Πρώτοι Ανταποκριτές : Ασφαλής συλλογή ψηφιακών πειστηρίων – A case Study

- ΚΑΤΣΟΥΛΗΣ Ν. Δημήτριος (MSc, CFCE, ACE)
Διεύθυνση Εγκληματολογικών Ερευνών
7ο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων

Διεύθυνση Εγκληματολογικών Ερευνών

- Αποτελεί την Εθνική Εγκληματολογική Υπηρεσία της χώρας, με έδρα την Αθήνα.

- Είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται διοικητικά απευθείας στον Αρχηγό της ΕΛ.ΑΣ.

Τμήμα Εξέτασης Ψηφιακών Πειστηρίων

- Ιδρύθηκε το 2012 ως αυτόνομο Τμήμα της Διεύθυνσης Εγκληματολογικών Ερευνών, με αντίστοιχο εργαστήριο στην Βόρεια Ελλάδα.

- Το Τμήμα στελεχώνεται από 33 Αστυνομικούς:
- 10 είναι Αστυνομικοί Ειδικών Καθηκόντων,
- 23 είναι Αστυνομικοί Γενικών Καθηκόντων

Τμήμα Εξέτασης Ψηφιακών Πειστηρίων

- Ακολουθείται Σύστημα Διαχείρισης Ποιότητας.
- Έχει πιστοποιηθεί με το Διεθνές Πρότυπο ΕΛΟΤ/ISO 9001:2015 και έχει διαπιστευθεί με το Διεθνές Πρότυπο ΕΛΟΤ EN ISO/IEC 17020.
- Εφαρμόζονται οι αρχές και οι κατευθυντήριες οδηγίες του ENFSI (European Network of Forensic Science Institutes).

Τμήμα Εξέτασης Ψηφιακών Πειστηρίων

Αντικείμενο - Αποστολή

Ενεργεί:

- εξετάσεις,
- ανάκτηση/επαναφορά,
- αποκρυπτογράφηση
- ανάλυση,
- σύγκριση και
- καταγραφή δεδομένων

Ψηφιακή Εγκληματολογία

Ορισμός:

Η επιστήμη ανάκτησης στοιχείων από τα ψηφιακά πειστήρια υπό συγκεκριμένες τεχνικές και αναλύσεις χρησιμοποιώντας αποδεκτές μεθόδους (Wayne Jansen, 2007)

Ψηφιακή Εγκληματολογία

Νομικά Αποδεκτές μέθοδοι – Κύρια Στοιχεία:

