Τεχνητή Νοημοσύνη και κυβερνοασφάλεια: Έρευνα στην Ναυτιλία

CSP007

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ: ΣΤΥΛΙΑΝΟΣ ΚΑΡΑΓΙΑΝΝΗΣ, (PDMFC, ΠΟΡΤΟΓΑΛΙΑ)

Ευπάθειες των συστημάτων θαλάσσιων μεταφορών

- Το VSAT είναι μια συσκευή που χρησιμοποιείται για την εγκαθίδρυση δορυφορικών επικοινωνιών, συνδέοντας πλοία με δορυφόρους για διάφορους σκοπούς.

- SAILOR 900 VSAT High-Power. Το συγκεκριμένο μοντέλο VSAT είναι εξοπλισμένο με εξυπηρετητή ιστού, ο οποίος είναι προσβάσιμος μέσω των θυρών 80 και 443.
- Εντοπισμένα σημεία Ευπάθειας: SAILOR 900 VSAT: Έχουν εντοπιστεί τρείς Ευπάθειες στο SAILOR 900 VSAT: CVE-2022-22707, CVE-2019-11072 και CVE-2018-19052.
- Ένα proof of concept για την εκμετάλλευση της ευπάθειας CVE-2018-19052 έχει δημιουργηθεί στο GitHub, επιτρέποντας στους δυνητικούς επιτιθέμενους να εκμεταλλευτούν αυτή την ευπάθεια.
- Η διαδικτυακή διεπαφή του SAILOR 900 VSAT παρέχει πρόσβαση σε διάφορες λειτουργίες, όπως:
- Πληροφορίες για τη θέση του πλοίου
- Λεπτομέρειες συσκευής
- Ρυθμίσεις δορυφορικής σύνδεσης

Προληπτικά μέτρα για το Hacking Πλοίου

Έλεγχος και αποκλεισμός έκθεσης

- Αξιολογήστε τις συσκευές που είναι συνδεδεμένες σε δημόσια δίκτυα.
- Αποκλείστε έκθεση ευπαθών συσκευών για να ελαχιστοποιήσετε τον κίνδυνο.

Αναθεώρηση χαλαρού ελέγχου και ρυθμίσεων ασφαλείας

- Αξιολογήστε τις απαιτήσεις του συστήματος για συνδέσεις δημόσιου δικτύου.
- Εξασφαλίστε ισχυρά δικαιώματα και ρυθμίσεις ασφαλείας για τον μετριασμό δυνητικών ευπαθειών.

Αλλαγή προεπιλογής κωδικών πρόσβασης

- Διαχειριστείτε τις αλλαγές κωδικών πρόσβασης για λογαριασμούς/απολογισμούς διαχειριστών.
- Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για να αποτρέψετε την ανεξουσιοδότητη πρόσβαση.

Διατηρήστε τις συσκευές και τα συστήματα ενημερωμένα

- Ενημερώστε τακτικά όλες τις συσκευές και τα συστήματα.
- Εγκαταστήστε τις τελευταίες ενημερώσεις για διόρθωση ασφαλείας για την αντιμετώπιση γνωστών ευπαθειών και την ενίσχυση της συνολικής ασφάλειας στον κυβερνοχώρο.

MITRE ATLAS

Βάση γνώσεων για τις συμπεριφορές των αντιπάλων κατά των συστημάτων ML.

Παράδειγμα: Δηληλιρίαση(Poison) Δεδομένων Εκπαίδευσης

- Οι επιτιθέμενοι τροποποιούν σύνολα δεδομένων για να ενσωματώσουν ευπάθειες.
- Ευπάθειες που ενεργοποιούνται από δείγματα δεδομένων με Προσθήκη Κρυφής πρόσβασης στο σύστημα.
- Δηλητηρίαση δεδομένων μέσω παραβίασης της αλυσίδας εφοδιασμού της Μηχανικής Μάθησης ή μετά την αρχική πρόσβαση.
- ID: AML.T0020
- Μελέτες περιπτώσεων: Δηλητηρίαση VirusTotal (υπηρεσία ανάλυσης αρχείων και URL για malware)

