ΠΙΣΤΕΥΕΤΕ ΟΤΙ ΤΟ SMARTPHONE ΣΑΣ ΕΙΝΑΙ ΑΣΦΑΛΕΣ;

Μέχρι τώρα υπήρχαν πολύ λίγες γνωστές, μεγάλης κλίμακας αναφορές κενών στην ασφάλεια των smartphone, αλλά, επειδή δεν έχουν γίνει, αυτό δεν σημαίνει ότι δεν θα συμβούν. Πολλοί χρήστες πιστεύουν ότι τα smartphone τους είναι αδύνατο να δεχθούν επίθεση από χάκερ, επειδή η Apple και η Google τα προστατεύουν από κακόβουλο λογισμικό, και ότι τα δίκτυα κινητής τηλεφωνίας είναι το ίδιο ασφαλή με το σύστημα σταθερής τηλεφωνίας.

Οι χάκερ μπορούν να κάνουν σε ένα smartphone οτιδήποτε μπορούν να κάνουν σε οποιαδήποτε συσκευή που συνδέεται στο Internet: αίτηση κακόβουλων αρχείων χωρίς παρέμβαση του χρήστη, διαγραφή αρχείων, μετάδοση αρχείων, εγκατάσταση προγραμμάτων που εκτελούνται στο παρασκήνιο, παρακολούθηση των δραστηριοτήτων του χρήστη και μετατροπή του τηλεφώνου σε ένα bot που μπορεί να χρησιμοποιηθεί σε ένα botnet για να στέλνει μηνύματα κειμένου και e-mail στους πάντες. Υπάρχουν σχεδόν 220 εκατομμύρια χρήστες smartphone στις ΗΠΑ οι οποίοι χρησιμοποιούν τα κινητά τους για δουλειά, για αγορές ή για εξόφληση λογαριασμών. Το μέγεθος κι ο πλούτος του πλαισίου στόχευσης των χάκερ στα smartphone είναι μεγαλύτερα από ποτέ και ο αριθμός των επιθέσεων αυξάνεται κάθε μέρα: 400% μέσα στο 2016. Διάφορα κακόβουλα προγράμματα λογισμικού μόλυναν το 1,35% του συνόλου των φορητών συσκευών στα τέλη του 2016 (το ίδιο ποσοστό ήταν 1,06% στις αρχές του ίδιου έτους).

Οι εφαρμογές είναι μία λεωφόρος πιθανών παραβιάσεων ασφάλειας. Οι Apple και Google προσφέρουν πλέον πάνω από 6 εκατομμύρια εφαρμογές συνολικά. Η Apple ισχυρίζεται ότι εξετάζει κάθε εφαρμογή ξεχωριστά προκειμένου να διασφαλίσει ότι τηρεί τους κανόνες του App Store της, αλλά οι κίνδυνοι παραμονεύουν. Το 2014 ένα κακόβουλο λογισμικό, το WireLurker, επιτέθηκε σε χρήστες iPhone και iPad στην Κίνα μέσω του λειτουργικού συστήματος Mac OS X. Αυτή ήταν η πρώτη επίθεση σε iPhone στα οποία δεν είχε γίνει jailbreak (ένα είδος τροποποίησης για "σπασμένες" εκδόσεις του iOS, το οποίο επιτρέπει την εγκατάσταση εφαρμογών από τρίτους). Τον Μάρτιο του 2016 ένα κακόβουλο λογισμικό με την ονομασία AceDeceiver μόλυνε συσκευές Apple στις οποίες δεν είχε γίνει jailbreak, σαρώνοντας το App Store για άλλες εκτεθειμένες εφαρμογές και, στη συνέχεια, εγκαθιστώντας τις εν λόγω εφαρμογές σ' αυτές τις συσκευές. Το γεγονός ότι αυτές οι εκτεθειμένες εφαρμογές έγιναν δεκτές από το App Store αποδεικνύει ότι η Apple δεν μπορεί να εξετάζει αποτελεσματικά όλες τις νέες εφαρμογές πριν τις εκθέσει στο κατάστημα εφαρμογών της. Οι χάκερ λαμβάνουν συχνά εφαρμογές και τις επανακυκλοφορούν στο App Store με ενσωματωμένο κακόβουλο λογισμικό. Επιπλέον, εξαγοράζουν εφαρμογές από τους αρχικούς προγραμματιστές τους και τοποθετούν κακόβουλο λογισμικό με παρόμοιο τρόπο.

