19 Ιουνίου 2015

Κακόβουλα αρχεία SVG χρησιμοποιούνται για διανομή Ransomware

/ Πεμπτουσία

Image not found or type unknown

ransomware

Ερευνητές ασφάλειας της AppRiver έχουν ανακαλύψει μια εξελιγμένη εκστρατεία διάδοσης κακόβουλου λογισμικού, η οποία προωθείται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και αξιοποιεί μια λιγότερο κοινή μέθοδο για τη διανομή Ransomware. Πιο συγκεκριμένα η διασπορά του κακόβουλου λογισμικού πραγματοποιείται μέσω αρχείων SVG (αρχεία εικόνων με υποστήριξη για διαδραστικό και κινούμενο περιεχόμενο), τα οποία εμπεριέχουν κακόβουλα links που οδηγούν στη λήψη crypto-malware.

Οι ερευνητές εντόπισαν ένα δείγμα email και έπειτα από ανάλυση της

συμπεριφοράς του κακόβουλου *SVG* κατέληξαν ότι το payload πρόκειται πιθανότατα για το CryptoWall, κρίνοντας από ορισμένους δείκτες που σχετίζονται με το συγκεκριμένο *Ransomware*.

Το μήνυμα που εμφανίζεται στα θύματα μετά την κρυπτογράφηση των δεδομένων τους, επισημαίνει επίσης τη συγκεκριμένη απειλή. Το χρηματικό ποσό που ζητά το ransomware για την αποκρυπτογράφηση των δεδομένων των χρηστών ανέρχεται στα 700 δολάρια.

Η συγκεκριμένη καμπάνια βασίζεται στην αποστολή spam μηνυμάτων, τα οποία φαίνεται να εμπεριέχουν ένα βιογραφικό σημείωμα. Το κείμενο είναι αρκετά σύντομο και παραπέμπει τους παραλήπτες στο κακόβουλο συνημμένο.

Τα αρχεία SVG (Scalable Vector Graphics) φέρουν υποστήριξη για JavaScript, χαρακτηριστικό που εκμεταλλεύτηκαν οι επιτιθέμενοι προκειμένου να συμπεριλάβουν σε αυτά κακόβουλους συνδέσμους, οι οποίοι παραπέμπουν στην τοποθεσία που φιλοξενεί το ransomware.

“Το κακόβουλο λογισμικό ενδέχεται να έχει και άλλες δυνατότητες πέρα από την κρυπτογράφηση αρχείων, καθώς θα μπορούσε να χρησιμοποιηθεί για να προκαλέσει χάος σε μια βάση δεδομένων SQL, επιτρέποντας στους επιτιθέμενους να εισάγουν ή να διαγράψουν εγγραφές από αυτή”, αναφέρουν οι ερευνητές, οι οποίοι αναλύοντας τον πηγαίο κώδικα του malware διαπίστωσαν ότι περιείχε hardcoded ορισμένες εντολές SQL που φαίνεται να στοχεύουν τη βάση δεδομένων ενός σχολείου.

Ωστόσο υπάρχει το ενδεχόμενο οι συγγραφείς του malware να εισήγαγαν σκοπίμως τις συγκεκριμένες εντολές στον πηγαίο κώδικα, προκειμένου να παραπλανήσουν τους ερευνητές και να κάνουν δυσκολότερη την ανάλυση του κακόβουλου λογισμικού.

Πηγή: SecNews.gr