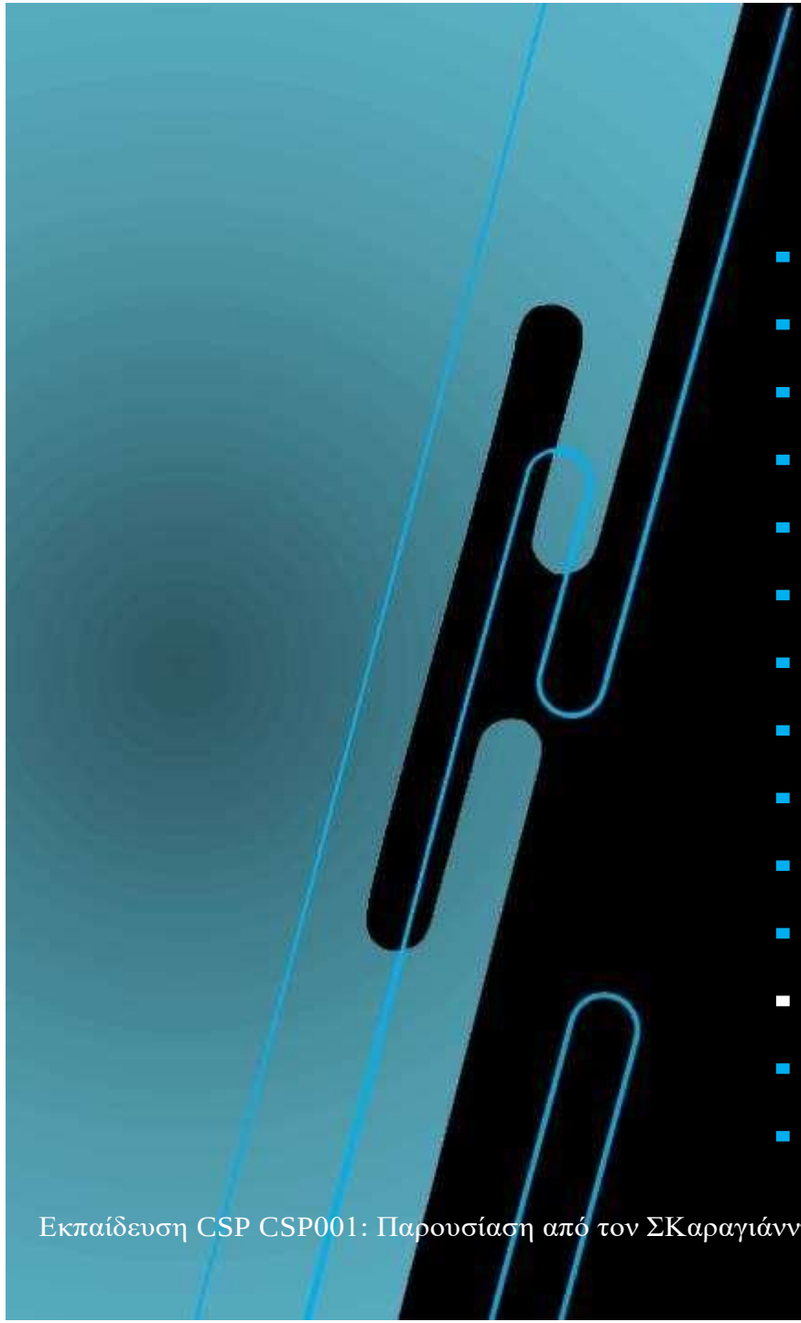
Μετριασμοί:

- Περιορισμός μοντέλου έκδοσης αντικειμένων
- Έλεγχος πρόσβασης σε μοντέλα ML και δεδομένα σε κατάσταση ηρεμίας
- Φιλτράρισμα δεδομένων Εκπαίδευσης

Τακτικές:

Ανάπτυξη Πόρων

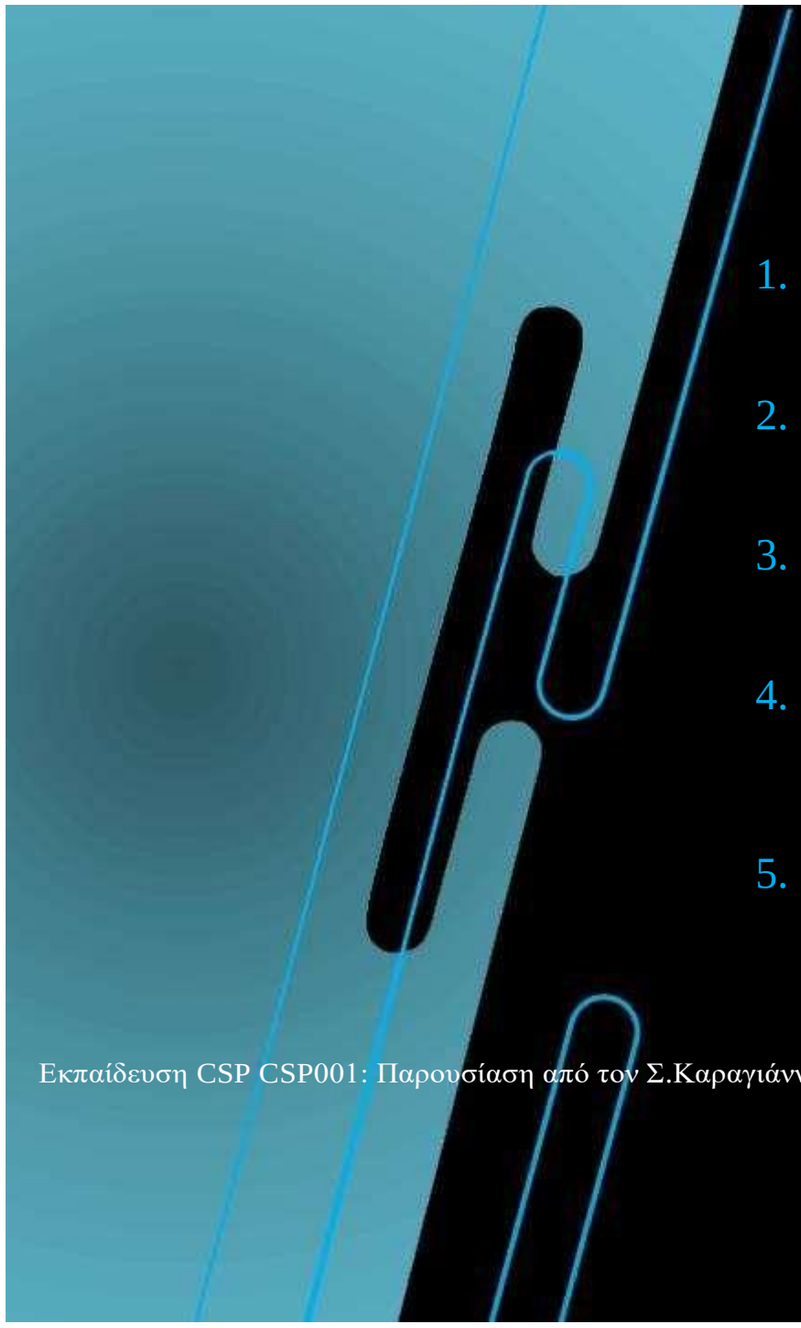
Επιμονή



ΠΛΑΙΣΙΟ ΛΟΓΙΣΜΙΚΟΥ MITRE ATT&CK

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

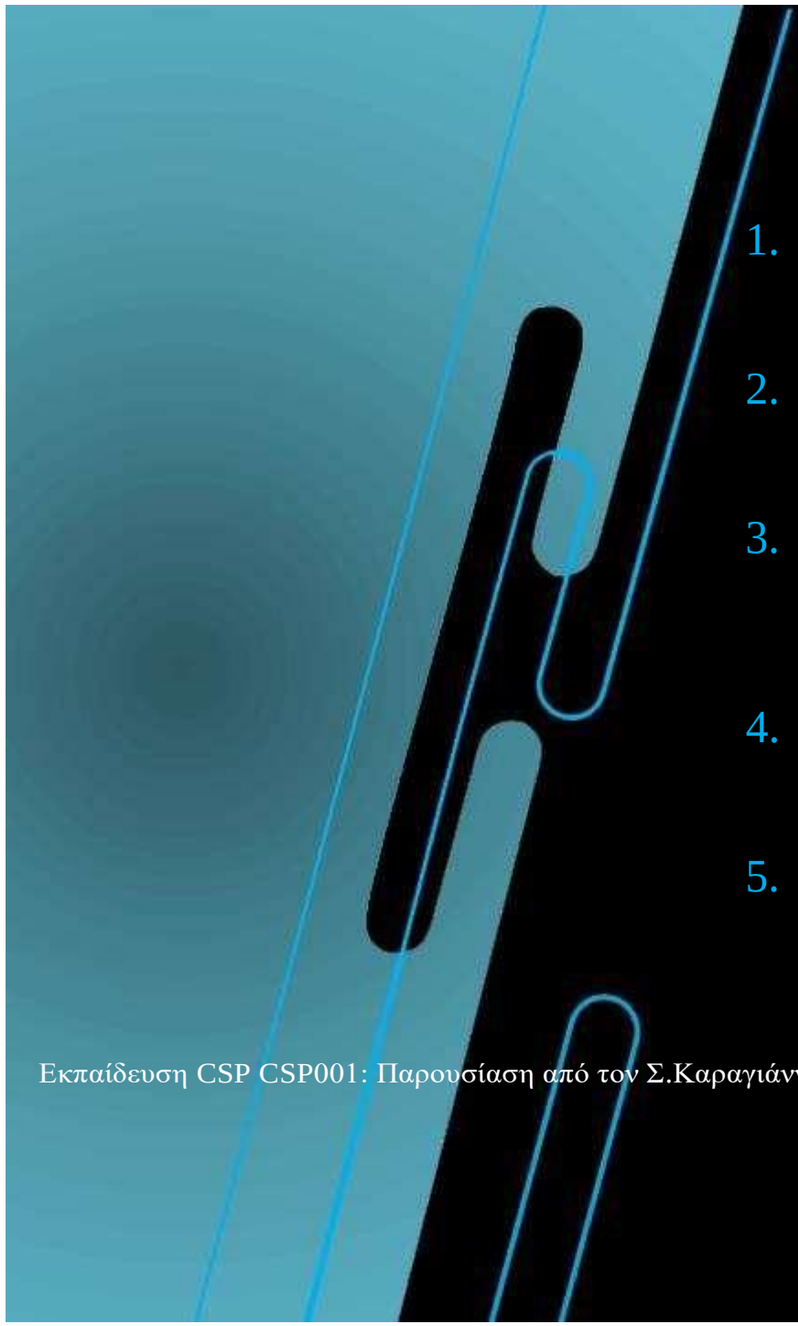
- Αναγνώριση: Συλλογή πληροφοριών για μελλοντικές λειτουργίες.
- Ανάπτυξη λογισμικού: Δημιουργία πόρων για την υποστήριξη των λειτουργικών δραστηριοτήτων.
- Αρχική πρόσβαση: Απόκτηση πρόσβασης στο δίκτυο-στόχο.
- Εκτέλεση: Εκτέλεση κακόβουλου κώδικα προγραμματισμού.
- Επιμονή: Συντήρηση της προόδου.
- Κλιμάκωση προνομίων: Κλιμάκωση Προνομίων: Απόκτηση δικαιωμάτων υψηλότερου επιπέδου.
- Παράκαμψη Άμυνας: Αποφύγετε την ανίχνευση.
- Πρόσβαση με διαπιστευτήρια: Κλοπή ονομάτων λογαριασμών και κωδικών πρόσβασης.
- Ανακάλυψη: Καθορισμός του περιβάλλοντος-στόχου.
- Πλευρική κίνηση: Μετακίνηση μέσα στο περιβάλλον του στόχου.
- Συλλογή: Συλλογή δεδομένων ενδιαφέροντος.
- Εντολές και Έλεγχος: Επικοινωνία με παραβιασμένα συστήματα.
- Διείσδυση: Κλοπή δεδομένων.
- Επιπτώσεις: Χειραγώγηση, διακοπή ή καταστροφή συστημάτων και δεδομένων



