18/1/2022

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε για έξαρση επιθέσεων τύπου "Ransomware" στον κυβερνοχώρο το τελευταίο διάστημα. Οι επιθέσεις τύπου ransomware είναι ένας τύπος επιθέσεων όπου οι επιτιθέμενοι αφού πάρουν πρόσβαση στο σύστημα, κρυπτογραφούν τα αρχεία/δεδομένα οργανισμών. Στη συνέχεια τα θύματα ενημερώνονται μέσω μηνύματος για την καταβολή λύτρων και οδηγίες αποπληρωμής τους. Εάν δεν καταβληθούν τα λύτρα, υπάρχει η απειλή να πωληθούν ή να διαρρεύσουν τα δεδομένα σε ιστοσελίδες που ελέγχονται από τους επιτιθέμενους.

Για την προστασία σας προτείνονται τα παρακάτω:

1. Τήρηση backup των συστημάτων εκτός δικτύου και ύπαρξη στρατηγικής αποκατάστασής του.

2. Ενημέρωση των λογισμικών που χρησιμοποιούνται με τις τελευταίες εκδόσεις.

3. Συντήρηση ενημερωμένης λίστας εξωτερικών κι εσωτερικών επαφών σε περίπτωση ανάγκης.

4. Προετοιμασία σχεδίου αποκατάστασης με συγκεκριμένους ρόλους και στρατηγική (σε περίπτωση που δεν υπάρχει)

5. Χρήση λογισμικού προστασίας από ιούς.

6. Χρήση anti-ransomware εργαλείων.

7. Αποφυγή ανοίγματος άγνωστων αρχείων ή πρόσβασης σε άγνωστους συνδέσμους παρά μόνο αφού ελεγχθούν προσεκτικά (scan) από λογισμικά προστασίας από ιούς.

8. Μπλοκάρισμα πρόσβασης σε γνωστές ιστοσελίδες που φιλοξενούν ransomware.

9. Να επιτρέπεται η εγκατάσταση μόνο εγκεκριμένων εφαρμογών.

10. Περιορισμός των προσωπικών συσκευών ώστε να μην έχουν πρόσβαση σε υπηρεσιακά δίκτυα όπου δεν είναι απαραίτητο.

11. Χρήση λογαριασμών χρηστών με περιορισμένα δικαιώματα κι όχι δικαιώματα διαχειριστή.

12. Αποφυγή χρήσης προσωπικών εφαρμογών και ιστοσελίδων (email, chat, μέσα κοινωνικής δικτύωσης) από υπηρεσιακούς υπολογιστές.

13. Ενημέρωση των χρηστών για τους κινδύνους που ελλοχεύουν και τις καλές πρακτικές.

Σε περίπτωση που ο οργανισμός σας έχει μολυνθεί από ransomware, προτείνονται τα εξής άμεσα μέτρα αντιμετώπισης:

1. Προσδιορισμός και άμεση απομόνωση των συστημάτων που έχουν μολυνθεί

- Αποσύνδεση δικτύου μολυσμένων συστημάτων και υποδικτύων.

- Στην περίπτωση που δεν είναι εφικτή η αποσύνδεση δικτύου μεμονωμένων συστημάτων και υποδικτύων, η απενεργοποίηση του δικτύου να γίνει σε επίπεδο switch.

- Στην περίπτωση που δεν μπορεί να τεθεί το δίκτυο εκτός, να αποσυνδεθούν τοπικά τα Ethernet καλώδια ή η Wi-Fi σύνδεση των μολυσμένων μηχανημάτων.

- Στην περίπτωση που είναι αδύνατη η αποσύνδεση συσκευών από το δίκτυο, μπορούν να τεθούν σε κατάσταση hibernate ή εκτός λειτουργίας(shutdown).
Σημείωση: Στην τελευταία περίπτωση ενδέχεται να καταστεί αδύνατη η αποκατάσταση των αρχείων/συστημάτων. Έχουν καταγραφεί περιπτώσεις όπου το ransomware ανιχνεύει ενέργειες επανεκκίνησης (restart) και καταστρέφει το σύστημα Windows ή διαγράφει τυχαία κρυπτογραφημένα αρχεία (Jisgaw). Επιπλέον, καθιστά δύσκολη τη συλλογή σημαντικών στοιχείων για σκοπούς ψηφιακής έρευνας.

2. Καταγραφή της έκτασης της μόλυνσης. Έλεγχος του δικτύου (shared folders) για επέκταση της μόλυνσης.

3. Λήψη φωτογραφίας (π.χ. μέσω smartphone) του "ransom note".

4. Λήψη αντιγράφου της μνήμης ενός μολυσμένου σταθμού εργασίας και στη συνέχεια του δίσκου .

5. Αλλαγή κωδικών online λογαριασμών κατόπιν αποσύνδεσης του συστήματος από το δίκτυο.

6. Αποφυγή διεξαγωγής διαπραγματεύσεων με τους επιτιθέμενους, καθώς η πληρωμή των λύτρων δεν εγγυάται την επιστροφή δεδομένων.

7. Αποφυγή επικοινωνίας με συνεργαζόμενους φορείς με χρήση του προσβεβλημένου συστήματος (π.χ. mail). Η επικοινωνία μπορεί να γίνει τηλεφωνικώς ή μέσω συστημάτων που δεν έχουν επηρεαστεί από την επίθεση.

8. Επικοινωνία με την Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - ΕΘΝΙΚΟ CERT για τυχόν αρωγή.

Ενδεικτικές πηγές:

hXXps://https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.cisa%5b.%5dgov%2fransomware%2dguides%2dand%2dservices&umid=8201C318-D5D7-B605-A6EA-6C2A6F61B9E9&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-0c846824d38231b7f997b95fb694a0eec6b29a71
hXXps://csrc.nist[.]gov/projects/ransomware-protection-and-response
hXXps://https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.ncsc.gov%5b.%5duk%2fguidance%2fmitigating%2dmalware%2dand%2dransomware%2dattacks&umid=8201C318-D5D7-B605-A6EA-6C2A6F61B9E9&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-b915fafa558dbb5b75d022a4de3fc03466e5b000
hxxps://https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.cisa%5b.%5dgov%2fsites%2fdefault%2ffiles%2fpublications%2fCISA%5fMS%2dISAC%5fRansomware%2520Guide%5fS508C%5f.pdf&umid=8201C318-D5D7-B605-A6EA-6C2A6F61
B9E9&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-c639f10aae70da47d0a8693c22283eec7b59b975