Η ΚΑΘΗΜΕΡΙΝΗ

Είδος: Εφημερίδα / Ένθετο
Ημερομηνία: Κυριακή, 22-10-2023
Σελίδα: 34,35,36 (από 3)
Μέγεθος: 1572 cm ²
Μέση κυκλοφορία: 4000
Επικοινωνία εντύπου:

: ΕΙΔΙΚΟ ΕΝΘΕΤΟ

Λέξη κλειδί: ΕΤΕΚ

Η ΚΑΘΗΜΕΡΙΝΗ ΨΗΦΙΟΠΟΙΗΣΗ

ΑΝΑΛΥΣΗ

Όλα όσα πρέπει να γνωρίζετε για τις κυβερνοεπιθέσεις

ΔΗΜΗΤΡΗΣ ΠΑΝΤΕΛΗ
Μέλος Γενικού Συμβουλίου ΕΤΕΚ

Οι κυβερνοεπιθέσεις αποτελούν αναμφίβολα μια από τις ταχύτερα αναπτυσσόμενες μορφές εγκλημάτων ανά το παγκόσμιο. Τα τελευταία χρόνια παρατηρείται αύξηση στα περιστατικά κυβερνοεπιθέσεων τύπου Ransomware. Πρόκειται για ένα κακόβουλο λογισμικό που καταστρέφει ή και εμποδίζει την πρόσβαση σε κρίσιμα δεδομένα, αρχεία ή και συστήματα έως ότου καταβληθούν λύτρα. Μάλιστα, στις πλείστες των περιπτώσεων, η καταβολή λύτρων γίνεται σε κρυπτονομίσματα.

> Έρευνα κατέγραψε ότι το 85% των χρηστών χρησιμοποιεί τον ίδιο κωδικό πρόσβασης σε διαφορετικές υπηρεσίες.

Τα περιστατικά κυβερνοεπιθέσεων σε Κτηματολόγιο, Πανεπιστήμιο Κύπρου και Ανοικτό Πανεπιστήμιο προκάλεσαν ιδιαίτερη ανησυχία και έντονο προβληματισμό, με αρκετούς πολίτες να διερωτώνται κατά πόσο η Κύπρος έχει πέσει θύμα χάκερς από το εξωτερικό με στόχο να πληγεί τόσο το κύρος όσο και η οικονομία της. Να σημειωθεί ότι κυβερνοεπίθεσεις πραγματοποιούνται σε παγκόσμιο επίπεδο εδώ και πολλά χρόνια και η Κύπρος δεν θα μπορούσε να αποτελεί εξαίρεση. Τα τελευταία χρόνια η πανδημία φαίνεται να πυροδότησε σε μεγάλο βαθμό το πρόβλημα, με τα στατιστικά στοιχεία να δεικνύουν τριπλασιασμό των περιστατικών τα τελευταία τρία χρόνια.

Στην Κύπρο, ιδιαίτερα κατά την πανδημική κρίση, έχουν σημειωθεί πολλές κυβερνοεπιθέσεις -οι περισσότερες τύπου Ransomware- σε εταιρείες και οργανισμούς οι οποίοι χρειάστηκε να πληρώσουν σημαντικά ποσά σε κρυπτονομίσματα για αποκρυπτογράφηση των δεδομένων τους. Είναι κοινά αποδεκτό πως η αυξημένη ασφάλεια και η σχετική ανωνυμία που προσφέρουν οι συναλλαγές με κρυπτονομίσματα, έχουν ενισχύσει την τάση που καταγράφεται και η οποία φέρει μεγαλύτερο αριθμό χάκερς να προχωρούν σε εγκληματικές δραστηριότητες. Στο σκοτεινό διαδίκτυο (dark web) πωλούνται υπηρεσίες «Ransomware as a Service» όπου δίδεται η δυνατότητα να «παραγγελθεί» μια κυβερνοεπίθεση. Η πλειοψηφία των κυβερνοεπιθέσεων τα τελευταία χρόνια γίνεται για λύτρα από επαγγελματίες εγκληματίες του κυβερνοχώρου, πίσω από τους οποίους κρύβονται εταιρείες με μεγάλους προϋπολογισμούς, με διαδικασίες και χρονοδιαγράμματα. Η μέση ηλικία τους είναι στα 25 χρόνια, αμείβονται όμως πολύ καλύτερα από το μέσο μισθό σε σχέση με τους συμπολίτες τους.

