ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Ε6 (ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

ΕΘΝΙΚΗ ΑΣΚΗΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

- Ενημέρωση Επεισοδίων
  - App Locker
  - Malware Analysis
  - Network Forensics
  - Windows -Linux Forensics
  - Ανταλλαγή κακόβουλων μηνυμάτων
  - Scoring Board

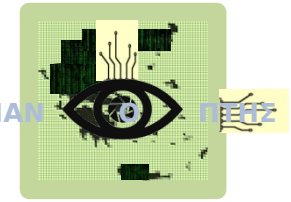
ΑΝ ΠΤΗΣ 201 9

ΕΝΗΜΕΡΩΣΗ ΕΠΕΙΣΟΔΙΩΝ

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

PORTAL

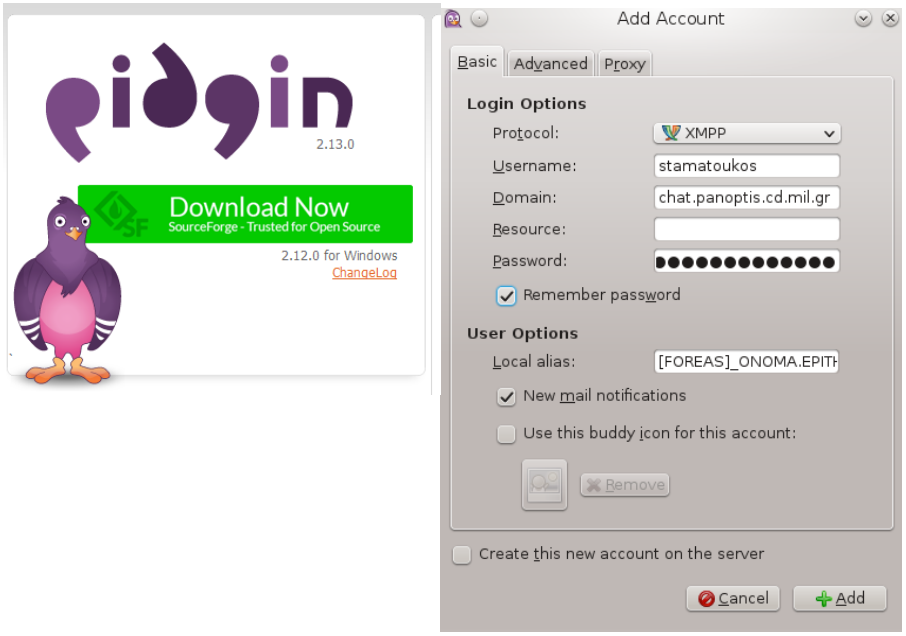
http://panoptis.cd.mil.gr/

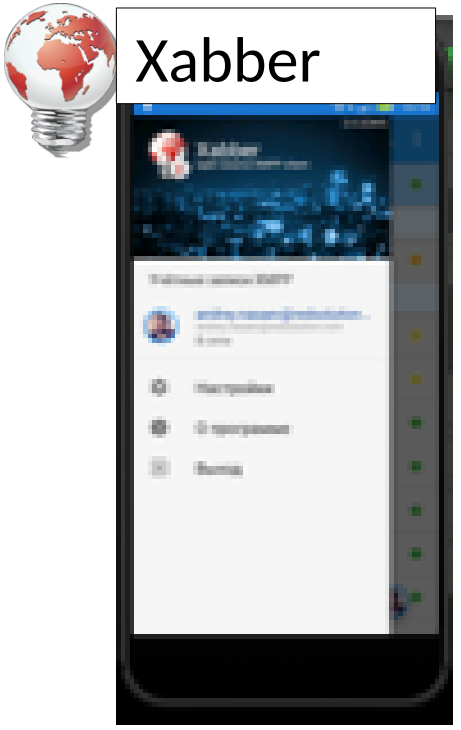


ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

CHAT

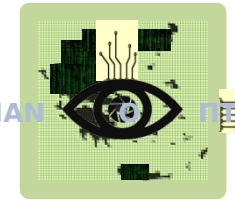
XMPP client





ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

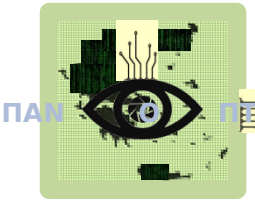
Οδηγίες Συμμετοχής



