ΕΛΛΑΚ - Επεισόδιο Data Exfiltration

Ευρήματα

Από τη διαδικασία αναζήτησης και ανάλυσης προέκυψαν ένα υπολογιστικό φύλλο excel με διάφορες απόρρητες πληροφορίες καθώς και ένα σκαρίφημα (blueprint) ενός αεροσκάφους σε 6 διαφορετικά τμήματα.

Αναλυτική Περιγραφή

Ξεκινήσαμε ελέγχοντας όλες τις σελίδες στο root application καθώς και τον html και css κώδικα αυτών προκειμένου να βρούμε οποιουδήποτε είδους hints. Παράλληλα δοκιμάσαμε κοινότυπα urls προς ανακάλυψη τυχόν άλλων βοηθητικών υπηρεσιών χωρίς επιτυχία.

Η πρώτη επιτυχής ανακάλυψη ήταν το αρχείο ήχου **intro19.wav** στη σελίδα *Career* > *Apply now*, η τροφοδότηση του οποίου σε *spectrum analyzer* έφερε στο φως 5 κωδικούς οι οποίοι χρησιμοποιήθηκαν αργότερα. Επιπλέον, με επιθεώρηση των *cookies* στον browser πήραμε το εξής μήνυμα το οποίο παρείχε βασικές πληροφορίες για την ολοκλήρωση του επεισοδίου: `info: Follow the robots. Always check for page0. Check F36.jpeg metadata. Passwds in intro music.`

Η ανάλυση των metadata της εικόνας **F36.jpeg** παρείχε το μήνυμα `Go to dir /cache89xyz`. Παράλληλα, βρίσκοντας το αρχείο **robots.txt** στο root application αποκτήσαμε επιπλέον πληροφορία για την ύπαρξη τριών πιθανών επόμενων προορισμών (**/admin**, **/data**, **/backup1**) εκ των οποίων μόνο ο ένας ήταν έγκυρος (**/backup1**). Στη σελίδα **page0** αυτού επαναλάβαμε την επιθεώρηση του html κώδικα, αποκαλύπτωντας κρυφό link προς τη σελίδα **HELLO.html**. Σε αυτή τη σελίδα, ο κώδικας html υπέδειξε την ύπαρξη μιας μικρής εικόνας (**02.jpg**), προσαρμοσμένη επάνω στη μεγάλη, η οποία αποτέλεσε και το πρώτο σημαντικό εύρημα - ένα από τα κομμάτια του σκαριφήματος. Πλέον ήταν εμφανές ότι η τελική λύση θα αποτελούνταν από τουλάχιστον 3 ακόμη τμήματα εικόνας τα οποία θα ήταν κρυμμένα πιθανώς μέσα σε άλλα αρχεία εικόνας. Στην ίδια σελίδα, ο html κώδικας υπέδειξε και δύο ακόμη μηνύματα: `Use openstego for cache item` και `3: use PDFMtEd`. Επίσης, η εικόνα **S402.jpeg** στη σελίδα **page0** συνοδευόταν από βοηθητικό μήνυμα `steghide S402`. Χρησιμοποιώντας τον πρώτο από τους κωδικούς που ανακαλύψαμε στην αρχή μπορέσαμε να εξάγουμε από αυτή ένα ακόμη τμήμα του απόρρητου σκαριφήματος. Στο directory **/cache89xyz/page0** βρήκαμε την εικόνα **S403.png**.

Τροχοπέδη στην όλη προσπάθεια αποτέλεσε η ανακάλυψη της σελίδας **test.html** στο root application η οποία περιείχε παραπλανητικές πληροφορίες που δεν βοήθησαν στη λύση του επεισοδίου.

Από το αρχείο **robots.txt** στα directories **/backup1** και **/cache89xyz** ανακαλύφθηκαν δύο επιπλέον directories με πληροφορίες, τα **/backup1/more/** και **/cache89xyz/north19/** αντίστοιχα. Από το πρώτο εξ αυτών, χρησιμοποιώντας την base64 encoded συμβολοσειρά που υπήρχε μέσα στο αρχείο **style22.css** καταλήξαμε στο τρίτο κομμάτι του σκαριφήματος. Ταυτόχρονα, από το δεύτερο, εξάγαμε από το αρχείο **secure.zip** με χρήση του δεύτερου από τους κωδικούς που είχαμε ανακαλύψει, το αρχείο ήχου **secret05sound**.

Στον html κώδικα της **cache89xyz/north19/page0.html** υπήρχε μήνυμα που υποδείκνυε τον έλεγχο των metadata της εικόνας **S401.jpg** που συνόδευε το zip. Μέσα από αυτή τη διαδικασία προέκυψε περαιτέρω πληροφορία για την αποδιαμόρφωση του αρχείου ήχου και την αποκωδικοποίησή του κατά base64 μέσω του comment "`unzip, minimodem (4800), base64`". Έτσι προέκυψε το τέταρτο κομμάτι του σκαριφήματος. Επίσης, με χρήση του προγράμματος binwalk, ανακαλύφθηκε μέσα στην εικόνα **Navy2.png** αρχείο xlsx με απόρρητες πληροφορίες σε μορφή zip.

Από το αρχείο **/docs/Presence.pdf**, με χρήση του προγράμματος PDFMtEd, ανακαλύφθηκε στα headers του αρχείου ακόμη μία συμβολοσειρά η οποία, με αποκωδικοποίηση base64, έδωσε το πέμπτο κομμάτι του σκαριφήματος. Τέλος, με χρήση του openstego (παλιά έκδοση που χρησιμοποιεί αλγόριθμο κρυπτογράφησης DES) πάνω στην εικόνα S403.png που είχαμε ήδη βρει, εξάγαμε το τελευταίο κομμάτι του σκαριφήματος.

Εργαλεία που χρησιμοποιήθηκαν

Sonic Visualiser, exiftool, pngcheck, openstego, steghide, burpsuite, dirb, binwalk, bulk_extractor