Αναφορά επεισοδίου 7
Social Network Communication Analysis

ΠΑΝΟΠΤΗΣ 2019

ΟΜΑΔΑ ΕΕΛΛΑΚ - ΒΟΛΟΣ

1 Αρχή του επεισοδίου

Το επεισόδιο αρχικά δεν παρήχε αρκετά στοιχεία ή hints για την επίλυση του, οπότε ψάξαμε την σελίδα του Panagiotis Optakis στο facebook και είδαμε τα ποστ του με χρονολογική σειρά. Η εκφώνηση έκανε λόγο για ανταλλαγή μηνυμάτων σε χρονολογική σειρά σε 3 φάσεις, και ποστς που σχετίζονται με το χόμπυ του υπόπτου. Γρήγορα καταλάβαμε ότι το χόμπυ του υπόπτου είναι η φωτογραφία, έχοντας ο ίδιος μια σελίδα wix με φωτογραφίες, μοιρασμένες μάλιστα σε Day 1,2,3 που θεωρήσαμε ότι ήταν αναφορά στις 3 χρονικές φάσεις της εκφώνησης.
Πριν γίνει προσπάθεια να αναλυθούν οι φωτογραφίες στο wix έγινε και μια προσπάθεια ανάλυσης της φωτογραφίας προφίλ του, που όπως φαινόταν πειραγμένη, έτσι αποδείχθηκε κιόλας βλέποντας στο xxd της φωτογραφίας το κείμενο Photoshop 3.0, χωρίς κάτι άλλο άξιο αναφοράς.

2 Διαφορές μεταξύ ”ίδιων” εικόνων

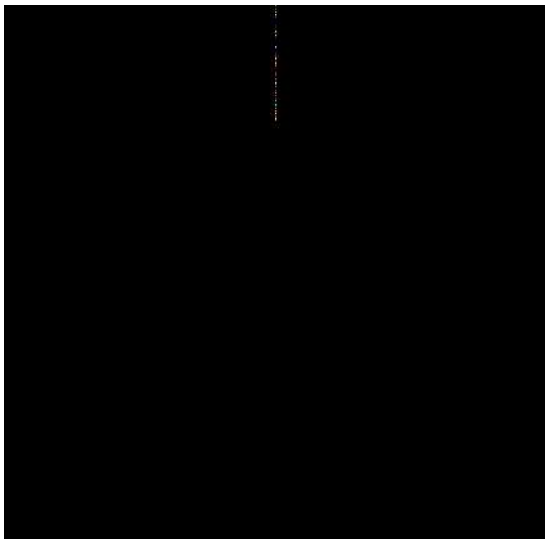
Ακολούθησαν κάποιες αναλύσεις μεταξύ ίδιων στο μάτι φωτογραφιών από διαφορετικές ημέρες με εργαλεία όπως το winmerge αρχικά και φάνηκε ότι στα δεδομένα τους δεν είναι ίδιες άρα μπορεί να κρύβουν δεδομένα στις διαφορές, που μας οδήγησε και σε ιδέες visual steganography, xor ομοίων φωτογραφιών κλπ. Αυτό μας οδήγησε στο να δούμε χρησιμοποιώντας το stegsolve με image combining και συγκεκριμένα την πράξη SUB (παρόμοια με τη χρήση compare από cli), ότι υπήρχε σε όμοιες φωτογραφίες μια γραμμή στο κέντρο και ψηλά με μεγάλες διαφορές στα δεδομένα που σχημάτιζαν μια γραμμή όπως στην εικ.1.
Αυτή η διαφορά παρουσίασε ενδιαφέρον που στην αρχή σκεφτήκαμε κώδικα morse, όμως απορρίψαμε την ιδέα καθώς οι παύλες δεν ήταν ίδιου μήκους. Επίσης απορρίψαμε προσωρινά το lead καθώς η εκφώνηση δεν συσχέτιζε χρονικά τις εικόνες οπότε έπρεπε να ασχοληθούμε αποκλειστικά με φωτογραφίες της day1.
Στη συνέχεια εφαρμόσαμε μια πληθώρα stego analysis tools σε μεμονωμένες εικόνες όπως το stegano, το zsteg, το pngcheck, το binwalk, το strings, το cloacked_pixel, το exiftool και άλλα. Όμως δεν βρήκαμε κρυφά μηνύματα ή leads κοιτώντας μεμονωμένα εικόνες.