- Υποβολή ανά φορέα:
  - e-mail συμμετεχόντων
  - 1 τηλέφωνο επικοινωνίας (σταθερό)
- Username & password e-mail
- Τυποποίηση Ονομάτων
  - [Φορέας]_[Όνομα].[Επώνυμο]
  - Dimokritos_Giannis.Agiannis
  - Unipi_Fotis.Karafotis
- Στοιχεία επικοινωνίας διοργανωτών:
  - grammateia@cd.mil.gr (Διοργανωτικά θέματα)
  - panoptis@cd.mil.gr (Τεχνικά θέματα)

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

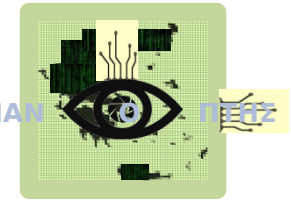
Πανόπτης 2019



Περιγραφή Επεισοδίων

- App Locker
- Malware Analysis
- Network Forensics
- Windows - Linux Forensics
- Scoring Board
- Ανταλλαγή κακόβουλων μηνυμάτων

App Locker

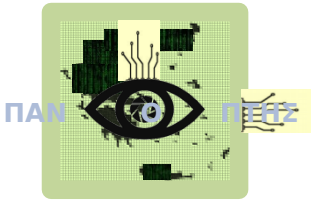


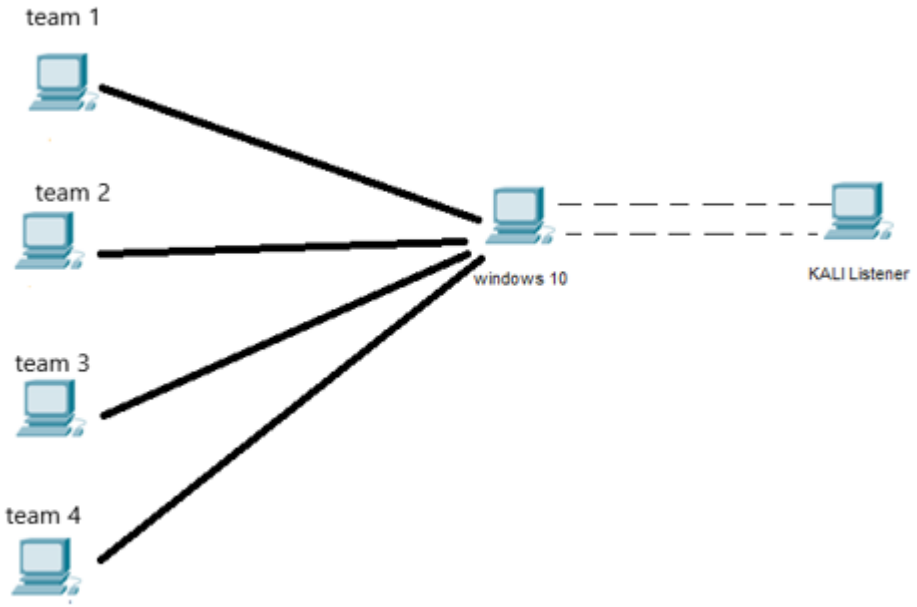
- Ζητούμενα
  - Εκτέλεση εκτελέσιμου αρχείου από τον χρήστη σε windows 10 με ενεργοποιημένο App Locker

