Όνομα: _____ **Ημερομηνία:** _____ **Βαθμολογία:** _____

Ανάλυση κακόβουλου λογισμικού και μετριασμός απειλών Οδηγός

Δούρειοι ίπποι, ransomware, λογισμικό υποκλοπής, rootkits, εικονικά περιβάλλοντα δοκιμών (sandboxes), περιορισμός

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΑΝΑΛΥΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στην ανάλυση και την πρόληψη κακόβουλου λογισμικού. Θα εξερευνήσεις spyware, trojans, ωφέλιμα φορτία ransomware, εργαλεία αντίστροφης μηχανικής, συμπεριφορά rootkit και στρατηγικές περιορισμού.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- [ ] **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- [ ] **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- [ ] **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- [ ] **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- [ ] **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/malware/

Η πορεία μάθησής σου: περιορισμός κακόβουλου λογισμικού

- Διαχώρισε τους τύπους κακόβουλου λογισμικού Trojan, worm και rootkit.
- Εφάρμοσε εκτέλεση εικονικοποίησης sandbox για την ανάλυση κώδικα.
- Σχεδίασε σχέδια περιορισμού και απολύμανσης για ενεργά ωφέλιμα φορτία ransomware.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΑΝΑΛΥΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στον περιορισμό του κακόβουλου λογισμικού. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΝΑΛΥΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ (ΕΙΣΑΓΩΓΗ)

Ο κακόβουλος κώδικας, όπως οι Trojans, τα worms και το ransomware, αποτελεί απειλή μεγάλου αντικτύπου για τα τερματικά και τους διακομιστές. Οι ομάδες ασφαλείας αναλύουν το κακόβουλο λογισμικό σε εικονικά sandbox και εφαρμόζουν γρήγορους ελέγχους απομόνωσης δικτύου για να περιορίσουν τη διάδοση του φορτίου.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. Ποιο είναι το καθοριστικό χαρακτηριστικό ενός Δούρειου Ίππου (Trojan);

- A. Μεταμφιέζεται σε νόμιμο λογισμικό για να εξαπατήσει τους χρήστες ώστε να το εκτελέσουν
- B. Αναπαράγεται αυτόματα μέσω των τοπικών γραμμών δικτύου
- C. Μολύνει αρχεία μέσα σε απομονωμένα εικονικά sandbox
- D. Αναχαιτίζει την κίνηση του παρόχου υπηρεσιών διαδικτύου

2. Ποιος τύπος κακόβουλου λογισμικού κρυπτογραφεί αρχεία και απαιτεί πληρωμή;

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3. Τι αντιπροσωπεύει το spyware;

- A. Κακόβουλο λογισμικό σχεδιασμένο να παρακολουθεί κρυφά τις πληκτρολογήσεις και τις δραστηριότητες του προγράμματος περιήγησης του χρήστη
- B. Κώδικας προγράμματος που εκτελείται μέσα σε εικονικό κοντέινερ sandbox
- C. Ενημερώσεις anti-malware που λαμβάνονται από μητρώα βάσεων δεδομένων
- D. Αυτόματη προσαρμογή φωτεινότητας οθόνης

4. Γιατί οι δημιουργοί κακόβουλου λογισμικού χρησιμοποιούν rootkits;

- A. Για να κρύβει ενεργές διεργασίες και κακόβουλα αρχεία από το λειτουργικό σύστημα
- B. Για την αύξηση της ταχύτητας επεξεργασίας της CPU στα τερματικά
- C. Για δημιουργία αντιγράφων ασφαλείας αρχείων βάσης δεδομένων σε ασφαλείς θυρίδες cloud
- D. Για βελτίωση της διάρκειας μπαταρίας στους φορητούς υπολογιστές

5. Τι σημαίνει sandboxing στην ανάλυση κακόβουλου λογισμικού;

- A. Εκτέλεση ύποπτων αρχείων σε απομονωμένο εικονικό θησαυροφυλάκιο για ασφαλή παρατήρηση της συμπεριφοράς
- B. Σάρωση κατακερματισμών αρχείων έναντι γνωστών βάσεων δεδομένων απειλών
- C. Επαναφορά αντιγράφων ασφαλείας βάσης δεδομένων μετά από εισβολή
- D. Αποσύνδεση των τοπικών δρομολογητών δικτύου από τις δημόσιες γραμμές

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Τα σκουλήκια υπολογιστών απαιτούν αλληλεπίδραση ανθρώπου-χρήστη για να εξαπλωθούν σε τοπικά δίκτυα.

- ◯ Σωστό
- ◯ Λάθος

7 Ερώτηση 7

7. Το adware είναι πάντα ακίνδυνο και δεν παρακολουθεί τη συμπεριφορά του χρήστη ή το ιστορικό περιήγησης.

- ◯ Σωστό
- ◯ Λάθος

8 Ερώτηση 8

8. Η επαναφορά καθαρών αντιγράφων ασφαλείας εκτός δικτύου επιτρέπει στα θύματα να ανακτήσουν κρυπτογραφημένα αρχεία χωρίς να πληρώσουν λύτρα.