Σε έρευνα που έγινε από τον ιστότοπο hackerone.com ανάμεσα σε 7.500 χάκερς, οι 8 στους 10 απάντησαν ότι το κάνουν για να βγάλουν χρήματα, ενώ οι 6 στους 10 για να εξελίξουν την καριέρα τους. Οι χάκερς προτιμούν να κτυπούν κατά κύριο λόγο (α) ιστοσελίδες, (β) πληροφοριακά συστήματα και (γ) συσκευές με λειτουργικό Android (Samsung, Xiaomi, Huawei κ.τλ.). Οι κλάδοι που έχουν κτυπηθεί περισσότερο από Ransomware τα τελευταία χρόνια είναι (α) πάροχοι υπη-

Η ΚΑΘΗΜΕΡΙΝΗ

Είδος: Εφημερίδα / Ένθετο
Ημερομηνία: Κυριακή, 22-10-2023
Σελίδα: 34,35,36 (2 από 3)
Μέγεθος: 1572 cm ²
Μέση κυκλοφορία: 4000
Επικοινωνία εντύπου:

Λέξη κλειδί: ΕΤΕΚ

: ΕΙΔΙΚΟ ΕΝΘΕΤΟ

Δεν ανοίγουμε αρχεία που επισυνάπτονται σε ηλεκτρονικά μηνύματα, εάν δεν είμαστε σίγουροι για το περιεχόμενό τους και αν δεν γνωρίζουμε τον αποστολέα.

ρεσιών πληροφορικής, (β) τράπεζες και οικονομικές υπηρεσίες, (γ) πανεπιστήμια καθώς και (δ) ναυτιλιακές εταιρείες (οι τέσσερις μεγαλύτερες παγκοσμίως). Φέτος τον Μάρτιο η Trend Micro, μια εκ των μεγάλων κατασκευαστών στον τομέα της κυβερνοασφάλειας, δημοσίευσε έκθεση επικεντρωμένη στο ransomware με τίτλο: «What Decision Makers Need to Know About Ransomware Risk», μέσω της οποίας προειδοποιεί ότι το ενώ μόνο το 10% των θυμάτων ransomware πληρώνουν τους εκβιαστές τους, ανοίγουν το δρόμο για νέες επιθέσεις σε πολλούς άλλους οργανισμούς. Το 10% των θυμάτων που συμφωνούν να πληρώσουν λύτρα, συνήθως λαμβάνουν την απόφαση βιαστικά και καταβάλλουν περισσότερα από το μέσο όρο. Η έκθεση καταδεικνύει ότι το ρίσκο δεν είναι ομοιογενές, δηλαδή διαφέρει ανά γεωγραφική περιοχή, τομείς/κλάδους και μεγέθους οργανισμού. Θύματα σε ορισμένους κλάδους και από συγκεκριμένες ηπείρους, όπως η Αφρική, πληρώνουν πιο συχνά από άλλους, αυξάνοντας με τον τρόπο αυτό τις πιθανότητες στοχοποίησης άλλων εταιρειών/οργανισμών από τους ίδιους κλάδους δραστηριοποίησης.

> Πρέπει να χρησιμοποιούμε κωδικό πρόσβασης με τουλάχιστον 8 χαρακτήρες που να περιλαμβάνει κεφαλαία, πεζά, αριθμούς, και σύμβολα.

Για τον πραγματικό αντίκτυπο των κυβερνοεπιθέσεων στην Ελλάδα, έρευνα έδειξε ότι ο μέσος χρόνος διάρκειας ενός περιστατικού Ransomware σε εταιρείες κατά το έτος 2021 ήταν 7,4 ημέρες, με το μέσο κόστος επαναφοράς δεδομένων να ανέρχεται σε €12.193, ενώ το μέσο κόστος προσωρινής διακοπής εργασιών των εταιρειών να ανέρχεται σε €31.321. Το μέσο ποσό που ζητήθηκε από ιδιώτες χρήστες το 2021 ήταν μέχρι €3.000, ενώ για μικρές επιχειρήσεις μέχρι 20 σημεία έφτανε τις €8.000. Σε επιχειρήσεις μέχρι 100 σημεία έφτανε μέχρι €50.000 και σε πολύ μεγάλους οργανισμούς μέχρι €50 εκατομμύρια. Αξίζει να σημειωθεί ότι υπήρξαν περιπτώσεις όπου ο επιτιθέμενος (α) ήταν στην υποδομή δύο μήνες χωρίς να γίνει αντιληπτός, (β) κατέστρεφε ως τελευταία πράξη τα αντίγραφα ασφαλείας (offline backup) και μετά έκανε κρυπτογράφηση τα στοιχεία του θύματος, (γ) είχε δικαιώματα διαχειριστή και (δ) μετά την πληρωμή των λύτρων, συχνά δεν δούλεψε η αποκρυπτογράφηση με τους κωδικούς που δόθηκαν.

Σχετικές αναλύσεις που έγιναν κατόπιν της μεγαλύτερης διαρροής δεδομένων το 2019, κατέληξαν σε ενδιαφέροντα συμπεράσματα που θα πρέπει να τύχουν περαιτέρω αξιοποίησης. Η διαρροή έγινε γνωστή από τα τέλη Ιανουαρίου του 2019 ως Collection #1 μέχρι Collection #5 στο σκοτεινό διαδίκτυο (dark web), όπου συνολικά 25 δισεκατομμύρια ηλεκτρονικές διευθύνσεις και κωδικοί πρόσβασης από διάφορες υπηρεσίες, τέθηκαν προς πώληση. Από τους πιο διαδεδομένους κωδικούς πρόσβασης παγκοσμίως ήταν ο κωδικός «LIVERPOOL».