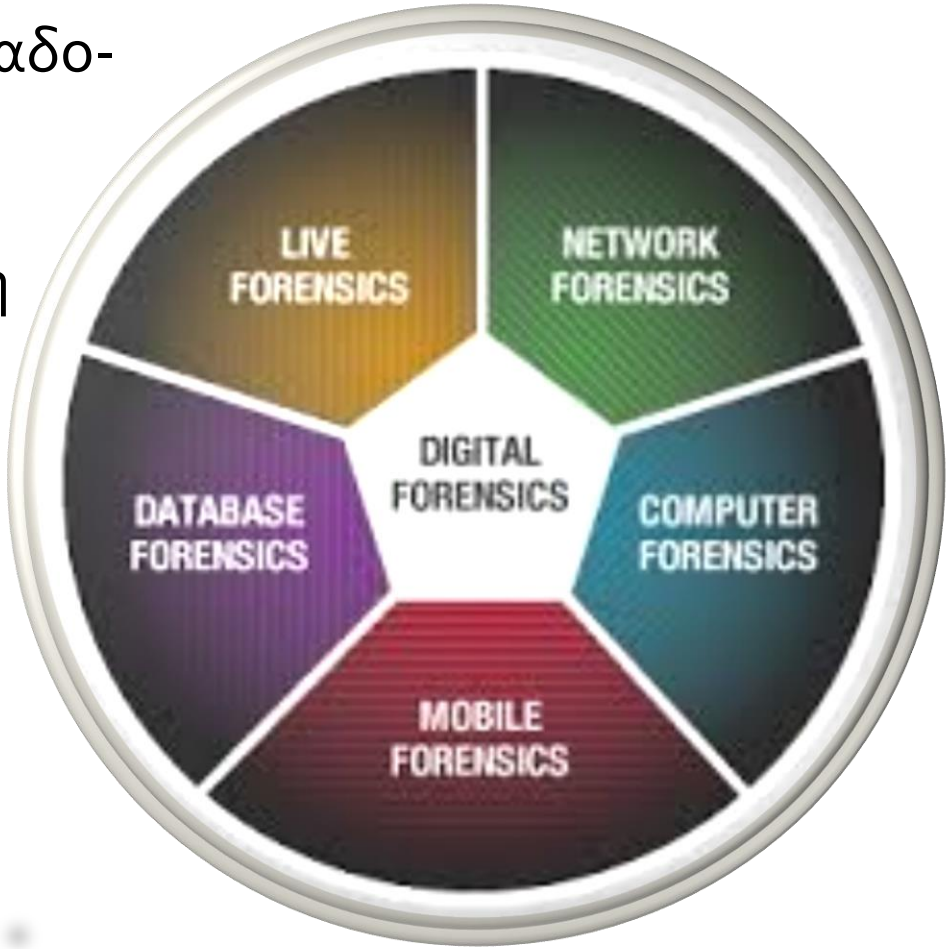
- Εξέταση επί εγκληματολογικού αντιγράφου (Forensic Image)
- Ακεραιότητα (Μοναδική Αλφαριθμητική Ταυτότητα – Hash Value)
- Αλυσίδα Επιτήρησης (Chain of custody)
- Επαναληψιμότητα (Ταυτόσημα αποτελέσματα σε κάθε νέα εξέταση με το ίδιο εγκληματολογικό εργαλείο)

Ψηφιακή Εγκληματολογία - Κατηγορίες

Βασικός Διαχωρισμός:

- Dead Box Forensics (Παραδοσιακή προσέγγιση)

- Live Forensics (Σύγχρονη αναγκαιότητα)



Live Forensics – Πρώτος Ανταποκριτής

- ✓ Bag & Tag / Αναφορά (Documentation)

- ✓ Κατάσχεση λοιπών ψηφιακών μέσων
- ✓ Εγκληματολογικό αντίγραφο σε live σύστημα

Ενέργειες Πρώτου Ανταποκριτή:

- ✓ Ασφάλεια κλιμακίου
- ✓ Προκαταρκτική έρευνα / Triage

- ✓ Συλλογή κύριας μνήμης (RAM)
- ✓ Φωτογράφιση / Καταγραφή

Προβληματικές Πρώτης Ανταπόκρισης

- Ασυμβατότητα Εξοπλισμού – Απαρχαιωμένα Συστήματα / Τεχνολογία (π.χ. Διεπαφή τύπου SCSI-SAS)
- Ασυμβατότητα Λογισμικού (π.χ. MacOS και εκτελέσιμα .exe)
- Ακεραιότητα του υπό εξέταση συστήματος / Αδυναμία Τερματισμού (π.χ. Server με απαραίτητη συνεχή λειτουργία)

Κυβερνοαπειλές σε Κρίσιμες Δημόσιες Υποδομές

Κακόβουλες επιθέσεις με στόχο να υπονομεύσουν τη λειτουργικότητα των δομών και να προάγουν τις Ιδεολογικές πεποιθήσεις των επιτιθέμενων.