- ◯ Σωστό
- ◯ Λάθος

9 Ερώτηση 9

9. Το antivirus που βασίζεται σε υπογραφές σταματά αξιόπιστα κακόβουλο λογισμικό zero-day πριν υπάρξει υπογραφή γι' αυτό.

- ◯ Σωστό
- ◯ Λάθος

10 Ερώτηση 10

10. Το κακόβουλο λογισμικό χωρίς αρχεία εκτελεί κακόβουλα scripts στη μνήμη του συστήματος, αποφεύγοντας την εγγραφή αρχείων στον δίσκο.

- ◯ Σωστό
- ◯ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Το κακόβουλο λογισμικό που μεταμφιέζεται σε ασφαλές βοηθητικό πρόγραμμα είναι ένας _____ .

2. Τα κακόβουλα φορτία που κλειδώνουν συστήματα βάσεων δεδομένων με αντάλλαγμα χρήματα αποτελούν _____ .

3. Τα keyloggers που καταγράφουν κρυφά κωδικούς πρόσβασης αποτελούν _____ λογισμικό.

4. Η απόκρυψη βαθιά μέσα στους πυρήνες του λειτουργικού συστήματος απαιτεί ένα _____ .

5. Η ανάλυση ύποπτων αρχείων σε ένα απομονωμένο θησαυροφυλάκιο χρησιμοποιεί ένα εικονικό _____ .

6. Ο περιορισμός της εξάπλωσης ενεργών κακόβουλων φορτίων απαιτεί άμεση _____ του δικτύου.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΠΟΚΡΥΨΗ ΑΠΟΜΟΝΩΣΗ ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ ΛΥΤΡΙΣΜΙΚΟ ΣΚΩΛΗΚΑΣ ROOTKIT SANDBOX

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

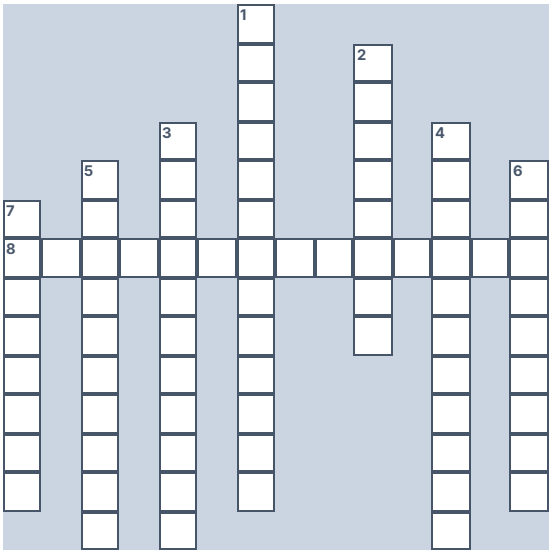
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. ΤΡΟΪΚΟΣ ΙΟΣ	**A**	Πρόγραμμα σχεδιασμένο να παρακολουθεί και να καταγράφει κρυφά τη δραστηριότητα και τις εισόδους του χρήστη.
☐	2. RANSOMWARE	**B**	Κακόβουλο λογισμικό που εκτελείται απευθείας στη RAM για να αποφύγει τον εντοπισμό από σαρωτές δίσκου.
☐	3. ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ	**C**	Περιορισμός των μολυσμένων τερματικών για την αποτροπή εξάπλωσης των κακόβουλων φορτίων.
☐	4. ROOTKIT	**D**	Κακόβουλο λογισμικό μεταμφιεσμένο σε αβλαβές ή χρήσιμο βοηθητικό πρόγραμμα.
☐	5. SANDBOX	**E**	Αυτοαναπαραγόμενο κακόβουλο λογισμικό που διαδίδεται σε δίκτυα χωρίς ανθρώπινη ενέργεια.
☐	6. ΠΕΡΙΟΡΙΣΜΟΣ	**F**	Κακόβουλο λογισμικό που κρυπτογραφεί τον αποθηκευτικό χώρο του συστήματος και απαιτεί πληρωμή για την παράδοση του κλειδιού.
☐	7. ΣΚΟΥΛΗΚΙ	**G**	Απομονωμένο εικονικό περιβάλλον που χρησιμοποιείται για την ασφαλή ανάλυση κακόβουλων αρχείων.
☐	8. ΧΩΡΙΣ ΑΡΧΕΙΑ	**H**	Κακόβουλο λογισμικό stealth που κρύβεται βαθιά στους πυρήνες του συστήματος για να διατηρεί διαχειριστικό έλεγχο.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

8. Πρόγραμμα σχεδιασμένο να παρακολουθεί και να καταγράφει κρυφά τη δραστηριότητα και τα δεδομένα εισόδου του χρήστη. (14)

ΚΑΘΕΤΑ

1. Κακόβουλο λογισμικό που μεταμφιέζεται σε αθώο ή χρήσιμο βοηθητικό πρόγραμμα. (13)

2. Τεχνική με την οποία κακόβουλο λογισμικό κρύβεται βαθιά στον πυρήνα του συστήματος για να διατηρεί δικαιώματα διαχειριστή. (8)