Παρότι η Apple κάνει ό,τι καλύτερο μπορεί, οι εφαρμογές του App Store δεν προστατεύονται πάντα από κακόβουλο λογισμικό. Ακόμα και το ίδιο το λειτουργικό σύστημα iOS της Apple έχει υποστεί παραβιάσεις στην ασφάλειά του. Οι αναβαθμίσεις του iOS το 2016 φανέρωσαν μία σειρά από τρωτά σημεία, τα οποία αναφέρονται συνολικά ως Trident και δίνουν στους επιτιθέμενους τη δυνατότητα να πάρουν τον πλήρη έλεγχο ενός τηλεφώνου εξ αποστάσεως, χρησιμοποιώντας το κακόβουλο λογισμικό Pegasus. Το Pegasus επιτρέπει την καταγραφή πληκτρολογήσεων, εισερχόμενων και απεσταλμένων μηνυμάτων και ήχου και όλα αυτά χωρίς την παραμικρή ένδειξη ότι κάτι δεν πάει καλά. Επιπλέον, το Trident απενεργοποιεί τις αναβαθμίσεις του iOS σε τηλέφωνα που έχει προσβάλει, αποτρέποντας τη λήψη επιδιορθώσεων ασφαλείας οι οποίες θα έλυναν το πρόβλημα. Το λογισμικό παρακολούθησης (spyware) μπορεί να αυτο-διαγραφεί αμέσως μόλις οι χάκερ πάρουν αυτό που ήθελαν. Παρότι η Apple έσπευσε να διορθώσει γρήγορα αυτή την αδυναμία με την κυκλοφορία μιας αναβάθμισης λειτουργικού συστήματος μέσα σε 10 μόλις μέρες, τα Trident και Pegasus απέδειξαν ότι το iOS δεν έχει ανοσία στο κακόβουλο λογισμικό όπως πιστεύουν πολλοί χρήστες. Το Pegasus είναι ένα εξαιρετικά ολοκληρωμένο κακόβουλο λογισμικό. Το κόστος ανάπτυξής του υπολογίζεται σε εκατοντάδες χιλιάδες δολάρια ενώ η εφαρμογή του κοστίζει χιλιάδες για κάθε στόχο. Λιγότερες από 40 συσκευές προσβλήθηκαν συνολικά από το Pegasus, αλλά το συγκεκριμένο κακόβουλο λογισμικό αποτελεί απόδειξη της δυνατότητας υλοποίησης μίας τέτοιου είδους επίθεσης.

Αν και το κακόβουλο λογισμικό επηρεάζει λιγότερο από το 1% των συσκευών iOS, περίπου το 3-4% των συσκευών με Android περιέχουν κακόβουλο λογισμικό. Αυτό οφείλεται στο γεγονός ότι οι χρήστες συσκευών Android μπορούν να λαμβάνουν εφαρμογές από τρίτους και καταστήματα εφαρμογών τρίτων, τα οποία δεν ελέγχονται επαρκώς,

ενώ οι χρήστες συσκευών της Apple είναι περιορισμένοι στο ιδιαίτερα ελεγχόμενο περιβάλλον του App Store. Το 2016 η εταιρεία ασφαλείας Check Point ανέφερε ότι το κακόβουλο λογισμικό με την ονομασία Hummingbad, το οποίο εγκαθιστά ανεπιθύμητες εφαρμογές και παράγει ανεπιθύμητες διαφημίσεις, είχε μολύνει περίπου 10 εκατομμύρια συσκευές Android. Το Pegasus έκανε κι αυτό την εμφάνισή του στις συσκευές Android, χρησιμοποιώντας ελαφρώς διαφορετικές τεχνικές από την έκδοση του για το iOS. Το 2017 το κακόβουλο λογισμικό WireX μόλυνε κινητά Android τα οποία χρησιμοποίησε για τη διενέργεια επιθέσεων DDoS. Τουλάχιστον 70.000 τηλέφωνα είχαν προσβληθεί.