Η ΚΑΘΗΜΕΡΙΝΗ

Είδος: Εφημερίδα / Ένθετο
Ημερομηνία: Κυριακή, 22-10-2023
Σελίδα: 34,35,36 (3 από 3)
Μέγεθος: 1572 cm ²
Μέση κυκλοφορία: 4000
Επικοινωνία εντύπου:

Λέξη κλειδί: ΕΤΕΚ

: ΕΙΔΙΚΟ ΕΝΘΕΤΟ

Στην Κύπρο έχουν σημειωθεί πολλές κυβερνοεπιθέσεις σε εταιρείες και οργανισμούς, οι περισσότερες τύπου Ransomware.

Σημειώνεται ότι περίπου 15% των χρηστών χρησιμοποιούν στους κωδικούς πρόσβασης τους όνομα ομάδας, ενώ σε ποσοστό 11%, περιλαμβάνονταν ονόματα γεωγραφικών περιοχών (π.χ. Cyprus1234). Σε ποσοστό 6% περιλαμβανόταν το όνομα του ίδιου του χρήστη. Το σημαντικότερο όμως στοιχείο που προκύπτει από την έρευνα, είναι ότι το 85% των χρηστών χρησιμοποιεί τον ίδιο κωδικό πρόσβασης σε διαφορετικές υπηρεσίες.

> Ελέγξετε για τυχόν παραβίαση των δεδομένων σας από την ιστοσελίδα https://haveibeenpwned.com χρησιμοποιώντας απλά το email σας.

Στο wikipedia υπάρχουν αναρτημένες εκατοντάδες κυβερνοεπιθέσεις όπου υπήρξαν διαρροές δεδομένων. Εταιρείες όπως το Facebook είχε οκτώ διαρροές δεδομένων από ιδρύσεως του, το 2004 μέχρι και το 2021. Η τελευταία μεγάλη διαρροή δεδομένων στο Facebook ανήλθε σε 533 εκατομμύρια στοιχεία που περιλάμβαναν μεταξύ άλλων τα ονόματα, τηλεφωνικούς αριθμούς, χώρα διαμονής, διευθύνσεις ηλεκτρονικού ταχυδρομείου και άλλα στοιχεία από τα προφίλ των χρηστών. Έκτοτε, λόγω των στοιχείων αυτών, πολλαπλασιάστηκαν τα sms και τα emails με παραπομπές σε ιστοσελίδες με κακόβουλο λογισμικό, καθώς και οι κλήσεις από δήθεν υπαλλήλους τραπεζών που μιλούσαν μάλιστα άπταιστα την κυπριακή διάλεκτο. Τον Αύγουστο 2022 παραδέχτηκε και το Twitter (τώρα X) ότι είχε διαρροή 5,4 εκατ. στοιχείων χρηστών που περιλάμβαναν τηλεφωνικούς αριθμούς και διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Με τις ηλεκτρονικές επιθέσεις να είναι πλέον καθημερινό φαινόμενο, χρειάζεται όλοι να επιδεικνύουμε την ανάλογη προσοχή σε ό,τι αφορά συγκεκριμένα ζητήματα που άπτονται της διαδικτυακής μας ασφάλειας. Πρέπει να χρησιμοποιούμε κωδικό πρόσβασης με τουλάχιστον 8 χαρακτήρες που να περιλαμβάνει κεφαλαία (A-Z), πεζά (a-z), αριθμούς (0-9) και σύμβολα (!,#,$, κλπ). Ο κωδικός πρόσβασης δεν πρέπει να είναι ο ίδιος για διαφορετικές υπηρεσίες και θα πρέπει να αλλάζει συχνά, π.χ. κάθε τρεις μήνες. Είναι χρήσιμο, όπου είναι εφικτό, να γίνεται χρήση τεχνικών αυθεντικοποίησης δύο βημάτων (κωδικός πρόσβασης και παραλαβή επιπλέον κωδικού μέσω sms, email ή άλλης εφαρμογής). Δεν ανοίγουμε αρχεία που επισυνάπτονται σε ηλεκτρονικά μηνύματα που μας έχουν σταλεί εάν δεν είμαστε σίγουροι για το περιεχόμενό τους και αν δεν γνωρίζουμε τον αποστολέα. Αποφεύγουμε επίσης την πλοήγηση σε ιστοσελίδες που δεν γνωρίζουμε, κρατάμε τα offline αρχεία σε ασφαλισμένο χώρο και προσέχουμε ιδιαίτερα τη πρόσβαση σε εταιρικά δεδομένα από δημόσια WIFI δίκτυα.