1. ΕΥΑΛΩΤΟΙ ΑΠΕΝΑΝΤΙ ΣΕ ΜΙΑ ΣΥΝΘΕΤΗ ΑΠΕΙΛΗ

Μέσο: . . . . . .ΚΑΘΗΜΕΡΙΝΗ ΚΥΡΙΑΚΗΣ
Ημ. Έκδοσης: . . .03/06/2023 Ημ. Αποδελτίωσης: . . .03/06/2023
Σελίδα: 24

Innews ΑΕ - Αποδελτίωση Τύπου - http://www.innews.gr

ΑΠΟΨΗ

Ευάλωτοι απέναντι σε μια σύνθετη απειλή

Του **ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΚΑΡΑΤΡΑΝΤΟΥ**

Η κυβερνοεπίθεση εναντίον της Τράπεζας Θεμάτων του Ινστιτούτου Εκπαιδευτικής Πολιτικής έφερε ξανά στην επικαιρότητα το ζήτημα της κυβερνοασφάλειας στην Ελλάδα. Σύμφωνα με τα δεδομένα που έχουν γίνει έως τώρα γνωστά, η υποδομή της Τράπεζας Θεμάτων δέχθηκε μία διήμερη κυβερνοεπίθεση τύπου DDoS (Distributed Denial of Service) – Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας. Επί της ουσίας, ο συγκεκριμένος τύπος επίθεσης έχει στόχο την πρόκληση τεχνητής υπερβολικής ζήτησης πρόσβασης σε ένα δίκτυο, με αποτέλεσμα αυτό να καθυστερήσει ή να διακόψει τη λειτουργία του. Ας φανταστούμε εκατοντάδες ανθρώπους να εισβάλουν την ίδια στιγμή σε ένα πολυκατάστημα και να ζητούν να εξυπηρετηθούν, μπλοκάροντας στην πράξη τη διαδικασία εξυπηρέτησης πελατών. Αυτό κάνει και η επίθεση DDoS σε ψηφιακό δίκτυο που παρέχει υπηρεσία και οι «πελάτες» είναι τα περίφημα bots ή botnets, μία σύντμηση από τη λέξη robot, δηλαδή ένα αυτοματοποιημένο πρόγραμμα που πραγματοποιεί προκαθορισμένες ενέργειες και προσποιείται τον χρήστη. Αυτός είναι και ο λόγος που πολύ συχνά συναντάμε καρτέλες που προσπαθούν να εντοπίσουν πως ο χρήστης δεν είναι robot-bot.

Η επίθεση στην Τράπεζα Θεμάτων φαίνεται πως ήταν συντονισμένη, καθώς μετρήθηκαν 165.000.000 χτυπήματα στη βάση, με τη διασπορά των bots να δείχνει 114 χώρες. Αυτό δεν σημαίνει απαραίτητα πως ενεπλάκησαν συσκευές από 114 χώρες, καθώς τα συγκεκριμένα προγράμματα συχνά χρησιμοποιούν διακλαδώσεις διαμοιρασμού στίγματος κ.λπ.

Είναι λογικό να προκύπτουν διάφορα ερωτήματα. Η Ελλάδα δεν αντιμετωπίζει για πρώτη φορά κυβερνοεπίθεση σε δημόσιο δίκτυο. Μια χαρακτηριστική περίπτωση αποτελεί η επίθεση στα ΕΛΤΑ τον Μάρτιο του 2022, η οποία ήταν της κατηγορίας Ransomware, δηλαδή κλείδωμα δεδομένων με στόχο τη ζήτηση λύτρων. Δεν είναι όμως μόνο αυτές. Τόσο η Ελλάδα όσο και όλες οι χώρες παγκοσμίως αντιμετωπίζουν καθημερινά μεγάλο όγκο κυβερνοεπιθέσεων, κυρίως DDoS και Ransomware, οι οποίες είναι και οι πλέον διαδεδομένες, τη συντριπτική πλειονότητα των οποίων αντιμετωπίζουν, γι' αυτό και δεν υπάρχει δημοσιότητα. Αν δούμε τις εκθέσεις ευρωπαϊκών υπηρεσιών και διεθνών οργανισμών θα διαπιστώσουμε πως οι κυβερνοεπιθέσεις είναι μια καθημερινή μάχη για όλες τις χώρες.