3 Hint 1: PIL and LSB

Το πρώτο χιντ που δώθηκε μας οδήγησε στο να χρησιμοποιήσουμε σε custom python scripts την βιβλιοθήκη PIL (Python Imaging Library) για να πάρουμε τα LSB (Least Significant Byte) από τις RGB τιμές των πίξελ και να προσπαθήσουμε να σχηματίσουμε μηνύματα. Δοκιμάστηκαν ξεχωριστά να μπουν σε σειρά τα LSBs από red, green, blue, αλλά και μαζί σε μορφή r1g1b1r2g2b2 κλπ χωρίς τύχη σε μεμονωμένες εικόνες. Ύστερα δοκιμάστηκε και π.χ. τα LSB της πρώτης σειράς κάθε φωτογραφίας με τη σειρά, επίσης χωρίς κάποιο ευνόητο μήνυμα.

4 Λύση Day 1

Η day 1 λύθηκε όταν παρατηρήσαμε την ύπαρξη όμοιας εικόνας στο ίδιο day , και συγκεκριμένα τις 5 και 7. Κάνοντας την πράξη sub όπως και πριν με το stegsolve, παρατηρήσαμε ότι και εδώ είχαμε ένα stripe με διαφορετικά δεδομένα που άξιζε να αναλύσουμε με python.



Εικ. 1. SUB 5.png 7.png

Έτσι, βρήκαμε ότι η γραμμή είναι ακριβώς στο κέντρο της 800χ800 εικόνας, και συγκεκριμένα στην στήλη 400. Χρησιμοποιώντας αυτό σαν lead πήραμε από μια τυχαία εικόνα (5.png) τα LSB και των τριών RGB values για κάθε pixel της στήλης 400 της εικόνας. Τοποθετώντας το stream των bits σε ένα binary to ascii converter είδαμε ότι προκύπτουν στην αρχή χαρακτήρες που δεν είναι ”gibberish”. Μοιάζαν με base64 και το decode μας το επιβεβαίωσε.
Έτσι, εκμεταλλευόμενοι και την εκφώνηση που έλεγε να αποκρυπτογραφήσουμε το μήνυμα αναλύοντας και τοποθετώντας τις εικόνες στη σωστή σειρά, πήραμε με τη σειρά τις εικόνες της πρώτης ημέρας ενώσαμε τα μηνύματα και βγάλαμε το μήνυμα της day 1:

Here are the instructions of the first attack. These are the coordinates that we will meet, Latitude 38.979677 Longitude 21.384962 and these are the coordinates of the target, Latitude 38.844609 Longitude 21.428907. The attack will take place on Tuseday 21:00. The van with the explosive will be already there. Hope our mail is well hidden. Make sure no one see you!!

Ο κώδικας που χρησιμοποιήσαμε για εξαγωγή του binary ήταν:

Εικ. 2. 5.png: LSB 400ής στήλης to ascii to base64 decode

Listing 1.1. Code for *LSB.py*

```
from PIL import Image
import numpy

im1 = Image.open("/home/anon/Downloads/Panoptakis_wix/Day2/1.png")
np_im1 = numpy.array(im1)

for k in range(400):
    for j in range(3):
        print (np_im1[k][400][j] & 1, end="")
```

5 Hint 2

Το hint που κοινοποιήθηκε έκανε λόγο για τη χρήση της βιβλιοθήκης fernet, που ουσιαστικά αφορά symmetric cryptography και θα την είχαμε υπόψη μας σε περίπτωση ύπαρξης ενός cyphertext και ενός κλειδιού. Κατασκευάσαμε και ένα γρήγορο python script για γρήγορη αποκρυπτογράφηση με fernet.

6 Day 2

Ακολουθώντας την μεθοδολογία της Day 1 ελέγξαμε την ύπαρξη διαφορετικών data στην 400η στηλη 2 ”ίδιων” εικόνων και υπήρχαν. Ακολουθώντας την ίδια διαδικασία LSB to Binary streams to Ascii εντοπίσαμε στην φωτογραφία 29.png της 2ης ημέρας το ascii string:

```
TheKeyForTheDecryptionIsiBcA84yu9qtsRdsiU4sVKxHv63JeTDzT3BhXWk-
WJDI=
```

Αναμένουμε ότι είναι το κλειδί για την αποκρυπτογράφηση με fernet ενός cyphertext της ημέρας 2.