Πρώτη ανταπόκριση σε Δημόσια Υποδομή

Ειδικά Χαρακτηριστικά:

- Αμεσότητα επέμβασης
- Αναγκαιότητα άμεσης επίλυσης – Διάδοση κακόβουλου λογισμικού σε έτερες Δημόσιες Δομές
- Απουσία κατηγορουμένου / Συνεργασία στελεχών

Case Study

ΙΣΤΟΡΙΚΟ

- Το Νοέμβριο του 2017, σε δημόσια υποδομή πραγματοποιήθηκε κυβερνοεπίθεση με κακόβουλο λογισμικό λύτρων (RANSOMWARE).
- Το κακόβουλο λογισμικό κρυπτογράφησε το σύνολο των αρχείων του κύριου υπολογιστή-διακομιστή (Server) της Υπηρεσίας.
- Τρείς ακόμα τερματικοί σταθμοί και τα αντίγραφα ασφαλείας που αποθηκεύονταν σε δικτυακή συσκευή αποθηκευτικού χώρου (NAS) κρυπτογραφήθηκαν πλήρως, καθιστώντας την Υπηρεσία πλήρως μη λειτουργική.
- Η Υπηρεσία μας κλήθηκε για τεχνική συνδρομή στην έρευνα.

Case Study

Ενέργειες Πρώτου Ανταποκριτή

- Συλλογή κύριας μνήμης από τον υπολογιστή-διακομιστή και κατάσχεση του σκληρού δίσκου
- Κατάσχεση της δικτυακής συσκευής αποθηκευτικού χώρου (NAS)
- Κατάσχεση του σκληρού δίσκου ενός εκ των τερματικών υπολογιστών

Case Study

Η εργαστηριακή έρευνα κατέδειξε εκατόν τριάντα πέντε χιλιάδες επτακόσια πενήντα τρία (135.753) κρυπτογραφημένα αρχεία κατάληξης «.wallet» στον υπολογιστή-διακομιστή, εκατόν είκοσι εννέα χιλιάδες διακόσια ογδόντα επτά (129.287) στη συσκευή NAS και εννέα χιλιάδες τριακόσια ένδεκα (9.311) στον υπολογιστή-πελάτη.

Case Study

Το εν λόγω κακόβουλο λογισμικό αναγνωρίστηκε πως άνηκε στην κατηγορία ιών (virus) τύπου «Ransomware» και σχετίζοταν με την ευρύτερη συνομοταξία ιών «Dharma Ransomware».

ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

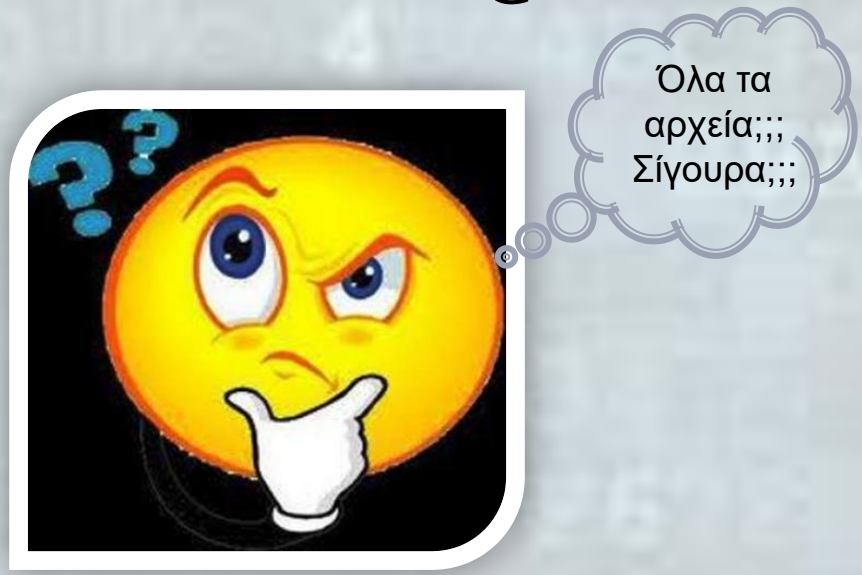
- Το εν λόγω κακόβουλο λογισμικό κρυπτογραφεί επιλεγμένους τύπους αρχείων.
- Μετονομάζει τα κρυπτογραφημένα αρχεία αλλάζοντας την κατάληξή τους σε «.wallet» και προσθέτει μία διεύθυνση ηλεκτρονικής αλληλογραφίας στην ονομασία τους.
- Τοποθετεί αρχείο κειμένου στο σύστημα με οδηγίες προς το χρήστη για τη διαδικασία αποκρυπτογράφησης.