  - Για αυτοματισμό της διαδικασίας:
    - Τρέξτε shellcode από το metasploit (payload windows/shell/reverse_tcp ή payload windows/meterpreter/reverse_tcp
    - Use lhost 10.0.0.254, lport ???? (ομάδα)
    - Με την εκτέλεση κώδικα θα δημιουργηθεί flag στην επιφάνεια εργασίας.
    - 2ο Flag με την αποστολή του Report

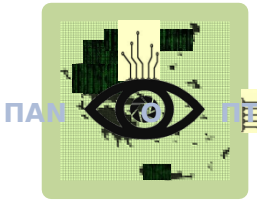
ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

App Locker





App Locker



Εργαλεία – Γενικές Γνώσεις

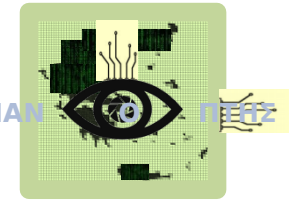
- OpenSSH
- wget
- msfConsole
- Γνώση για παραβίαση του App Locker
- Περιορισμός επανεκίννησης.

Malware Analysis

- Ανάλυση κακόβουλων αρχείων
- Απάντηση ερωτήσεων στο Scoring Board
  - Οι ερωτήσεις θα ανοίγουν μια-μια με την απάντηση κάθε ερώτησης.
  - Η πρώτη ερώτηση είναι : Τι τύπος κακόβουλου λογισμικού είναι; worm, trojan, keylogger, ransomware, rootkit, virus (multi action).
    - Θα μπορείτε να απαντήσετε σε αυτήν την ερώτηση αφού κάνετε στατική και δυναμική ανάλυση (χωρίς την χρήση debugger)

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Malware Analysis

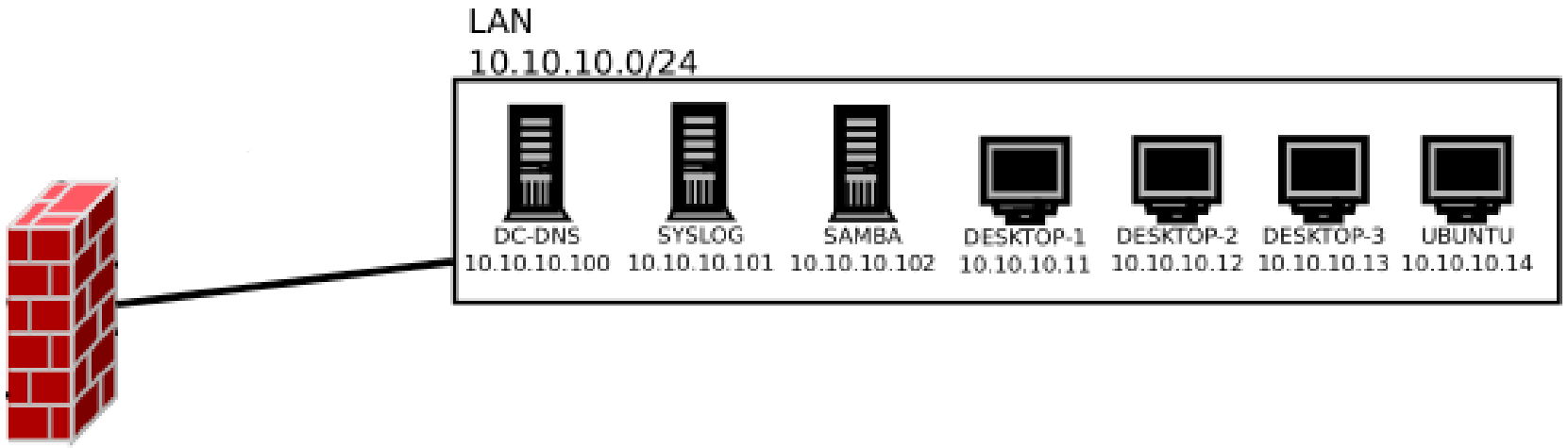


Εργαλεία – Γενικές Γνώσεις
Χρήση Ida, ollydebugger

Στατική ανάλυση
Δυναμική ανάλυση

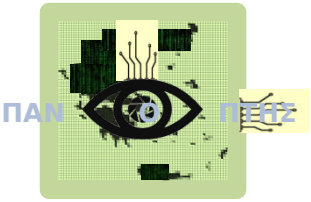
Χρήση εργαλείων για strings, fakenet, process