3. Εικονικό περιβάλλον εκτέλεσης, χωριστό από το σύστημα, για την ασφαλή ανάλυση κακόβουλων αρχείων. (11)

4. Κακόβουλο λογισμικό που εκτελείται απευθείας στη μνήμη RAM ώστε να αποφεύγει τον εντοπισμό από σαρωτές δίσκου. (11)

5. Κακόβουλο λογισμικό που κρυπτογραφεί την αποθήκευση του συστήματος και απαιτεί πληρωμή για την παράδοση του κλειδιού. (10)

6. Περιορισμός των μολυσμένων τερματικών ώστε να μην εξαπλωθούν τα κακόβουλα φορτία απειλών. (9)

7. Κακόβουλο λογισμικό που αναπαράγεται μόνο του και εξαπλώνεται στα δίκτυα χωρίς ανθρώπινη ενέργεια. (8)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

8 οριζόντια: Πρόγραμμα σχεδιασμένο να παρακολουθεί και να καταγράφει κρυφά τη δραστηριότητα και τα δεδομένα εισόδου του χρήστη. (14 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Κακόβουλο λογισμικό που μεταμφιέζεται σε αθώο ή χρήσιμο βοηθητικό πρόγραμμα. (13 γράμματα):

2 κάθετα: Τεχνική με την οποία κακόβουλο λογισμικό κρύβεται βαθιά στον πυρήνα του συστήματος για να διατηρεί δικαιώματα διαχειριστή. (8 γράμματα):

3 κάθετα: Εικονικό περιβάλλον εκτέλεσης, χωριστό από το σύστημα, για την ασφαλή ανάλυση κακόβουλων αρχείων. (11 γράμματα):

4 κάθετα: Κακόβουλο λογισμικό που εκτελείται απευθείας στη μνήμη RAM ώστε να αποφεύγει τον εντοπισμό από σαρωτές δίσκου. (11 γράμματα):

5 κάθετα: Κακόβουλο λογισμικό που κρυπτογραφεί την αποθήκευση του συστήματος και απαιτεί πληρωμή για την παράδοση του κλειδιού. (10 γράμματα):

6 κάθετα: Περιορισμός των μολυσμένων τερματικών ώστε να μην εξαπλωθούν τα κακόβουλα φορτία απειλών. (9 γράμματα):

7 κάθετα: Κακόβουλο λογισμικό που αναπαράγεται μόνο του και εξαπλώνεται στα δίκτυα χωρίς ανθρώπινη ενέργεια. (8 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Σ Ψ Ξ Ψ Χ Σ Η Τ Χ Α Ο Υ Ν Ν Ω
Ο Α Ι Ε Χ Ρ Α Σ Ι Ρ Ω Χ Ξ Θ Ο
Π Σ Θ Ο Α Π Ο Κ Ρ Υ Ψ Η Υ Τ Ξ
Π Υ Τ Κ Α Ε Ξ Μ Λ Α Ν Υ Ζ Η Ο
Ι Π Χ Ψ Ι Κ Υ Ι Ω Φ Ψ Ο Κ Θ Ω
Σ Ι Ι Ν Α Ε Θ Α Σ Α Ι Ε Φ Ε Κ
Ο Ω Κ Ε Κ Π Ν Ι Α Ζ Ξ Κ Ν Γ Ν
Ι Γ Δ Η Θ Η Σ Ω Ν Ο Μ Ο Π Α Β
Ε Α Ξ Ρ Λ Ο Φ Τ Θ Ψ Ζ Ω Ρ Η Χ
Ρ Φ Ο Κ Ι Μ Σ Ι Ρ Τ Υ Λ Θ Ε Π
Υ Κ Α Τ Α Σ Κ Ο Π Ε Υ Τ Ι Κ Ο
Ο Τ Ν Σ Κ Ω Λ Η Κ Α Σ Τ Κ Ρ Δ
Δ Τ Π Ρ Ο Σ Ο Μ Ο Ι Ω Σ Η Σ Λ
Ο Λ Μ Σ Θ Κ Ο Θ Ψ Ξ Λ Χ Υ Ν Ψ
Π Π Β Α Λ Ο Μ Β Λ Θ Ζ Ι Ν Ψ Β

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΔΟΥΡΕΙΟΣΙΠΠΟΣ
ΛΥΤΡΙΣΜΙΚΟ
ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ
ΑΠΟΚΡΥΨΗ
ΠΡΟΣΟΜΟΙΩΣΗ
ΑΠΟΜΟΝΩΣΗ
ΣΚΩΛΗΚΑΣ
ΧΩΡΙΣΑΡΧΕΙΑ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΔΟΥΡΕΙΟΣΙΠΠΟΣ

B. ΛΥΤΡΙΣΜΙΚΟ

C. ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ

D. ΑΠΟΚΡΥΨΗ

E. ΠΡΟΣΟΜΟΙΩΣΗ

F. ΑΠΟΜΟΝΩΣΗ

G. ΣΚΩΛΗΚΑΣ

H. ΧΩΡΙΣΑΡΧΕΙΑ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Τεχνική με την οποία κακόβουλο λογισμικό κρύβεται βαθιά στον πυρήνα του συστήματος για να διατηρεί δικαιώματα διαχειριστή.