Case Study

Ottention!!!

All your files are encrypted!

To decrypt your files, please contact us by email m.subzero@aol.com or reverse-mksubzero@india.com.



Case Study

Αντιθέτως με τα όσα δήλωνε το Ransom Note, τα αρχεία καταγραφής συμβάντων του λειτουργικού συστήματος ήταν ανέπαφα! Η ανάλυσή τους προσέφερε την αλληλουχία συμβάντων που έλαβαν χώρα πριν την κρυπτογράφηση.

Case Study

1. «06/Nov/2017 6:49:21 AM UTC» σύνδεση χρήστη μέσω πρωτοκόλλου απομακρυσμένης σύνδεσης (RDP) από την διεύθυνση IP 77.243.xxx.xxx, κάνοντας χρήση των διαπιστευτηρίων του χρήστη με ονομασία «admin» του δικτυακού τόμου (Domain Name) με ονομασία «xxxx».
2. «06/Nov/2017 6:50:11 AM UTC» καταγραφή έναρξης εγκατάστασης λογισμικού από την υπηρεσία εγκατάστασης των Windows (Windows installer), η οποία αφορά το αρχείο με ονομασία «16188419.msi14760», το οποίο βρισκόταν στη διαδρομή «C:\Windows\Installer\».
3. «06/Nov/2017 6:50:23 AM UTC» διακοπή της υπηρεσίας (service) με ονομασία «Kaspersky Anti-Virus Service 17.0.0», η οποία σχετίζεται με λογισμικό ανίχνευσης ιών.

Case Study

4. «06/Nov/2017 6:50:48 AM UTC» επιτυχής απεγκατάσταση του λογισμικού με ονομασία «Kaspersky Anti-Virus».
5. «06/Nov/2017 6:51:44 AM UTC» εκτέλεση του αρχείου με ονομασία «processhacker-2.39-setup.exe» από τη διαδρομή «C:\Users\user\Downloads\back\».
6. «06/Nov/2017 6:51:52 AM UTC» εγκατάσταση υπηρεσίας στο σύστημα με ονομασία «KProcessHacker3», η οποία χρησιμοποιεί το αρχείο με ονομασία «kprocesshacker.sys» από την διαδρομή «C:\Program Files\Process Hacker 2\». Η υπηρεσία είναι τύπου «πρόγραμμα οδήγησης λειτουργίας πυρήνα» και η εκκίνησή της πραγματοποιείται κατόπιν αιτήματος του χρήστη.

Case Study

7. «06/Nov/2017 6:52:05 AM UTC» μη αναμενόμενος τερματισμός των υπηρεσιών με ονομασίες «SQL Server VSS Writer» και «SQL Server (SQLEXPRESS)».
8. «06/Nov/2017 6:52:40 AM UTC» εκτέλεση του αρχείου με ονομασία «m.subzero@aol.com.exe» από την διαδρομή «C:\Users\user\Downloads\ back\», ταυτόχρονη δημιουργία μηχανισμού αυτόματης εκκίνησης κατά την επανεκκίνηση του υπολογιστή και έναρξη της κρυπτογράφησης των αρχείων.
9. «06/Nov/2017 7:29:53 AM UTC» αποσύνδεση της συνεδρίας, πρωτοκόλλου απομακρυσμένης σύνδεσης, με προέλευση από τη διεύθυνση IP «77.243.183.197».

Case Study

Η κύρια μνήμη του υπολογιστή-διακομιστή αναλύθηκε και τα αποτελέσματα βοήθησαν επικουρικά για τη μόρφωση πλήρους άποψης περί του τρόπου επίτευξης της κακόβουλης επίθεσης.