Network Forensics



ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Network Forensics
Logs analysis



- Θα δοθεί αρχείο pcap για ανάλυση
  - Ολη η κίνηση του δικτύου που παιρνά από το firewall (pfsense)
- Logs από όλα τα μηχανήματα
  - Logs των windows (win 10, server 2016)
  - Logs από το pfsense
  - Logs από IDS (suricata)
  - Logs από τα linux machines (ubuntu)

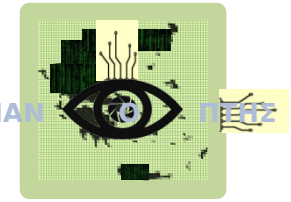
Network Forensics

Εργαλεία – Γενικές Γνώσεις

- **WireShark**
- **NetworkMiner**
- **Xplico**
- **Κάποιο custom script**

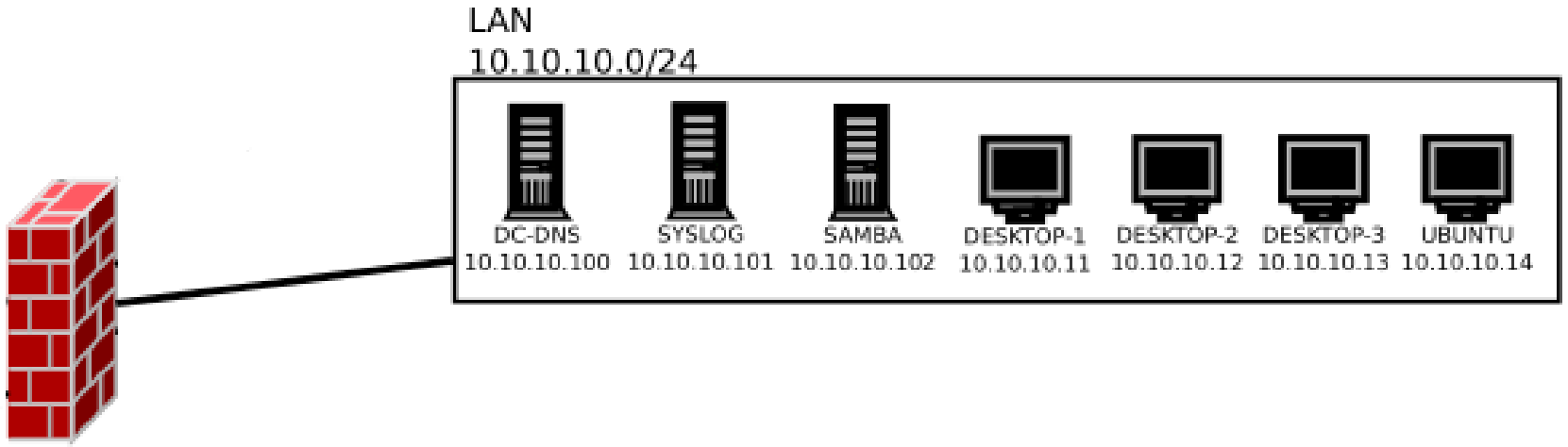
ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Windows, Linux Forensics



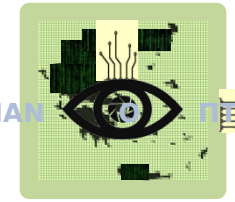
ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Windows, Linux Forensics



ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Windows, Linux Forensics



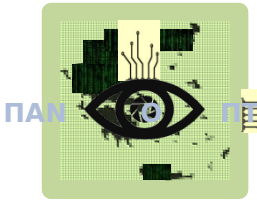
Εργαλεία – Γενικές Γνώσεις

Η λύση θα προκύπτει χρησιμοποιώντας open source tools.

