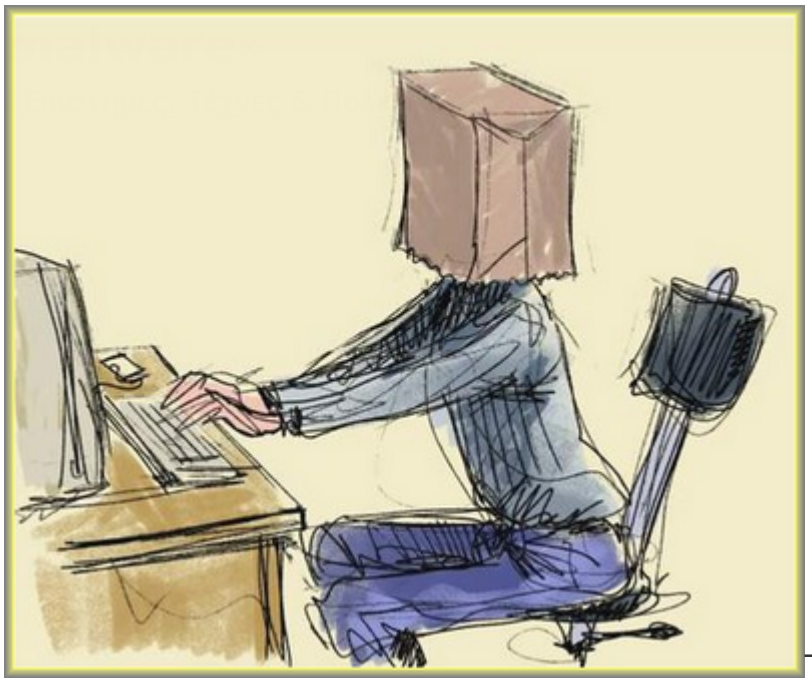
25 Οκτωβρίου 2015

# Προσοχή! Κακόβουλο στο λογισμικό «crypto-



Τα κακόβουλα λογισμικά της οικογένειας «crypto-malware» μπορούν να επηρεάσουν όλες τις εκδόσεις λειτουργικών συστημάτων και εξαπλώνονται, κυρίως, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου

Τις τελευταίες ημέρες το φαινόμενο βρίσκεται σε πλήρη έξαρση με εκατοντάδες αναφορές για περιστατικά «μολύνσεων» εταιρικών δικτύων

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, ενημερώνει τους πολίτες για την επανεμφάνιση του κακόβουλου λογισμικού «CryptoWall» στη χώρα μας.

Το συγκεκριμένο λογισμικό, που αποτελεί εξέλιξη του γνωστού κακόβουλου λογισμικού «Cryptolocker», συγκαταλέγεται στις ψηφιακές απειλές τύπου Crypto-Malware, ενώ μπορεί να επηρεάσει όλες τις εκδόσεις λειτουργικού συστήματος.

Ειδικότερα, το κακόβουλο λογισμικό εξαπλώνεται – μεταδίδεται όταν επισκεπτόμαστε επισφαλείς ή «μολυσμένες» ιστοσελίδες, εμφανιζόμενο ως δήθεν νόμιμη ενημέρωση δημοφιλών εφαρμογών. Ωστόσο, στις περισσότερες περιπτώσεις, το «CryptoWall» εξαπλώνεται μέσω «μολυσμένων» μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Πιο συγκεκριμένα, μετά την εγκατάστασή του στο λειτουργικό σύστημα, το κακόβουλο αυτό λογισμικό, χρησιμοποιώντας ένα εξελιγμένο σύστημα κρυπτογράφησης, «κλειδώνει» όλα τα ψηφιακά αρχεία και τα δεδομένα (διαφόρων τύπων αρχείων, ενδεικτικά: *.doc, *.docx, *.xls, *.ppt, *.psd, *.pdf, *.eps, *.ai, *.cdr, *.jpg, κ.λπ.), που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του χρήστη