7 Λύση Day 2

Αρχικά δοκιμάσαμε να βάλουμε με αριθμητική σειρά όπως και πριν τα cyphertexts των εικόνων χωρίς αποτέλεσμα, αφού δεν λειτουργούσε το decryption με fernet. Έτσι, αρχικά απορρίψαμε τις φωτογραφίες που δεν είχαν δεδομένα που φαινόταν να είναι αναγνώσιμοι ascii χαρακτήρες και την εικόνα που είναι το κλειδί, που έτυχε και να αντιστοιχούν στις φωτογραφίες 11,12,13,14,15 της Day1. Έτσι, κατασκευάσαμε ενα python script για να κάνουμε bruteforce όλες τις διαφορετικές σειρές των μηνυμάτων (9! permutations). Και βρήκαμε το κρυφό μήνυμα σχετικά γρήγορα:

> As you all understood our messages got decrypted. But, i have come up with better hidding techniques so there is nothing to be afraid of. Here are the new coords of the next target. Our meeting point, Lat 37.923677 Long 22.334262 and the target, Latitude 35.846699 Longitude 20.421958. The attack will take place on Thursday at 20:00.

Ο κώδικας που χρησιμοποιήθηκε ήταν:

Listing 1.2. Code for *Bruteforcing.py*

```
from cryptography.fernet import Fernet
from itertools import permutations

# Extracted keys
key1 = b'iBcA84yu9qtsRdsiU4sVKxHv63JeTDzT3BhXWkWJDI='

# Create fernetshits
f1 = Fernet(key1)

# Initial fernetshit
initialfernet = b'gAAAAABc_myj4Lh_cKxJbAumHewUUmh0Q7jJ2t4PnAflx56DUihF'

# Other fernetshits
parts = [
    b'vIWjht1AhAQGVRwHVHz0dWGPaSMaq222vjpm3rdsIkoNcO1TrRJZ',
    b'KlV-e5h3BZ1AY1FglcGmiR_2zaqBQaLzVzbtr7o3FN5alUspWUnv',
    b'1oPKXHxp4VoNBkhT6M03I1_bmhTOO9BRH14lNixouuRGPdUs1zdX',
    b'P-gDUxFJrGmzvBYMe_thCdhzrxEHrmm0SjtVzdFBUmI731xy14kr',
    b'zuTZKuwnuT9Ngz75wQIQliePmohODo1rUcPtFS0qTAvR0BeChMJ7',
    b'qNezoihYp535X2g8tD22JIW3YDDDMA7HB5XI3p1DeKz6mCHPyTal',
    b'VlkY1PIe-ZUeB2GtfKJt3uYL3h6lmr4uD3lL5mx9NQF4IoYg_XRs',
    b'dyIuwfzT_6YcAjBOuNqf9ma3MlX9nWXXnt573vpeDZfq1YN_Hx2s',
    b'UY_9M3WjItDxA71eTZ1PFD1jxHdIXTa1EiP9LkR13rsF3QbaejeVz1KQ' # This one seems
        off
]

# Get all permutations
perms = permutations(parts)

for perm in perms:
```

```
        ciphertext = initialfernet
        for part in perm:
            ciphertext += part
    try:
        deciphered1 = f1.decrypt(ciphertext)
        print(deciphered1)
        input('Waiting for input...')
    except Exception as e:
        pass
```

8 Day 3

Ακολουθώντας την ίδια μεθοδολογία εντοπίσαμε σε φωτογραφία της Day 3 το ascii string:

TheKeyForTheDecryptionIsNgmAlpbEwK9yZ33–dRxe2nKOU5P7LysvcnbgmtIZxg=

Αναμένουμε ότι είναι το κλειδί για την αποκρυπτογράφηση με fernet ενός cyphertext της ημέρας 3.

9 Λύση Day 3

Για την day 3 ακολουθήσαμε την ίδια διαδικασία. Παρατηρήσαμε ότι παρά τις πολλές φωτογραφίες υπήρχαν διπλότυπα των cyphertexts σε διάφορες φωτογραφίες. Επίσης εύκολα ξεχωρίσαμε το κομμάτι της αρχής και του τέλους του cyphertext οπότε είχαμε να κάνουμε 4! permutations για να βρούμε τη λύση. Και βρέθηκε:

Comrades viva la revolution. Attack on the building of the parliament and on the building of the presidential authority on the elections day 7th of July 2019 07072019 at 190707 time EET. Firing squad teams and bomb squad teams to plan and act jointly with sharp precision and decisive force. Be ready for glory. People will remember our actions for ever.

10 Acknowledgements

Ευχαριστούμε το Πανεπιστήμιο Θεσσαλίας, τον καθ.Χρήστο Αντωνόπουλο ,τη γραμματεία του ΤΗΜΜΥ και τον καθηγητή Βασίλειο Βλάχο του ΤΕΙΛΑΡ για τη βοήθεια τους, όπως και όλη τη συντονιστική ομάδα του Πανόπτη 2019 για τη συνεργασία.