50 παραβιάσεις κωδικών πρόσβασης την ώρα: Εισβολείς μπορούν να θέσουν σε κίνδυνο οποιοδήποτε εταιρικό δίκτυο με τη χρήση συσκευής αξίας μόλις 20 δολαρίων

Οι ερευνητές της Kaspersky Lab εξέτασαν τα δημοσίως διαθέσιμα εργαλεία hardware και λογισμικού για κρυφή υποκλοπή κωδικών πρόσβασης και ανακάλυψαν ότι ένα ισχυρό εργαλείο hacking μπορεί να δημιουργηθεί με μόλις 20$ και λίγες ώρες δουλειάς από κάποιον που διαθέτει βασικές γνώσεις προγραμματισμού. Σε ένα πείραμα που πραγματοποίησαν χρησιμοποίησαν μία USB συσκευή που βασίζεται σε ένα αυτοσχέδιο Raspberry Pi, ρυθμισμένο με συγκεκριμένο τρόπο και μάλιστα χωρίς να έχει εγκατεστημένο κάποιο κακόβουλο λογισμικό. Οπλισμένοι με αυτήν τη συσκευή, ήταν σε θέση να συλλέγουν κρυφά δεδομένα που σχετίζονται με την ταυτοποίηση των χρηστών από ένα εταιρικό δίκτυο, με ρυθμό 50 παραβιάσεων κωδικών πρόσβασης την ώρα.

Οι έρευνες ξεκίνησαν με μία αληθινή ιστορία: Σε άλλη έρευνα που συμμετείχαν οι ειδικοί της Kaspersky Lab, κάποιος από το εσωτερικό της επιχείρησης (υπάλληλος μιας εταιρείας καθαρισμού) χρησιμοποίησε ένα USB-stick για να «μολύνει» έναν στοχοποιημένο οργανισμό με κακόβουλο λογισμικό. Από τη στιγμή που άκουσαν την ιστορία οι ειδικοί ασφάλειας της Kaspersky

Lab, ήταν περίεργοι τι άλλο θα μπορούσε να χρησιμοποιηθεί από το εσωτερικό μιας εταιρείας και να εκθέσει ένα στοχοποιημένο δίκτυο. Επίσης, θα ήταν δυνατό να εκθέσουν σε κίνδυνο ένα δίκτυο χωρίς κανένα κακόβουλο λογισμικό;

Πήραν έναν μικροϋπολογιστή Raspberry-Pi, τον ρύθμισαν σαν μετασχηματιστή Ethernet, έκαναν μερικές πρόσθετες αλλαγές στις ρυθμίσεις του λειτουργικού συστήματος που έτρεχε ο μικροϋπολογιστής και εγκατέστησαν κάποια δημοσίως διαθέσιμα εργαλεία για ανακάλυψη πακέτων και συλλογή και επεξεργασία δεδομένων. Τελικά, οι ερευνητές εγκατέστησαν και έναν server ώστε να συλλέγουν τα υποκλεμμένα δεδομένα. Έπειτα, η συσκευή συνδέθηκε στο στοχοποιημένο μηχάνημα και ξεκίνησε αυτόματα να γεμίζει τον server με κλεμμένα στοιχεία σύνδεσης.

Ο λόγος για τον οποίο συνέβη αυτό ήταν ότι το λειτουργικό σύστημα στον επιτιθέμενο υπολογιστή αναγνώρισε τη συνδεδεμένη συσκευή Raspberry-Pi ως προσαρμογέα ασύρματου LAN και αυτόματα του εκχώρησε υψηλότερη προτεραιότητα σε σχέση με τις υπόλοιπες διαθέσιμες συνδέσεις. Το σημαντικότερο όμως είναι ότι έδωσε στον μικροϋπολογιστή πρόσβαση στη διαδικασία ανταλλαγής δεδομένων στο δίκτυο. Το πειραματικό δίκτυο ήταν μία προσομοίωση ενός πραγματικού τμήματος του εταιρικού δικτύου. Σαν αποτέλεσμα, οι ερευνητές ήταν σε θέση να συλλέξουν δεδομένα ελέγχου ταυτότητας που στέλνονταν από τον υπολογιστή που δεχόταν επίθεση και τις εφαρμογές του, καθώς προσπάθησαν να πιστοποιήσουν το domain και τους απομακρυσμένους server. Επιπρόσθετα, οι ερευνητές είχαν τη δυνατότητα να συλλέξουν τα ίδια δεδομένα και από τους υπόλοιπους υπολογιστές που ήταν συνδεδεμένοι στο ίδιο τμήμα δικτύου.