MITRE ATT&CK στη ναυτιλία Μέρος 1

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

1. Αναγνώριση: Συγκέντρωση πληροφοριών σχετικά με τα συστήματα επικοινωνίας των πλοίων, τις λιμενικές υποδομές και τα μέτρα ασφάλειας στον κυβερνοχώρο. Χάκερς που ερευνούν τα πρωτόκολλα επικοινωνίας πλοίων και τις άμυνες κυβερνοασφάλειας λιμένων.
2. Προγραμματισμός πόρων: Απόκτηση εργαλείων και προγραμματισμός κακόβουλου λογισμικού προσαρμοσμένου στα θαλάσσια συστήματα. Οι εγκληματίες του κυβερνοχώρου αναπτύσσουν κακόβουλο λογισμικό σχεδιασμένο να εκμεταλλεύεται ευπάθειες σε συστήματα πλοήγησης πλοίων.
3. Αρχική πρόσβαση: Εκμετάλλευση ευπάθειας σε συστήματα πληροφορικής πλοίων ή λιμενικά δίκτυα. Χάκερς που αποκτούν μη εξουσιοδοτημένη πρόσβαση στα συστήματα ενός πλοίου μέσω μιας επίθεσης phishing με στόχο τα μέλη του πληρώματος.
4. Εκτέλεση: Εκκίνηση κακόβουλου κώδικα προγραμματισμού για την διακοπή των λειτουργιών του σκάφους ή την παραβίαση ευαίσθητων δεδομένων. Διαδικασία εγκατάστασης και εκτέλεσης κακόβουλου λογισμικού για τη χειραγώγηση των συστημάτων πλοήγησης, με αποτέλεσμα ένα πλοίο να παρεκκλίνει από την προβλεπόμενη πορεία του.
5. Επιμονή: Εγκαθίδρυση κρυφής πρόσβασης σε συστήματα ή συντήρηση πρόσβασης σε παραβιασμένα ναυτιλιακά συστήματα. Οι χάκερ εγκαθιστούν μόνιμο κακόβουλο λογισμικό στα συστήματα ενός πλοίου για τη διατήρηση του ελέγχου ακόμη και μετά τον εντοπισμό και τον μετριασμό της αρχικής πρόσβασης.