Θα υπάρξει μόλυνση και μετά την λήψη του pcap file. Συνεπώς η λύση των προηγούμενων επεισοδίων δεν θα λύσει πλήρως το επεισόδιο.

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

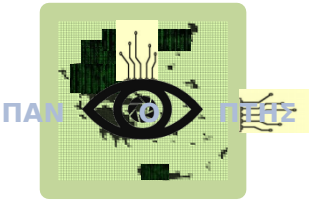
Scoring Board

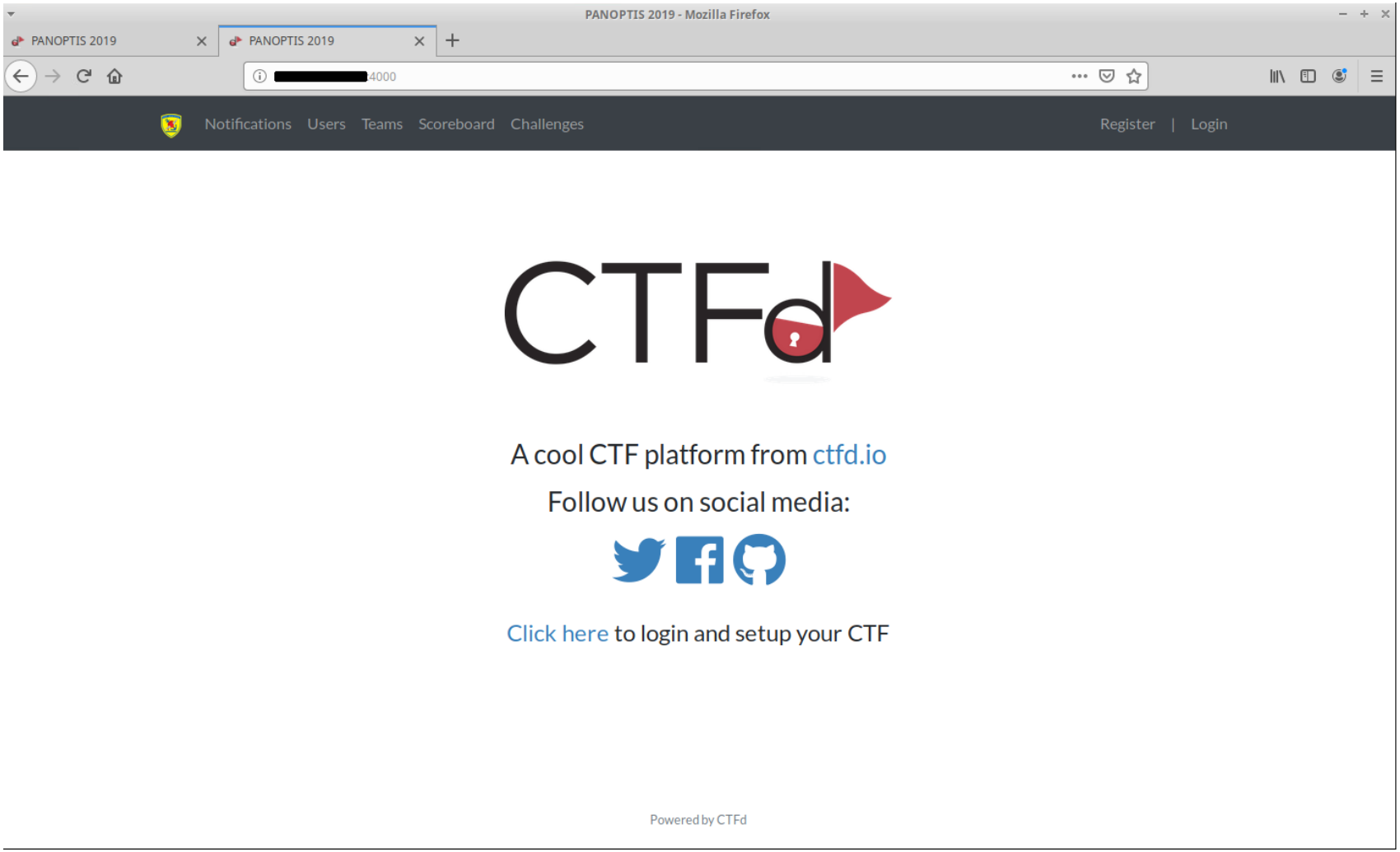


- Στο Scoring Board θα γίνεται:
  - Η παρακολούθηση τις πορεία κάθε ομάδας
  - Θα δίνονται οι ερωτήσεις που θα πρέπει να απαντήσουν οι ομάδες
  - Θα βοηθήσει την αποστολή report. Το report θα παίρνει βαθμολογία ή όχι (δεν θα έχει ενδιάμεσα στάδια)

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

Scoring Board





Ανταλλαγή κακόβουλων μηνυμάτων

Σενάριο:
Πληροφορίες αναφέρουν ανταλλαγή πληροφοριών μεταξύ hacktivists σε κανάλι των social media μέσω κρυπτογραφημένης επικοινωνίας

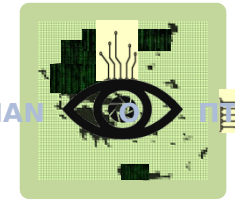
Ανταλλαγή κακόβουλων μηνυμάτων

Στόχος:
Θα σας δοθεί το όνομα ενός λογαριασμού social media όπου θα πρέπει να:

1. Εντοπίσετε τον τρόπο ανταλλαγής των μηνυμάτων
2. Βρείτε το περιεχόμενο των μηνυμάτων

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)

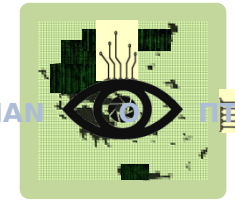
Εξαγωγή δεδομένων μέσω ιστοτόπου



