευμένης ηλεκτρονικής αλληλογραφίας.

2. ΒΑΣΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ

Όπως ήδη έχουμε αναφέρει ένα κακόβουλο email που έρχεται στο γραμματοκιβώτιο μας, δείχνει να προέρχεται από κάποιο πιστωτικό ίδρυμα, μια κρατική υπηρεσία ή ένα μεγάλο site ηλεκτρονικού εμπόριο, από οποιαδήποτε εταιρία ή οργανισμό αλλά και από μεμονωμένους αποστολείς. Συνήθως μας προτρέπει να ενεργήσουμε άμεσα π.χ. επιλέγοντας έναν σύνδεσμο ή να ανοίξουμε ένα επισυναπτόμενο αρχείο.

Οι βασικές κατηγορίες αυτών των επιθέσεων είναι:

- **Βασικό Phishing**: Αποστέλλεται μαζικά για απόσπαση προσωπικών δεδομένων, όπως: κωδικούς πρόσβασης, στοιχεία τραπεζικών λογαριασμών και πιστωτικών κρατών.
- **Spear Phishing**: Έχει ένα και μοναδικό στόχο: είτε ένα μεμονωμένο άτομο, είτε μία συγκεκριμένη με κοινά χαρακτηριστικά ομάδα (π.χ. μέλη όλα του ίδιου οργανισμού κ.τ.λ.) και προσαρμόζεται ανάλογα.
- **Clone Phishing**: Όπου οι επιτιθέμενοι, ένα νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει συνημμένο ή σύνδεσμο το αντικαθιστούν σε κακόβουλο.
- **Whaling Phishing:** Επιτίθενται συγκεκριμένα σε ανώτερα στελέχη ή διακεκριμένες προσωπικότητες και προσαρμόζονται αναλόγως.

3. ΤΡΟΠΟΙ ΑΝΑΓΝΩΡΙΣΗΣ

1. Χρησιμοποιεί συνήθως γενικές προσφωνήσεις, όπως ¨Αγαπητέ πελάτη¨, στην θέση του πραγματικού ονόματος παραλήπτη με αρκετά ορθογραφικά και συντακτικά λάθη.
2. Εκμεταλλεύεται κάποιο γνωστό πρόβλημα, δηλώνει κάποια κρίσιμη αλλαγή κατάστασης ή παρουσιάζει μια μοναδική ευκαιρία, και χρησιμοποιώντας φρασεολογία που δημιουργεί την αίσθηση του επείγοντος, ζητά από τον

παραλήπτη να ενεργήσει άμεσα ζητώντας να παραχωρήσει προσωπικά στοιχεία (π.χ. Όνομα χρήστη, Κωδικό Πρόσβασης κ.α.) ή στοιχεία οικονομικού χαρακτήρα (π.χ. Αριθμοί λογαριασμών – Πιστωτικών Καρτών, PIN κ.α.).

3. Απαιτούν γρήγορη ανταπόκριση, ώστε ο παραλήπτης να μην προλάβει να υποψιαστεί κι αντιδράσει.

4. Απαιτούν να μην απαντήσεις πίσω στο email. Αν όμως δοθεί email απάντησης η ηλεκτρονική διεύθυνση είναι πολύ διαφορετική από τις συνηθισμένες.

4. ΤΡΟΠΟΙ ΠΡΟΦΥΛΑΞΗΣ

- Χρησιμοποιούμε πάντα λογισμικό προστασίας από ιούς (antivirus). Παρόλο που τα antvirus δεν μπορούν να μας αποτρέψουν να ανοίξουμε ένα πλαστό ηλεκτρονικό μήνυμα, μπορούν εντούτοις να μας προστατεύσουν από ιούς ή λογισμικά υποκλοπής (spyware) που θα προέλθουν από τέτοιες ενέργειες.

- Εγκαθιστούμε ψηφιακό φίλτρο που μπλοκάρει τα spam emails (antispam).

- Δεν απαντάμε σε μηνύματα ηλεκτρονικού ταχυδρομείου που μας ζητούν να αποκαλύψουμε αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό email.

- Προσέχουμε την ηλεκτρονική διεύθυνση στην οποία βρισκόμαστε. Αντί για το απλό «http://», θα πρέπει να αρχίζει με «https://». Έτσι διασφαλίζουμε ότι χρησιμοποιείτε ασφαλή σύνδεση web (http secure).

- Δεν ακολουθούμε (κάνουμε κλικ) σε συνδέσμους που μας προτρέπουν σε ιστοσελίδες ώστε να εισάγουμε ευαίσθητες πληροφορίες.

- Παρατηρούμε προσεκτικά το όνομα χώρου (domain name) της ιστοσελίδας στην οποία μας προτρέπουν να επισκεφθούμε. Τοποθετούμε τον δείκτη του

ποντικιού πάνω στον σύνδεσμο και ελέγχουμε αν δίνεται ένδειξη για το URL στο οποίο μας υποδεικνύουν να κατευθυνθούμε. Τα phishing websites μπορεί να μοιάζουν πολύ με τα αληθινά αλλά το domain name τους δεν μπορεί να είναι το ίδιο (θα είναι σίγουρα κάτι παραπλήσιο ώστε να παραπλανήσει τον χρήστη).

- Αν εντοπίσουμε κάποιο ύποπτο μήνυμα email αλλά δεν είμαστε σίγουροι ότι είναι κακόβουλο προσπαθούμε να επικοινωνήσουμε απευθείας με την εταιρία ή τον οργανισμό από τον οποίο υποτίθεται ότι προέρχεται το μήνυμα. Για την επικοινωνία δεν χρησιμοποιούμε στοιχεία που υπάρχουν μέσα στο ύποπτο μήνυμα. Κάνουμε μια αναζήτηση στο Google για να ανακαλύψουμε το αληθινό site της εταιρίας.
- Δεν ανοίγουμε ύποπτα email attachments και ειδικά όσα έχουν καταλήξεις: (.cmd, .bat, .exe, .hta, .ocx, .pif, .scr, .chm, .shs, .vbe, .vbs, .ps1, .com, js, .wsf).
- Κάνουμε πάντα τις απαραίτητες ενημερώσεις (updates) σε όλες τις συσκευές που χρησιμοποιούμε στο διαδίκτυο (Η/Υ, laptops, κινητά, tablets κλπ.) ώστε να μειώσουμε τον κίνδυνο μόλυνσης από κάποιο κακόβουλο λογισμικό.

Στην πιθανή περίπτωση που αντιληφθούμε ότι είμαστε θύματα τέτοιας κυβερνοεπίθεσης, πραγματοποιούμε άμεσα αλλαγή κωδικού κι ενημερώνουμε στο τηλέφωνο 800-3900 (210.6553900), αναφέροντας το γεγονός καθώς και περισσότερες πληροφορίες για την φύση της επίθεσης.