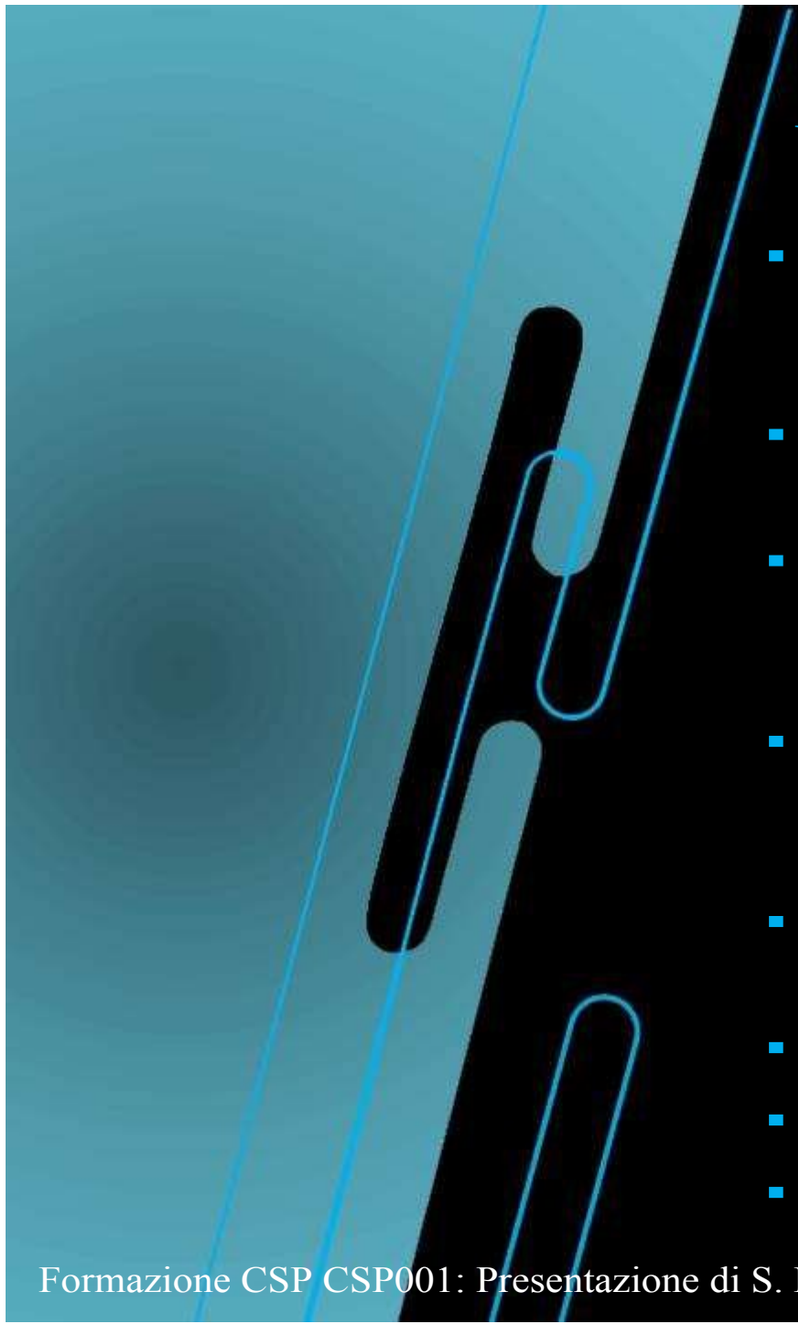
IA e sicurezza informatica: Ricerca in ambito marittimo

