# Data Leakage Progress

Ζητείται η διεύθυνση MAC του υπολογιστή του υπόπτου και στοιχεία που να αποδεικνύουν την κακόβουλη ενέργεια εις βάρος της εταιρείας.

Αναλύοντας το αρχείο traffic.pcap που μας δόθηκε ανακαλύπτουμε ότι ο χρήστης έχει κατεβάσει γνωστό λογισμικό στεγανογραφίας (SilentEye, Stegomagic). Επίσης, παρατηρουμε ότι έχει πραγματοποιήσει google search για οδηγίες στεγανογράρφισης και απόκρυψης δεδομένων σε αρχεία ήχου και εικόνας. Επίσης, φαίνεται ότι ο ύποπτος χρήστης έχει ανεβάσει στο uptobox.com ένα αρχείο με όνομα ProductSales-students.part1-rar.axx και έχει κατεβάσει το λογισμικό Axcrypt, με το οποίο κωδικοποίησε το συγκεκριμένο αρχείο. Από περεταίρω αναζήτηση, μαθαίνουμε ότι το λογισμικό αυτό κωδικοποιεί αρχεία χρησιμοποιώντας “κλειδιά” (keyfiles), τα οποία πρέπει να ανακτήσει όποιος επιθυμεί να το αποκωδικοποιήσει. Επομένως επικεντρωνόμαστε στην ανάκτηση των keyfiles.

**Πληροφορίες υπόπτου:**

IP Address   : 192.168.66.207 , MAC-Address: cadmusco\_1c:c4:44 08:00:27:1c:c4:44

[#GET /projects/silenteye/files/Application/0.4/silenteye-0.4.1-win32.exe/download HTTP/1.1

Host: [sourceforge.net](http://sourceforge.net)

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:41.0) Gecko/20100101 Firefox/41.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,**​/​**;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer:<http://www.silenteye.org/download.html?i2>

Connection: keep-alive

Από τα 4 emails που μας δίνονται, παρατηρούμε σημεία με κωδικοποιημένη πληροφορία Base64.

Αποκωδικοποιούμε τα σημεία αυτά με Base64 και παίρνουμε σαν έξοδο τα παρακάτω:

**1)** Το email που στάλθηκε στις **Fri Feb 29 03:29:15 2016** περιέχει την πληροφορία:

*Odigies: Gia tin oloklirosi tou epeisodiou tha xreiastei na sygkentrosete epta (7) synolika "stoixeia-tmimata" (parts) ta opoia tha sas dosoun ti lysi tou epeisodiou. | I ekseliksi tou einai ayksanomenis dyskolias kai xrisimopoiithikan ergaleia kai texnikes pou kalyptoun to megalytero fasma tis steganographias kai ton texnologion pou xrisimopoiountai. | Kata ti diarkeia tis askisis tha dinontai, efoson zitithoun, hints pou tha voithisoun stin ekseliksi tou epeisodiou. | Mporeite na ksekinisete tin epilysi tou epeisodiou arxizontas apo to 2o mail.%PDF-1.5*

Οι επόμενες γραμμές αποτελούσαν ένα κρατικό έγγραφο σε μορφή PDF: <https://drive.google.com/open?id=0B3Mkr-G7WiW3MGJ2c1FDcDd6SnM>

**2)**Το email που στάλθηκε στις **Thu Mar 10 03:30:33 2016** περιέχει 2 εικόνες JPG:

Image1: <https://drive.google.com/open?id=0B3Mkr-G7WiW3LWp1UTY2SUlhWU0>

Image2: <https://drive.google.com/open?id=0B3Mkr-G7WiW3SkRhQUpXTkxkbEE>

Παρατηρούμε ότι η 1η εικόνα περιέχει ΚΑΙ ΑΥΤΗ Base64 κωδικοποίηση σε ένα σημείο της!

Επίσης, το μέγεθος της 2ης εικόνας είναι σχετικά μεγάλο. Αυτό μας δημιούργησε υποψίες για κρυφά data μέσα στην εικόνα.