_____ 2. Περιορισμός των μολυσμένων τερματικών ώστε να μην εξαπλωθούν τα κακόβουλα φορτία απειλών.

_____ 3. Κακόβουλο λογισμικό που εκτελείται απευθείας στη μνήμη RAM ώστε να αποφεύγει τον εντοπισμό από σαρωτές δίσκου.

_____ 4. Κακόβουλο λογισμικό που αναπαράγεται μόνο του και εξαπλώνεται στα δίκτυα χωρίς ανθρώπινη ενέργεια.

_____ 5. Κακόβουλο λογισμικό που κρυπτογραφεί την αποθήκευση του συστήματος και απαιτεί πληρωμή για την παράδοση του κλειδιού.

_____ 6. Πρόγραμμα σχεδιασμένο να παρακολουθεί και να καταγράφει κρυφά τη δραστηριότητα και τα δεδομένα εισόδου του χρήστη.

_____ 7. Κακόβουλο λογισμικό που μεταμφιέζεται σε αθώο ή χρήσιμο βοηθητικό πρόγραμμα.

_____ 8. Εικονικό περιβάλλον εκτέλεσης, χωριστό από το σύστημα, για την ασφαλή ανάλυση κακόβουλων αρχείων.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της κυβερνοασφάλειας. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. ΟΥΙΟΙΟΣΠΔΠΣΕΡ
2. ΣΑΚΤΟΚΚΙΠΟΥΤΕΑ
3. ΠΟΜΙΟΡΣΗΟΩΣ
4. ΛΑΣΚΗΣΚΩ
5. ΙΣΟΥΡΜΙΛΚΤ
6. ΨΗΚΥΑΡΠΟ
7. ΝΑΣΗΩΜΠΟΟ
8. ΕΡΑΑΡΧΣΩΙΧΙ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	**Μέρη για να κατεβάζεις ασφαλείς εφαρμογές**			
2	**Συσκευές που μπορούν να παραβιαστούν**			
3	**Πράγματα που παίρνεις αντίγραφο ασφαλείας**			
4	**Προειδοποιητικά σημάδια σε ένα email**			
5	**Ενδείξεις ότι ένα κινητό έχει κακόβουλο λογισμικό**			
6	**Τύποι κακόβουλου λογισμικού που γνωρίζεις**			
7	**Τύποι αρχείων που θέλουν προσοχή**			
8	**Τρόποι με τους οποίους το κακόβουλο λογισμικό μπαίνει σε έναν υπολογιστή**			
9	**Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα**			
10	**Λέξεις που σχετίζονται με την κυβερνοασφάλεια**			
11	**Πράγματα που κάνεις μετά από μια διαρροή δεδομένων**			
12	**Λόγοι για να ενημερώνεις το λογισμικό**			
13	**Ζώα ή χαρακτήρες με ονόματα που θυμίζουν κακόβουλο λογισμικό**			
14	**Πράγματα που μπορεί να κλέψει το κακόβουλο λογισμικό**			
15	**Πράγματα που κάνεις αν πατήσεις σε λάθος σύνδεσμο**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΕΡΙΟΡΙΣΜΟΣ ΩΦΕΛΙΜΟΥ ΦΟΡΤΙΟΥ RANSOMWARE ΣΕ ΕΠΙΧΕΙΡΗΣΗ

👷

Σενάριο: Ένα εταιρικό τοπικό δίκτυο έχει παραβιαστεί από ενεργό ransomware. Βασικοί διακομιστές αρχείων άρχισαν να εμφανίζουν επεκτάσεις αρχείων .locked. Καθιέρωσε πολιτικές περιορισμού.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τα βήματα περιορισμού και περίγραψε συνοπτικά το πρωτόκολλο ανάκτησης δεδομένων.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΕΓΧΥΣΗ ΣΤΗ ΜΝΗΜΗ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΧΩΡΙΣ ΑΡΧΕΙΑ

👷

Σενάριο: Ένας αναλυτής εντοπίζει ύποπτα μοτίβα σεναρίων που εκτελούνται απευθείας στην πτητική μνήμη RAM του συστήματος με τυπικά διαχειριστικά εργαλεία, αλλά δεν υπάρχουν κακόβουλα αρχεία στον δίσκο.

Ερώτηση συζήτησης: Εξήγησε τη στρατηγική ανάλυσης μνήμης και προσδιόρισε εργαλεία για τον αποκλεισμό της εκτέλεσης χωρίς αρχεία (fileless).

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

5	13	19	15	16	9	18	5		1	16	5	9	11	5	18		12	5		
16	1	17	1	10	15	11	15	20	8	7	18	7								
18	20	12	16	5	17	9	21	15	17	1	18									

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Τι είναι το κακόβουλο λογισμικό;

Κακόβουλο λογισμικό που σχεδιάζουν οι παράγοντες απειλών για να προκαλέσει ζημιά, να αποκτήσει τον έλεγχο ή να κλέψει δεδομένα από συσκευές και δίκτυα.

