Day 18 - Create Command and Control

Command and Control

Cosa possono fare i malware una volta eseguiti?

Fase di Discovery: Esecuzione di comandi come ipconfig, net user, ecc., per raccogliere informazioni sul sistema e sulla rete.

Persistenza: Creazione di servizi o schedule tasks per garantire che il malware sopravviva ai riavvii del sistema.

Sessioni C&C (Command and Control): La fase più critica: il malware stabilisce una connessione con il server di comando e controllo per ricevere istruzioni aggiuntive, esfiltrare dati o distribuire payload.

Command and Control

Cosa è il Command and Control (C&C)?

Definizione secondo MITRE ATT&CK:C&C (Command and Control) è una fase in cui gli attaccanti stabiliscono un canale di comunicazione con il sistema compromesso per mantenere il controllo.

Perché è importante?
Permette agli attaccanti di eseguire azioni aggiuntive, come:

- Movimento laterale nella rete.
- Accesso a informazioni sensibili.
- Distribuzione di ransomware o altri payload dannosi.

Tecniche C&C (MITRE ATT&CK):
Esistono **18 tecniche** documentate, che includono vari metodi per mantenere la comunicazione con il sistema compromesso, come:

- Comandi via HTTP/S.
- Utilizzo di DNS.
- Canali crittografati.

Command and Control

Tool e Framework per C&C
Uno dei framework più noti per la gestione di attacchi C&C è **Metasploit**, una piattaforma che fornisce strumenti per sviluppare, testare e gestire exploit su sistemi vulnerabili. Oltre a permettere di creare payload personalizzati, è spesso utilizzato per la simulazione di attacchi e pen-test.

Cobalt Strike è un altro potente strumento che consente di eseguire attività di post-exploitation e gestione di attacchi C&C. È utilizzato dagli attaccanti per lanciare comandi, muoversi lateralmente nella rete e mantenere la persistenza su macchine compromesse, simulando attacchi avanzati.
Per la **rilevazione** e l'analisi forense di attacchi C&C, il **DFIR Report** è una risorsa chiave. Offre report dettagliati su incidenti reali, descrivendo tecniche, strumenti e artefatti da cui difendersi, supportando investigazioni e mitigazioni.

Sliver è un framework open-source alternativo a Cobalt Strike, sempre più utilizzato per test di sicurezza e attacchi di simulazione. Fornisce molte delle stesse funzionalità, permettendo di gestire attacchi C&C con una maggiore flessibilità e meno costi.

Command and Control

Mythic è un framework open-source progettato per gestire e orchestrare attività di Command and Control (C&C). Sviluppato con **linguaggio Python**, Mythic è estremamente modulare e permette agli operatori di creare e gestire payload in modo flessibile.
Una delle sue caratteristiche distintive è la capacità di **track payloads**, ovvero tenere traccia delle operazioni di ciascun payload distribuito. Questo consente di monitorare in tempo reale le attività svolte dai malware sulla rete compromessa, migliorando la gestione operativa.
Inoltre, Mythic utilizza diversi **profiles**, ovvero configurazioni che definiscono il modo in cui il payload comunica con il server di comando. I profiles permettono di simulare diversi tipi di comunicazioni, come HTTP, DNS o TCP, consentendo agli attaccanti di eludere più facilmente i controlli di sicurezza.
Grazie alla sua flessibilità e modularità, Mythic è diventato uno strumento molto utilizzato per simulare attacchi reali in ambienti di pen-test avanzati e per migliorare la difesa contro tecniche sofisticate.