5 Ιουλίου 2021

Σε άνοδο οι παγκόσμιες ψηφιακές επιθέσεις φωνητικού phishing

/ Επιστήμες, Τέχνες & Πολιτισμός

Το “ηλεκτρονικό ψάρεμα” (phishing), η γνωστή απάτη μέσω ηλεκτρονικού ταχυδρομείου, στην οποία ο απατεώνας παρουσιάζεται ως αξιόπιστη πηγή, για να εξαπατήσει τους παραλήπτες ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να κατεβάσουν κακόβουλο λογισμικό.

Το vishing είναι μια αντίστοιχη απάτη “φωνητικού ψαρέματος”. Είναι ένα κόλπο με πολλές παραλλαγές που μπορεί να ξεγελάσει άτομα και μεγάλους οργανισμούς – με πιθανές καταστροφικές συνέπειες.

«Μπορεί να σας φαίνεται απίθανο να πέσετε εσείς θύμα τέτοιας απάτης, όμως το 2020, το phishing, το smishing, το pharming και το vishing κόστισαν σε περισσότερα από 241.000 θύματα πάνω από 54 εκατομμύρια δολάρια. Και αυτές είναι μόνο οι περιπτώσεις που καταγγέλθηκαν στο FBI, καθώς πολλές περιπτώσεις απάτης δε δηλώνονται στις Αρχές» αναφέρει η εταιρεία κυβερνοασφάλειας ESET.

Το “φωνητικό ψάρεμα” λειτουργεί με επιτυχία τόσο στους καταναλωτές όσο και τις επιχειρήσεις για έναν πολύ απλό λόγο: την ανθρώπινη φύση. Οι απατεώνες χρησιμοποιούν την κοινωνική μηχανική (Social Engineering) για να χειραγωγήσουν τα θύματά τους.

Οι απατεώνες παρουσιάζονται ως ένας φορέας που εμπιστεύεστε – πχ η τράπεζά σας, η εταιρεία τεχνολογίας με την οποία συνεργάζεστε, κάποια υπηρεσία του Δημοσίου, κάποιος εργαζόμενος στο τμήμα τεχνικής υποστήριξης – και σας δημιουργούν την αίσθηση ότι πρόκειται για κάποιο επείγον ή ανησυχητικό συμβάν. Αυτή η αίσθηση του επείγοντος ή του φόβου που δημιουργούν υπερισχύει κάθε φυσικής προσοχής ή υποψίας που μπορεί να έχει το θύμα.

Οι Vishers
Αυτές οι τεχνικές χρησιμοποιούνται σε ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος (phishing) και ψεύτικα μηνύματα κειμένου (γνωστά ως smishing από το SMS Phishing). Αλλά ίσως είναι πιο αποτελεσματικά όταν χρησιμοποιούνται “ζωντανά” μέσω τηλεφώνου.

Οι Vishers – δηλαδή οι απατεώνες που χρησιμοποιούν τεχνικές φωνητικού ψαρέματος – έχουν πολλά επιπλέον εργαλεία και τακτικές για να κάνουν τις απάτες τους πιο επιτυχημένες. Εργαλεία πλαστογράφησης αναγνώρισης κλήσης, τα οποία μπορούν να χρησιμοποιηθούν για την απόκρυψη της πραγματικής τοποθεσίας του απατεώνα και ακόμη και την αλλαγή των αριθμών τηλεφώνου ώστε να φαίνεται ότι το τηλεφώνημα προέρχεται από κάποιο αξιόπιστο οργανισμό.

Απάτες με συνδυαστική χρήση διαφορετικών τακτικών που ενδέχεται να ξεκινούν με ένα ψεύτικο μήνυμα SMS (smishing), ένα email ηλεκτρονικού “ψαρέματος” (phishing) ή ένα φωνητικό μήνυμα και να ενθαρρύνουν τον χρήστη να καλέσει έναν αριθμό. Αν το θύμα καλέσει θα μιλήσει απευθείας με έναν απατεώνα.

Το vishing στο χώρο εργασίας

Στο εταιρικό περιβάλλον το Vishing είναι πιθανόν να χρησιμοποιηθεί για την κλοπή διαπιστευτηρίων. Το FBI έχει προειδοποιήσει πολλές φορές για τέτοιες επιθέσεις.

Τον Αύγουστο του 2020, περιέγραψε μια εξελιγμένη επιχείρηση στην οποία οι κυβερνοεγκληματίες μελέτησαν με λεπτομέρεια τους στόχους τους και στη συνέχεια τους κάλεσαν το τηλέφωνο προσποιούμενοι ότι τηλεφωνούν από το τμήμα IT. Τα θύματα ενθαρρύνθηκαν να συμπληρώσουν τα στοιχεία σύνδεσης τους σε ένα website ηλεκτρονικού ψαρέματος που έχει σχεδιαστεί ώστε να μοιάζει με τη σελίδα σύνδεσης στο VPN της εταιρείας. Αυτά τα διαπιστευτήρια χρησιμοποιήθηκαν στη συνέχεια για πρόσβαση σε βάσεις δεδομένων της εταιρείας για την κλοπή προσωπικών στοιχείων των πελατών.

Θύματα καταναλωτές
Οι απατεώνες χρησιμοποιούν το vishing για να επιτεθούν και στους καταναλωτές. Σε αυτές τις επιθέσεις, ο απώτερος στόχος είναι να κερδίσουν χρήματα: είτε κλέβοντας απευθείας τραπεζικούς λογαριασμούς ή στοιχεία κάρτας, είτε εξαπατώντας σας για να παραχωρήσετε προσωπικά στοιχεία και διαπιστευτήρια που μπορούν να χρησιμοποιήσουν για πρόσβαση σε αυτούς τους λογαριασμούς.

Μερικές τυπικές απάτες είναι η «απάτη τεχνικής υποστήριξης». Τα θύματα συχνά προσεγγίζονται από κάποιον που προσποιείται ότι καλεί από τον τηλεπικοινωνιακό πάροχο ή από έναν γνωστό προμηθευτή λογισμικού ή υλικού. Οι απατεώνες θα ισχυριστούν ότι βρήκαν ένα πρόβλημα στον υπολογιστή σας και, στη συνέχεια, θα ζητήσουν αμοιβή (και τα στοιχεία της κάρτας σας) για να το επιδιορθώσουν. Μερικές φορές, η διαδικασία περιλαμβάνει και λήψη κακόβουλου λογισμικού εν αγνοία του θύματος.

Άλλη τακτική είναι η αποστολή μηνυμάτων σε μεγάλο αριθμό τηλεφωνικών αριθμών – Wardialing. Αυτή είναι η πρακτική της αποστολής αυτοματοποιημένων φωνητικών μηνυμάτων σε μεγάλο αριθμό θυμάτων, και συνήθως προσπαθεί να τους τρομάξει ώστε να καλέσουν πίσω – για παράδειγμα ισχυριζόμενοι ότι τα θύματα έχουν απλήρωτους λογαριασμούς στην εφορία ή άλλα πρόστιμα.

Μια άλλη δημοφιλής τακτική είναι το τηλεφώνημα στο οποίο ο απατεώνας ισχυρίζεται ότι έχετε κερδίσει ένα έπαθλο. Το μόνο πρόβλημα είναι ότι απαιτείται χρηματική προκαταβολή προτού το θύμα μπορεί να λάβει το βραβείο.

Πηγή: sepe.gr