Q2: Ποια είναι η διαφορά μεταξύ ιού και worm;

Ένας ιός χρειάζεται ανθρώπινη ενέργεια (όπως το άνοιγμα ενός αρχείου) για να εξαπλωθεί, ενώ ένα σκουλήκι (worm) εξαπλώνεται αυτόματα στα δίκτυα.

Q3: Πώς μολύνει έναν υπολογιστή ένας Δούρειος Ίππος (Trojan);

Εξαπατά τους χρήστες παριστάνοντας ένα αβλαβές ή ασφαλές πρόγραμμα, κρύβοντας μέσα του το κακόβουλο φορτίο του.

Q4: Τι είναι το ransomware;

Ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία του συστήματος-στόχου και απαιτεί οικονομική πληρωμή με αντάλλαγμα το κλειδί αποκρυπτογράφησης. [1]

Q5: Τι είναι το spyware;

Κακόβουλο λογισμικό που καταγράφει κρυφά τα πλήκτρα, τους κωδικούς πρόσβασης και τις συνήθειες περιήγησης του χρήστη για να τα στείλει στους επιτιθέμενους.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Τι σημαίνει sandboxing;

Εκτέλεση ύποπτων αρχείων σε ασφαλές, απομονωμένο εικονικό περιβάλλον για την παρατήρηση της συμπεριφοράς τους χωρίς κίνδυνο για τα συστήματα παραγωγής.

Q7: Τι είναι το κακόβουλο λογισμικό χωρίς αρχεία (fileless malware);

Κακόβουλο λογισμικό που εκτελείται απευθείας στη μνήμη του συστήματος (RAM) χρησιμοποιώντας νόμιμα βοηθητικά προγράμματα και αποφεύγει να γράφει αρχεία στον δίσκο ώστε να παρακάμπτει τους βασικούς σαρωτές.

Q8: Πώς προστατεύει ένα rootkit το κακόβουλο λογισμικό;

Κρύβει κακόβουλες διεργασίες και αρχεία, συχνά υπονομεύοντας τον πυρήνα του λειτουργικού συστήματος, οπότε οι σαρωτές antivirus μπορεί να τα προσπεράσουν.

Q9: Τι είναι η δυναμική παρακολούθηση συμπεριφοράς;

Σάρωση antivirus που παρακολουθεί σε πραγματικό χρόνο τις ενεργές διεργασίες, ώστε να αποκλείει ενέργειες χαρακτηριστικές του κακόβουλου λογισμικού, όπως η μαζική κρυπτογράφηση αρχείων.

Q10: Γιατί είναι επείγων ο περιορισμός κατά την ανταπόκριση σε περιστατικά;

Η απομόνωση των παραβιασμένων τελικών σημείων εμποδίζει τα ενεργά κακόβουλα φορτία να εξαπλωθούν σε άλλες συσκευές του δικτύου.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς παρακάμπτουν οι δημιουργοί κακόβουλου λογισμικού τους σαρωτές antivirus που βασίζονται σε υπογραφές;

Χρησιμοποιούν πολυμορφισμό, αλλάζοντας το hash και τη δομή κώδικα του αρχείου με κάθε μόλυνση, ενώ διατηρούν την ίδια κακόβουλη συμπεριφορά.

Q2: Ποιος είναι ο κίνδυνος των εργαλείων διπλής χρήσης σε εκστρατείες κακόβουλου λογισμικού;

Οι επιτιθέμενοι χρησιμοποιούν νόμιμα διαχειριστικά εργαλεία (όπως το PowerShell ή τα Sysinternals) για να συγχέονται με την κανονική κίνηση δικτύου, δυσκολεύοντας τον εντοπισμό.

Q3: Πώς εκτελεί κακόβουλα φορτία η τεχνική process hollowing;

Εκκινεί μια νόμιμη διεργασία συστήματος σε αναστολή, αντικαθιστά τον κώδικα στη μνήμη της με κακόβουλο λογισμικό και συνεχίζει την εκτέλεση.

Q4: Ποιος είναι ο ρόλος ενός διακομιστή εντολών και ελέγχου (C2);

Ένας απομακρυσμένος διακομιστής που λειτουργεί από χάκερ για να στέλνει εντολές και φορτία σε κακόβουλο λογισμικό που τρέχει σε παραβιασμένα μηχανήματα.

Q5: Γιατί είναι δύσκολο να εντοπιστεί το keylogging;

Τα βασικά keyloggers καταναλώνουν ελάχιστους πόρους CPU και κρύβουν τις διεργασίες τους μέσα σε νόμιμα βοηθητικά προγράμματα χώρου χρήστη.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Πώς καθυστερεί η συσκότιση κώδικα την ανάλυση κακόβουλου λογισμικού;

Κρυπτογραφεί ή αναδιατάσσει τον πηγαίο κώδικα, καθιστώντας τον μη αναγνώσιμο για τα εργαλεία ανάλυσης και τους σαρωτές ασφαλείας.