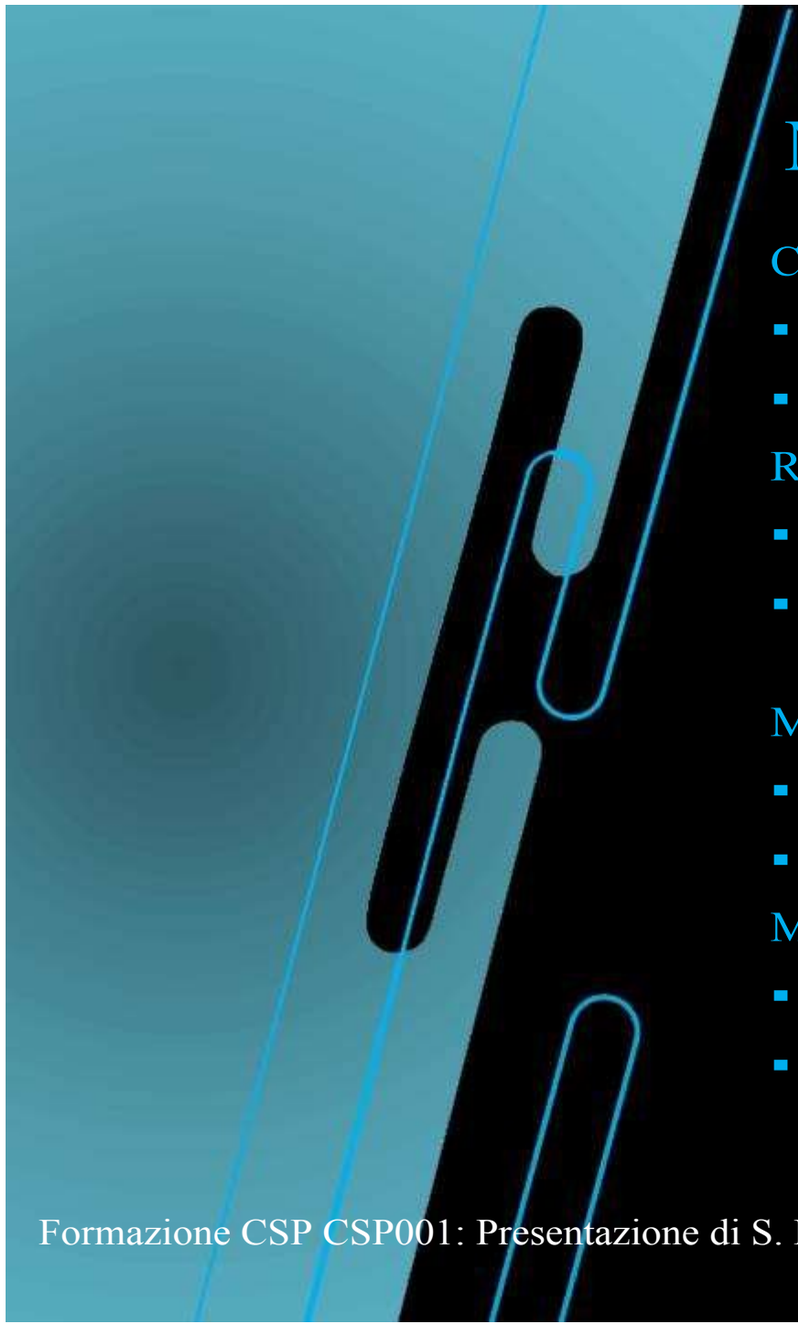
CSP007

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS, (PDMFC, PORTOGALLO)



Vulnerabilità dei sistemi di trasporto marittimo

- VSAT è a dispositivo utilizzato per stabilire satellite comunicazioni satellitari,
  collegare le navi ai satelliti per vari scopi.
- SAILOR 900 VSAT ad alta potenza. Questo modello specifico di VSAT è dotato di un server Web accessibile tramite le porte 80 e 443.
- Vulnerabilità identificate: Sono state identificate tre vulnerabilità nel SAILOR 900 VSAT: CVE-2022-22707, CVE-2019-11072 e CVE-2018-19052.
- Su GitHub è stato reso disponibile un proof of concept per lo sfruttamento di CVE-2018-19052, che consente ai potenziali aggressori di sfruttare questa vulnerabilità.
- L'interfaccia web del SAILOR 900 VSAT consente di accedere a varie funzionalità, tra cui:
- Informazioni sulla posizione della nave
- Dettagli del dispositivo
- Impostazioni della connessione satellitare



Misure preventive per l'hacking navale

Controllo e blocco dell'esposizione

- Valutare i dispositivi collegati alle reti pubbliche.
- Bloccare l'esposizione dei dispositivi vulnerabili per ridurre al minimo i rischi.

Rivedere le autorizzazioni e le impostazioni di sicurezza

- Valutare i requisiti di sistema per le connessioni alla rete pubblica.
- Garantire autorizzazioni e impostazioni di sicurezza solide per ridurre le potenziali vulnerabilità.

Modifica delle password predefinite

- Amministrare la modifica della password per gli account di amministratore.
- Utilizzate password forti e uniche per evitare accessi non autorizzati.

Mantenere aggiornati i dispositivi e i sistemi

- Aggiornare regolarmente tutti i dispositivi e i sistemi.
- Installare le patch di sicurezza più recenti per risolvere le vulnerabilità note e migliorare la sicurezza informatica complessiva.

MITRE ATLAS

Base di conoscenza dei comportamenti degli avversari contro i sistemi di ML.