που έχει «μολυνθεί» από τον ιό, ενώ για να «ξεκλειδωθούν» τα αρχεία του, πρέπει να καταβληθεί χρηματικό ποσό (ransom), διότι σε διαφορετική περίπτωση καθίστανται απροσπέλαστα για το χρήστη τους.
Το λογισμικό κυκλοφορεί στην 3η έκδοσή του από τον Ιανουάριο του 2015 παγκοσμίως και γίνεται ιδιαίτερη μνεία ότι τόσο για την τρέχουσα έκδοση, όσο και για την προηγούμενη (v2.0), ενώ υπάρχουν διαθέσιμες λύσεις για την απομάκρυνση του ίδιου του κακόβουλου λογισμικού, δεν υπάρχει κανένας γνωστός τρόπος αποκρυπτογράφησης των αρχείων, λόγω της πολύ ισχυρής κρυπτογράφησης (2048-bit RSA key), που χρησιμοποιείται.
Το εν λόγω κακόβουλο λογισμικό έχει επιπλέον τη δυνατότητα να «αυτοδιαδίδεται» μέσω του τοπικού δικτύου και να κρυπτογραφεί τα αρχεία κάθε συστήματος, στο οποίο αποκτά πρόσβαση. Η δυνατότητα αυτή το καθιστά εξαιρετικά επικίνδυνο σε εταιρικά δίκτυα, όπου η διάδοση μπορεί να είναι ραγδαία.
Η καταβολή του χρηματικού ποσού γίνεται, μέσω ανώνυμου προγράμματος περιήγησης, με τη χρήση του ψηφιακού νομίσματος «bitcoin» (BTC), κατόπιν μηνύματος που εμφανίζεται στο χρήστη, με υποδείξεις και οδηγίες για την πληρωμή.
Οι χρήστες του διαδικτύου και ιδιαιτέρως οι διαχειριστές των εταιρικών δικτύων καλούνται να μην πληρώνουν τα χρήματα που ζητούνται, προκειμένου να αποθαρρύνονται τέτοιες παράνομες πρακτικές, καθώς και για να μην εξαπλωθεί το φαινόμενο, ενώ θα πρέπει να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν μέτρα ψηφιακής προστασίας και ασφάλειας για την αποφυγή προσβολής από το κακόβουλο λογισμικό.
Συγκεκριμένα:
• Οι χρήστες που λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή άγνωστη προέλευση, καλούνται να μην ανοίγουν τους συνδέσμους (links) και να μην κατεβάζουν τα συνημμένα αρχεία, που περιέχονται σε αυτά, για τα οποία δεν γνωρίζουν με βεβαιότητα τον αποστολέα και το περιεχόμενο του συνημμένου αρχείου. Επιπλέον, οι χρήστες πρέπει να είναι εξαιρετικά καχύποπτοι στα μηνύματα ηλεκτρονικού ταχυδρομείου, που ως αποστολέας φαίνεται να είναι κάποια υπηρεσία ή εταιρεία, η οποία δεν είναι γνωστή σε αυτούς.
• Συστήνεται να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον περιηγητή (browser), αντί να χρησιμοποιούνται υπερσυνδέσμοι (links).
• Να χρησιμοποιούνται γνήσια λογισμικά προγράμματα και να ενημερώνονται τακτικά (updates), ενώ θα πρέπει να υπάρχει πάντα ενημερωμένο πρόγραμμα προστασίας του ηλεκτρονικού υπολογιστή από «ιούς».
• Να ελέγχουν και να έχουν πάντοτε ενημερωμένη την έκδοση του λειτουργικού τους συστήματος.
• Να δημιουργούνται αντίγραφα ασφαλείας των αρχείων (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης, έτσι ώστε σε περίπτωση

«προσβολής» από το κακόβουλο λογισμικό, να είναι δυνατή η αποκατάσταση τους.
• Ιδιαίτερη προσοχή στην τακτική και ασφαλή τήρηση αντιγράφων ασφαλείας συστήνεται στους διαχειριστές των εταιρικών δικτύων καθότι τα αντίγραφα αποτελούν το μόνο τρόπο επαναφοράς των αρχείων στο σύνολό τους.
Υπενθυμίζεται ότι για ανάλογα περιστατικά ή για παροχή διευκρινίσεων – συμβουλών, οι πολίτες μπορούν να επικοινωνούν με την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας:
• Τηλεφωνικά: 210-6476464 ή 11188
• Στέλνοντας e-mail στο: ccu@cybercrimeunit.gov.gr
• Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smartphones) με λειτουργικό σύστημα iOS – Android: CYBERKID
• Μέσω Twitter «Γραμμή SOS Cyber Alert»: @cyberalertGR.
**Πηγή:** thrakitoday.com