Ακόμα, καθώς οι προδιαγραφές της επίθεσης επέτρεπαν την αποστολή των υποκλεμμένων δεδομένων μέσω του δικτύου σε πραγματικό χρόνο, όσο περισσότερο η συσκευή παρέμενε συνδεδεμένη στον υπολογιστή τόσα περισσότερα δεδομένα ήταν σε θέση να συλλεχθούν και να μεταφερθούν σε έναν εξωτερικό server. Μετά από μόλις μισή ώρα πειραματισμών, οι ερευνητές μπορούσαν να συλλέξουν περίπου 30 διαφορετικούς κωδικούς

πρόσβασης, που μεταφέρονταν μέσω τον επιτιθέμενων δικτύων, οπότε είναι εύκολο να φανταστείτε πόσα πολλά δεδομένα μπορούν να συλλεχθούν μέσα σε μόνο μία ημέρα. Στο χειρότερο σενάριο, τα δεδομένα ελέγχου ταυτότητας του διαχειριστή μπορούν επίσης να κλαπούν κατά την προσπάθεια σύνδεσης στους λογαριασμούς τους και εφόσον η συσκευή είναι συνδεδεμένη σε έναν από τους υπολογιστές του συστήματος – δικτύου.

Η πιθανή επιφάνεια επίθεσης για αυτή τη μέθοδο υποκλοπής δεδομένων είναι μεγάλη: το πείραμα αναπαράχθηκε επιτυχώς τόσο σε κλειδωμένους όσο και σε ξεκλείδωτους υπολογιστές Windows και Mac OS. Ωστόσο, οι ερευνητές δεν μπόρεσαν να αναπαράγουν την επίθεση σε συσκευές που βασίζονται σε Linux.

«Υπάρχουν δύο βασικά πράγματα που μας ανησυχούν ως αποτέλεσμα αυτού του πειράματος: πρώτον – το γεγονός ότι δε χρειάστηκε στην πραγματικότητα να αναπτύξουμε το λογισμικό – χρησιμοποιήσαμε εργαλεία ελεύθερα διαθέσιμα στο Διαδίκτυο. Δεύτερον – ανησυχούμε για το πόσο εύκολο ήταν να προετοιμάσουμε την επικύρωση της ιδέας για τη hacking συσκευή μας. Αυτό σημαίνει ότι ενδεχομένως οποιοσδήποτε, που είναι εξοικειωμένος με το Διαδίκτυο και έχει βασικές δεξιότητες προγραμματισμού, θα μπορούσε να αναπαράγει αυτό το πείραμα. Και είναι εύκολο να προβλέψουμε τι θα μπορούσε να συμβεί εάν αυτό γινόταν με κακόβουλη πρόθεση. Ο τελευταίος είναι ο κύριος λόγος για τον οποίο αποφασίσαμε να επιστήσουμε την προσοχή του κοινού σε αυτό το πρόβλημα. Οι χρήστες και οι εταιρικοί διαχειριστές θα πρέπει να είναι προετοιμασμένοι για τέτοιου είδους επίθεση», δήλωσε ο Sergey Lurye, security enthusiast και συν-συγγραφέας της έρευνας της Kaspersky Lab.

Παρόλο που η επίθεση επιτρέπει την υποκλοπή των τιμών κατατεμαχισμού (hashes) των κωδικών (δηλ. μία κρυπτογραφική αλφαβητική ερμηνεία ενός κειμένου κωδικού πρόσβασης μετά την επεξεργασία του από έναν συγκεκριμένο αλγόριθμο κατατεμαχισμού), τα hashes μπορούν να αποκρυπτογραφηθούν σε κωδικούς πρόσβασης, δεδομένου ότι οι αλγόριθμοι είναι γνωστοί ή χρησιμοποιούνται σε pass-the-hash επιθέσεις.