Esempio: Dati di addestramento al veleno

- Gli avversari modificano i set di dati per incorporare le vulnerabilità.
- Vulnerabilità attivate da campioni di dati con Insert Backdoor Trigger.
- Dati avvelenamento tramite ML Fornitura Catena di distribuzione Compromissione o accesso successivo a quello iniziale.
- ID: AML.T0020
- Casi di studio: Avvelenamento di VirusTotal, avvelenamento di Tay

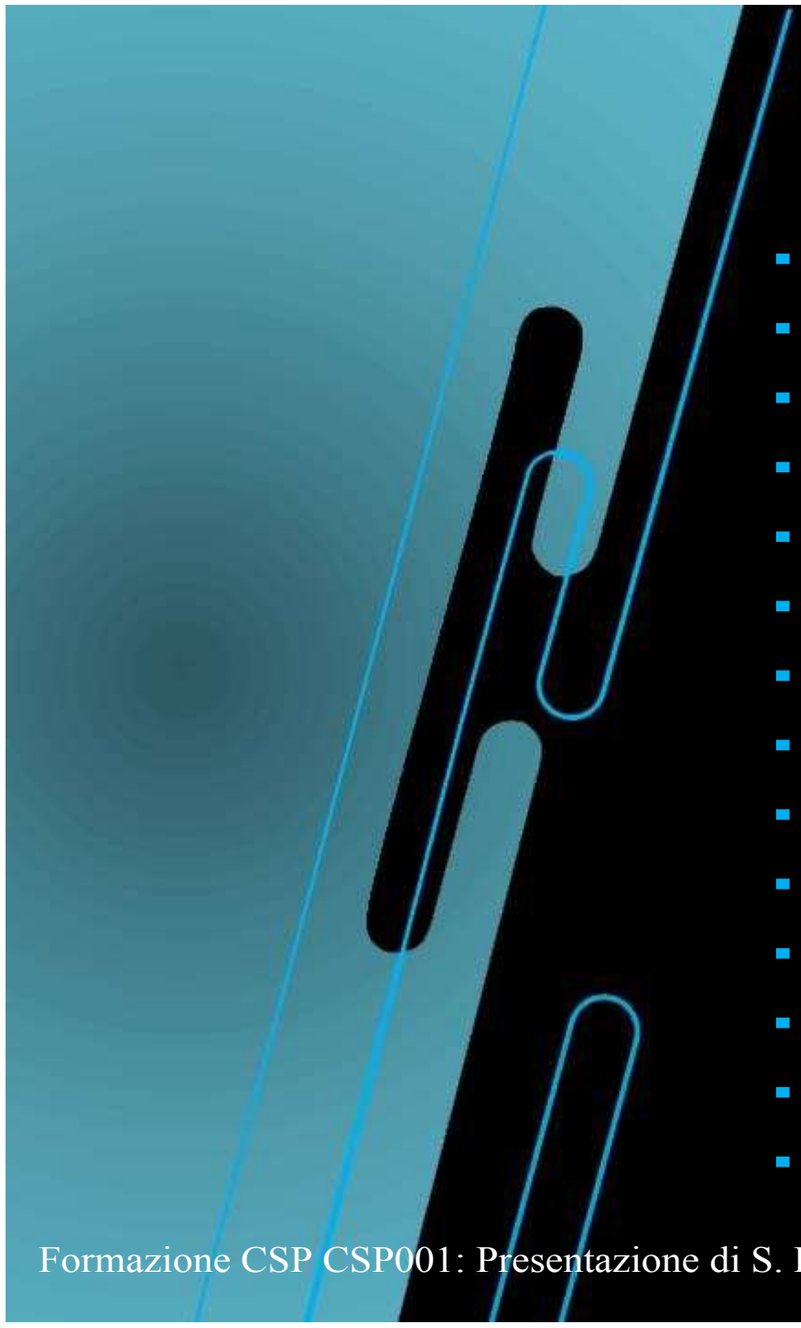
Mitigazioni:

- Modello limite Rilascio di artefatti
- Controllo dell'accesso ai modelli di ML e ai dati a riposo
- Sanificazione dei dati di formazione

Tattica:

Sviluppo delle risorse

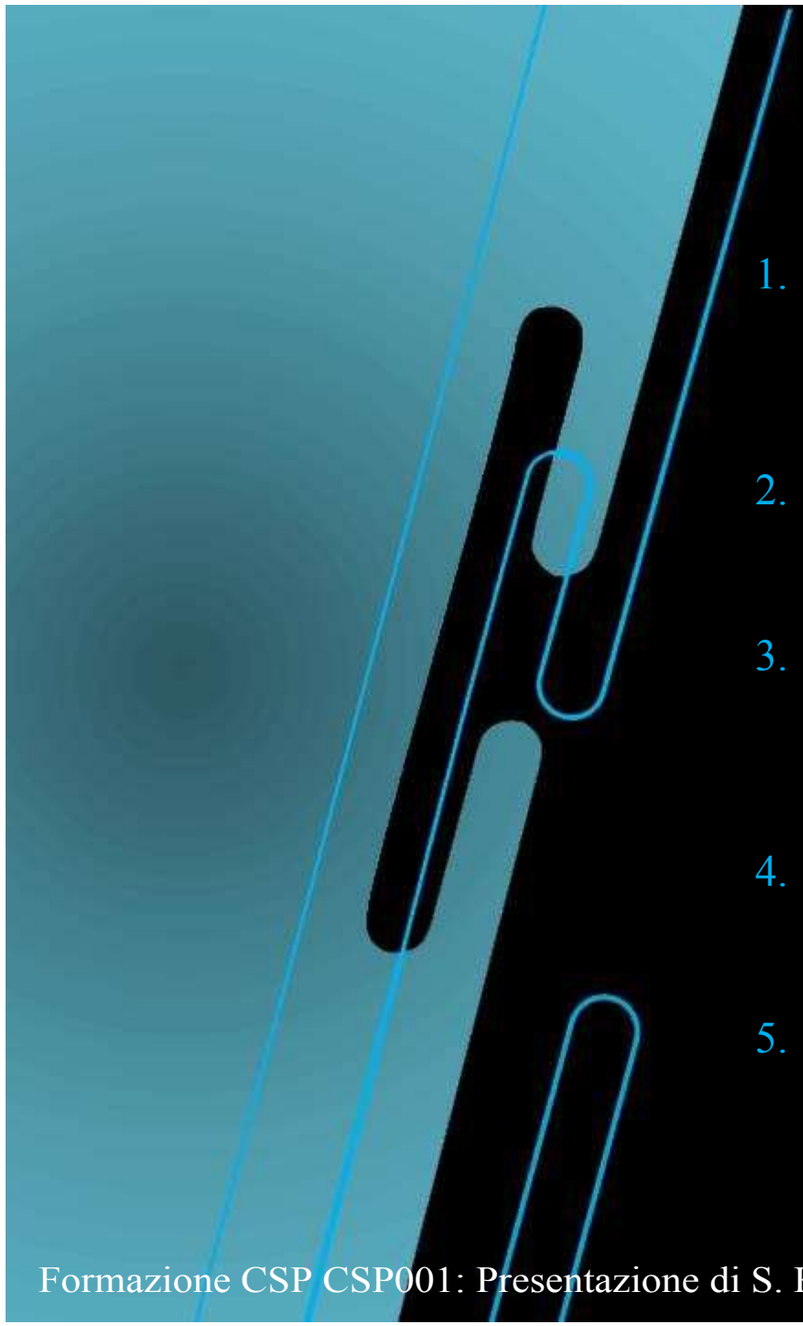
Persistenza



STRUTTURA MITRE ATT&CK

Tattiche, tecniche e conoscenze comuni dell'avversario

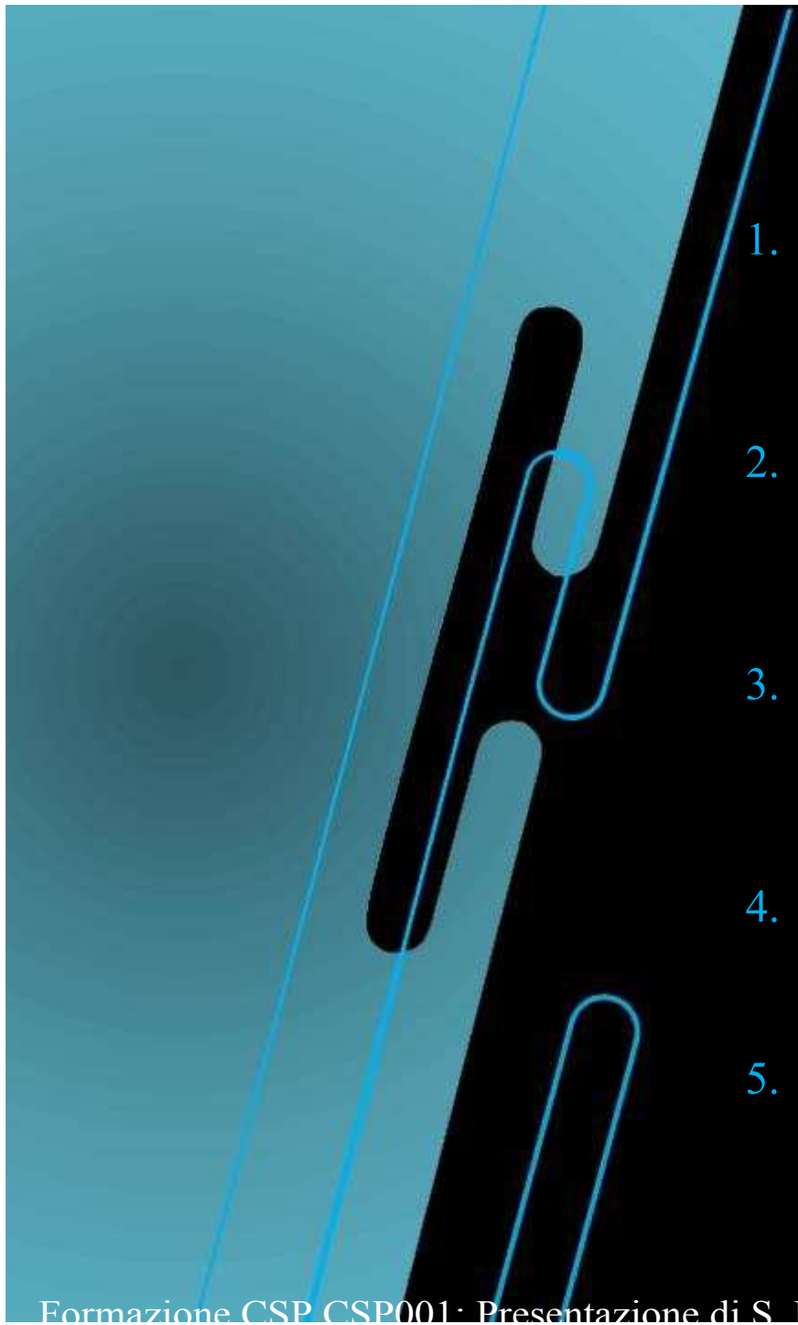
- Ricognizione: Raccogliere informazioni per operazioni future.
- Sviluppo delle risorse: Stabilire le risorse per sostenere le operazioni.
- Accesso iniziale: Ottenere l'accesso alla rete di destinazione.
- Esecuzione: Esecuzione di codice dannoso.
- Persistenza: Mantenere i progressi.
- Escalation dei privilegi: Ottenere autorizzazioni di livello superiore.
- Difesa Evasione: Evita il rilevamento.
- Accesso alle credenziali: Rubare nomi di account e password.
- Individuazione: Determinare l'ambiente di destinazione.
- Movimento laterale: Muoversi nell'ambiente di destinazione.
- Raccolta: Raccogliere i dati di interesse.
- Comando e controllo: Comunicare con i sistemi compromessi.
- Esfiltrazione: Rubare i dati.
- Impatto: Manipolare, interrompere o distruggere sistemi e dati.