- Το αρχείο «16188419.msi14760» είχε δημιουργηθεί (spawn) από γονική διεργασία με αναγνωριστικό (PID) 4389.
- Η εν λόγω διεργασία είχε εγκαθιδρύσει δικτυακή σύνδεση (established) με κακόβουλη ηλεκτρονική διεύθυνση IP.
- Από την ανωτέρω διεύθυνση είχαν μεταφορτωθεί στο σύστημα τα εκτελέσιμα αρχεία «processhacker-2.39-setup.exe» και m.subzero@aol.com.exe.

Case Study

Ανάλυση κύριας μνήμης

- Το αρχείο «m.subzero@aol.com.exe» είχε δημιουργήσει τέσσερις (4) άλλες διεργασίες-παιδιά (child processes) οι οποίες είχαν αποκτήσει δικτυακή σύνδεση (Listening) με έτερες κακόβουλες ηλεκτρονικές διευθύνσεις IP, καθεμία σε διαφορετική πόρτα.
- Εντοπίστηκαν οι εντολές στο τερματικό παράθυρο (cmd terminal) με τις οποίες αντιγράφηκε/διαδόθηκε το κακόβουλο αρχείο «m.subzero@aol.com.exe» σε όλους τους σταθμούς του τοπικού δικτύου.

Case Study

ΚΑΤΑΛΗΞΗ

Τα κλειδιά αποκρυπτογράφησης για το συγκεκριμένο κακόβουλο λογισμικό ανακτήθηκαν από τον ιστοχώρο της Europol "www.nomoreransom.org" και κατόπιν το σύνολο των πειστηρίων αποκρυπτογραφήθηκε και κατέστη και πάλι λειτουργικό.

Case Study

ΚΑΤΑΛΗΞΗ

Αναζητήθηκαν στα αρχεία καταγραφής συμβάντων του λειτουργικού συστήματος οι καταγεγραμμένες απομακρυσμένες συνδέσεις και κατόπιν εξήχθησαν οι ηλεκτρονικές διευθύνσεις IP από τις οποίες πραγματοποιήθηκαν αυτές. Εν συνεχεία, για τις ανωτέρω διευθύνσεις IP, αναζητήθηκαν οι πάροχοι υπηρεσιών διαδικτύου, οι χώρες όπου είναι καταχωρημένοι και τα στοιχεία επικοινωνίας αυτών (IP Resolve). Τα στοιχεία δόθηκαν στην Προανάκριση για συνέχεια της Ποινικής Δίωξης κατά των υπαιτίων.

Η Κρίσιμη Δημόσια Υποδομή ήταν και πάλι πλήρως λειτουργική εντός της ίδιας εβδομάδας!

Case Study

ΣΗΜΕΙΑ ΤΡΩΤΟΤΗΤΑΣ ΤΗΣ ΚΡΙΣΙΜΗΣ ΥΠΟΔΟΜΗΣ

- Υπολογιστής-Διακομιστής με παλαιό Λ.Σ. (Windows Server 2000) το οποίο δεν υποστηριζόταν πλέον από την Εταιρεία.
- Ενεργοποιημένο πρωτόκολλο απομακρυσμένης σύνδεσης στον κύριο υπολογιστή-διακομιστή του δικτύου και προσβάσιμη η πόρτα αυτού από το εξωτερικό δίκτυο.
- Απουσία οιασδήποτε πολιτικής για περιοδική αλλαγή κωδικών σύνδεσης (password) των χρηστών.
- Λήψη αντιγράφων ασφαλείας (back up) και διατήρησή τους εντός του ίδιου τοπικού δικτύου.

Σας ευχαριστώ

Διεύθυνση Εγκληματολογικών Ερευνών
7ο Τμήμα Εξέτασης Ψηφιακών
Εργαστήριο Εξέτασης Πειστήριων Υπολογιστικών Συστημάτων
Τηλ: 210 5103201, Φαξ: 210 6430238
Email: dee7@astynomia.gr