1. ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ ΤΕΧΝΟΛΟΓΙΚΗ ΕΠΙΤΗΡΗΣΗ ΧΩΡΙΣ ΟΡΙΑ

Μέσο: . . . . . .ΤΑ ΝΕΑ
Ημ. Έκδοσης: . . .16/08/2022 Ημ. Αποδελτίωσης: . . .16/08/2022
Σελίδα: 14

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

Λογισμικό κατασκοπείας: τεχνολογική επιτήρηση χωρίς όρια

Τα λογισμικά κατασκοπείας επανήλθαν πρόσφατα στο προσκήνιο με αφορμή την αποκάλυψη ότι μια από τις πιο ακριβές και κακόβουλες εκδοχές τους χρησιμοποιήθηκε για την κατασκόπευση αρχηγού πολιτικού κόμματος αλλά και δημοσιογράφων. Για τους παροικούντες την – τεχνολογική – Ιερουσαλήμ ήταν απλά θέμα χρόνου η χρήση αυτού του είδους των λογισμικών που μπορούν να διαβάσουν τα SMS και τα email ανυποψίαστων πολιτών, να ακούσουν και καταγράψουν τηλεφωνικές κλήσεις, να αποθηκεύσουν στιγμιότυπα οθόνης, να καταγράψουν πληκτρολογήσεις και να αποκτήσουν πρόσβαση σε επαφές και ιστορικό προγράμματος περιήγησης, να αποκτήσει καθαρά πολιτική διάσταση και να καταστεί μέσο πολιτικής επιτήρησης. Ηδη τα τελευταία χρόνια έχουν έρθει στην επιφάνεια παραβιάσεις με τέτοιου τύπου λογισμικά δεκάδων κινητών δημοσιογράφων, ακτιβιστών και πολιτικών σε πολλά μήκη και πλάτη του πλανήτη αλλά και στην ίδια την καρδιά της Ευρωπαϊκής Ενωσης. Μέσω ενός «αθώου» SMS που συνοδεύεται από ένα link στο οποίο εάν κάνεις κλικ, η συσκευή ενός πολίτη μπορεί να μολυνθεί με spyware που παρέχει τη δυνατότητα στον υποκλοπέα να μπορεί να βλέπει στην οθόνη του και να ακούει ό,τι ο παρακολουθούμενος από τη δική του συσκευή.

ΓΝΩΜΗ

ΤΟΥ **ΜΙΧΑΛΗ ΚΡΗΤΙΚΟΥ**

Οι δυνατότητες παρακολούθησης, υποκλοπής και υφαρπαγής συνομιλιών, μηνυμάτων και δεδομένων ακόμη και από τις διαδικτυακές πλατφόρμες επικοινωνίας, όπως το Viber, το WhatsApp που παρέχει ένα τέτοιο ενσωματωμένο λογισμικό, το έχει καταστήσει ιδιαίτερα ελκυστικό για ιδιώτες και μυστικές υπηρεσίες που σπεύδουν επίσης να καταφύγουν στις υπηρεσίες του. Μιλάμε στην πραγματικότητα για συστήματα που επιτρέπουν την εξατομικευμένη παρακολούθηση μέσα από τον συνδυασμό συστημάτων συλλογής, αποθήκευσης και ανάλυσης δεδομένων με τη βοήθεια εφαρμογών τεχνητής νοημοσύνης και παρέχουν στους χειριστές τους πλήρη πρόσβαση σε ένα κινητό τηλέφωνο και στα κρυπτογραφημένα δεδομένα του.

Οι τρομακτικές τεχνολογικές δυνατότητες παρακολούθησης που παρέχουν τέτοιου είδους λογισμικά, που βασίζονται στη ραγδαίως εξελισσόμενη τεχνική ικανότητα αθόρυβης υποκλοπής και επεξεργασίας τεράστιων βάσεων δεδομένων, εγείρουν μια σειρά ερωτήματα: παρέχει η υφιστάμενη ενωσιακή νομοθεσία για την προστασία της ιδιωτικής ζωής, των προσωπικών δεδομένων και κυβερνοασφάλειας το απαραίτητο θεσμικό οπλοστάσιο για την αποτροπή μιας άνευ προηγουμένου υπονόμευσης και διάβρωση των ίδιων των ευρωπαϊκών αξιών; Δύναται η διαρκής επίκληση λόγων εθνικής ασφάλειας να αποτρέψει τις αρνητικές επιπτώσεις της χρήσης εργαλείων spyware επί των θεμελιωδών δικαιωμάτων, και ιδίως των δικαιωμάτων στην ιδιωτική ζωή και την προστασία των δεδομένων;

Στην ελληνική περίπτωση που φιγουράρει στα πρωτοσέλιδα του διεθνούς Τύπου τον τελευταίο καιρό, η κατασκοπευτική τεχνολογία φαίνεται ότι όχι μόνο χρησιμοποιήθηκε με βάση μια διασταλτική και μάλλον αόριστη επίκληση του ορού «εθνική ασφάλεια», αλλά και ότι πλέον η χρήση τέτοιων τεχνολογικών μεθόδων ως πολιτικών πρακτικών έχει επεκταθεί από την Κίνα στις «ώριμες» δημοκρατίες της Ευρώπης και απειλεί να ναρκοθετήσει, μέσω της υπερσυγκέντρωσης εξουσιών παντί τεχνολογικώ τρόπω, την ίδια την πεμπτουσία του κοινοβουλευτικού μας πολιτεύματος.

Οι ανησυχητικές αυτές εξελίξεις με την εκθετική χρήση ενός ιδιαίτερα επεμβατικού κατασκοπευτικού λογισμικού, πέρα από το ότι επαναφέρουν στον δημόσιο διάλογο τη συζήτηση περί το τι είναι νόμιμο, ηθικό, τεχνολογικά εφικτό και πολιτικά αποδεκτό, μας υπενθυμίζουν ότι η δημοκρατία χρειάζεται διαρκή επαγρύπνηση για να αποτραπεί η πολιτική εργαλειοποίηση τέτοιων τεχνολογιών αιχμής. Δεδομένης της συχνά καταχρηστικής επίκλησης των λόγων εθνικής ασφαλείας, θα ήταν χρήσιμο ίσως να σκεφτούμε την ανάγκη θέσπισης νομικών, πολιτικών και θεσμικών αντιβάρων σε πανευρωπαϊκό πλέον επίπεδο. Μια τέτοια υπερεθνική εργαλειοθήκη που θα μπορούσε να παρέχει επαρκείς δικλίδες ασφαλείας και αποτελεσματικές εγγυήσεις κατά της αυθαίρετης χρήσης τέτοιου είδους τεχνολογιών θα μπορούσε να καταστεί το τελευταίο καταφύγιο για την αποτροπή τυχόν κανονικοποίησης τέτοιων οργουελικών πρακτικών, αλλά και για την αποφυγή δημιουργίας ενός νέου είδους τεχνολογικού μιθριδατισμού.

Ο δρ Μιχάλης Κρητικός είναι ερευνητής του ΕΛΙΑΜΕΠ και ερευνητικός εταίρος σε θέματα Τεχνητής Νοημοσύνης και Ψηφιακής Μετάβασης στη Σχολή Διακυβέρνησης του Ελεύθερου Πανεπιστημίου των Βρυξελλών.