Moonlight Maze: Μία 20ετής επίθεση που παραμένει ακόμα επίκαιρη

Οι ερευνητές της Kaspersky Lab και του Πανεπιστημίου King's College του Λονδίνου, αναζητώντας πώς συνδέεται ένας σύγχρονος απειλητικός φορέας με τις επιθέσεις Moonlight Maze που είχαν στόχο το Πεντάγωνο, τη NASA και άλλους οργανισμούς στα τέλη της δεκαετίας του '90, έφεραν στο φως δείγματα, αρχεία καταγραφής και αντικείμενα που ανήκουν στην «αρχαία» επίθεση τύπου APT. Τα ευρήματα δείχνουν ότι ένα backdoor που χρησιμοποιούνταν το 1998 από το Moonlight Maze για τη διοχέτευση πληροφοριών εκτός του δικτύου των θυμάτων συνδέεται με ένα backdoor που χρησιμοποιήθηκε από τον Turla το 2011 και, ενδεχομένως, και μέχρι το 2017. Αν η σχέση μεταξύ Turla και Moonlight Maze αποδειχθεί, θα τοποθετήσει τον εξελιγμένο απειλητικό φορέα μαζί με τον φορέα Equation Group αναφορικά με τη μακροβιότητά του, καθώς μερικοί από τους command-and-control servers του Equation χρονολογούνται από το 1996.

Σύγχρονες εκθέσεις για το Moonlight Maze δείχνουν ότι, ξεκινώντας από το 1996, στρατιωτικά και κυβερνητικά δίκτυα των ΗΠΑ, καθώς και πανεπιστήμια, ερευνητικά ιδρύματα και ακόμη και το Υπουργείο Ενέργειας ξεκίνησαν να εντοπίζουν παραβιάσεις στα συστήματά τους. Το 1998, το FBI και το Υπουργείο Άμυνας ξεκίνησαν μια τεράστια έρευνα. Η ιστορία είδε το φως της δημοσιότητας το 1999, αλλά πολλά από τα στοιχεία παρέμειναν απόρρητα, διατηρώντας άκρα μυστικότητα και αφήνοντας τις λεπτομέρειες για το Moonlight Maze να αποτελούν μύθο.

Με την πάροδο των χρόνων, αρχικοί ερευνητές σε τρεις διαφορετικές χώρες έχουν δηλώσει ότι το Moonlight Maze εξελίχθηκε στον Turla, ένα ρωσόφωνο απειλητικό φορέα γνωστό και ως Snake, Uroburos, Venomous Bear, και Krypton. Ο Turla θεωρείται συμβατικά ότι είναι ενεργός από το 2007.

Τα «ξεχασμένα» δείγματα

Το 2016, ο Thomas Rid από το Πανεπιστήμιο Kings College του Λονδίνου, ενώ βρισκόταν σε έρευνα για το βιβλίο του «Η Άνοδος των Μηχανών», εντόπισε έναν πρώην διαχειριστή συστήματος του οποίου ο υπηρεσιακός server είχε καταληφθεί ως proxy από τους επιτιθέμενους του Moonlight Maze. Αυτός ο server, με το όνομα «HRTest», είχε χρησιμοποιηθεί για να εξαπολύσει επιθέσεις στις ΗΠΑ. Ο πλέον συνταξιούχος επαγγελματίας του τομέα της Πληροφορικής είχε κρατήσει τον αρχικό server και αντίγραφα από οτιδήποτε αφορούσε τις επιθέσεις, τα οποία και έδωσε στο πανεπιστήμιο Kings College και στην Kaspersky Lab για περαιτέρω ανάλυση.

Οι ερευνητές της Kaspersky Lab, Juan Andres Guerrero-Saade και Costin Raiu, μαζί με τους Thomas Rid και Danny Moore από το πανεπιστήμιο Kings College, πέρασαν εννιά μήνες πραγματοποιώντας μια λεπτομερή τεχνική ανάλυση αυτών των δειγμάτων. Ανακατασκεύασαν τις λειτουργίες, τα εργαλεία και τις τεχνικές των επιτιθέμενων και διεξήγαγαν μια παράλληλη έρευνα για να δουν αν θα μπορούσαν να αποδείξουν τη σύνδεση που υποστηρίζεται ότι υπάρχει με τον Turla.

