Zelus SpamRival

Προστασία Ηλεκτρονικού Ταχυδρομείου

Ιούλιος 2022

www.zelus.gr

Τατοΐου 92, 14452

Μεταμόρφωση, Αθήνα - GR

Σύντομη Περιγραφή

Η ψηφιακή ωρίμανση των επιχειρήσεων, μέσω του ψηφιακού μετασχηματισμού των διαδικασιών τους και της χρήσης αντίστοιχων εργαλείων, και η τάση στην υιοθέτηση του μοντέλου της απομακρυσμένης εργασίας, έχει αναπόφευκτα οδηγήσει σε ραγδαία αύξηση των επιθέσεων στον κυβερνοχώρο, με τις επιθέσεις τύπου ηλεκτρονικού ψαρέματος (phishing) να αποτελούν μία από τις βασικότερες απειλές για τους οργανισμούς. Σύμφωνα με την έρευνα του τοπίου κυβερνο-απειλών της ENISA για το 2021, το phishing αποτελεί την κύρια αιτία συμβάντων κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ), γεγονός που έχει ενισχυθεί από την εξέλιξη της πανδημίας του COVID-19 παγκοσμίως, παρουσιάζοντας μία αξιοσημείωτη αύξηση της τάξης του 667% εντός ενός μήνα πανδημίας το 2020.

Το ηλεκτρονικό ψάρεμα (phishing) αποτελεί μία μορφή εγκλήματος στον κυβερνοχώρο, που αποσκοπεί στην εγκατάσταση κακόβουλου λογισμικού στις τερματικές συσκευές ενός χρήστη και την υποκλοπή προσωπικών δεδομένων, όπως οι κωδικοί πρόσβασης σε κρίσιμες εφαρμογές του χρήστη και πληροφορίες ηλεκτρονικών πληρωμών, χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής (social engineering). Ο πιο συνηθισμένος τρόπος επιθέσεων εκφράζεται μέσω αποστολής παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (phishing emails), τα οποία αποσκοπούν στην παραπλάνηση του αποδέκτη, ώστε να ανοίξει ένα κακόβουλο επισυναπτόμενο αρχείο ή να ακολουθήσει ένα σύνδεσμο προς μια κακόβουλη ηλεκτρονική διεύθυνση. Εάν ο χρήστης εξαπατηθεί, τότε, και στις δύο περιπτώσεις, ο επιτιθέμενος μπορεί να αποκτήσει τον πλήρη έλεγχο των εφαρμογών και συστημάτων του χρήστη ή/και, εν δυνάμει, του δικτύου της Επιχείρησης, στην οποίο δραστηριοποιείται ο χρήστης.

Προς την κατεύθυνση αυτή, η εταιρεία Zelus διαθέτει τη λύση SpamRival, που είναι ένα σύστημα ανίχνευσης και παρακολούθησης ενεργειών ηλεκτρονικού ψαρέματος (phishing). Πιο συγκεκριμένα, η λύση Zelus SpamRival παρέχει προστασία του ηλεκτρονικού ταχυδρομείου των χρηστών μίας επιχείρησης από επιθέσεις phishing, κάνοντας χρήση σύγχρονων μηχανισμών και τεχνολογιών τεχνητής νοημοσύνης και μηχανικής μάθησης.

Προδιαγραφές

Η λύση Zelus SpamRival αναλύει σε πραγματικό χρόνο την αλληλογραφία ηλεκτρονικού ταχυδρομείου των χρηστών, για να εντοπίσει κακόβουλα αρχεία ή προσπάθειες για κυβερνοεπιθέσεις, μέσω ηλεκτρονικού ψαρέματος. Τα κύρια χαρακτηριστικά της λύσης είναι:

- Εφαρμογή πολλαπλών πολιτικών αντιμετώπισης εντοπισμένων ενεργειών ηλεκτρονικού ψαρέματος (phishing), προσαρμοσμένες στις ανάγκες μίας επιχείρησης.
- Έλεγχος εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου (email) των χρηστών σε πραγματικό χρόνο.
- Αυτοματοποιημένη διαδικασία εντοπισμού ενεργειών ηλεκτρονικού ψαρέματος μέσω Τεχνητής Νοημοσύνης (AI).
- Κρυπτογραφημένη διαχείριση μηνυμάτων και προστασία προσωπικών δεδομένων.
- Κεντρική διαχείριση λογαριασμών ηλεκτρονικού ταχυδρομείου και οπτικοποίηση και εξαγωγή αναφορών στατιστικών στοιχείων.

Πιο συγκεκριμένα, η λύση βασίζεται σε πολλαπλούς αλγόριθμους Τεχνητής Νοημοσύνης, οι οποίοι εκτελούνται κατά τη λήψη νέων μηνυμάτων ηλεκτρονικού ταχυδρομείου για την αναγνώριση στοιχείων, που συνδέονται με προσπάθειες ηλεκτρονικού ψαρέματος. Η λύση παρέχει

αυτοματοποιημένη διαδικασία αποστολής ειδοποιήσεων εντοπισμού επιθέσεων από ενέργειες phishing. Οι αλγόριθμοι Τεχνητής Νοημοσύνης συνεχώς ανανεώνονται και προσαρμόζονται σε ένα συνεχώς εξελισσόμενο περιβάλλον νέων απειλών που εμφανίζονται.

Η λύση παρέχει τη δυνατότητα κεντρικής διαχείριση πολλαπλών λογαριασμών ηλεκτρονικού ταχυδρομείου για το σύνολο των επιλεγμένων λογαριασμών emails χρηστών μίας επιχείρησης. Επίσης, η λύση παρέχει τη δυνατότητα οπτικοποίησης των προσπαθειών phishing και της εξαγωγής αναφορών με στατιστικά στοιχεία. Σημειώνεται ότι κατά τη διαδικασία ανάλυσης των εισερχόμενων μηνυμάτων του χρήστη για τον εντοπισμό κακόβουλου υλικού ή προσπαθειών phishing λαμβάνονται υπόψη θεμελιώδεις κανόνες προστασίας της ιδιωτικότητας των χρηστών, μέσω της κρυπτογράφησης της επικοινωνίας, και συμμόρφωσης με το Γενικό Κανονιστικό Πλαίσιο Προστασίας δεδομένων προσωπικού χαρακτήρα.

Τέλος, μέσω του SpamRival, ενισχύεται το επίπεδο επίγνωσης των χρηστών σχετικά με τις τεχνικές phishing και τους κινδύνους που εγκυμονούν, μέσω καινοτόμων μηχανισμών εκπαίδευσης και ενημέρωσης, όπως ελεγχόμενες καμπάνιες αποστολής phishing emails, για την αξιολόγηση της συμπεριφοράς των χρηστών σε σχετικά περιστατικά και αποστολής ενημερώσεων.