Προκειμένου να προστατεύσετε τον υπολογιστή ή το δίκτυό σας από επιθέσεις με τη βοήθεια παρόμοιων DIY συσκευών, οι ειδικοί ασφαλείας της Kaspersky Lab συμβουλεύουν τα παρακάτω:

Για τακτικούς χρήστες:

1. Όταν επιστρέφετε στον υπολογιστή σας, ελέγξτε αν υπάρχουν επιπλέον συσκευές USB που εξέχουν από τις θύρες σας.
2. Αποφύγετε την αποδοχή flash drives από μη αξιόπιστες πηγές. Αυτή η μονάδα θα μπορούσε στην πραγματικότητα να είναι ένας υποκλοπέας κωδικού πρόσβασης.
3. Αποκτήστε τη συνήθεια να τερματίζετε τις συνεδρίες σε ιστότοπους που απαιτούν έλεγχο ταυτότητας. Συνήθως, αυτό σημαίνει να κάνετε κλικ σε ένα κουμπί “αποσύνδεσης”.
4. Να αλλάζετε τους κωδικούς πρόσβασης τακτικά – τόσο στον υπολογιστή σας, όσο και στις ιστοσελίδες που χρησιμοποιείτε συχνά. Θυμηθείτε ότι δεν χρησιμοποιούν όλες οι αγαπημένες σας ιστοσελίδες μηχανισμούς προστασίας από την αντικατάσταση δεδομένων cookie (cookie data substitution). Μπορείτε να χρησιμοποιήσετε εξειδικευμένο λογισμικό διαχείρισης κωδικών πρόσβασης για την εύκολη διαχείριση ισχυρών και ασφαλών κωδικών πρόσβασης, όπως το δωρεάν εργαλείο Kaspersky Password Manager.
5. Ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων ζητώντας, για παράδειγμα, επιβεβαίωση σύνδεσης ή χρήση ενός διακριτικού υλικού hardware.
6. Να εγκαταστήσετε και να ενημερώνετε τακτικά μια λύση ασφαλείας από έναν αποδεδειγμένο και αξιόπιστο προμηθευτή.

Για τους διαχειριστές συστημάτων

1. Αν το επιτρέπει η τοπολογία του δικτύου, προτείνουμε να χρησιμοποιείτε αποκλειστικά πρωτόκολλο Kerberos για τον έλεγχο ταυτότητας των χρηστών του domain.
2. Περιορίστε τους χρήστες με προνόμια στο domain από τη

σύνδεση στα συστήματα παλαιού τύπου, ειδικά οι διαχειριστές τομέα.

3. Οι κωδικοί πρόσβασης των domain users πρέπει να αλλάζονται τακτικά. Εάν, για οποιονδήποτε λόγο, η πολιτική του οργανισμού δεν συνεπάγεται τακτικές αλλαγές κωδικού πρόσβασης, φροντίστε να αλλάξετε αυτήν την πολιτική.
4. Όλοι οι υπολογιστές εντός ενός εταιρικού δικτύου πρέπει να προστατεύονται με λύσεις ασφάλειας και πρέπει να εξασφαλίζονται τακτικές ενημερώσεις.
5. Για να αποφευχθεί η σύνδεση μη εξουσιοδοτημένων συσκευών USB, μπορεί να είναι χρήσιμη μια λειτουργία ελέγχου συσκευής, όπως αυτή που είναι διαθέσιμη στη σουίτα Kaspersky Endpoint Security for Business.
6. Εάν είστε ιδιοκτήτης της διαδικτυακής πηγής, σας συνιστούμε να ενεργοποιήσετε το HSTS (αυστηρή ασφάλεια μεταφοράς HTTP), το οποίο εμποδίζει την εναλλαγή από το HTTPS σε πρωτόκολλο HTTP και την πλαστογράφηση των στοιχείων σύνδεσης από ένα κλεμμένο cookie.
7. Αν είναι δυνατόν, απενεργοποιήστε τη λειτουργία ακρόασης και ενεργοποιήστε τη ρύθμιση απομόνωσης Client (AP) σε Wi-Fi routers και switches, απενεργοποιώντας τους από την ακρόαση της κίνησης σε άλλους σταθμούς εργασίας.
8. Ενεργοποιήστε τη ρύθμιση DHCP Snooping για να προστατεύσετε τους χρήστες των εταιρικών δικτύων από τη λήψη αιτημάτων DHCP από πλαστούς DHCP server.

Εκτός από την παρεμπόδιση των δεδομένων ελέγχου ταυτότητας από εταιρικό δίκτυο, η πειραματική συσκευή μπορεί να χρησιμοποιηθεί για τη συλλογή cookies από προγράμματα περιήγησης στα μηχανήματα που δέχονται επίθεση.

Διαβάστε περισσότερα σχετικά με το πείραμα και τα μέτρα που μπορούν να ληφθούν για την προστασία εταιρειών και οικιακών χρηστών από επιθέσεις αυτού του τύπου στον ειδικό ιστότοπο Securelist.com.