Οι εφαρμογές Android μπορούν να χρησιμοποιήσουν προσωπικά δεδομένα που υπάρχουν σε ένα τηλέφωνο Android, αλλά πρέπει επίσης να ενημερώνουν τον χρήστη για όσα μπορεί να κάνει κάθε εφαρμογή και ποια προσωπικά δεδομένα απαιτεί. Η Google χρησιμοποιεί ένα ενιαίο σύστημα ελέγχου εφαρμογών το οποίο ελέγχει άμεσα κάθε εφαρμογή για την ύπαρξη επικίνδυνου κώδικα και αφαιρεί εφαρμογές που παραβιάζουν τους κανόνες κατά της κακόβουλης δραστηριότητας. Το 2017 η Google ξεκίνησε το πρόγραμμα Google Play Project, το οποίο σχεδιάστηκε ώστε να προσομοιάζει στη διαδικασία ελέγχου που χρησιμοποιείται στο App Store της Apple. Η Google μπορεί επίσης να εκτελέσει απομακρυσμένη διαγραφή κακόβουλων εφαρμογών από όλα τα τηλέφωνα Android χωρίς την παρέμβαση του χρήστη. Σε ένα περιστατικό, η Google χρησιμοποίησε τη δυνατότητα για απομακρυσμένη διαγραφή προκειμένου να σταματήσει το κακόβουλο λογισμικό ExpensiveWall, το οποίο πραγματοποιεί εγγραφές χρηστών σε προνομιακές υπηρεσίες χωρίς την συγκατάθεσή τους. Το κακόβουλο λογισμικό είχε ληφθεί 4,2 εκατομμύρια φορές και είχε ενσωματωθεί σε 50 διαφορετικές εφαρμογές. Η Google λαμβάνει επιπλέον προληπτικά μέτρα στην προσπάθειά της να μειώσει τις κακόβουλες εφαρμογές, όπως το να απαιτεί από τους προγραμματιστές να καταγράφονται και να λαμβάνουν έγκριση από την Google πριν ξεκινήσουν να διανέμουν εφαρμογές μέσω του Google Play.

Πέρα από την απειλή των εγκληματικών εφαρμογών, όλα τα smartphone είναι ευάλωτα σε πιο παραδοσιακό κακόβουλο λογισμικό για προγράμματα περιήγησης. Τα μη ασφαλή ασύρματα δίκτυα αποτελούν επίσης πρόβλημα, με περισσότερο από το 35% των χρηστών του iOS και σχεδόν το 45% των χρηστών του Android να έχει επιχειρήσει να συνδεθεί σε μη ασφαλές ασύρματο δίκτυο το 2016. Επιπλέον, τα περισσότερα smartphone, συμπεριλαμβανομένου του iPhone, επιτρέπουν στους κατασκευαστές να λαμβάνουν εξ αποστάσεως αρχεία ρυθμίσεων προκειμένου να ενημερώνουν λειτουργικά συστήματα και προγράμματα προστασίας. Δυστυχώς, ανακαλύφθηκαν ατέλειες σε διαδικασίες κρυπτογράφησης με δημόσιο κλειδί, το οποίο έδινε τη δυνατότητα σε απομακρυσμένους διακομιστές να προσπελαύνουν το iPhone, δημιουργώντας ακόμα περισσότερα ερωτήματα για την ασφάλεια από τέτοιες ενέργειες. Οι επιτιθέμενοι έχουν αναπτύξει επίσης μεθόδους για την κατάληψη των τηλεφώνων χρησιμοποιώντας αδυναμίες στις κάρτες SIM. Υπάρχουν τουλάχιστον 500 εκατομμύρια ευάλωτες κάρτες SIM που χρησιμοποιούνται σήμερα, και τα κενά επιτρέπουν στους χάκερ να αποκτούν το κλειδί κρυπτογράφησης που προστατεύει τα προσωπικά δεδομένα των χρηστών, καθώς και πρόσβαση σε όλο σχεδόν το τηλέφωνο κατά τη διαδικασία. Πολλοί χρήστες δεν εκμεταλλεύονται τις διαθέσιμες δυνατότητες για την ασφάλεια, όπως τη χρήση οθόνης κλειδώματος, την οποία έχει ενεργοποιήσει μόνο το ένα τρίτο των χρηστών Android, ενώ σχεδόν το 50% δεν λαμβάνουν τις επιδιορθώσεις ασφαλείας.