**3)**Το email που στάλθηκε στις **Wed Mar 18 03:32:47 2016** περιέχει την JPG εικόνα: <https://drive.google.com/open?id=0B3Mkr-G7WiW3Nmx6V3F4WkdIS2M>

Αλλάζοντας την κατάληξη της εικόνας αυτή σε RAR παρατηρούμε ότι μέσα της περιέχει μια εικόνα με όνομα *inception\_movie\_poster\_high\_definition.jpg* <https://drive.google.com/open?id=0B3Mkr-G7WiW3VUc5ck5sbWhSWG8>

**4)**Το email που στάλθηκε στις **Wed Mar 18 03:32:47 2016** περιέχει την **cyber.jpg** εικόνα: <https://drive.google.com/open?id=0B3Mkr-G7WiW3Mk8wOWpSc29adjg>

[Όλα τα παραπάνω email περιείχαν και ενοχοποιητικά μηνύματα, όπως το email4 που ειδοποιεί τον παραλήπτη ότι η ασφάλεια έχει γίνει αυστηρότερη και πρέπει να αλλάξει μορφή η επικοινωνία τους.](https://drive.google.com/open?id=0B3Mkr-G7WiW3Mk8wOWpSc29adjg)

Γνωρίζοντας ότι ο χρήστης-στόχος έχει στην κατοχή του το SilentEye εκτελούμε στεγανάλυση σε όλες τις εικόνες αποκρυπτογραφώντας με το προεπιλεγμένο password το “SilentEye”.

Από την εικόνα IMAGE\_1 παίρνουμε ένα text αρχείο το οποίο μας βοηθάει στην ανακάλυψη του ProductSales-students.part2-rar.axx, το οποίο είναι κρυμμένο στην image2 από το ίδιο email.

Αυτό το είχαμε υποπτευθεί ήδη, καθώς βρίσκοντας την αυθεντική εικόνα μέσω του google reverse image search και συγκρίνοντάς την (diff) με την τροποποιημένη, παρατηρούμε ότι έχουν προστεθεί δεδομένα προς το τέλος της εικόνας, χωρίς να έχει υποστεί άλλη αλλοίωση. Τα δεδομένα ήταν σε base64 και είχαν ίδιο μέγεθος με το ProductSales-students.part1-rar.axx, το οποίο ήταν αρκετό για να μας υποψιάσει ότι βρήκαμε το 2ο μέρος.

Η εικόνα *inception\_movie\_poster\_high\_definition.jpg* μας δίνει: *1cDE Npyd nIn3 FDPZ Lprl 3hJn Fw0M 58wW oyEJ Ydll 8Fg=*, το οποίο είναι και το πρώτο Keyfile*.*

[SilentEye - Steganography is yours](http://www.silenteye.org/download.html?i2)   SilentEye is a cross-platform application design for an easy use of steganography, in this case hiding messages into pictures and sounds. It provides a pretty nice interface and an easy integration of new steganography algorithm and cryptography process by using a plug-ins system.

Η εικόνα cyber.jpg από το email 4 είναι στεγανογραφημένη με το steghide καθώς φαίνεται το Watermark στην μέση της εικόνας. Από την στεγανάλυση προκύπτει αρχείο με το παρακάτω περιεχόμενο:

*+++++ +++++ [->++ +++++ +++<] >++++ .<+++ [->++ +<]>+ ++..- ---.+ ++.<+*

*+++++ +[->- ----- -<]>- ----- --.<+ ++[-> ---<] >--.. <++++ ++++[ ->+++*

*+++++ <]>++ +++++ +++.< +++[- >---< ]>-.+ +++++ .-.+. <++++ ++++[ ->---*

*----- <]>-- ----- .<+++ ++++[ ->+++ ++++< ]>+++ .+++. <++++ +++[- >----*

*---<] >---- -.<++ +[->+ ++<]> +.<++ +[->+ ++<]> ++.<+ +++++ +[->+ +++++*

*+<]>+ .--.< +++++ +++[- >---- ----< ]>--- -.<++ ++++[ ->+++ +++<] >+++.*

*<+++[ ->--- <]>-- ----. <++++ [->-- --<]> ---.< +++[- >+++< ]>+++ .<+++*

*+++[- >++++ ++<]> ++.<+ +++++ [->-- ----< ]>--. <*

*https://drive.google.com/file/d/0B6B-Q38gA6WqR3ltUUpnTDNjTDg/view?usp=sharing*

Ο σύνδεσμος αυτός περιέχει ένα αρχείο ήχου που μας λέει τους αριθμούς :

2 18 1 9 14 6 21 3 11

Για Α=1, Β=2, κτλ οι αριθμοί αυτοί μας δίνουν την λέξη “BRAINFUCK”

Η εκτέλεση του κώδικα brainfuck δίνει το παρακάτω URL: <https://youtu.be/9Dvt0WH5AgA>