Q7: Ποια είναι η λειτουργία ενός bootkit;

Ένα rootkit που μολύνει τη διαδικασία εκκίνησης (το MBR, τον τομέα εκκίνησης ή το υλικολογισμικό UEFI), ώστε να εκτελείται πριν φορτωθεί το λειτουργικό σύστημα.

Q8: Πώς εντοπίζει η ευρετική σάρωση απειλές μηδενικής ημέρας (zero-day);

Σαρώνει για ύποπτα μοτίβα κώδικα και διοικητικές εντολές αντί να αναζητά ταιριαστό κατακερματισμό βάσης δεδομένων.

Q9: Ποια είναι η απειλή της υφαρπαγής DLL (DLL hijacking);

Εξαναγκασμός μιας νόμιμης εφαρμογής να φορτώσει μια κακόβουλη δυναμική βιβλιοθήκη συνδέσμων (DLL), τοποθετώντας την στη διαδρομή του καταλόγου της εφαρμογής.

Q10: Πώς χρησιμοποιούν την εικονικοποίηση οι αυτοματοποιημένες διαδικασίες ανάλυσης κακόβουλου λογισμικού;

Εκτελούν ύποπτα αρχεία σε πολλαπλές εικονικές μηχανές λειτουργικών συστημάτων, δημιουργώντας αυτόματα αρχεία καταγραφής συμπεριφοράς και αρχεία PCAP δικτύου.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι δούρειοι ίπποι παραμένουν συνηθισμένος τρόπος μόλυνσης επειδή κρύβουν κακόβουλο κώδικα μέσα σε προγράμματα που φαίνονται αθώα.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το IC3 του FBI έλαβε πάνω από 3.600 καταγγελίες για ransomware το 2025, με δηλωμένες απώλειες που ξεπερνούν τα 32 εκατ. $. [3]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα σκουλήκια (worms) μπορούν να εξαπλωθούν γρήγορα σε δίκτυα εκμεταλλευόμενα ανεπιδιόρθωτες ευπάθειες πρωτοκόλλων, όπως το EternalBlue στο SMB.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το κακόβουλο λογισμικό χωρίς αρχεία είναι δύσκολο να εντοπιστεί επειδή τρέχει στη μνήμη μέσω νόμιμων εργαλείων και αφήνει λίγα ίχνη στον δίσκο.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα sandbox ανάλυσης συνήθως επιστρέφουν σε ένα καθαρό στιγμιότυπο μετά από κάθε εκτέλεση, ώστε κάθε δοκιμή να ξεκινά από γνωστή κατάσταση.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα rootkit μπορούν να τροποποιήσουν τις κλήσεις συστήματος του πυρήνα, αναφέροντας ψευδή διαγνωστικά αποτελέσματα στους σαρωτές κακόβουλου λογισμικού.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η απόκρυψη κώδικα χρησιμοποιεί προγράμματα packer για να συμπιέσει και να κρύψει την πραγματική δομή του δυαδικού ωφέλιμου φορτίου του κακόβουλου λογισμικού.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το πολυμορφικό κακόβουλο λογισμικό αλλάζει τον κώδικά του, και επομένως το hash του αρχείου, με κάθε νέο αντίγραφο ώστε να αποφεύγει τους ελέγχους υπογραφών.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η υφαρπαγή DLL εκμεταλλεύεται τις διαμορφώσεις σειράς αναζήτησης σε συνηθισμένα λειτουργικά συστήματα όπως τα Windows.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι προμηθευτές ασφαλείας εντοπίζουν καθημερινά τεράστιο αριθμό νέων δειγμάτων κακόβουλου λογισμικού, επομένως οι υπογραφές χρειάζονται συνεχείς ενημερώσεις.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιο είναι το καθοριστικό χαρακτηριστικό ενός Δούρειου Ίππου (Trojan); → Μεταμφιέζεται σε νόμιμο λογισμικό για να εξαπατήσει τους χρήστες ώστε να το εκτελέσουν

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος τύπος κακόβουλου λογισμικού κρυπτογραφεί αρχεία και απαιτεί πληρωμή; → Ransomware

3 Ερώτηση 3

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι αντιπροσωπεύει το spyware; → Κακόβουλο λογισμικό σχεδιασμένο να παρακολουθεί κρυφά τις πληκτρολογήσεις και τις δραστηριότητες του προγράμματος περιήγησης του χρήστη

4 Ερώτηση 4

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Γιατί οι δημιουργοί κακόβουλου λογισμικού χρησιμοποιούν rootkits; → Για να κρύβει ενεργές διεργασίες και κακόβουλα αρχεία από το λειτουργικό σύστημα

5 Ερώτηση 5

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι σημαίνει sandboxing στην ανάλυση κακόβουλου λογισμικού; → Εκτέλεση ύποπτων αρχείων σε απομονωμένο εικονικό θησαυροφυλάκιο για ασφαλή παρατήρηση της συμπεριφοράς

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ερώτηση 6** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: τα σκουλήκια (worms) αναπαράγονται μόνα τους και εξαπλώνονται στα δίκτυα χωρίς καμία ενέργεια του χρήστη.