MITRE ATT&CK in ambito marittimo Pt.1

Tattiche, tecniche e conoscenze comuni dell'avversario

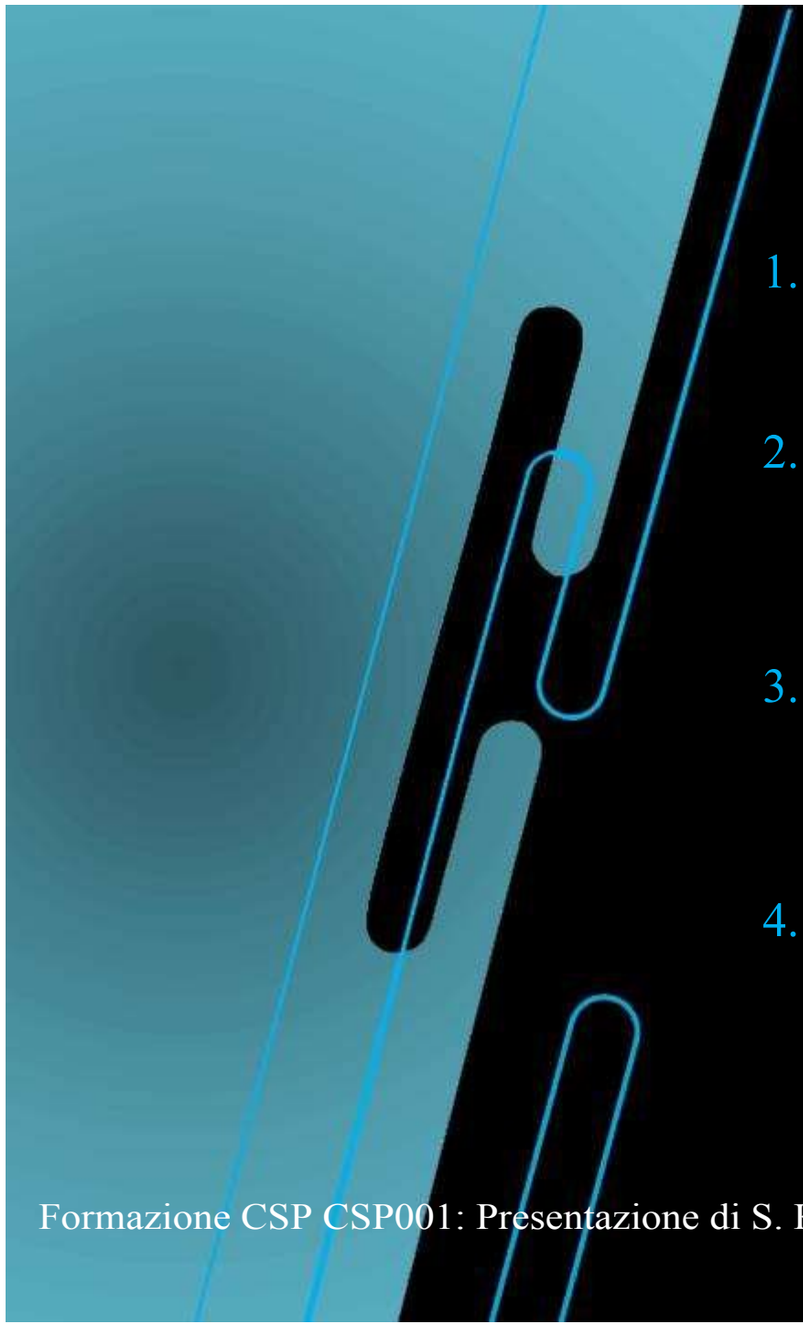
1. Ricognizione: Raccolta di informazioni sui sistemi di comunicazione delle navi, sulle infrastrutture portuali e sulle misure di sicurezza informatica marittima. Gli hacker ricercano i protocolli di comunicazione delle navi e le difese di sicurezza informatica dei porti.
2. Sviluppo delle risorse: Acquisizione di strumenti e sviluppo di malware su misura per i sistemi marittimi. Criminali informatici che sviluppano malware progettato per sfruttare le vulnerabilità dei sistemi di navigazione delle navi.
3. Accesso iniziale: Sfruttamento delle vulnerabilità nei sistemi informatici delle navi o nelle reti portuali. Gli hacker ottengono l'accesso non autorizzato ai sistemi di bordo di una nave attraverso un attacco di phishing rivolto ai membri dell'equipaggio.
4. Esecuzione: Lancio di codice maligno per interrompere le operazioni della nave o compromettere dati sensibili. Malware distribuito per manipolare i sistemi di navigazione, facendo deviare una nave dalla rotta prevista.
5. Persistenza: Creazione di backdoor o mantenimento dell'accesso a sistemi marittimi compromessi. Gli hacker installano malware persistente sui sistemi di un'imbarcazione per mantenere il controllo anche dopo che l'accesso iniziale è stato rilevato e mitigato.