> *Μέσα σε λίγα χρόνια καλύφθηκε σημαντικό έδαφος και σήμερα η Ελλάδα έχει ένα ολοκληρωμένο οικοσύστημα κυβερνοασφάλειας. Ωστόσο υπάρχουν πολλά που πρέπει να γίνουν ακόμη.*

Οι συγκεκριμένες επιθέσεις δεν πραγματοποιούνται ωστόσο μόνο εναντίον δημόσιων υπηρεσιών, αλλά και κατά εταιρειών, ακόμη και ιδιωτών. Μια επίθεση DDoS μπορεί να στοχεύσει από το online τραπεζικό σύστημα μέχρι μια ηλεκτρονική πλατφόρμα παραγγελίας φαγητού, αλλά και ένα μέσο κοινωνικής δικτύωσης. Ενώ η πιο απλή μορφή επίθεσης Ransomware γίνεται κατά ιδιώτη, όπου με κλείδωμα του υπολογιστή του ζητούν ένα συγκεκριμένο χρηματικό ποσό ως αντάλλαγμα.

Τα πράγματα γίνονται δυσκολότερα όταν συζητάμε για το ποιος μπορεί και πραγματοποιεί τέτοιες επιθέσεις και γιατί. Πρόκειται για μια πραγματική Λερναία Υδρα. Μεμονωμένοι χάκερ, ομάδες κυβερνοακτιβιστών, κυβερνοεγκληματίες που μισθώνουν τις υπηρεσίες τους, αλλά και παρακρατικές και κρατικές υπηρεσίες συγκεκριμένων κρατών. Ως παράδειγμα, πίσω από μια τέτοια επίθεση μπορούμε να βρούμε από τους Anonymous μέχρι τη Mustang Panda, κινεζική κυβερνοομάδα ή τους Killnet, που είναι οι πλέον ειδικοί σε επιθέσεις DDoS και λειτουργούν για τα συμφέροντα της Ρωσίας. Οι κυβερνοεπιθέσεις είναι άλλωστε συστατικό στοιχείο του υβριδικού δόγματος πολέμου και επιχειρήσεων, που αποτελεί τη βασική στρατηγική της Ρωσίας τα τελευταία χρόνια.

Η απειλή λοιπόν είναι σύνθετη και με μεγάλο εύρος και ένταση δράσης. Αυτός είναι και ο λόγος που η κυβερνοασφάλεια αποτελεί το κύριο ζητούμενο των κρατών τα τελευταία χρόνια. Η Ελλάδα, δυστυχώς, ανήκει στις χώρες που έχουν καθυστερήσει σημαντικά στην κούρσα της κυβερνοασφάλειας. Τα τελευταία χρόνια και κυρίως από το 2020 τρέχουμε να καλύψουμε το χαμένο έδαφος, που εκ των πραγμάτων δημιουργεί τρωτότητες. Μόλις τον Οκτώβριο του 2019 αποκτήσαμε εθνικό κατάλογο με τις κρίσιμες ψηφιακές υποδομές. Για τις κρίσιμες υποδομές, εκτός του ψηφιακού χώρου, δεν έχουμε κάτι αντίστοιχο, αν και όλες λειτουργούν στο ψηφιακό πεδίο. Μέσα σε λίγα χρόνια καλύφθηκε σημαντικό έδαφος και σήμερα η Ελλάδα έχει ένα ολοκληρωμένο οικοσύστημα κυβερνοασφάλειας (υπουργείο Ψηφιακής Διακυβέρνησης, ΕΥΠ, Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, Διεύθυνση Κυβερνοάμυνας). Ωστόσο, υπάρχουν πολλά που πρέπει να γίνουν ακόμη και κυρίως από τους ίδιους τους παρόχους και τους λειτουργούς υποδομών και υπηρεσιών. Μέτρα προστασίας, σχέδια ασφάλειας, ομάδες άμεσης ανταπόκρισης κ.ά. Δυστυχώς όμως η κυβερνοασφάλεια δεν κατάφερε να βρει τον χώρο που πρέπει να της δώσουμε κατά τη διάρκεια της προεκλογικής περιόδου.

Ο κ. Τριαντάφυλλος Καρατράντος είναι δρ Ευρωπαϊκής Ασφάλειας και Νέων Απειλών, κύριος ερευνητής ΕΛΙΑΜΕΠ.