7 **Ερώτηση 7** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το adware δεν είναι πάντα ακίνδυνο· μεγάλο μέρος του παρακολουθεί την περιήγηση για να στοχεύει διαφημίσεις.

8 **Ερώτηση 8** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: τα καθαρά αντίγραφα ασφαλείας εκτός δικτύου επαναφέρουν τα κρυπτογραφημένα αρχεία χωρίς πληρωμή, αν και τα κλεμμένα δεδομένα μπορεί και πάλι να διαρρεύσουν.

9 **Ερώτηση 9** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: οι σαρωτές υπογραφών χρειάζονται γνωστό δείγμα, οπότε το ολοκαίνουργιο κακόβουλο λογισμικό zero-day μπορεί να τους ξεφύγει.

10 **Ερώτηση 10** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το κακόβουλο λογισμικό χωρίς αρχεία εκτελεί κακόβουλα scripts στη μνήμη του συστήματος, αποφεύγοντας την εγγραφή αρχείων στον δίσκο.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

D 1. ΤΡΟΪΚΟΣ ΙΟΣ	F 2. RANSOMWARE	A 3. ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ	H 4. ROOTKIT
G 5. SANDBOX	C 6. ΠΕΡΙΟΡΙΣΜΟΣ	E 7. ΣΚΟΥΛΗΚΙ	B 8. ΧΩΡΙΣ ΑΡΧΕΙΑ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ	2 ΛΥΤΡΙΣΜΙΚΟ	3 ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ	4 ROOTKIT
5 SANDBOX	6 ΑΠΟΜΟΝΩΣΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 D – ΑΠΟΚΡΥΨΗ	2 F – ΑΠΟΜΟΝΩΣΗ	3 H – ΧΩΡΙΣΑΡΧΕΙΑ	4 G – ΣΚΩΛΗΚΑΣ
5 B – ΛΥΤΡΙΣΜΙΚΟ	6 C – ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ	7 A – ΔΟΥΡΕΙΟΣΙΠΠΟΣ	8 E – ΠΡΟΣΟΜΟΙΩΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΤΡΟΪΚΟΣ ΙΟΣ, RANSOMWARE και ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

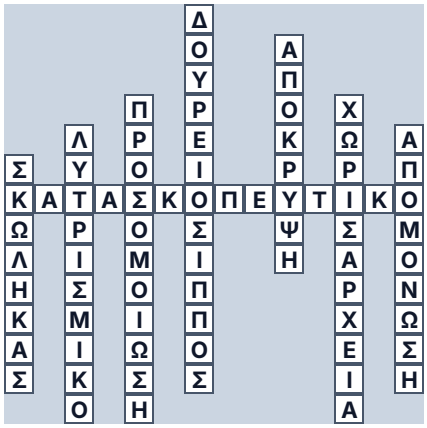
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Σ	Ψ	Ξ	Ψ	Χ	Σ	Η	Τ	Χ	Α	Ο	Υ	Ν	Ν	Ω
Ο	Α	Ι	Ε	Χ	Ρ	Α	Σ	Ι	Ρ	Ω	Χ	Ξ	Θ	Ο
Π	Σ	Θ	Ο	Α	Π	Ο	Κ	Ρ	Υ	Ψ	Η	Υ	Τ	Ξ
Π	Υ	Τ	Κ	Α	Ε	Ξ	Μ	Λ	Α	Ν	Υ	Ζ	Η	Ο
Ι	Π	Χ	Ψ	Ι	Κ	Υ	Ι	Ω	Φ	Ψ	Ο	Κ	Θ	Ω
Σ	Ι	Ι	Ν	Α	Ε	Θ	Α	Σ	Α	Ι	Ε	Φ	Ε	Κ
Ο	Ω	Κ	Ε	Κ	Π	Ν	Ι	Α	Ζ	Ξ	Κ	Ν	Γ	Ν
Ι	Γ	Δ	Η	Θ	Η	Σ	Ω	Ν	Ο	Μ	Ο	Π	Α	Β
Ε	Α	Ξ	Ρ	Λ	Ο	Φ	Τ	Θ	Ψ	Ζ	Ω	Ρ	Η	Χ
Ρ	Φ	Ο	Κ	Ι	Μ	Σ	Ι	Ρ	Τ	Υ	Λ	Θ	Ε	Π
Υ	Κ	Α	Τ	Α	Σ	Κ	Ο	Π	Ε	Υ	Τ	Ι	Κ	Ο
Ο	Τ	Ν	Σ	Κ	Ω	Λ	Η	Κ	Α	Σ	Τ	Κ	Ρ	Δ
Δ	Τ	Π	Ρ	Ο	Σ	Ο	Μ	Ο	Ι	Ω	Σ	Η	Σ	Λ
Ο	Λ	Μ	Σ	Θ	Κ	Ο	Θ	Ψ	Ξ	Λ	Χ	Υ	Ν	Ψ
Π	Π	Β	Α	Λ	Ο	Μ	Β	Λ	Θ	Ζ	Ι	Ν	Ψ	Β