Αυτήν την περίοδο η εταιρεία ΟΠΛΙΚΑ ΣΥΣΤΗΜΑΤΑ 'ΖΕΥΣ' αναπτύσσει ένα νέο όπλο υπό συνθήκες απόλυτης μυστικότητας. Ο αναλυτής ασφάλειας της εταιρείας διαπίστωσε μέσω των αρχείων καταγραφής πως προ ολίγων ημερών τροποποιήθηκε το περιεχόμενο μερικών αρχείων του ιστοχώρου χωρίς φαινομενική αλλαγή στην λειτουργία και στην εμφάνιση των ιστοσελίδων. Ο διαχειριστής φαίνεται να επικοινωνεί με άτομα εκτός εταιρείας μέσω του viber. Η δνση της εταιρείας ανησυχεί για παράνομη εξαγωγή απόρρητων πληροφοριών σχετικά με τα νέα οπλικά συστήματα της εταιρείας και παρακολουθεί όλες τις επικοινωνίες.

Ο αναλυτής ασφάλειας υποπτεύεται ότι ο διαχειριστής του web server τροποποιεί και κρύβει απόρρητες σε αρχεία του ιστοχώρου (μαζί με κατάλληλλες οδηγίες), προς πιθανό εξωτερικό συνεργάτη του. Σας δίνεται το URL του ιστοχώρου για να τα αναλύσετε και να βρήτε τυχόν κρυμμένα στοιχεία ώστε να στοιχειοθετηθεί κατηγορία εναντίον του – εάν είναι ένοχος.

ΓΕΕΘΑ / Ε6
(ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ)



Επικοινωνία

grammateia@cd.mil.gr (Διοργανωτικά θέματα)
panoptis@cd.mil.gr (Τεχνικά θέματα)
Τηλ. 210 657 4282 Επγος (Ι) Γιαννακόπουλος Νικόλαος)