Η κατανόηση και η αποτροπή από τις επιθέσεις του Phising

Από μαθητές της Γ΄ τάξης του 4ου Γυμνασίου Πύργου
Έτος 2022-23

Εισαγωγή

- Το phishing είναι μια προσπάθεια, συνήθως μέσω ηλεκτρονικού ταχυδρομείου ή διαδικτυακής ιστοσελίδας, να σας εξαπατήσουν αποσπώντας προσωπικές ή οικονομικές πληροφορίες με ερωτήσεις που εμφανίζονται να είναι προερχόμενες από μια νόμιμη πηγή, όπως η Atradius.
- Οι επιθέσεις phising λειτουργούν εξαπατώντας τα θύματα να παρέχουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή άλλες προσωπικές πληροφορίες. Αυτό γίνεται συνήθως μέσω δόλιων μηνυμάτων ηλεκτρονικού ταχυδρομείου, ιστοτόπων ή μηνυμάτων μέσων κοινωνικής δικτύωσης που φαίνεται να είναι νόμιμα.
- Η κατανόηση και η πρόληψη των επιθέσεων phishing είναι σημαντική γιατί μπορεί να βοηθήσει άτομα και επιχειρήσεις να προστατευτούν από οικονομική απώλεια, κλοπή ταυτότητας και άλλες αρνητικές συνέπειες. Βοηθά επίσης στη διατήρηση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές και επικοινωνίες.

Είδη επιθέσεων phising

- Το Spear phishing στοχεύει συγκεκριμένα άτομα ή ομάδες, το whaling στοχεύει άτομα υψηλού προφίλ και το clone phishing περιλαμβάνει τη δημιουργία ενός ψεύτικου ιστότοπου που φαίνεται να είναι νόμιμος, ενώ άλλοι τύποι επιθέσεων phishing μπορεί να περιλαμβάνουν διαφορετικές μεθόδους εξαπάτησης.
- Αυτές οι επιθέσεις πραγματοποιούνται με τη χρήση τεχνικών κοινωνικής μηχανικής όπως η εξαπάτηση, η χειραγώγηση και η πλαστοπροσωπία για να εξαπατήσουν τα θύματα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να προβούν σε επιβλαβείς ενέργειες.
- Μεταξύ 2013 και 2015, το Facebook και η Google εξαπατήθηκαν για να κερδίσουν 100 εκατομμύρια δολάρια λόγω μιας εκτεταμένης καμπάνιας phishing. Ο phisher εκμεταλλεύτηκε το γεγονός ότι και οι δύο εταιρείες χρησιμοποίησαν την Quanta, μια εταιρεία με έδρα την Ταϊβάν, ως πωλητή. Ο εισβολέας έστειλε μια σειρά από πλαστά τιμολόγια στην εταιρεία που υποδύθηκε την Quanta, τα οποία πλήρωσαν τόσο το Facebook όσο και η Google.

Πώς να εντοπίσουμε ένα phising email

- Οι κοινές red flag, δηλαδή σημεία που πρέπει να προσέχετε σε ένα ηλεκτρονικό μήνυμα phising περιλαμβάνουν τα ορθογραφικά λάθη, ύποπτους συνδέσμους ή συνημμένα, επείγουσα γλώσσα ή αιτήματα για προσωπικές πληροφορίες. Όλα αυτά μπορεί να είναι σημάδια ότι το email δεν είναι νόμιμο και θα πρέπει να εξεταστεί προσεκτικά πριν προβείτε σε οποιαδήποτε ενέργεια.
- Για να επαληθεύσετε την αυθεντικότητα ενός μηνύματος ηλεκτρονικού ταχυδρομείου, ελέγξτε προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, τοποθετήστε το δείκτη του ποντικιού πάνω από συνδέσμους για να ελέγξετε τον προορισμό τους πριν κάνετε κλικ και ελέγξτε τυχόν αιτήματα για προσωπικά στοιχεία ή επείγουσες ενέργειες. Συνιστάται επίσης να χρησιμοποιείτε λογισμικό κατά του phishing και να διατηρείτε τον υπολογιστή και το λογισμικό σας ενημερωμένα με τις πιο πρόσφατες ενημερώσεις κώδικα ασφαλείας.

Πώς να προστατευτούμε από επιθέσεις phising

- Η διατήρηση του λογισμικού ενημερωμένο είναι σημαντική, διότι συμβάλλει στην προστασία από γνωστά τρωτά σημεία ασφαλείας και διασφαλίζει ότι ο υπολογιστής ή η συσκευή σας διαθέτει τις πιο πρόσφατες δυνατότητες ασφαλείας και διορθώσεις σφαλμάτων.
- Συμβουλές για τη δημιουργία ισχυρών κωδικών πρόσβασης και την τακτική αλλαγή τους είναι να χρησιμοποιείτε έναν συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων και να αποφεύγετε τη χρήση προσωπικών στοιχείων όπως γενέθλια ή ονόματα. Συνιστάται επίσης η αλλαγή κωδικών πρόσβασης κάθε λίγους μήνες και η χρήση διαφορετικών κωδικών πρόσβασης για διαφορετικούς λογαριασμούς
- Ο έλεγχος ταυτότητας δύο παραγόντων μπορεί να βελτιώσει την ασφάλεια απαιτώντας ένα πρόσθετο βήμα επαλήθευσης πέρα από έναν κωδικό πρόσβασης, όπως έναν κωδικό που αποστέλλεται σε μια κινητή συσκευή, για να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε έναν λογαριασμό ή ένα σύστημα.