MITRE ATT&CK in ambito marittimo Pt.2

Tattiche, tecniche e conoscenze comuni dell'avversario

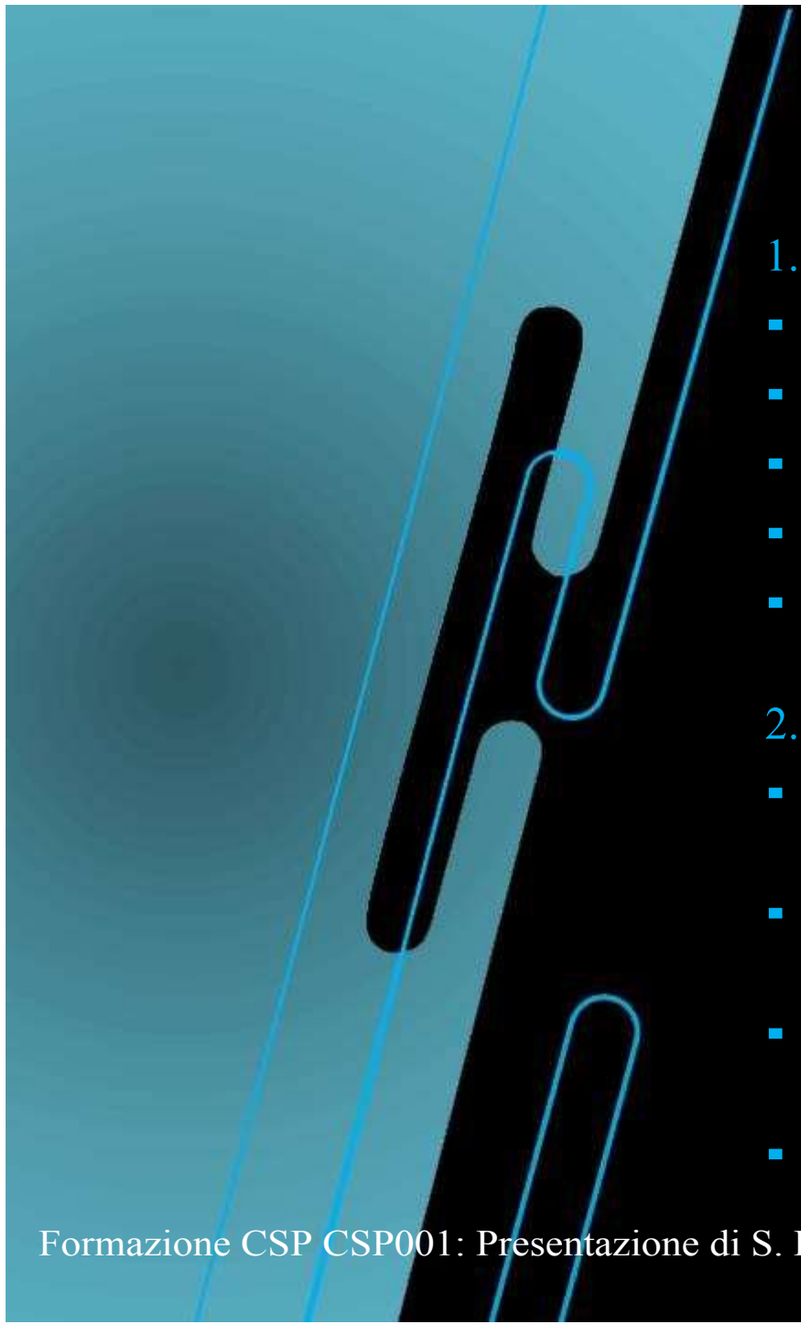
1. Escalation dei privilegi: Elevazione dell'accesso ai sistemi marittimi critici o agli archivi di dati. Gli hacker sfruttano le vulnerabilità per aumentare i privilegi e ottenere l'accesso a manifesti di carico o controlli di navigazione sensibili.
2. Evasione della difesa: Elusione del rilevamento da parte delle difese di sicurezza informatica marittima. Malware progettato per eludere il rilevamento da parte del software antivirus o dei sistemi di rilevamento delle intrusioni a bordo delle navi.
3. Accesso alle credenziali: Rubare le credenziali del personale marittimo per ottenere un accesso non autorizzato. I criminali informatici compromettono gli account dei membri dell'equipaggio per accedere a sistemi e dati marittimi sensibili.
4. Scoperta: Mappatura delle reti navali, identificazione delle vulnerabilità e dei potenziali obiettivi. Gli hacker effettuano scansioni della rete per identificare le imbarcazioni vulnerabili con protezioni di cybersicurezza obsolete.
5. Movimento laterale: Spostamento laterale all'interno delle reti navali per ampliare l'accesso e il controllo. Gli hacker passano dai dispositivi compromessi dell'equipaggio ai sistemi di controllo di bordo, come i controlli dei motori o i sistemi di gestione del carico.