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

8 οριζόντια: ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ Πρόγραμμα σχεδιασμένο να παρακολουθεί και να καταγράφει κρυφά τη δραστηριότητα και τα δεδομένα εισόδου του χρήστη. (14 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΔΟΥΡΕΙΟΣΙΠΠΟΣ Κακόβουλο λογισμικό που μεταμφιέζεται σε αθώο ή χρήσιμο βοηθητικό πρόγραμμα. (13 γράμματα)

2 κάθετα: ΑΠΟΚΡΥΨΗ Τεχνική με την οποία κακόβουλο λογισμικό κρύβεται βαθιά στον πυρήνα του συστήματος για να διατηρεί δικαιώματα διαχειριστή. (8 γράμματα)

3 κάθετα: ΠΡΟΣΟΜΟΙΩΣΗ Εικονικό περιβάλλον εκτέλεσης, χωριστό από το σύστημα, για την ασφαλή ανάλυση κακόβουλων αρχείων. (11 γράμματα)

4 κάθετα: ΧΩΡΙΣΑΡΧΕΙΑ Κακόβουλο λογισμικό που εκτελείται απευθείας στη μνήμη RAM ώστε να αποφεύγει τον εντοπισμό από σαρωτές δίσκου. (11 γράμματα)

5 κάθετα: ΛΥΤΡΙΣΜΙΚΟ Κακόβουλο λογισμικό που κρυπτογραφεί την αποθήκευση του συστήματος και απαιτεί πληρωμή για την παράδοση του κλειδιού. (10 γράμματα)

6 κάθετα: ΑΠΟΜΟΝΩΣΗ Περιορισμός των μολυσμένων τερματικών ώστε να μην εξαπλωθούν τα κακόβουλα φορτία απειλών. (9 γράμματα)

7 κάθετα: ΣΚΩΛΗΚΑΣ Κακόβουλο λογισμικό που αναπαράγεται μόνο του και εξαπλώνεται στα δίκτυα χωρίς ανθρώπινη ενέργεια. (8 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΟΥΙΟΙΟΣΠΔΠΣΕΡ — **ΔΟΥΡΕΙΟΣΙΠΠΟΣ**
2. ΣΑΚΤΟΚΚΙΠΟΥΤΕΑ — **ΚΑΤΑΣΚΟΠΕΥΤΙΚΟ**
3. ΠΟΜΙΟΡΣΗΟΩΣ — **ΠΡΟΣΟΜΟΙΩΣΗ**
4. ΛΑΣΚΗΣΚΩ — **ΣΚΩΛΗΚΑΣ**
5. ΙΣΟΥΡΜΙΛΚΤ — **ΛΥΤΡΙΣΜΙΚΟ**
6. ΨΗΚΥΑΡΠΟ — **ΑΠΟΚΡΥΨΗ**
7. ΝΑΣΗΩΜΠΟΟ — **ΑΠΟΜΟΝΩΣΗ**
8. ΕΡΑΑΡΧΣΩΙΧΙ — **ΧΩΡΙΣΑΡΧΕΙΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΝΤΟΠΙΣΕ ΑΠΕΙΛΕΣ ΜΕ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΣΥΜΠΕΡΙΦΟΡΑΣ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Περιορισμός ωφέλιμου φορτίου ransomware σε επιχείρηση

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα εταιρικό τοπικό δίκτυο έχει παραβιαστεί από ενεργό ransomware. Βασικοί διακομιστές αρχείων έχουν αρχίσει να εμφανίζουν αρχεία με κατάληξη .locked. Καθόρισε πολιτικές περιορισμού.
- Προτεινόμενη στρατηγική και λύση: Αποσύνδεσε όλους τους επηρεασμένους διακομιστές από το τοπικό δίκτυο (LAN). Τερμάτισε τις ενεργές διαχειριστικές συνεδρίες. Επανάφερε τα μη παραβιασμένα αρχεία από ένα ασφαλές σύστημα αντιγράφων ασφαλείας εκτός σύνδεσης με προστασία εγγραφής.

B Μελέτη περίπτωσης 2: Έγχυση στη μνήμη από κακόβουλο λογισμικό χωρίς αρχεία

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας αναλυτής εντοπίζει ύποπτα μοτίβα σεναρίων που εκτελούνται απευθείας στην πτητική μνήμη RAM του συστήματος χρησιμοποιώντας τυπικά διαχειριστικά εργαλεία, αλλά δεν υπάρχουν κακόβουλα αρχεία στον δίσκο.
- Προτεινόμενη στρατηγική και λύση: Απομόνωσε πρώτα τα επηρεασμένα τερματικά και κατέγραψε ένα στιγμιότυπο μνήμης. Εξέτασε τα αρχεία καταγραφής PowerShell και WMI, απέκλεισε μη εγκεκριμένα σενάρια με το AppLocker και μετά επανεκκίνησε για να εκκαθαριστεί το κακόβουλο φορτίο.