Μέτρα προς αποφυγή επιθέσεων phising

- Για να αποφύγετε επιθέσεις phishing, να είστε προσεκτικοί με τα αιτήματα προσωπικών πληροφοριών, να επαληθεύετε τους αποστολείς email, να αποφεύγετε άγνωστους συνδέσμους και συνημμένα, να χρησιμοποιείτε έλεγχο ταυτότητας δύο παραγόντων, να ενημερώνετε το λογισμικό και να είστε σε επαγρύπνηση.
- Για να επαληθεύσετε τα στοιχεία του αποστολέα, ελέγξτε προσεκτικά τη διεύθυνση email και το όνομα τομέα για τυχόν ορθογραφικά λάθη ή ασυνέπειες.
- Προσέξτε για ύποπτη χρήση της γλώσσας ή αιτήματα
- Μην κάνετε κλικ σε συνδέσμους και μην κάνετε λήψη συνημμένων από άγνωστες πηγές
- Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης και έλεγχο ταυτότητας δύο παραγόντων

Η σημαντικότητα της αναφοράς επιθέσεων phising

- Η αναφορά προσπαθειών ηλεκτρονικού "ψαρέματος" είναι σημαντική γιατί βοηθάει στο να αποτραπούν άλλοι από το να πέσουν θύματα της ίδιας επίθεσης και δίνει τη δυνατότητα στις αρχές να εντοπίσουν και να σταματήσουν τους εισβολείς.
- Εάν υποπτεύεστε επίθεση phishing, είναι σημαντικό να επικοινωνήσετε αμέσως με το προσωπικό IT ή ασφάλειας για να τους ειδοποιήσετε για την πιθανή απειλή και να λάβετε τα απαραίτητα μέτρα για την προστασία των συστημάτων και των δεδομένων του οργανισμού.
- Η προώθηση ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε καθορισμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου βοηθά τους οργανισμούς να εντοπίζουν και να αποκλείουν επιθέσεις ηλεκτρονικού ψαρέματος και παρέχει πολύτιμες πληροφορίες για τη διερεύνηση και την πρόληψη μελλοντικών επιθέσεων.

Περίληψη

Είναι απαραίτητο να είστε προσεκτικοί όταν αντιμετωπίζετε μηνύματα ηλεκτρονικού ταχυδρομείου και διαδικτυακές επικοινωνίες, καθώς οι εγκληματίες του κυβερνοχώρου γίνονται όλο και πιο εξελιγμένοι στις μεθόδους κλοπής ευαίσθητων πληροφοριών και ακόμη και ένα μόνο κλικ σε έναν κακόβουλο σύνδεσμο μπορεί να οδηγήσει σε σημαντικές παραβιάσεις δεδομένων και οικονομικές απώλειες. Η ενημέρωση και η υιοθέτηση ασφαλών πρακτικών μπορεί να συμβάλει σημαντικά στην προστασία του εαυτού σας και του οργανισμού σας από τις καταστροφικές συνέπειες των επιθέσεων ηλεκτρονικού ψαρέματος και άλλων διαδικτυακών απειλών για την ασφάλεια.

Πηγές για περαιτέρω πληροφορίες

Ακολουθούν ορισμένες αναφορές και πόροι για περισσότερες πληροφορίες σχετικά με το phising:

Πληροφορίες καταναλωτών Ομοσπονδιακής Επιτροπής Εμπορίου (FTC): Phishing
Σύνδεσμος: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
National Cyber Security Alliance (NCSA) Μείνετε ασφαλείς στο Διαδίκτυο: Phishing
Σύνδεσμος: https://staysafeonline.org/identity-theft-phishing-and-other-scams/phishing/
Ομάδα Ετοιμότητας Έκτακτης Ανάγκης Υπολογιστών Ηνωμένων Πολιτειών (US-CERT): Phishing
Σύνδεσμος: https://www.us-cert.gov/ncas/tips/ST04-014
Ομάδα Εργασίας κατά του Phishing (APWG)
Σύνδεσμος: https://apwg.org/
Sophos Naked Security: Phishing
Σύνδεσμος: https://nakedsecurity.sophos.com/category/phishing/

Αυτοί οι πόροι παρέχουν χρήσιμες πληροφορίες για την αναγνώριση και την αποφυγή απατών phishing, καθώς και βήματα που πρέπει να λάβετε εάν πιστεύετε ότι έχετε πέσει θύμα επίθεσης phishing.

Εν κατακλείδι

Το ηλεκτρονικό ψάρεμα (phishing) αποτελεί σοβαρή απειλή τόσο για άτομα όσο και για οργανισμούς, καθώς μπορεί να οδηγήσει σε σημαντική οικονομική ζημιά και ζημιά στη φήμη. Είναι σημαντικό να είστε προσεκτικοί και προσεκτικοί όταν αντιμετωπίζετε μηνύματα ηλεκτρονικού ταχυδρομείου και άλλες διαδικτυακές επικοινωνίες και να ακολουθείτε τις βέλτιστες πρακτικές για την αποφυγή επιθέσεων phishing. Επαληθεύοντας τις πληροφορίες αποστολέα, αναζητώντας ύποπτη γλώσσα ή αιτήματα και αποφεύγοντας άγνωστους συνδέσμους ή συνημμένα, μπορείτε να προστατεύσετε τον εαυτό σας από το να πέσετε θύμα επίθεσης phishing. Θυμηθείτε, εάν λάβετε ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, είναι σημαντικό να το αναφέρετε στο προσωπικό πληροφορικής ή ασφάλειας ή να το προωθήσετε σε καθορισμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου. Μείνετε ασφαλείς στο διαδίκτυο και προστατεύστε τον εαυτό σας από επιθέσεις phishing.