MITRE ATT&CK in ambito marittimo Pt.3

Tattiche, tecniche e conoscenze comuni dell'avversario

1. Raccolta: Raccolta di dati marittimi sensibili o di proprietà intellettuale. Spie informatiche che rubano informazioni proprietarie sulle rotte di navigazione o sui manifesti di carico a scopo di spionaggio economico.
2. Comando e controllo: Stabilire canali di comunicazione con sistemi marittimi compromessi. I criminali informatici utilizzano i server di comando e controllo per manipolare da remoto i sistemi di navigazione delle navi o le apparecchiature di movimentazione del carico.
3. Esfiltrazione: Estrazione di dati marittimi rubati o di informazioni preziose sul carico. Gli hacker esfiltravano manifesti di carico sensibili o protocolli di sicurezza portuale per utilizzarli in attacchi futuri o per venderli sul dark web.
4. Impatto: Gravi interruzioni delle operazioni navali, del commercio marittimo o delle infrastrutture critiche. Cyberattacchi che causano il blocco delle navi in mare o la paralisi delle operazioni portuali, con perdite finanziarie significative e danni alla reputazione.



MITRE ATT&CK in Maritime Ex.1

Tattiche, tecniche e conoscenze comuni dell'avversario

1. Ricognizione

- L'avversario ottiene informazioni sull'equipaggiamento della nave bersaglio.
- L'avversario cerca apparecchiature di comunicazione satellitare marittime.
- Gli aggressori possono utilizzare i motori di ricerca IoT.
- Esempi di parole chiave di ricerca in Censys: services.banner= "sailor 600".
- L'avversario ottiene la password del BWMS attraverso la rete sociale. Servizio del membro dell'equipaggio.

2. Sviluppo delle risorse

- L'avversario identifica le vulnerabilità note dei terminali di comunicazione satellitare marittima (CVE-2013-6034, CVE-2013-6035).
- Alcuni dispositivi di comunicazione satellitare possono essere accessibili tramite la porta TCP 1827 senza autenticazione.
- Il avversario identifica a valido conto presso il marittimo terminale di comunicazione satellitare.
- Alcuni dispositivi utilizzano l'account predefinito ("admin")

MITRE ATT&CK in Maritime Ex.1

Tattiche, tecniche e conoscenze comuni dell'avversario

3. Accesso iniziale

- L'avversario accede alla rete di bordo con un account valido.