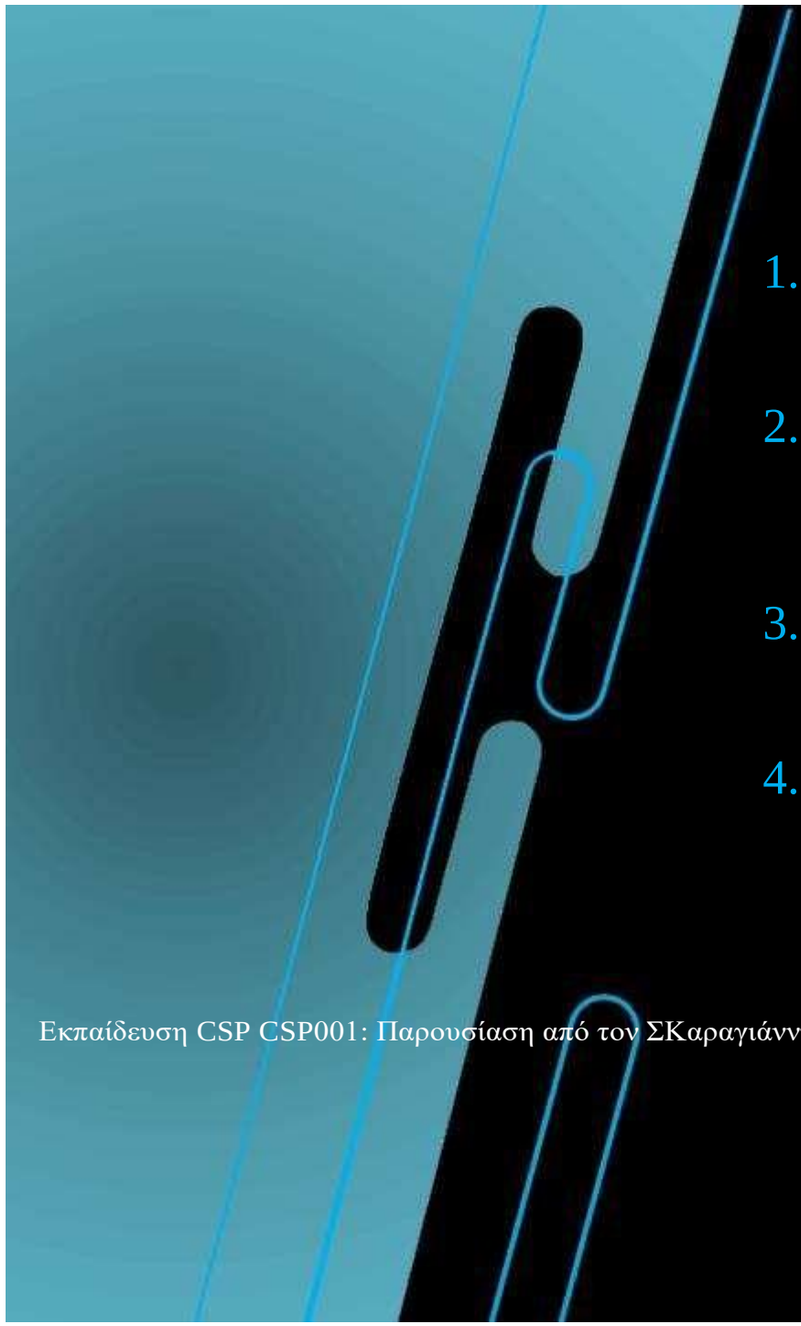


MITRE ATT&CK στη ναυτιλία Μέρος 2

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

1. Κλιμάκωση προνομίων: Αύξηση της πρόσβασης σε κρίσιμα ναυτιλιακά συστήματα ή αποθετήρια δεδομένων. Χάκερς που εκμεταλλεύονται ευπάθειες για την κλιμάκωση των προνομίων και την απόκτηση πρόσβασης σε ευαίσθητα δελτία φορτίου ή ελέγχους πλοήγησης.
2. Παράκαμψη Άμυνας: Αποφυγή ανίχνευσης από τους μηχανισμούς άμυνας της ναυτιλιακής κυβερνοασφάλειας. Κακόβουλο λογισμικό σχεδιασμένο για να αποφεύγει την ανίχνευση από λογισμικό προστασίας από ιούς ή συστήματα ανίχνευσης εισβολών στα πλοία.
3. Πρόσβαση με διαπιστευτήρια: Κλοπή διαπιστευτηρίων του ναυτικού προσωπικού για την απόκτηση μη εξουσιοδοτημένης πρόσβασης. Οι εγκληματίες του κυβερνοχώρου παραβιάζουν τους λογαριασμούς των μελών του πληρώματος για να αποκτήσουν πρόσβαση σε ευαίσθητα ναυτιλιακά συστήματα και δεδομένα.
4. Ανακάλυψη: Αντιστοιχίσεις δικτύων σκαφών, εντοπισμός Ευπαθειών και δυνητικών στόχων. Οι χάκερς διεξάγουν σαρώσεις δικτύων για τον εντοπισμό ευάλωτων πλοίων με ξεπερασμένες προστασίες κυβερνοασφάλειας.
5. Πλευρική κίνηση: Πλευρική μετακίνηση εντός δικτύων πλοίων για την επέκταση της πρόσβασης και του ελέγχου. Οι χάκερς μετακινούνται από κρίσιμες συσκευές του πληρώματος σε συστήματα ελέγχου του πλοίου, όπως τα συστήματα ελέγχου των μηχανών ή τα συστήματα διαχείρισης φορτίου.

Εκπαίδευση CSP CSP001: Παρουσίαση από τον Σ.Καραγιάννη, PDMFC, Πορτογαλία



MITRE ATT&CK στη ναυτιλία Μέρος 3

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

1. Συλλογή: Συλλογή ευαίσθητων ναυτιλιακών δεδομένων ή πνευματικής ιδιοκτησίας. Κατασκοπεία στον κυβερνοχώρο που κλέβουν ιδιοταγείς πληροφορίες σχετικά με τις ναυτιλιακές διαδρομές ή τα δηλωτικά φορτίου για σκοπούς οικονομικής κατασκοπείας.
2. Διοίκηση και έλεγχος: Καθιέρωση διαύλων επικοινωνίας με θαλάσσια συστήματα που έχουν τεθεί σε κίνδυνο. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν διακομιστές/εξυπηρετητές ελέγχου για να χειρίζονται εξ αποστάσεως τα συστήματα πλοήγησης πλοίων ή τον εξοπλισμό χειρισμού φορτίου.
3. Διείσδυση: Εξαγωγή κλεμμένων ναυτιλιακών δεδομένων ή πολύτιμων πληροφοριών φορτίου. Οι χάκερς εξαπολύουν ευαίσθητα δελτία φορτίου ή πρωτόκολλα ασφαλείας λιμένων για χρήση σε μελλοντικές επιθέσεις ή για πώληση στο dark web.
4. Επιπτώσεις: Σοβαρές ανατρεπτικές επιπτώσεις στις λειτουργίες των πλοίων, το θαλάσσιο εμπόριο ή τις κρίσιμες υποδομές. Επιθέσεις στον κυβερνοχώρο που προκαλούν τον αποκλεισμό πλοίων στη θάλασσα ή την παράλυση των λιμενικών λειτουργιών, με αποτέλεσμα σημαντικές οικονομικές απώλειες και ζημία στη φήμη.