To video ονομάζεται “welcome to the next level”

To link παραπέμπει σε youtube video με παράξενους ήχους. Κάναμε το video convert σε mp3. Επίσης η σελίδα του youtube παραπέμπει το link:<https://twitter.com/opanoptis>

Η επεξεργασία του ήχου με audacity εμφανίζει το φάσμα των ήχων που σχηματίζει το παρακάτω μήνυμα: “Congratulations you are almost there! Here is the password to decrypt the file. Password: Pa\_16\_\_“

Στο twitter, παρατηρούμε 2 ύποπτα μηνύματα:

1. Animated\_57049.mp4 seead://octgp.rzzrwp.nzx/zapy?to=0M6M-B38rL6HbmvatFECKlOKJCHX
2. ykkgj://uizmv.xffxcv.tfd/wzcv/u/0S6S-H38xR6NhQLL4MYIqKeV4P1b/mzvn?ljg=jyrizex

Τα μηνύματα είναι encrypted με ceasarian cipher.Χρησιμοποιούμε το online decrypter: http://www.xarg.org/tools/caesar-cipher/

Μήνυμα 1) με n= 15 αποκαλύπτεται το μήνυμα : <https://drive.google.com/open?id=0B6B-Q38gA6WqbkpiUTRZaDZYRWM>

Μήνυμα 2) με n=9 αποκαλύπτεται το μήνυμα :

<https://drive.google.com/file/d/0B6B-Q38gA6WqZUU4VHRzTnE4Y1k/view?usp=sharing>

Από link <https://drive.google.com/open?id=0B6B-Q38gA6WqbkpiUTRZaDZYRWM>

κατεβάζουμε το αρχείο : Animated\_57049.mp4

Χρησιμοποιώντας το εργαλείο Stegomagic (binary version), δίνοντας ως είσοδο για αποκρυπτογράφιση το παραπάνω video με κωδικό 57049 (από το όνομα του αρχείου) πήραμε μια εικόνα (cybersecurity\_54.jpg).

Εδώ πρέπει να σημειωθεί ότι η εικόνα δεν ονομαζόταν όντως έτσι και έλειπε πληροφορία για το παραπάτω βήμα!

Εφαρμόζοντας το Stegomagic (text version) στην παραπάνω εικόνα δίνοντας ως κωδικό το 54 από το όνομά της, πήραμε ένα keyfile ακόμα (keyfile2).

Από link <https://drive.google.com/file/d/0B6B-Q38gA6WqZUU4VHRzTnE4Y1k/view?usp=sharing>

κατεβάζουμε το αρχείο : cloaked.jpg

Ανοίγοντας με text editor το cloaked.jpg εντοπίσουμε το παρακάτω link στο τέλος του αρχείου:

<https://drive.google.com/file/d/0B6B-Q38gA6WqSWJ1VUpvc05nQVE/view?usp=sharing>

Σε αυτό το link αποκτάμε το 3ο μέρος του encrypted αρχείου ProductSales-student.part3-rar.axx.

Επίσης, χρησιμοποιώντας το εργαλείο steghide και ως passphrase την λέξη “anonymous” που βρήκαμε από το περιεχόμενο της εικόνας (μάσκα anonymous), πήραμε το τελευταίο keyfile (keyfile3).

Φαίνεται πως κάθε part χρησιμοποιεί διαφορετικό key file και όλα έχουν το ίδιο password για να γίνουν decrypt.

Έχοντας ανακτήσει τα παραπάνω στοιχεία, δηλαδή τα 3 parts του .rar και τα 3 keyfiles, παρατηρώντας ότι τα 2 πρώτα αρχεία (part1, part2) έχουν το ίδιο μέγεθος, με το τρίτο αρχείο να είναι κατά πολύ μικρότερό τους, υποψιαζόμαστε ότι έχουμε όλα τα τμήματα της πληροφορίας που προσπαθεί να στείλει ο υποκλοπέας. Επομένως, χρησιμοποιώντας το Axcrypt με τα keyfiles 1,2,3 στα αντίστοιχα parts, παίρνουμε τα αποκρυπτογραφημένα τμήματα του ProductSales-students.rar. Προχωρώντας σε αποσυμπίεση, καταλήξαμε στο αρχείο ProductSales-student.mdb, το οποίο περιέχει μέσα τα ευαίσθητα δεδομένα που εκλάπησαν από την εταιρεία.