Το Moonlight Maze ήταν μία ανοικτού κώδικα, Unix-based επίθεση με στόχο τα συστήματα Solaris, με τα ευρήματα να δείχνουν ότι πιθανώς χρησιμοποιούσε ένα κενό ασφαλείας που υπήρχε στο LOKI2 (ένα πρόγραμμα που κυκλοφόρησε το 1996 και έδινε τη δυνατότητα στους χρήστες να εξάγουν δεδομένα από συγκαλυμμένα κανάλια). Αυτό οδήγησε τους ερευνητές στο να έχουν τη δυνατότητα για μία δεύτερη ματιά σε κάποια σπάνια δείγματα Linux που χρησιμοποιήθηκαν από τον Turla, τα οποία είχε ανακαλύψει η Kaspersky Lab το 2014. Με την ονομασία Penquin Turla, τα

συγκεκριμένα δείγματα βασίζονται επίσης στο LOKI2. Ακόμη, η επανεξέταση έδειξε ότι όλοι τους χρησιμοποιούσαν κώδικα που δημιουργήθηκε μεταξύ 1999 και 2004.

Είναι αξιοσημείωτο ότι αυτός ο κώδικας χρησιμοποιείται ακόμα και σήμερα σε επιθέσεις. Εντοπίστηκε ελεύθερος στο Διαδίκτυο το 2011, όπου πραγματοποιούσε επίθεση στην ελβετική αμυντική εταιρεία Ruag, μία επίθεση που αποδίδεται στον Turla. Έπειτα, το Μάρτιο του 2017, οι ερευνητές της Kaspersky Lab ανακάλυψαν ένα νέο δείγμα του backdoor Penquin Turla σε ένα σύστημα στη Γερμανία. Είναι πιθανό ότι ο Turla χρησιμοποιεί τον παλιό κώδικα για επιθέσεις σε υψηλής ασφάλειας οργανισμούς, καθώς ενδέχεται να είναι δυσκολότερο να παραβιαστούν χρησιμοποιώντας τα περισσότερο τυπικά εργαλεία των Windows.

«Στα τέλη της δεκαετίας του 1990, κανείς δεν προέβλεψε την εμβέλεια και την επιμονή μιας συντονισμένης εκστρατείας ψηφιακής κατασκοπείας. Πρέπει να αναρωτηθούμε γιατί οι επιτιθέμενοι είναι ακόμη σε θέση να αξιοποιούν με επιτυχία «αρχαίο» κώδικα για σύγχρονες επιθέσεις. Η ανάλυση των δειγμάτων του Moonlight Maze δεν είναι απλά μια συναρπαστική αρχαιολογική μελέτη. Είναι επίσης μια υπενθύμιση ότι οι αντίπαλοι με καλές πηγές δεν πρόκειται να πάνε πουθενά. Είναι στο χέρι μας να υπερασπιστούμε τα συστήματα αναπτύσσοντας τις κατάλληλες δεξιότητες», δήλωσε ο Juan Andres Guerrero-Saade, Ερευνητής Ασφαλείας στην Παγκόσμια Ομάδα Έρευνας και Ανάλυσης της Kaspersky Lab.

Τα αρχεία του Moonlight Maze που ήρθαν πρόσφατα στο φως αποκαλύψαν πολλές συναρπαστικές λεπτομέρειες σχετικά με το πώς πραγματοποιήθηκαν οι επιθέσεις χρησιμοποιώντας ένα πολύπλοκο δίκτυο proxies, και το υψηλό επίπεδο των δεξιοτήτων και των εργαλείων που χρησιμοποιούνταν από τους επιτιθέμενους. Περισσότερες πληροφορίες σχετικά με την ακολουθία της επίθεσης και την τυπολογία της μπορείτε να βρείτε εδώ.

Για περισσότερες πληροφορίες μπορείτε να διαβάσετε το blogpost στον ειδικό ιστότοπο Securelist.com.

Τα προϊόντα της Kaspersky Lab εντοπίζουν και εμποδίζουν το κακόβουλο λογισμικό που χρησιμοποιείται από τα Moonlight Maze και Penguin Turla.

Αναλυτική Πληροφόρηση για τις τελευταίες απειλές και απειλητικούς φορείς είναι διαθέσιμη στους πελάτες της Kaspersky Lab μέσω της υπηρεσίας «Kaspersky Lab APT Intelligence reporting». Εδώ μπορείτε να βρείτε περισσότερες πληροφορίες.