MITRE ATT&CK στην ναυτιλία Παράδειγμα 1

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

1. Αναγνώριση

- Ο αντίπαλος αποκτά πληροφορίες σχετικά με τον εξοπλισμό του πλοίου-στόχου.
- Ο αντίπαλος αναζητά εξοπλισμό δορυφορικών επικοινωνιών στη θάλασσα.
- Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν μηχανές αναζήτησης IoT.
- Παραδείγματα λέξης-κλειδιού αναζήτησης στο Censys: services.banner = "sailor 600".
- Ο αντίπαλος αποκτά τον κωδικό πρόσβασης του BWMS μέσω της υπηρεσίας κοινωνικού δικτύου του μέλους του πληρώματος.

2. Προγραμματισμός λογισμικού

- Ο αντίπαλος εντοπίζει τις γνωστές Ευπάθειες των τερματικών δορυφορικών επικοινωνιών στη ναυτιλία CVE-2013-6034, CVE-2013-6035).
- Ορισμένες συσκευές δορυφορικής επικοινωνίας μπορούν να προσπελαστούν χρησιμοποιώντας τη θύρα TCP (Transmission Control Protocol - πρωτόκολλο επικοινωνίας δικτύου που χρησιμοποιείται στο διαδίκτυο) 1827 χωρίς επαλήθευση χρήστη.
- Ο αντίπαλος προσδιορίζει έναν έγκυρο λογαριασμό στο τερματικό δορυφορικής επικοινωνίας.
- Ορισμένες συσκευές χρησιμοποιούν τον προεπιλεγμένο λογαριασμό ("admin")

MITRE ATT&CK στην ναυτιλία Παράδειγμα 1

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

3. Αρχική πρόσβαση

- Ο αντίπαλος αποκτά πρόσβαση στο δίκτυο του σκάφους με έγκυρο λογαριασμό.

4. Πλευρική κίνηση

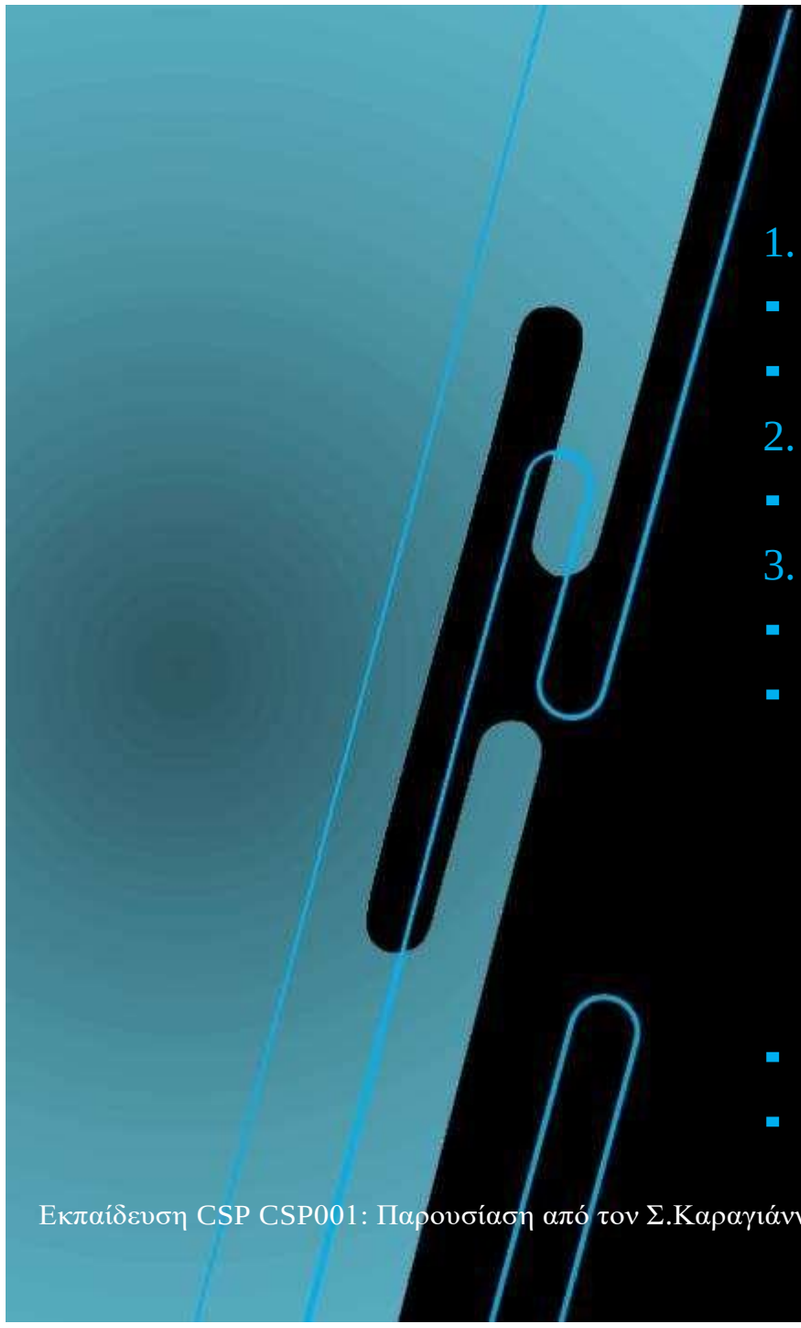
- Ο αντίπαλος αποκτά πρόσβαση στο BWMS μέσω του δικτύου επί του σκάφους.