Μετά από αυτές τις αποκαλύψεις καθώς και έναν ταραχώδη χρόνο παραβιάσεων ασφαλείας τόσο στο iOS όσο και στο Android, τα smartphone και τα tablet δεν φαίνονται όσο ασφαλή νομίζαμε ότι είναι.

ΠΗΓΕΣ: "Which Phone Protects Your Security the Best? We Asked the Experts," by Lucinda Shen, Time.com, September 25, 2017; "Google Gets Rid of Infected Android Apps After Millions Download Malware," by Abigail Abrams, Time.com, September 14, 2017; "Smartphones Under Fire: Why We Need to Keep Our Android Devices Safe," by Michael Miley, Blog.trendmicro.com, September 6, 2017; "New Malware Turns Smartphones into Cyberattackers," by Hiawatha Bray, Bostonglobe.com, August 30, 2017; "The iPhone at 10: Still No Major Malware," by Kirk McElhearn, Intego.com, July 6, 2017; "Six Ways Your iPhone or iPad Could Get Pown3d: What to Watch Out For and How to Stay Safe," by David Gewirtz, Zdnet.com, July 5, 2017; "Here's How Malware Gets Inside Your Phone's Apps," by Peter Hannay, Businessinsider.com, June 23, 2017; "Pegasus: The Ultimate Spyware for iOS and Android," by John Snow, Kaspersky.com, April 11, 2017; "Total-Takeover iPhone Spyware Lurks on Android, Too," by Lily Hay Newman, Wired.com, April 6, 2017; "Businesses Beware: Smartphone Malware Rises 400% in 2016, Nokia Reports," by Allison DeNisco Rayome, Techrepublic.com, March 27, 2017; "Trident iOS Flaws; Researchers Detail How the Spyware Stayed Hidden," by Danny Palmer, Zdnet.com, November 7, 2016; "Beware, iPhone Users: Fake Retail Apps Are Surging Before Holidays," by Vindu Goel, *New York Times*, November 6, 2016; "Microsoft: 'Apple Can No More Secure Your iPhone Than Google Can Secure Android,'" by Zdnet.com, October 14, 2016; "iPhone Malware That Steals Your Data Proves No Platform Is Truly Secure," by Liam Tung and Raymond Wong, Mashable.com, August 26, 2016; "IPhone Users Urged to Update Software After Security Flaws Are Found," by Nicole Perlroth, *New York Times*, August 25, 2016; "Hummingbad Malware Infects 10 Million Devices: How to Check If Your Phone or Tablet Is Among Them," by Aaron Mamiit, Techtimes.com, July 6, 2016; "This Nasty New Malware Can Infect Your Apple iPhone or iPad," by Jonathan Vanian, *Fortune*, March 16, 2016; "XAgent iPhone Malware Attack Steals Data Without Jailbreaking," by Jeff Gamet, Macobserver.com, February 5, 2015; "Apple Blocks Apps Infected with WireLurker Malware Targeting iPhones and iPads," by Carly Page, Theinquirer.net, November 6, 2014.