12 Αυγούστου 2022

Αυτά είναι τα επικίνδυνα sites που έχουν το Predator – Μην κλικάρετε στις συγκεκριμένες ιστοσελίδες

/ Επιστήμες, Τέχνες & Πολιτισμός

Σε έρευνα που δημοσίευσε τον Μάιο το insidestory.gr, αποκαλύπτεται ότι η υπόθεση των παρακολουθήσεων έχει πολύ μεγαλύτερες διαστάσεις.

Η υπόθεση της παρακολούθησης των κινητών τηλεφώνων με το σύγχρονο λογισμικό κατασκοπίας Predator (αρπακτικό), όπως έγινε στην περίπτωση του δημοσιογράφου Θανάση Κουκάκη και του Προέδρου του ΠΑΣΟΚ-ΚΙΝΑΛ, Νίκου Ανδρουλάκη, φαίνεται ότι έχει πολύ μεγαλύτερες διαστάσεις, όπως αποκαλύπτεται σε έρευνα που δημοσίευσε τον Μάιο το insidestory.gr.

Στο κείμενο, το οποίο υπογράφουν ο Τάσος Τέλλογλου και η Ελίζα Τριανταφύλλου, αποκαλύπτεται ότι ένας μεγάλος αριθμός ιστοσελίδων είχαν μολυνθεί και λειτουργούσαν ως παγίδες για τον εντοπισμό και τον εγκλωβισμό προς παρακολούθηση διαφόρων στόχων, οι οποίοι ξεκινούσαν από απλούς πολίτες και δημοσιογράφους και έφταναν μέχρι και σε περιπτώσεις αξιωματικών των Ενόπλων Δυνάμεων.

Σύμφωνα με το ρεπορτάζ, πρόκειται για ένα πλέγμα δεκάδων domains που μέρα με τη μέρα αυξάνονται και υπερβαίνουν τα 43, τα οποία είχε ήδη εντοπίσει η META (facebook), έναν ιστό που στήθηκε με σκοπό να μολύνει κινητά τηλέφωνα υποψήφιων στόχων με ένα σύγχρονο λογισμικό κατασκοπίας με την ονομασία Predator (αρπακτικό).

Τι δείχνει η έρευνα
Τον Ιούλιο του 2020 (τέσσερις μήνες μετά την εγκατάσταση της Intellexa στην Ελλάδα, που έγινε τον Μάρτιο του 2020), αγοράζονται τα πρώτα δύο domain-παγίδα με σκοπό να αποσταλούν από αγνώστους σε υποψήφιους στόχους παρακολούθησης, συνοδευόμενα από ένα προσωποποιημένο μήνυμα προκειμένου να τους παρακινήσουν να πατήσουν πάνω στο ψευδεπίγραφο link και να μολύνουν εν αγνοία τους το κινητό τους. Ένα από αυτά ήταν μία παραλλαγή του ενημερωτικού site του Μιχάλη Ιγνατίου, hellasjournal (hellasjournal[.]company), που εστιάζει στις ελληνοαμερικανικές σχέσεις με απήχηση στην ομογένεια το οποίο διαθέτει και αγγλική έκδοση. Η συγκεκριμένη ειδησεογραφική σελίδα στην πορεία παραλλάχθηκε άλλες δύο φορές (hellasjournal[.]website, heiiasjournai[.]com). Το δεύτερο site που αγοράστηκε τον Ιούλιο του 2020 ήταν το altsantiri[.]news.

Σύμφωνα με την έρευνα των εξειδικευμένων τεχνικών για λογαριασμό του inside story, τα μέχρι σήμερα γνωστά domains-παγίδες που έχουν αγοραστεί ανέρχονται στα 50, επτά περισσότερα από τα 43 που μάθαμε στις 16 Δεκεμβρίου όταν δημοσιοποιήθηκε η έρευνα της META. Αποτελούν μέρος από τα συνολικά 310 sites που εντόπισε η μητρική εταιρεία του facebook – πρόκειται για ποσοστό επί του συνόλου σχεδόν 15%, που φαίνεται ότι στήθηκε για ελληνόφωνους στόχους.

Εκτός από το blogspot.edolio5.com, που μόλυνε το κινητό του δημοσιογράφου

Θανάση Κουκάκη (και δεν ήταν στη λίστα της ΜΕΤΑ), αποκαλύφθηκαν ακόμη έξι ιστοσελίδες που μοιάζουν με γνωστές ελληνικές και καταχωρήθηκαν επίσης για να παγιδεύσουν κινητά ανυποψίαστων:

Στη λίστα των ψεύτικων domain, πρώτη θέση με διαφορά έχουν παραλλαγές γνωστών ειδησεογραφικών ιστοσελίδων όπως kathimerini.news, protothema.live, efsyn.online, tovima.live (περισσότερα από τα μισά σε σύνολο 50 ιστοσελίδων). Ως δόλωμα χρησιμοποιήθηκαν επίσης αρκετά domains που μοιάζουν με αυτά κατασκευαστών οχημάτων π.χ. nissan.gr[.]com, bmw.gr[.]com και suzuki.gr[.]com. Στον κατάλογο εμφανίζονται και κάποιες ιστοσελίδες πιο εστιασμένες γεωγραφικά, όπως το orchomenos.news, το politika[.]bid (μοιάζει με το politikalesvos[.]gr) και stonisi[.]news.