5. Διοίκηση και έλεγχος:

- Ο αντίπαλος επιτίθεται στις επιφάνειες επίθεσης του BWMS.
- Ο αντίπαλος εκτελεί τους φορείς επίθεσης BWMS.
- Ο αντίπαλος διαμορφώνει τα δεδομένα της αντλίας λειτουργία της αριστερής ή της δεξιάς αντλίας). Ο αντίπαλος μεταβάλλει τα δεδομένα της αντλίας (λειτουργώντας την αντλία της αριστερής πλευράς ή την αντλία της δεξιάς πλευράς).

6. Επιπτώσεις

- Το πλοίο βυθίζεται.
- Το πλοίο ανατρέπεται.



MITRE ATT&CK στην ναυτιλία Παράδειγμα 2

Τακτικές Αντιπαράθεσης, Τεχνικές και Κοινή Γνώση

1. Αναγνώριση

- Απόκτηση δικαιωμάτων επιβίβασης στο πλοίο.
- Φυσική πρόσβαση στο λογισμικό ECDIS.

2. Αρχική πρόσβαση

- Χρήση του προεπιλεγμένου κωδικού πρόσβασης του ECDIS(pw: 0000) για να αποκτήσετε πρόσβαση.

3. Άμυνα Αποφυγή

- Φόρτωση ψεύτικου Windock DLL.
- Διαδικασία για επίθεση έγχυσης DLL

  - Επισυνάψτε τη διαδικασία.
  - Κατανομή μνήμης εντός της διεργασίας.
  - Αντιγράψτε το DLL ή τη διαδρομή DLL στη μνήμη της διεργασίας και προσδιορίστε τη κατάλληλη διεύθυνση μνήμης.
  - Εντολοδοτήστε τη διεργασία να εκτελέσει το ψεύτικο DLL.
- Εισαγωγή του ωφέλιμου φορτίου που είναι αποθηκευμένο στο USB στο ECDIS.
- Ενεργοποίηση του πληκτρολογίου με τη συντομεύση πληκτρολογίου "Windows + R ".

MITRE ATT&CK στο Maritime Ex.2

Αντιδικτυακές τακτικές, τεχνικές και κοινή

4. Επιμονή

- Εκτέλεση του ωφέλιμου φορτίου.

5. Συλλογή

- Τροποποίηση του Winsock DLL αρχείο για μια Man-in-the-Middle (MITM) επίθεση από το λογισμικό ECDIS.

6. Διοίκηση και έλεγχος

- Τροποποίηση της εντολής NMEA, με αποτέλεσμα το πλοίο να εκτός πορείας.

7. Επιπτώσεις

- Παράλυση του ECDIS (μπλε οθόνη).
- Προσάραξη του πλοίου.
- Με αποτέλεσμα το πλοίο να βγει εκτός πορείας.

Σας ευχαριστώ

Οργανώσεις: PDMFC

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
stylianos.karagiannis@pdmfc.com