4. Movimento laterale

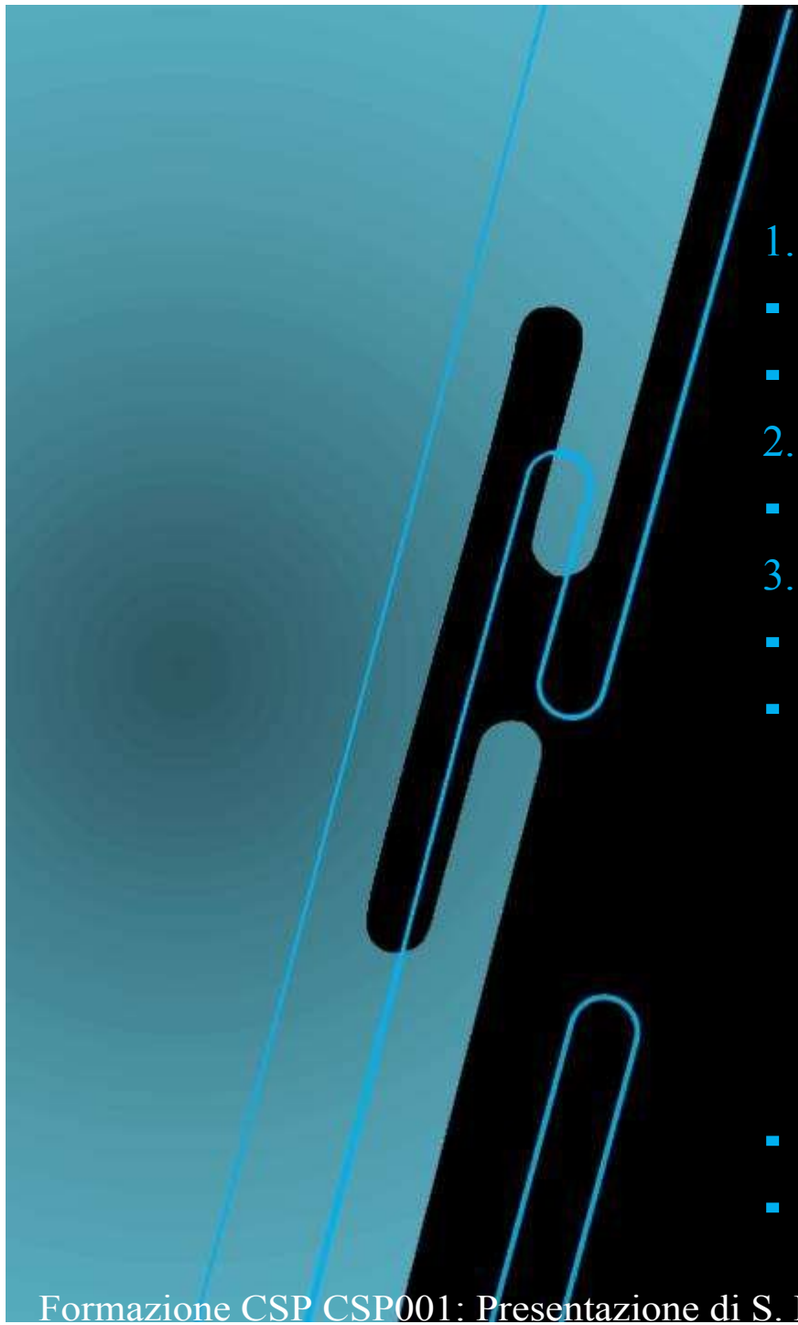
- L'avversario accede al BWMS attraverso la rete di bordo.

5. Comando e controllo:

- L'avversario attacca le superfici di attacco del BWMS.
- L'avversario esegue i vettori di attacco BWMS.
- L'avversario modula i dati della pompa (facendo funzionare la pompa di sinistra o quella dritta).
- L'avversario disattiva l'allarme della pompa.

6. Impatto

- La nave affonda.
- La nave si capovolge.



MITRE ATT&CK in Maritime Ex.2

Tattiche, tecniche e conoscenze comuni dell'avversario

1. Ricognizione

- Acquisizione dei diritti di imbarco sulla nave.
- Accesso fisico al software ECDIS.

2. Accesso iniziale

- Utilizzare la password di fabbrica dell'ECDIS (pw: 0000) per accedere.

3. Difesa Evasione

- Caricamento di una DLL Windock falsa.
- Procedura per l'attacco con iniezione di DLL

  - Allegare il processo.
  - Allocare la memoria all'interno del processo.
  - Copiare la DLL o il percorso della DLL nella memoria del processo e determinare il percorso della DLL.
    indirizzo di memoria appropriato.
  - Indicare al processo di eseguire la DLL fittizia.
- Iniettare il carico utile memorizzato nella USB nell'ECDIS.
- Attivazione della tastiera con la scorciatoia "Windows+ R".

MITRE ATT&CK in Maritime Ex.2

Tattiche, tecniche e conoscenze comuni dell'avversario

4. Persistenza
   - Esecuzione del payload.
5. Collezione
   - Modificare il Winsock DLL per il file pera Man-in-the-Middle (MiTM) da parte del software ECDIS.
6. Comando e controllo
   - Alterando il comando NMEA, la nave esce dalla rotta.
7. Impatto
   - Paralisi dell'ECDIS (schermata blu).
   - Incaglio della nave.
   - causando un'uscita di rotta della nave.

Grazie

Organizzazione: PDMFC

Si prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com