27 Δεκεμβρίου 2015

Symantec: προειδοποιήσεις για τρομοκρατικές επιθέσεις κρύβουν ιούς!

/ Πεμπτουσία

Image not found or type unknown

Πλαστά «τρομοκρατικά» e-mails έχουν λάβει πολλοί άνθρωποι σε διάφορες χώρες, συμπεριλαμβανομένου του Καναδά, του Ντουμπάι, του Μπαχρέιν και της Τουρκίας. Σύμφωνα με την Symantec, που εντόπισε και τα επικίνδυνα αυτά e-mails, οι ψεύτικες ειδοποιήσεις συμβουλεύουν τους αποδέκτες να προσέχουν τις οικογένειές τους και τις εταιρείες τους από κάποια επικείμενη επίθεση. Η «παγίδα» βρίσκεται στο ένα εκ των δύο συνημμένων των συγκεκριμένων μηνυμάτων, που κρύβει ένα κακόβουλο λογισμικό που χρησιμοποιείται για να μολύνει τον υπολογιστή του θύματος.

Δεν υπάρχει αμφιβολία ότι οι εγκληματίες του κυβερνοχώρου είναι «τσακάλια» και πάντα προετοιμασμένοι να εκμεταλλευτούν κάθε συμβάν στα πρωτοσέλιδα των εφημερίδων, ακόμα και τα πιο δραματικά. Έχουμε επισημάνει στο παρελθόν πολλές

περιπτώσεις στις οποίες οι απατεώνες εκμεταλλεύτηκαν γεγονότα, όπως η μυστηριώδης εξαφάνιση της πτήσης MH370 της Malaysian Airlines ή το περιστατικό που συνέβη στην πτήση QZ8501 της AirAsia.

Η συγκεκριμένη εκστρατεία αφορά σε κακόβουλα e-mails με δύο συνημμένα, τα οποία σύμφωνα με το περιεχόμενο της αλληλογραφίας είναι μια σύντομη αναφορά σχετικά με τα μέτρα που χρειάζονται για να παραμείνει κάποιος ασφαλής. Ένα από τα συννημένα είναι στην πραγματικότητα ένα έγγραφο που περιέχει ενδείξεις για τα μέτρα ασφαλείας ενώ το δεύτερο είναι ένα κακόβουλο λογισμικό που χρησιμοποιείται για να μολύνει τον υπολογιστή του θύματος.

Ο κακόβουλος κώδικας είναι multiplatform Trojan (RAT) που έχει ονομαστεί Jsocket (Backdoor.Sockrat), ένα RAT που αναπτύχθηκε από τους ίδιους δημιουργούς του AlienSpy RAT.

Οι χειριστές πίσω από την καμπάνια χρησιμοποιούν τις υπογραφές υπαλλήλων της τοπικής υπηρεσίας επιβολής του νόμου προκειμένου να εξαπατήσουν τα θύματα τους, δίνοντας μεγαλύτερη αξιοπιστία στα e-mails.

«Νωρίτερα αυτό το μήνα, η Symantec παρατήρησε κακόβουλα e-mails να πλαστογραφούν τη διεύθυνση ηλεκτρονικού ταχυδρομείου μιας υπηρεσία των Ηνωμένων Αραβικών Εμιράτων (HAE), συγκεκριμένα της Αστυνομίας του Ντουμπάι. Αυτά τα emails, τα οποία θεωρούνται από τα θύματα σαν μια προειδοποίηση από την αστυνομία του Ντουμπάι, βασίζονται στο φόβο των χρηστών για τρομοκρατική επίθεση ώστε να τους ξεγελάσει και να εκτελέσουν τα κακόβουλα συνημμένα αρχεία. Τα συνημμένα μεταμφιέζονται σε πολύτιμες συμβουλές ασφαλείας που θα μπορούσαν να βοηθήσουν τους δικαιούχους να προστατεύσουν τον εαυτό τους, καθώς και τις εταιρείες και οικογένειές τους, από ενδεχόμενες τρομοκρατικές επιθέσεις» αναφέρει η Symantec σε ένα blog post.

«Για να προσθέσουν μεγαλύτερη αξιοπιστία στα emails, οι απατεώνες υποδύονται τον αντιστράτηγο της Αστυνομίας του Ντουμπάι , ο οποίος είναι επίσης επικεφαλής της γενικής ασφάλειας για το εμιράτο του Ντουμπάι, υπογράφοντας τα e-mails με το όνομά του.»

Οι ειδικοί παρατήρησαν ότι τα μηνύματα ήταν καλογραμμένα και όλοι οι υπάλληλοι που χρησιμοποιούνται ως υποτιθέμενοι αποστολείς βρίσκονται στην υπηρεσία.

Ένα άλλο ενδιαφέρον στοιχείο που τονίζεται από τη Symantec είναι η προσπάθεια των θυτών να πείσουν τα θύματά τους, όπως για παράδειγμα, στις περισσότερες περιπτώσεις ο αποστολέας έχει το όνομα ενός υπαλλήλου που εργάζεται για τη

στοχευμένη εταιρεία. Αυτή η κατάσταση κάνει τους εμπειρογνώμονες να πιστεύουν ότι οι επιτιθέμενοι γνωρίζουν κατά κάποιο τρόπο τα θύματά τους.

Οι εμπειρογνώμονες της Symantec επιβεβαιώνουν ότι μπορεί να δούμε ακόμα περισσότερα από αυτά τα είδη τακτικής εκφοβισμού, οπότε να είστε προσεκτικοί!

Πηγή: secnews.gr