Υπάρχουν και άλλες ιστοσελίδες πιο ειδικού ενδιαφέροντος, όπως π.χ. το paok-24[.]com (η μοναδική αθλητική ομάδα του καταλόγου), το hempower[.]shop που μοιάζει με κατάστημα προϊόντων κάνναβης με ηλεκτρονικό κατάστημα και έδρα έξω από την Κόρινθο, το itcgr[.]live, παραπλήσιο με την ιστοσελίδα γνωστής εταιρείας που αναλαμβάνει τεχνικοοικονομικές μελέτες σε θέματα προηγμένης τεχνολογίας και το sepenet[.]gr[.]com, που μιμείται την ιστοσελίδα ενός δημόσιου οργανισμού, του Σώματος Επιθεώρησης Εργασίας, ενδεχομένως με στόχο κάποιον κρατικό λειτουργό. Μια ακόμη ανησυχητική ένδειξη για το ποιοι μπορεί να έχουν στοχοποιηθεί με αυτό το λογισμικό κατασκοπίας είναι το γεγονός πως ένα από τα site που παραποιήθηκαν για να ξεγελάσουν τους εν δυνάμει στόχους είναι και το kranosgr.com (που το έκαναν kranos.gr[.]com), μια ενημερωτική ιστοσελίδα που απευθύνεται κατά βάση σε στελέχη των ελληνικών ενόπλων δυνάμεων και σωμάτων ασφαλείας.

Στο πλέγμα των ψεύτικων domains υπάρχουν και αρκετά που παραπέμπουν σε πολύ γνωστούς παρόχους υπηρεσιών, όπως για παράδειγμα η Viva (viva[.]gr[.]com), η Cosmote (ebill[.]cosmote[.]center), η Uber (ube[.]gr[.]com) και το youtube (youtube[.]gr[.]live).

Τι μπορεί να κάνει το Predator

Σύμφωνα με την τρισέλιδη έκθεση του Citizen Lab, που συντάχθηκε μετά την τεχνική ανάλυση αρχείου που εξήχθη από το κινητό του δημοσιογράφου (sysdiagnose) και απεστάλη στο καναδικό εργαστήριο για έλεγχο, η τηλεφωνική συσκευή του Θανάση Κουκάκη, τουλάχιστον κατά το διάστημα 12 Ιουλίου με 24 Σεπτεμβρίου 2021, είχε μολυνθεί με το spyware Predator. Όπως διευκρινίζει το Citizen Lab, "αυτό δεν αποκλείει το ενδεχόμενο και άλλων μολύνσεων".

Το τι μπορεί να κάνει το συγκεκριμένο spyware απαντιέται με δύο λέξεις: τα πάντα, αφού μετατρέπει το κινητό σε εξελιγμένη συσκευή παρακολούθησης. "Το Predator είναι ένα εργαλείο παρακολούθησης που προσφέρει στον χειριστή του πλήρη και διαρκή πρόσβαση στην κινητή [τηλεφωνική] συσκευή του στόχου. Το Predator επιτρέπει στον χειριστή να κάνει εξαγωγή μυστικών κωδικών [passwords], αρχείων, φωτογραφιών, ιστορικού περιήγησης στο διαδίκτυο, επαφών καθώς επίσης και δεδομένων ταυτότητας (όπως πληροφορίες για την κινητή συσκευή)" διαβάζουμε στο ίδιο έγγραφο του Citizen Lab.

"Το Predator μπορεί να τραβήξει στιγμιότυπα οθόνης [screen captures], να καταγράφει τις καταχωρήσεις του χρήστη [στο κινητό του], καθώς επίσης μπορεί να ενεργοποιεί το μικρόφωνο και την κάμερα της συσκευής. Αυτό δίνει τη δυνατότητα στους επιτιθέμενους να παρακολουθούν οποιαδήποτε ενέργεια πραγματοποιείται μέσω συσκευής ή κοντά σε αυτήν, όπως τις συνομιλίες που γίνονται μέσα σε ένα δωμάτιο.

Το Predator επιτρέπει επίσης στον χειριστή του να καταγράφει γραπτά μηνύματα που αποστέλλονται ή λαμβάνονται (συμπεριλαμβανομένων αυτών που στέλνονται μέσω "κρυπτογραφημένων εφαρμογών", ή εφαρμογών που επιτρέπουν την εξαφάνιση των μηνυμάτων, όπως είναι το WhatsApp ή το Telegram) καθώς επίσης απλών και VoIP τηλεφωνικών κλήσεων (συμπεριλαμβανομένων τηλεφωνικών συνομιλιών μέσω "κρυπτογραφημένων" εφαρμογών)".

Με άλλα λόγια, αυτοί που έχουν μολύνει το κινητό ενός στόχου μπορούν να παρακολουθούν από προσωπικές στιγμές του ατόμου με την οικογένεια και τους κοντινούς του ανθρώπους, μέχρι εμπιστευτικές επαγγελματικές συνομιλίες.

Πηγή : thetoc.gr